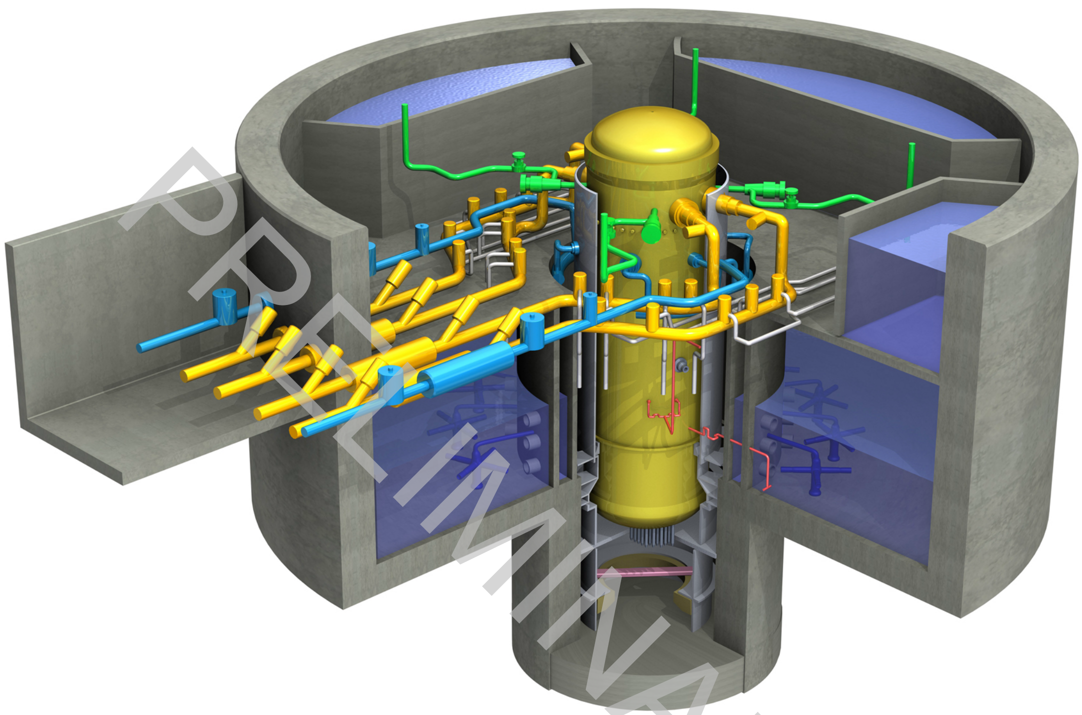
GE-Hitachi Nuclear Energy

26A6642AW
Revision 6
June 2009



ESBWR Design Control Document
Tier 2

Chapter 7
Instrumentation and Control Systems

Contents

List of Tables

List of Illustrations

7. INSTRUMENTATION AND CONTROL SYSTEMS

7.1 INTRODUCTION

This chapter presents specific detailed design and performance information for the Instrumentation and Control (I&C) systems that are significant for plant operation and that are used throughout the plant. I&C Distributed Control and Information Systems (DCIS) are designated as either Safety-related DCIS (Q-DCIS) or Nonsafety-related DCIS (N-DCIS). A description of the system of classification is found in Section 3.2.

The following subsections, tables, and figures provide a synopsis of the DCIS.

- Subsection 7.1.1 contains a brief description of the DCIS.
- Subsection 7.1.2 summarizes the Q-DCIS.
- Subsection 7.1.3 contains a detailed description of the Q-DCIS.
- Subsection 7.1.4 summarizes the N-DCIS.
- Subsection 7.1.5 contains a detailed description of the N-DCIS.
- Subsection 7.1.6 discusses DCIS conformance to regulatory requirements, guidelines, and industry codes and standards.
- Table 7.1-1 is a regulatory requirements applicability matrix.
- Table 7.1-2 is a section roadmap of an evaluation of IEEE Std. 603 specific criteria compliance.
- Figure 7.1-1 is a simplified network functional diagram of the DCIS.
- Figure 7.1-2 is deleted.
- Figure 7.1-3 is a distributed power-sensor diversity diagram.
- Figure 7.1-4 is a hardware/software (architecture) diversity diagram.

7.1.1 Distributed Control and Information System

The DCIS is an arrangement of I&C networked components and individual systems that together provide:

- Digital processing and logic capability;
- Remote and local data acquisition;
- Datalinks and gateways (when necessary) between systems and components;
- Operator monitoring and control interfaces;
- Secure communications to external computer systems and networks;
- Alarm management functions; and
- Communications between the systems.

Figure 7.1-1 shows a simplified network functional diagram of the DCIS. The data communication systems embedded in the DCIS perform the data communication functions that are part of or support the systems described in Sections 7.2 through 7.8. Figure 7.1-1 is a simplified functional representation of the DCIS.

The Q-DCIS and N-DCIS architectures, their relationships, and their acceptance criteria are further described throughout Section 7.1.

The Q-DCIS and N-DCIS functions are implemented with diverse power and sensors as indicated in Figure 7.1-3, and diverse hardware and software architectures as shown in Figure 7.1-4. These are discussed in Reference 7.1-4, the Licensing Topical Report (LTR), "ESBWR I&C Diversity and Defense-In-Depth Report," NEDO-33251.

The Q-DCIS comprise the platforms that are defined in Table 7.1-1. The N-DCIS comprise the network segments that are defined in Table 7.1-1. These platforms or network segments comprise systems of integrated software and hardware elements. Software projects are developed for the various platforms or networks segments. The software development process is described in Appendix 7B.

7.1.2 Q-DCIS General Description Summary

The Q-DCIS, which performs the safety-related control and monitoring functions of the DCIS, is organized into four physically and electrically isolated divisions. The Q-DCIS uses three diverse platforms that operate independently of each other: Reactor Trip Isolation Function-Neutron Monitoring System (RTIF-NMS), Safety System Logic and Control/Engineered Safety Features (SSLC/ESF), and the Independent Control Platform (ICP). The ICP provides independent logic control of the Anticipated Transient Without Scram mitigation and Standby Liquid Control (ATWS/SLC) functions, vacuum breaker (VB) isolation function, and the High Pressure Control Rod Drive (HP CRD) isolation bypass function that is diverse from the RTIF-NMS platform and the SSLC/ESF platform and not susceptible to a common-cause failure.

The Q-DCIS major cabinets are Reactor Trip and Isolation Function (RTIF) cabinet, Neutron Monitoring System (NMS) Function cabinet and the SSLC/ESF cabinet. These cabinets include the following systems and functions:

- RTIF Platform Systems and Functions
  - Reactor Protection System (RPS) (Refer to Subsection 7.2.1);
  - Main Steam Isolation Valve (MSIV) functions of the Leak Detection and Isolation System (LD&IS) (Refer to Subsection 7.3.3); and
  - Suppression Pool Temperature Monitoring (SPTM) function of the Containment Monitoring System (CMS) (Refer to Subsection 7.2.3).
- ICP Systems and Functions
  - VB isolation function of the containment system (Refer to Subsection 7.3.6); and
  - ATWS/SLC functions (Refer to Subsection 7.4.1 and 7.8.1).
  - HP CRD Isolation Bypass function (Refer to Section 4.6 as well as Subsections 7.1.2.8.8, 7.3.3, and 7.4.5).

- NMS Functions:

  NMS is implemented using the same hardware/software platform as RTIF systems; NMS includes the following systems and functions:

  – Startup Range Neutron Monitor (SRNM) functions and

  – Power Range Neutron Monitor (PRNM) functions that include:

    ▪ Local Power Range Monitor (LPRM) functions,

    ▪ Average Power Range Monitor (APRM) functions, and

    ▪ Oscillation Power Range Monitor (OPRM) functions.

- Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) system

  – Emergency Core Cooling System (ECCS) functions that include:

    ▪ Automatic Depressurization System (ADS) functions,

    ▪ Gravity-Driven Cooling System (GDCS) functions,

    ▪ Isolation Condenser System (ICS) functions, and

    ▪ SLC system functions.

  – LD&IS Functions (except the MSIV functions);

  – Control Room Habitability System (CRHS) functions; and

  – Safety-related information systems.

The Q-DCIS major components include:

- Fiber optic cable and hardwired networks,
- System control processors,
- Non-microprocessor based logic,
- Remote multiplexer units (RMUs),
- Load drivers (discrete outputs),
- Communication interface modules (CIMs),
- Video display units (VDUs),
- Hard controls/indicators (for monitoring), and
- Cabinets for housing devices such as power supplies.

The Q-DCIS provides most of the interface functions for the RTIF, NMS, and SSLC/ESF protection systems. These functions include data acquisition, monitoring, communication, and control functions. As a safety-related system, Q-DCIS is qualified for the environments and conditions that exist before, during, and following the abnormal events identified in Table 15.0-2. Each division of the Q-DCIS is electrically isolated from other Q-DCIS divisions and from the N-DCIS. Data communication is controlled between the Q-DCIS divisions and between the Q-DCIS and the N-DCIS. Communication between Q-DCIS divisions and between the Q-DCIS and the N-DCIS is via fiber optic cable. Data communication between the Q-DCIS and the N-DCIS is managed by isolation devices, which are safety-related components within the Q-DCIS, via datalinks and N-DCIS gateways (when necessary). The RTIF, NMS, and SSLC/ESF protection systems are designed so that no safety-related function depends on the existence or function of any nonsafety-related component, data, or communication channel.

The Q-DCIS uses RMUs for data acquisition for the RTIF, NMS, and SSLC/ESF protection systems and for safety-related displays in the MCR and Remote Shutdown System (RSS). These data acquisition units are either distributed within the division or reside in specific chassis and are not dedicated to specific RTIF, NMS, or SSLC/ESF protection systems.

For added reliability and diversity, the architecture of the RTIF and NMS protection systems is different from the architecture of the SSLC/ESF protection system (refer to Figure 7.1-3 and Figure 7.1-4). These systems operate automatically under normal conditions, without operator input.

The RTIF and NMS status is monitored on the divisional Q-DCIS safety-related MCR and RSS VDUs that are connected to the SSLC/ESF (the N-DCIS VDUs also have the capability to independently monitor the RTIF and NMS statuses but only after isolation and with no capability to control the Q-DCIS). The RTIF and NMS process data are sent per division through the required safety-related isolation and via a one-way dedicated communication path (datalink and gateway if necessary) for display on the corresponding divisional safety-related VDU. The RTIF, NMS, and SSLC/ESF operate independently of the VDUs, they continue to perform their safety-related functions if there is a failure of the VDU network and the VDUs have no capability to control the RTIF or the NMS. Safety-related VDUs are provided in the MCR and at the RSS panels and operate independently of one another. The safety-related VDUs provide data display capability for the RTIF, NMS, and SSLC/ESF safety-related systems but manual control capability only for the SSLC/ESF safety-related systems in the same division as the safety-related VDU, all in a Human Factors Engineering (HFE) approved format.

The divisional Q-DCIS components outside of the MCR are located in physically separate DCIS divisional rooms or compartments in the Reactor Building (RB) and Control Building (CB) that have appropriate fire barriers between them.

The divisional Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies (UPS) dedicated to their division with battery backup (per division) for at least 72 hours. After 72 hours, the Q-DCIS can operate continuously on power from diesel generators or from off-site power. (Refer to Chapter 8 for additional information about the power sources for the isolation load centers and safety-related uninterruptible AC power).

The Q-DCIS provides self-diagnostics that monitor communication, power, and processors to the replaceable card, module, or chassis level. Process diagnostics include system alarms and the capability to identify sensor failures. Process and self-diagnostic system alarms are provided to the MCR.

7.1.2.1 Q-DCIS Safety-Related Design Bases Summary

The safety-related design bases applicable to the Q-DCIS are found in IEEE Std. 603, Sections 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, and 4.12. They specifically address reading signals, performing signal conditioning, transmitting data signals and commands, performing safety-related logic independently, providing alarms, and isolating data communication.

7.1.2.2 Q-DCIS Power Generation (Nonsafety-Related) Design Bases Summary

The power generation design bases for the Q-DCIS are to transmit safety-related system data through qualified isolation devices to the N-DCIS (via datalinks and gateways when necessary) for historical trending, analysis, and alarm management functions.

7.1.2.3 Q-DCIS Safety Evaluation Summary

The Q-DCIS conforms to IEEE Std. 603 criteria for safety-related I&C systems.

The Q-DCIS is arranged into four divisions. The intra-divisional and safety-related to nonsafety-related fiber optic cable communication paths are redundant to support reliability and to allow self-diagnostics to be communicated in the presence of a single failure. No failure of any single hardware component, in any one division, can lead to an inadvertent trip. Safety-related cabinets and chassis are powered by redundant safety-related UPS for both reliability and diagnostic capability. For communications between divisions of safety-related systems, there is no single communication or power failure that results in the loss of a safety-related function. A dual communication or power failure can result in the loss of a single division but not in the loss of a safety-related function. A two-division failure, which requires four communications or power failures, does not result in the loss of a safety-related function, in accordance with the N-2 design basis.

Safety-related systems perform their safety-related functions with three out of four safety-related divisions available, in the presence of a single failure.

Table 7.1-1 identifies the DCIS systems and the associated regulatory requirements, guidelines, and codes and standards applied in accordance with the Standard Review Plan (SRP). The following subsection summarizes conformance of I&C systems to regulatory requirements, guidelines, and industry standards.

7.1.2.4 Q-DCIS Regulatory Requirements Conformance Summary

The Q-DCIS conforms to the applicable portions of:

- 10 CFR 50.34, 10 CFR 50.44, 10 CFR 50.49, 10 CFR 50.55, 10 CFR 50.62, 10 CFR 50.63, and 10 CFR 52.47;
- NUREGs 694, 718, 737, NUREG/CR-6083, and NUREG/CR-6303;
- IEEE Std. 7-4.3.2, 323, 344, 379, 338, 383, 384, 497, 518, 603, 828, 829, 830, 1008, 1012, 1028, 1050, and 1074;
- American National Standards Institute (ANSI)/Instrument Society of America (ISA) 67.02.01 and 67.04.01;
- General Design Criteria (GDC) 1, 2, 4, 10, 12, 13, 15, 16, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 33, 34, 35, 37, 41, 43, 44, 63, and 64;
- Staff Requirements Memorandum (SRM) II.Q and II.T on SECY 93-087;

- Regulatory Guides (RGs) 1.22, 1.45, 1.47, 1.53, 1.62, 1.75, 1.89, 1.97, 1.100, 1.105, 1.118, 1.151, 1.152, 1.153, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, 1.204, and 1.209; and
- Branch Technical Positions (BTPs) HICB-1, 8, 9, 10, 11, 12, 14, 16, 17, 18, 19, and 21.

7.1.2.5 Q-DCIS Testing and Inspection Requirements Summary

The Q-DCIS integrated hardware and software functions, including the network parameters and data status, are checked and tested together. The Analog-to-Digital (A/D) converters in the RMUs are the only components requiring periodic calibration checks. Key diagnostics include:

- The central processing unit (CPU) status check,
- Parity checks, watchdog timer status,
- Voltage level in controllers,
- Data path integrity and data validation checks,
- Data cycling time, and
- Processor clock time.

7.1.2.6 Q-DCIS Operator Interface Requirements Summary

The Q-DCIS VDUs support operator monitoring and manual control of the safety-related systems. The VDUs present process and diagnostic alarm information. When one of the two power supplies or communications paths within a division fails, the division and VDU operation continue automatically, without operator intervention. Failures in three divisions are required before there is a loss of a safety-related function.

The Q-DCIS indications and alarms provided in the MCR, as a minimum, are :

- Q-DCIS MCR alarms for Division 1, 2, 3, and 4 trouble; and
- Q-DCIS MCR indications for Division 1, 2, 3, and 4 diagnostic displays.

7.1.2.7 Q-DCIS Boundary Summary

There are no Q-DCIS components in the N-DCIS. The Q-DCIS does not include the sensors or the sensor wiring to the RMUs or the RMU output wiring to the actuators.

7.1.2.8 Q-DCIS Major Systems Description Summary

The Q-DCIS systems and components include equipment for the Reactor Trip System (RTS), and Engineered Safety Features Actuation System (ESFAS). The RTS includes the RPS function, the SRNM and PRNM functions of the NMS, and the SPTM function of the CMS. The SSLC/ESF is the designated ESFAS. The automatic decision-making and trip logic functions associated with the safety-related RTS and ESFAS are accomplished by independent, separate, and diverse protection logic platforms, each using four logic-processing divisions. Input signals from redundant channels of safety-related instrumentation are used to perform logic operations that result in decisions for safety-related action through the associated actuation devices (for example, pilot solenoid valves, squib valves, and air operated valves). The Q-DCIS also includes the ATWS/SLC functions, the VB isolation function, and HP CRD isolation bypass function.

7.1.2.8.1 Reactor Protection System Description Summary

The RPS implements the reactor trip functions. The RPS is the overall complex of instrument channels, trip logics, trip actuators, manual controls and scram logic circuitry that initiates rapid insertion of control rods to shut down the reactor in situations that could result in unsafe reactor operations. This action prevents or limits fuel damage and system pressure excursions, minimizing the release of radioactive material.

The RPS also establishes appropriate logic for different reactor operating modes, provides monitoring and control signals to other systems, and actuates alarms.

The RPS overrides selected operator actions and process controls and is based on a fail-safe design philosophy. The RPS design provides reliable, single-failure-proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. This is accomplished through the combination of fail-safe and fault-tolerant equipment design, and a two-out-of-four voting logic algorithm.

Although the RTIF cabinets house the RPS, the ATWS/SLC functions, the VB isolation function, and the HP CRD isolation bypass function, the logics for the ATWS/SLC, VB isolation, and the HP CRD isolation bypass functions use diverse hardware and their designs are not fail-safe. The RPS hardware/software platform is diverse from the SSLC/ESF, the VB isolation function, the ATWS/SLC , the HP CRD isolation bypass function, and the DPS hardware/software platforms; the RPS and DPS sensors are diverse and RPS sensors are not shared with other Q-DCIS or N-DCIS systems.

7.1.2.8.2 Neutron Monitoring System Description Summary

The NMS monitors neutron flux in the reactor core 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 system provides indication of neutron flux that can be correlated with thermal power level for the entire range of flux conditions that can exist in the core. The NMS comprises the following systems.

- The SRNM system monitors thermal neutron flux levels from very low average power levels to a power level above 15% of rated power. Between 1% and 15% of rated power the monitoring function overlaps the LPRM/APRM systems functions to assure continuous monitoring of thermal neutron flux levels. The SRNM channel is able to provide local power information up to 100% of rated power. The SRNM system generates trip signals to prevent fuel damage resulting from abnormal positive reactivity insertions under conditions that are not covered by the APRMs. The SRNMs generate a high neutron flux trip and a high rate of neutron flux increase trip.

- The PRNM system includes the LPRM, the APRM, and the OPRM functions. The outputs of the individual LPRMs are averaged to provide the average power level of the reactor core, and the OPRM System provides monitoring of neutron flux and core thermal hydraulic instabilities.

- The Automatic Fixed In-core Probe (AFIP) is a nonsafety-related component of the NMS system and does not provide information to the Q-DCIS. It calibrates the LPRM system by providing neutron flux information to 3D MONICORE.
- The Multi-Channel Rod Block Monitor (MRBM) is a nonsafety-related component of the NMS system and is completely isolated from the Q-DCIS by one-way communication through qualified safety-related isolation devices and via fiber optic cable communication. It provides control rod blocks to the Rod Control and Information System (RC&IS) to prevent core thermal limit violations.

7.1.2.8.3 SSLC/ESF System Description Summary

The SSLC/ESF is the overall complex of instrument channels, trip logics, trip actuators, manual controls, and actuation logic circuitry that initiates protective action to mitigate the consequences of DBEs. Input signals from redundant channels of safety-related instrumentation are used to make trip decisions and perform logic operations that result in accident mitigating actions. The SSLC/ESF provides the automatic decision-making and trip logic to actuate:

- The various ECCS;
- Leak detection, containment isolation, and radioactivity release barrier defense; and
- Control room habitability

7.1.2.8.3.1 Emergency Core Cooling System Description Summary

The ECCS provides emergency core cooling for events that threaten reactor coolant inventory, such as a Loss-of-Coolant-Accident (LOCA). The ECCS comprises the ADS, the GDCS, the ICS, and the SLC system. The ECCS function is discussed more fully in Subsection 7.3.1.

7.1.2.8.3.1.1 Automatic Depressurization System Description Summary

The ADS resides within the Nuclear Boiler System (NBS) and comprises Safety Relief Valves (SRVs), Depressurization Valves (DPVs), and associated I&C. The ADS depressurizes the reactor to allow the low head GDCS to provide make-up coolant to the reactor. The ADS logic resides in the SSLC/ESF portion of the Q-DCIS.

7.1.2.8.3.1.2 Gravity-Driven Cooling System Description Summary

Following the receipt of an actuation signal, the GDCS provides emergency core cooling when the reactor has been depressurized. The GDCS is capable of injecting large volumes of water into the Reactor Pressure Vessel (RPV) to keep the core covered for at least 72 hours following a LOCA. The GDCS also performs a deluge function that drains the GDCS pools to the lower drywell if a severe accident core melt sequence occurs. The GDCS deluge logic, which is nonsafety-related except for permissives to avoid inadvertent actuation, is separate and diverse from the Q-DCIS. The basic components of the GDCS are within the containment. The GDCS pools, piping, and valves are in the drywell. The suppression pool is on the outer periphery of the drywell within the containment envelope. The GDCS I&C is designed to:

- Automatically initiate the GDCS to prevent fuel cladding temperatures from reaching their limits;
- Respond to a need for emergency core cooling following reactor depressurization;

- Be completely automatic in operation. Manual initiation of the GDCS is possible at any time providing protective permissive conditions have been satisfied; and
- Prevent the inadvertent actuation of the deluge valves, thus preventing inadvertent draining of the GDCS pools.

7.1.2.8.3.1.3 Isolation Condenser System Description Summary

The ICS removes reactor decay heat following reactor shutdown and isolation. It also prevents unnecessary reactor depressurization and operation of the ECCS. The primary function of the ICS is to limit reactor pressure and prevent SRV operation following an isolation of the main steam lines. The ICS, together with the water stored in the RPV, provides sufficient reactor coolant volumes to avoid automatic depressurization caused by low reactor water level. The ICS passively removes excess sensible and core decay heat from the reactor, with minimal loss of coolant inventory from the reactor, when the normal heat removal systems are unavailable. The ICS logic resides in the SSLC/ESF portion of the Q-DCIS. Refer to Subsection 7.4.4 for additional information.

7.1.2.8.3.1.4 Standby Liquid Control System Description Summary

The SLC system performs dual functions. In its ECCS mode, it provides additional coolant inventory to respond to a LOCA. It is also a backup method for bringing the nuclear reactor to subcriticality, by adding soluble poison, and then maintaining subcriticality as the reactor cools.

The SLC system bases are discussed in Subsection 7.4.1. The SLC logic resides in the SSLC/ESF and the ATWS/SLC portions of the Q-DCIS.

7.1.2.8.3.2 Leak Detection and Isolation System Description Summary

The LD&IS monitors leakage sources from the Reactor Coolant Pressure Boundary (RCPB). It automatically initiates closure of the appropriate valves to isolate the source of the leak if monitored system variables exceed preset limits. This limits coolant release from the RCPB and, therefore, the release of radioactive materials into the environment. Refer to Subsection 7.3.3 for additional information.

The MSIV isolation logic of the LD&IS is fail-safe and therefore performed as part of the RTIF logic platform. The non-MSIV isolation logic of the LD&IS is performed as part of the SSLC/ESF logic platform.

7.1.2.8.3.3 Control Room Habitability System Description Summary

The primary function of the CRHS is to provide a safe environment for the operators to control the nuclear reactor and its auxiliary systems. The CRHS monitors the Control Room Habitability Area (CRHA) inlet ventilation air and actuates logic to isolate and filter the CRHA on detection of hazardous environmental conditions. The CRHS logic resides in the SSLC/ESF portion of the Q-DCIS.

7.1.2.8.4 ATWS/SLC System Description Summary

The ATWS mitigation logic provides a diverse means of reducing power excursions from certain transients and a diverse means of emergency shutdown. The ATWS mitigation logic, which uses the soluble boron injection capability of the SLC system as a diverse means of negative reactivity insertion, is implemented using the ICP as safety-related logic (designated as ATWS/SLC), which is diverse from the RTIF-NMS platform and the SSLC/ESF platform and therefore not susceptible to a common-cause failure. The ATWS/SLC logic also provides a feedwater run-back signal to attenuate power excursions.

In the event that the control rods cannot provide sufficient negative reactivity insertion, the SLC system provides the capability of an orderly and safe shutdown by a diverse means. In addition to providing hot shutdown capability, the SLC is sized to counteract the positive reactivity that results from shutting down from rated power to a cold shutdown condition. The SLC system can be initiated manually, or automatically via the ATWS mitigation logic or the SSLC/ESF logic as an ECCS function. (Refer to Subsection 7.1.2.8.3.1.4.) The SLC logic resides on the SSLC/ESF and ATWS/SLC portions of the Q-DCIS.

The nonsafety-related ATWS mitigation logic is implemented in the DPS. Refer to Subsection 7.8.1.1.

7.1.2.8.5 Passive Containment Cooling System Description Summary

The Passive Containment Cooling System (PCCS) cools the containment following a rise in containment pressure and temperature without requiring any component actuation. The PCCS does not have instrumentation, control logic, or power-actuated valves, and does not need or use electrical power for its operation in the first 72 hours after a LOCA. For long-term effectiveness of the PCCS, the vent fans are manually initiated by operator action. Refer to Subsections 7.3.2 and 6.2.2 for additional information.

7.1.2.8.6 Containment Monitoring System Description Summary

The CMS provides the functions identified in Subsections 7.1.2.8.6.1 and 7.1.2.8.6.2. Refer to Subsection 7.5.2 for additional information.

7.1.2.8.6.1 Suppression Pool Temperature Monitoring Subsystem Description Summary

The safety-related SPTM function is part of the CMS and monitors suppression pool temperatures under all operating and accident conditions. Should the suppression pool temperature exceed established limits, SPTM provides input for both a reactor scram and for automatic initiation of the suppression pool cooling mode of the Fuel Auxiliary Pools Cooling System (FAPCS) operation. The RTIF cabinet houses the equipment that performs the Suppression Pool Temperature Monitoring functions for the CMS discussed in Subsection 7.5.2.

7.1.2.8.6.2 Other Containment Monitoring Systems Description Summary

Other CMS functions, some of which are nonsafety-related, include monitoring several key containment parameters. These include fluid and radiation levels, pressures, temperatures, hydrogen/oxygen concentrations, and dew point/humidity values. These parameters are monitored during normal reactor operations and post accident conditions to evaluate the containment integrity and other conditions. Abnormal measurements and indications initiate alarms in the MCR.

7.1.2.8.7 Vacuum Breaker Isolation Function

The safety-related VB isolation function prevents the loss of long-term containment integrity by automatically isolating an excessively leaking VB using a VB isolation valve. The RTIF cabinet houses the equipment that performs the VB isolation function. The VB isolation function is implemented using the ICP, which is diverse from the RTIF-NMS platform and the SSLC/ESF platform and not susceptible to a common-cause failure. Refer to Subsection 7.3.6 for additional information.

7.1.2.8.8 HP CRD Isolation Bypass Function

The safety-related HP CRD isolation bypass function automatically bypasses the HP CRD injection isolation (intended to prevent the over-pressurization of the containment and therefore loss of long-term containment integrity) to compensate for a failure of the GDCS to inject. The RTIF cabinet houses the equipment that performs the HP CRD isolation bypass function. The HP CRD isolation bypass function is implemented using the ICP, which is diverse from the RTIF-NMS platform and the SSLC/ESF platform and not susceptible to a common-cause failure. Refer to Section 4.6 as well as Subsections 7.3.3 and 7.4.5 for additional information.

7.1.3 Q-DCIS Specifics

The Q-DCIS architecture, its relationships, and its acceptance criteria are described below. The Q-DCIS data communication systems are embedded in the DCIS, which performs the data communication functions that are part of or support the systems described in Sections 7.2 through 7.8. A simplified network functional diagram of the DCIS appears as Figure 7.1-1, which shows the elements of the Q-DCIS and the N-DCIS, and is a functional representation of the design.

7.1.3.1 Q-DCIS Design Bases

7.1.3.1.1 Q-DCIS Safety-Related Design Bases

The safety-related design bases applicable to the Q-DCIS are found in IEEE Std. 603, Sections 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, and 4.12. These sections specify that the Q-DCIS:

- Reads signals from the safety-related instrumentation locally and through RMUs;
- Performs required signal conditioning, if this function is required, and then digitizes and formats the input signals into messages for transmission on the Q-DCIS network or data path;
- Transmits the data signals and commands onto the Q-DCIS network or data path for interface with other safety-related systems;
- Supports safety-related system monitoring and operator input to and from the MCR and RSS VDUs;
- Performs safety-related logic functions;
- Performs closed loop control and logic independently of the VDUs;
- Transmits the actuation signals to safety-related equipment via load drivers or contactors;
- Provides self-diagnostic and process alarm information to the operator; and
- Isolates data communication to and from the N-DCIS.

7.1.3.1.2 Q-DCIS Power Generation (Nonsafety-Related) Design Bases

The power generation design basis for the Q-DCIS is to transmit plant parameters and other safety-related system data through qualified safety-related isolation devices to the N-DCIS for use by nonsafety-related system logic and displays for power generation.

7.1.3.1.3 Q-DCIS Setpoint Methodology

To determine setpoints and select appropriate I&C, the following are considered: range, accuracy, resolution, instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability. The recommended test frequency is greater for instrumentation that demonstrates a stronger tendency to drift. Adequate margin between safety limits and instrument setpoints is provided to allow for instrument error. The response time of the instrument is assumed in the safety analysis and verified in plant-specific surveillance testing. The amount of instrument error is determined by test and experience. The setpoint is selected based on a known error; the Q-DCIS equipment is microprocessor-based with discrete setpoints that do not drift.

The actual settings are determined from operating experience or conservative analyses when specific instrument operating experience is not available. The settings are far enough from the values expected in normal operation to preclude inadvertent initiation of the safety-related action. At the same time, they are far enough from the analyzed trip values to ensure that appropriate margins are maintained between the actual settings and the analyzed values. The margin between the limiting safety-related system settings and the actual safety limits (where applicable) include consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from historical data on setpoint drift and from quantitative reliability requirements for each system and its components. Setpoints are established for the Q-DCIS systems in accordance with Reference 7.1-9.

7.1.3.2 Q-DCIS Description

The Q-DCIS provides the data processing and transmission network that encompasses the four independent and separate data multiplexing divisions (1, 2, 3, and 4), corresponding to the four divisions of safety-related electrical and I&C equipment. Each Q-DCIS division consists of the RMUs, the intra-divisional fiber optic cable signal transmission pathways, the RTIF cabinets, the NMS cabinets, the SSLC/ESF cabinets, the ICP equipment, the cabinet power supplies, the safety-related VDUs, and safety-related fiber optic CIMs.

The Q-DCIS contains multiple dual redundant fiber optic cable networks for each of the four divisions. The networks connect the RMUs with:

- Divisional safety-related VDUs;
- RTIF and NMS Digital Trip Modules (DTMs);
- RTIF and NMS CIMs;
- SSLC/ESF CIMs;
- RTIF, NMS, and SSLC/ESF cabinets, located in the safety-related Q-DCIS equipment rooms in the RB and CB; and

- The N-DCIS, through qualified safety-related isolation devices via datalinks and gateways (when necessary).

Each Q-DCIS system is housed in a set of uniquely identified cabinets. Separate cabinets are provided for each of the four divisions and the remotely mounted components within each division.

An RMU is an assembly of divisional Input/Output (I/O) equipment, power supplies and possibly some logic housed in one cabinet. The field sensors and process transmitters are hardwired to the divisional local RMUs in the RB and CB. At the input module of the field RMUs, the analog data are delivered to the analog input modules and discrete data are delivered to the digital input modules. The field sensors, actuators, and wiring belong to the process system to which they are attached and are not part of the Q-DCIS. Analog signal conditioning, A/D conversion, and digital signal conditioning such as filtering and voltage level conversion are performed at the input modules.

Each field RMU formats and transmits input signals as data messages to the dual network and then to the RTIF, NMS, and SSLC/ESF components within its own division. The field RMUs receive the SSLC/ESF equipment control signals from the network for distribution by hardwired connection to the equipment actuators of the ESF functions.

The corresponding divisional Q-DCIS networks send data to the RTIF, NMS, and SSLC/ESF components in separate RTIF, NMS, and SSLC/ESF divisional cabinets. The data are also sent to other safety-related logic equipment such as the safety-related logic test cabinets for control of the functional tests, the CIMs, and through qualified safety-related isolation devices (CIMs) for communication with the N-DCIS via datalinks and gateways (when necessary).

The Q-DCIS RMUs in the RB and safety-related logic cabinets in the CB are located in mild environments. The rooms containing this equipment are cooled by nonsafety-related Heating, Ventilation and Air Conditioning (HVAC) during normal operation when either offsite or diesel generator power is available. When no active cooling is available, such as when the system is operating on only battery power during a SBO, the cooling is passive. The Q-DCIS components, including the fiber optic cable network, are not located in containment or in high radiation areas. Signals from within these areas are hardwired by copper cable to the RMUs. Electromagnetic compatibility (EMC) of the RMUs and Q-DCIS equipment is ensured by conformance to the following program.

- The Q-DCIS components are designed to minimize susceptibility to and generation of electromagnetic interference (EMI) and radio frequency interference (RFI).
- The Q-DCIS components are subjected to tests for EMI, RFI, and surge conditions that conform to guidelines in RG 1.180.
- Grounding of RMU and Q-DCIS equipment follows the guidance given in IEEE Std. 518 and IEEE Std. 1050.

To minimize EMI effects, the Q-DCIS electrical equipment incorporates shielding and filtering. The equipment is mounted in grounded panels provided with isolated instrument grounds.

The four divisions of Q-DCIS are physically located in four separate quadrants of the reactor building and four separate equipment rooms in the control building. These locations represent separate fire areas. Within the reactor building, there are separate fire areas within a division.

The intra division fire areas are used to separate the RMUs that contain the series-connected load drivers used to operate safety-related solenoids and squib valves. The same reactor building fire areas are used to separate the DPS RMUs that contain the series-connected multiple load drivers used to operate nonsafety-related solenoids and squib valves. The fire area separation for both the safety-related and nonsafety-related RMUs will prevent inadvertent actuations affecting safe shutdown whether from hot shorts or fires in a single fire area. Finally, the control building Q-DCIS, N-DCIS, and DPS rooms are all separated into different fire areas.

7.1.3.2.1 Reactor Trip Systems

The Reactor Trip Systems include the RPS, the NMS, and SPTM functions.

7.1.3.2.1.1 Reactor Protection System

The safety-related RPS initiates an automatic reactor shutdown by rapid insertion of control rods (scram) if monitored system variables exceed pre-established limits. This action prevents fuel damage, limits system pressure, and, thus, minimizes the release of radioactive material. Refer to Subsection 7.2.1 for additional information.

7.1.3.2.1.2 Neutron Monitoring System

The safety-related NMS monitors the core thermal 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. Refer to Subsection 7.2.2 for additional information.

7.1.3.2.1.3 Suppression Pool Temperature Monitoring Subsystem

The safety-related SPTM function of the CMS monitors suppression pool temperatures under all operating and accident conditions. This subsystem operates continuously during reactor operation. If the suppression pool temperature exceeds established limits, SPTM provides input for a reactor scram and for automatic initiation of the suppression pool cooling mode of the FAPCS. Refer to Subsection 7.2.3 for additional information.

7.1.3.2.2 Safety System Logic and Control / Engineered Safety Features System

The SSLC/ESF system performs the control logic processing of the plant sensor data and manual control switch signals activating the functions of the LD&IS (non-MSIV), ECCS, and CRHS. Input signals from redundant channels of safety-related instrumentation are used to perform logic operations that result in decisions for safety-related action. Trip logic outputs to the actuation devices, such as pilot solenoid valves and squib valves, initiate the appropriate plant protection actions. Refer to Subsection 7.3.5 for additional information.

7.1.3.2.2.1 Emergency Core Cooling System

The safety-related ECCS is an engineered safety feature that mitigates LOCAs by automatically initiating:

- The ICS (Refer to Subsection 7.4.4),
- The ADS (Refer to Subsection 7.3.1.1),
- The GDCS (Refer to Subsection 7.3.1.2), and

- The SLC system (Refer to Subsection 7.4.1).

7.1.3.2.2.2 (Deleted)

7.1.3.2.2.3 Leak Detection and Isolation System

The safety-related LD&IS monitors leakage sources from the RCPB. It automatically initiates closure of the appropriate valves to isolate the source of the leak if the monitored system variables exceed preset limits. This action limits the loss of coolant from the RCPB and the release of radioactive materials to the environment. Refer to Subsection 7.3.3 for additional information.

7.1.3.2.2.4 Control Room Habitability Systems

The safety-related CRHS provides a safe environment within the MCR that allows the operator(s) to:

- Control the nuclear reactor and its auxiliary systems during normal conditions,
- Safely shut down the reactor, and
- Maintain the reactor in a safe condition during abnormal events and accidents.

The CRHS includes CB shielding, area radiation monitoring and a CRHA Heating, Ventilation, and Air Conditioning (HVAC) System. The CRHS provides emergency food and water storage; emergency kitchen and sanitary facilities; protection from and removal of airborne radioactive contaminants; and the capability to remove smoke. The CRHA envelope, ventilation inlet/return isolation dampers, redundant Emergency Filter Units (EFUs) in the emergency HVAC system, and associated controls are safety-related. Refer to Subsection 7.3.4 for more information.

7.1.3.2.2.5 (Deleted)

7.1.3.2.2.6 Passive Containment Cooling System

A description is included in Subsection 7.1.2.8.5 for completeness. Refer to Subsections 7.3.2 and 6.2.2 for additional information.

7.1.3.2.3 Safe Shutdown Systems

Safe shutdown systems include the SLC system and the RSS.

7.1.3.2.3.1 Standby Liquid Control System

The safety-related SLC system provides a diverse means to shut down the reactor from full power to a subcritical condition, and then maintains the reactor subcritical using soluble boron injection. The SLC system can be manually initiated or initiated automatically for ATWS mitigation. The SLC system is also initiated automatically in response to LOCAs as part of the ECCS. Refer to Subsections 7.1.2.8.3.1.4, 7.1.2.8.4, and 7.4.1 for additional information.

7.1.3.2.3.2 Remote Shutdown System

The RSS has two redundant and independent panels located in two different areas in the RB. If the MCR becomes uninhabitable, Division 1 and 2 safety-related parameters and nonsafety-related parameters displayed or controlled at a Q-DCIS, and N-DCIS MCR VDU can be monitored and controlled from either of the RSS panels. Refer to Subsection 7.4.2 for additional information.

7.1.3.2.4 Safety-Related Information Systems

Safety-related information systems include the Post-accident Monitoring (PAM) instrumentation, the CMS instrumentation, and Process Radiation Monitoring System (PRMS) instrumentation.

7.1.3.2.4.1 Post-Accident Monitoring Instrumentation

The PAM instrumentation monitors variables and systems under accident conditions to ensure plant and personnel safety. An assessment of conformance to RG 1.97 is presented in Subsection 7.5.1.

7.1.3.2.4.2 Containment Monitoring System

The CMS instrumentation measures and records radiation levels and the oxygen/hydrogen concentration levels in containment under post-accident conditions. The CMS is designed to operate continuously during normal operation and is automatically put in service upon detection of LOCA conditions. Refer to Subsection 7.5.2 for additional information.

7.1.3.2.4.3 Process Radiation Monitoring System

Safety-related PRMS instrumentation monitors the following for radioactive materials: discharges from the ICS vent, and ventilation discharges. The nonsafety-related PRMS is discussed in Subsection 7.1.5.2.2.1. The MCR display, recording, and alarm capabilities are provided along with controls that provide automatic trip inputs to the respective systems to prevent further radiation release. Refer to Subsection 11.5.3 for additional information.

7.1.3.2.5 Interlock Logic

The interlock logic functions are embedded in the DCIS logic, so that a separate interlock system is not required. Refer to Section 7.6 for additional information.

7.1.3.2.6 Nuclear Boiler System Instrumentation

Redundant NBS safety-related instrumentation provides the following data for operator monitoring:

- RPV water level indicated in the MCR on displays associated with the different water level ranges;
- The reactor pressure indicated in the MCR and at four local instrument racks in the Reactor Building (RB);
- The discharge line temperatures of the SRVs viewed on safety-related video display units (VDUs) in the MCR. Any temperature exceeding the trip setting is alarmed to indicate leakage of a SRV seat;
- RPV temperature is indicated in the MCR, and high bottom head to reactor coolant differential temperature is alarmed in the MCR; and
- Main steam flow rate is indicated in the MCR.

The NBS instrumentation also provides inputs to the safety-related actuation systems during normal, transient, and accident conditions. Refer to Sections 7.2 and 7.3 for additional information.

7.1.3.2.7 Data Communication Systems

The DCIS data communication functions are embedded within the Q-DCIS and the N-DCIS architectures. Safety-related Q-DCIS internal and external communication protocols are deterministic.

7.1.3.3 Q-DCIS Safety Evaluation

All communication between the Q-DCIS and the N-DCIS is through safety-related CIMs, via datalinks and fiber optic cable. Fiber optic cable is also used for:

- Limited communication between the Q-DCIS divisions (such as the two-out-of-four voting logic);
- Communication within a division;
- Providing data to the VDU monitors; and
- Transferring VDU outputs corresponding to manual initiation actions.

The dual redundant fiber optic cable data networks described below replace the many conventional, long length, copper conductor cables of existing nuclear power plants. This reduces the cost and complexity of divisional cable runs that connect components of the plant protection and safety-related systems such as the RPS, MSIV isolation logic functions, LD&IS containment isolation functions, SSLC/ESF, and safety-related VDUs. The fiber optic cable provides transmission path immune from EMI for plant sensor data and safety-related system control signals.

7.1.3.3.1 Safety-Related Isolation

The use of fiber optic cable provides complete electrical isolation between components and noise free communication pathways, but is not credited for either the safety-related isolation or the safety-related separation. The safety-related fiber optic CIMs are the isolation devices, including data isolation, and convert signals between electricity and light on the safety-related side of the fiber optic cable. These safety-related fiber optic CIMs are powered by the division within which they are physically located. The safety-related fiber optic CIMs, which provide the safety-related isolation and separation, are qualified safety-related components.

The IEEE Std. 603, Sections 5.6 and 6.3, isolation and separation (electrical, physical, data, and communications) occurs in the safety-related fiber optic CIM (transmitter or receiver) where the signal is converted between electricity and light. Although IEEE Std. 383 is applicable to electrical cable, the fiber optic cables are sheathed in material meeting the IEEE Std. 383 that addresses fire propagation mitigation.

The physical communication between safety-related and safety-related systems and between safety-related and nonsafety-related systems is always via fiber optic cable. Within the safety-related system, the electrical to light interface (the CIM) is always safety-related. There is no credible seismic event, design basis accident (DBA), etc. that could cause a failure of the isolation barrier between the safety-related/safety-related or safety-related/nonsafety-related portions of the isolator (specifically, the components at each end of the fiber optic cable). Although unlikely, the worst-case failure is loss of communication. Therefore, the design complies with IEEE Std. 603, Section 5.6.

In addition to the assured electrical isolation and separation, data/communication isolation enforces the design basis that no safety-related function depends on nonsafety-related communication. The safety-related Q-DCIS communications are governed by both hardware and software protocols. These protocols are governed by References 7.1-10 and 7.1-12 and control the transmission, acceptance, and authentication of data from outside the division so that these communications cannot adversely affect the operation or safety-related functions of that division. The communication protocols meet the design principles of the Q-DCIS CIMs described below. Note that whether or not the CIM is operable or whether there is anything functional on the nonsafety-related side or other divisional safety-related side of the CIM, the operation of the safety-related system is not affected.

7.1.3.3.2 Communication Pathways (CIMs, Fiber Optic Cable, Datalinks, and Nonsafety-Related Gateways)

Instances of nonsafety-related to safety-related communication (described below) are also via fiber optic cable, datalinks, gateways (when necessary), and through safety-related fiber optic CIMs (in order to provide the required safety-related isolation, separation, and message authentication). The safety-related fiber optic CIMs receiving data from the N-DCIS are qualified safety-related (Q-DCIS) components. Safety-related system functions do not depend on the correctness or even the existence of the safety-related/nonsafety-related communications. The loss of any communication in either direction only results in alarms and the potential loss of data between the Q-DCIS and the N-DCIS. Any single divisional data loss to N-DCIS does not affect power generation or safety. The loss of all safety-related data to N-DCIS can potentially affect power generation but only in a long-term situation, such as core thermal limits monitoring.

The Q-DCIS is arranged into four independent divisions. Other than the RPS and NMS point-to-point communication used for two-out-of-four voting logic, the intra-divisional and safety-related to nonsafety-related fiber optic cable communication pathways are redundant in order to support reliability and to allow self-diagnostics to be communicated in the presence of a single failure. The RPS and NMS two-out-of-four voting logic communication redundancy is acceptable because loss of communication is interpreted as a trip from the sending division. Similarly, all safety-related cabinets and chassis are powered by redundant UPS for reliability and self-diagnostics. For all safety-related to safety-related communication, safety-related functions continue to be initiated and executed in the presence of any single or dual communication or power failure. A dual communication or power failure could result in the loss of a single independent division but not in the loss of a safety-related function. A dual-division failure, requiring four communications or power failures, does not result in the loss of a safety-related function.

The safety-related fiber optic CIMs (which are the isolation devices, as described above) within the Q-DCIS along with datalinks and gateways (when necessary) within the N-DCIS transmit safety-related data to the N-DCIS via fiber optic cable. The gateways are specific to the communication link between the sending and receiving components. For example, the gateway between the SSLC/ESF and N-DCIS is different from the gateway between the RTIF-NMS and the N-DCIS. The sending sources are different even though the receivers are the same.

Safety-related software is as simple as possible so that Q-DCIS components have neither interrupts from nonsafety-related devices nor do they respond to nonsafety-related component queries for information. The Q-DCIS components simply put information on the safety-related (Q-DCIS) networks in a known format so that other safety-related devices can retrieve what is needed for their function. Self-diagnostics information is also put on the DCIS networks. The safety-related fiber optic CIMs provide the safety-related isolation. The CIMs indiscriminately retrieve all of the divisional information from the safety-related (Q-DCIS) networks and send it one way to the N-DCIS (via fiber optic cable and a datalink or via a combination of fiber optic cable, datalinks and nonsafety-related gateways). Time tags are described below.

7.1.3.3.3 Nonsafety-Related Gateways

The nonsafety-related gateways translate the information sent between the Q-DCIS (always through the required isolation, via datalinks and fiber optic cable) and the N-DCIS into a format that the other portion of the DCIS (either N-DCIS or Q-DCIS) can apply. The N-DCIS gateways package the safety-related information into the necessary message packets to support specific N-DCIS components for monitoring and alarm management purposes. The N-DCIS gateways also respond to interrupts and queries. Safety-related to nonsafety-related communication pathways that do not involve nonsafety-related gateways use safety-related fiber optic CIMs (which provide the safety-related isolation), datalinks, and fiber optic cable. Nonsafety-related gateways are not used when the N-DCIS (nonsafety-related receiver) is capable of receiving and extracting the data signal generated by the Q-DCIS (safety-related fiber optic CIM) without the need for data conversion. One example of datalink communication between the Q-DCIS and the N-DCIS without the use of a nonsafety-related gateway is the communication from the NMS to the MRBM and automated thermal limit monitor (ATLM). The nonsafety-related gateways, when necessary, handle the data translation/packaging interface, but do not serve to provide the required safety-related isolation for communications between the Q-DCIS and the N-DCIS. When nonsafety-related gateways are necessary they package the data for the various N-DCIS functions, respond to the N-DCIS requests for information and monitor communication link status. The safety-related isolation and separation for communications between the Q-DCIS and the N-DCIS is always provided by the safety-related CIMs, as described above, regardless of whether a combination of datalinks and gateways is used or only a datalink is used.

7.1.3.3.4 Communication from N-DCIS to Q-DCIS (DCIS Time tagging and NMS Calibration)

The safety-related systems are designed to not depend on nonsafety-related communication to function, therefore, loss of communication is never a safety issue. Specifically, no process feedback signals are sent from the N-DCIS to the Q-DCIS. The only signals sent from nonsafety-related components to safety-related components are those involved in time tagging and the transmission of data for calibration of the safety-related NMS, which is only possible under the specific circumstances described below.

Nonsafety-related time signals are sent to Q-DCIS safety-related fiber optic CIMs through the nonsafety-related gateways for display on the Q-DCIS (SSLC/ESF) safety-related VDUs and for use by the Q-DCIS to allow time tagging of data sent to the N-DCIS. These time signals are only used by the Q-DCIS for VDU indication so that all displays show the same time of day. The time signals sent from the N-DCIS to the Q-DCIS are never used to synchronize logic nor is the safety-related logic dependent in any way on the absence, presence, or correctness of the time signal.

The only other instance of nonsafety-related to safety-related communication involves the calibration of the APRM and LPRM. LPRM and APRM calibration gain adjustment factors, which are calculated in the nonsafety-related plant computer functions (PCF) of the N-DCIS, are transmitted to the safety-related LPRM/APRM equipment through proper signal isolation (the safety-related fiber optic CIMs). However, this data transmission can only be implemented and accepted by the safety-related equipment with the operator's acknowledgment. This transfer of data is similar to that used by retrofit Nuclear Measurement Analysis and Control (NUMAC) PRNM systems already licensed for some U.S. nuclear power plants, which is done manually and is rigorously controlled. Before the RTIF-NMS platform can accept new calibration data, even if it has been continuously sent by 3D MONICORE, the operator must use a keylock switch to make the particular chassis inoperable (INOP). If the operator has not additionally put the corresponding division in bypass, the INOP is interpreted as an NMS trip. It is physically impossible to simultaneously bypass more than one division. Trips and bypasses are alarmed in the MCR.

After the chassis has been made INOP, the operator reviews the download received by the chassis being calibrated. Additionally, the operator can determine that a checkback signal interchange indicates that the RTIF-NMS platform has correctly received the 3D MONICORE data. If a checkback signal is utilized, it is initiated by the RTIF-NMS equipment and sent to 3D MONICORE. 3D MONICORE receives the checkback signal, verifies/validates that the information received by the RTIF-NMS equipment is what was sent, and then sends a signal back to the RTIF-NMS equipment confirming that the data was received accurately. There is no automatic/automated system response to a good or bad checkback signal. Only after the operator is satisfied that the calibration data are accurate and correct (through manual verification of the data and/or the use of a confirming electronic checkback signal) can the operator instruct the RTIF-NMS platform that it is acceptable to use the downloaded data. This process is equivalent, but more convenient and accurate, to carrying the calibration data to the RTIF-NMS platform then entering it manually. The manual process is still possible. After the download is accepted by the RTIF-NMS platform, the operator uses the keylock switch to make the instrument operable (removing it from the INOP state) and then resets the bypass for the division.

7.1.3.3.5 Dataflow, RMUs, Processor Cabinets, and VDUs

Dataflow within each of the four divisions of the Q-DCIS is from the RMUs located in the CB, RB, and Fuel Building (FB) in areas appropriate to their division; there are no safety-related RMUs in any other building. Data such as that from transducers and switches is acquired by the RMUs, the signal appropriately conditioned, and sent via the redundant fiber optic cable communication links (datalinks) along with diagnostic data to the RTIF, NMS and SSLC/ESF cabinets. The RTIF, NMS, and SSLC/ESF cabinets are distributed throughout the division to perform the logic required by the safety-related systems.

There are always RTIF, NMS, and SSLC/ESF cabinets located in the MCR back panel area where there are four Q-DCIS rooms, one per division. The back panel area is where the interdivisional communication is physically performed to support the two-out-of-four voting that initiates safety-related action. Additionally RTIF, NMS, and SSLC/ESF safety-related fiber optic CIMs are used to operate the safety-related VDUs in that division and to provide isolation between the Q-DCIS and the N-DCIS. Finally, calculated outputs from the RTIF, NMS, and SSLC/ESF cabinets are sent via the redundant Q-DCIS communication system to the RMUs that provide outputs to the safety-related actuators (i.e., solenoids, explosive squib valves, etc.) via load drivers. Note that some may use point-to-point optical fiber or hardwiring to the final load drivers or final actuators if higher speeds are required.

There are at least two safety-related VDUs per division in the MCR. Divisions 1 and 2 have an additional VDU located on each RSS panel. The VDUs are used to monitor safety-related information from their connected division and are used to provide manual operator inputs to the safety-related (SSLC/ESF) logic. The VDUs provide access to a full range of plant parameters in accordance with the requirements of 10 CFR 50.34(f)(2)(iv), TMI Action Item I.D.2. The VDUs are also used for divisional self-diagnostics and divisional alarms.

The four VDU divisions allow checking of the operational availability of each sense and command feature input sensor for the RTIF, NMS, and SSLC/ESF systems. This is accomplished with a high degree of confidence by cross-checking between channels that bear a known relationship with each other.

7.1.3.3.6 Two-out-of-four Voting Logic

The interconnections between Divisions 1, 2, 3, and 4 are used for two-out-of-four voting logic. The interconnections are provided between safety-related fiber optic CIMs through fiber optic cable; there are no electrical connections between divisions. Fail-safe systems like the RPS or the NMS interpret loss of interdivisional communication as a trip from that division. The trip counts toward the two-out-of-four voting logic initiations, unless the failed division is bypassed. Fail-as-is systems like the ECCS do not interpret loss of communications as a trip. The chances of a CIM card hardware failure in a manner that simultaneously sets all trip inputs to "trip" is negligible, the chances of a CIM card hardware failure in a manner that simultaneously sets all trip inputs to "trip' without an accompanying diagnostic is even smaller. The I&C design basis is N-2, therefore, safety-related systems are capable of performing all safety-related functions, with three out of four safety-related divisions available in the presence of a single failure.

The four redundant divisions of the Q-DCIS satisfy the single failure criterion of IEEE Std. 603, Section 5.1. They also satisfy the independence, testing, and repair requirements outlined in IEEE Std. 603, Sections 5.6, 5.7, and 6.5. The safety-related fiber optic CIMs (transmitters/receivers), fiber optic cable, and network that are part of the Q-DCIS within and between the four redundant divisions satisfy the separation and independence requirements of divisional equipment. The cable routing separation meets the requirements of the SRP Subsection 9.5.1, “Fire Protection Programs”.

7.1.3.3.7 Continuous Online Diagnostics and Redundant Power Supplies

The DCIS performs continuous online diagnostic functions that monitor transmission path quality and integrity as well as the integrity of most of the system components. Self-diagnostics extend down to the replaceable card or module level. Off-line tests with simulated input signals can also be used to verify the overall system integrity. Segments of Q-DCIS can be tested and calibrated while on-line when portions of safety-related logic are bypassed. These components and the dual redundant data communication pathways are repairable on-line if one pathway fails.

Because of the redundant power supplies and communication pathways, almost all self-diagnostic alarms can be viewed in the MCR while a single failure and most multiple failures exist. The Q-DCIS failures are alarmed in the MCR.

The Q-DCIS components and cabinets have redundant power supplies that are supplied by redundant uninterruptible power feeds within each division. These power feeds support the Q-DCIS operation for 72 hours with neither diesel-generator nor offsite power available. The loss of one power feed or power supply does not affect any safety-related system function.

The Q-DCIS includes the safety-related hardware and software for the RTIF, NMS, and SSLC/ESF protection functions and parallels the four-division design of those systems. No failure of any two divisions prevents a safety-related action, such as a detection or a trip, from being accomplished successfully. Component self-testing reconfigures the system to the approved safe state upon detection of uncorrectable errors. The capability for off-line test and calibration of the Q-DCIS components is designed into the system. An individual division can be disconnected for maintenance and calibration through the use of bypasses within the safety-related logic division without compromising the operations of the other divisions. Only one division can be bypassed at any one time and the existence of a bypass is alarmed in the MCR.

7.1.3.3.8 Acceptance Criteria, Guidance, and Conformance

The regulatory acceptance criteria and guidance applicable to each of the Q-DCIS systems identified in the "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", NUREG-0800 are stated in Table 7.1-1, "Regulatory Requirements Applicability Matrix". Sections 7.2 through Section 7.8 contain regulatory conformance discussions for each specific system. The degree of applicability and conformance, along with any clarification or justification for exceptions, is presented in the safety evaluation sections for each specific system.

7.1.3.4 Q-DCIS Testing and Inspection Requirements

The Q-DCIS uses three diverse safety-related platforms: RTIF-NMS (RPS, NMS, and the MSIV isolation function) and SSLC/ESF, and ICP.

The RTIF-NMS and SSLC/ESF platforms are readily accessible for testing purposes. Their continuous automatic online diagnostics detect data transmission errors and hardware failures at the replaceable card or module level. Online diagnostics for RTIF-NMS and SSLC/ESF are qualified as safety-related in conjunction with functional software qualification, and also meet the self-diagnostic characteristics for digital computer based protection systems recommended by IEEE Std. 7-4.3.2.

Both RTIF-NMS and SSLC/ESF have self-diagnostic features that check the validity of input signals. An analog input outside expected limits creates an alarm.

The RTIF-NMS hardware has watchdog timers for various logic processors and logic functions that monitor the execution of the software. If the software stops executing (suspending the self-diagnostics), its watchdog timer resets the affected logic processor or logic function. This results in a channel trip and alarm while the logic processor or logic function is resetting.

The SSLC/ESF platform is a Triple Modular Redundant (TMR) system, with three Main Processors (MPs). The MPs are monitored by individual watchdog timers that reset or fail an

MP depending on the severity of the problem. A single or double MP failure causes alarms, but the division continues to function to provide the required automatic protective actions.

Both RTIF-NMS and SSLC/ESF are cyclically tested from the sensor input point to logic contact output. The self-diagnostic capabilities include power supply checks, microprocessor checks, system initialization, watchdog timers, memory integrity checks, I/O data integrity checks, communication bus interfaces checks, and checks on the application program (checksum). Cyclically monitored items include:

- Sensor inputs to the I/O for unacceptably high/low levels;
- Proper execution of application code/checksum verification of code integrity;
- Internal clocks;
- Functionality of input cards/modules, and their MP communication;
- MP communication with the output contact (SSLC/ESF platform);
- Inter-divisional communication between RPS and NMS logic processors or logic functions (RTIF-NMS platform);
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (SSLC/ESF platform); and
- Power supplies.

Subsequent to verification and validation (V&V) of software during factory and preoperational testing in accordance with approved test procedures, there is no mechanism for the RTIF-NMS or SSLC/ESF code, response time, or coded trip setpoints to inadvertently change. For user adjustable parameters a new checksum is calculated at the time acceptable changes are implemented. The new checksum is used from that point forward to validate the application software. The trip setpoint parameters are continuously sent to the N-DCIS technical specifications monitor (TSM) for comparison of the setpoints to confirm consistency between divisions and the required values.

The ICP is similar to the RTIF-NMS and SSLC/ESF platforms in that it contains self-diagnostic capabilities to ensure that the platform is functioning properly. The ICP self-diagnostics possess the capability to:

- Detect data transmission errors,
- Detect hardware failures, and
- Check platform operability.

The following describes the provisions made to allow periodic testing of safety-related platforms. Additional information on testing and inspection requirements for each system within the Q-DCIS is presented in specific subsections in Chapter 7.

Channel Check

The channel check is a qualitative assessment of channel behavior during operation. The online self-diagnostic features of the safety-related platforms, in conjunction with the TSM, accomplish the channel check requirements for detecting unacceptable deviations by automatic cyclic comparison of channel outputs. TSM provides a log of the results and sends out-of-limits alarms to the Alarm Management System (AMS). The TSM uses a hardware/software platform diverse from the safety-related platforms. The TSM functions are listed in Subsection 7.1.5.2.4.5.

If there are any self-diagnostic test results and indicating alarms, a summary report is available to the operator on demand.

Sensor and actuation logic channel monitoring capability are provided at the VDUs to enable manual validation of TSM report results.

Channel Functional Test

The channel functional test ensures that the entire sensor channel performs its intended function. The online self-diagnostic features of the safety-related platforms, in conjunction with the TSM, support the channel functional test requirements. The channel functional test can be conducted by manual injection of a simulated signal, one division at a time. The channel functional test confirms the channel through the DTM function is functioning correctly. The coincidence logic, involving more than one channel, and the final control elements are not activated in the channel functional test.

Logic System Functional Test

A LOGIC SYSTEM FUNCTIONAL TEST shall be a test of all logic components required for OPERABILITY of a logic circuit, from as close to the sensor as practicable up to, but not including, the actuated device, to verify OPERABILITY. The LOGIC SYSTEM FUNCTIONAL TEST may be performed by means of any series of sequential, overlapping, or total system steps so that the entire logic system is tested.

Response Time Test

The response time test is performed by a series of sequential, overlapping, or total steps to measure the entire response time. The logic processor or logic function self-diagnostics and the TSM support the performance of the response time test for the safety-related platforms. Watchdog timers monitor logic processor or logic function internal clocks and alarms for out-of-limit conditions and the completion of application code per logic processor or logic function cycle. Since the clocks set the response time, there is no mechanism for the response time to change without alarm or trip. All time delays incorporated into system logics are performed by software and the values are set during factory and preoperational testing in accordance with approved test procedures. Subsequent to final V&V of the code, there is no mechanism for the time delay values to inadvertently change.

The response time tests for the remaining portions (i.e. sensors [except neutron radiation detectors] and final control elements/actuators) are performed separately from self-diagnostics and the TSM.

7.1.3.5 Q-DCIS Instrumentation and Control Requirements

The data transmission function delivers system data to all nodes in the network, such as distributed logics of the Q-DCIS RMUs and specific safety-related logic system components, and in certain safety-related systems through dedicated data paths. The Q-DCIS thus provides the necessary integrated support for the distributed control logic functions of the RMUs and safety-related logic equipment. The data I/O and transmission functions do not require any manual operator intervention and have no operator controls.

The Q-DCIS operates continuously in all modes of plant operation to support the data transmission requirements of the interfacing systems. When one network of the dual network system fails, operation continues automatically without operator intervention. In the event that a channel failure occurs, the network alarms in the MCR indicate the failed component. The failed segment of the channel can be isolated from the operating segments and repaired on-line.

The following Q-DCIS displays and alarms, as a minimum, are provided in the MCR.

- MCR Alarms:
  - Division 1 Q-DCIS trouble,
  - Division 2 Q-DCIS trouble,
  - Division 3 Q-DCIS trouble, and
  - Division 4 Q-DCIS trouble.
- MCR Indications:
  - Division 1 Q-DCIS diagnostic displays,
  - Division 2 Q-DCIS diagnostic displays,
  - Division 3 Q-DCIS diagnostic displays, and
  - Division 4 Q-DCIS diagnostic displays.

7.1.3.6 Q-DCIS Boundaries

The Q-DCIS does not include any N-DCIS components. The field sensors, actuators, and wiring belong to the process system to which they are attached and are not part of the Q-DCIS.

7.1.4 N-DCIS General Description Summary

The N-DCIS comprises the nonsafety-related portion of the DCIS. The N-DCIS components are redundant when they are needed to support power generation and are segmented into systems. Segmentation allows, but does not require, the systems to operate independently of each other. The N-DCIS major systems and functions are defined in Subsection 7.1.4.8.

The N-DCIS major components include:

- Fiber optic cable and hardwired networks;
- System control processors;
- Workstations;
- Dedicated network switches;
- RMUs;
- Gateways, datalinks, signal isolators, and I/O modules;
- MCR consoles and display panels;
- Fiber optic modems and media converters; and
- Computer peripherals, such as printers and plotters.

Although the N-DCIS is larger and more complex than the Q-DCIS, it is designed with a segmented architecture that allows the different portions of the system to operate independently of one another. Redundant automatic network switches manage the network so that during normal operation the segments appear seamless to the MCR operator; the network is designed to tolerate a single hardware failure (and many dual hardware failures) without loss of power generation capability or challenge to a safety-related system. The N-DCIS cannot control any Q-DCIS component. The N-DCIS accepts one-way communication from the Q-DCIS so that the safety-related information can be monitored, archived and alarmed seamlessly with the N-DCIS data.

The N-DCIS performs control functions with logic processing modules using signals acquired by the RMUs. The N-DCIS logic processing can be found in the N-DCIS cabinets dedicated to specific system logic functions, such as Steam Bypass and Pressure Control (SB&PC) System and the Turbine-Generator Control System (TGCS), and in cabinets where several system logic functions are combined. The N-DCIS logic is implemented in triple redundant control systems for core nonsafety-related key systems, such as the Feedwater Control System (FWCS), SB&PC System, and Plant Automation System (PAS). The N-DCIS logic is always at least redundant for systems required for power generation, so that no single failure of an active DCIS component can cause or prevent a BOP trip or reactor scram.

The N-DCIS provides the control and monitoring operator interface on the N-DCIS nonsafety-related VDUs in the MCR and RSS panels. The VDUs operate independently of one another yet each can access any component in the N-DCIS. This gives the RSS panels the same control and monitoring capability as the displays in the MCR. The N-DCIS provides datalinks and gateways as necessary to allow vendor supplied or prepackaged ("foreign") control systems to be integrated into the DCIS. Examples include the Condensate Purification System (CPS) and the Area Radiation Monitoring System (ARMS).

The N-DCIS components that support power generation are provided with two or three sources of uninterruptible power with battery backup for at least two hours. For loss of offsite power events or after DCIS battery backup power is lost, the N-DCIS operates continuously from diesel generators.

The N-DCIS provides extensive self-diagnostics that monitor communication, power, and other failures to the replaceable card, module or chassis level. Process diagnostics include system alarms and the capability to identify sensor failures. All of the process and self-diagnostic system alarms are provided in the MCR.

7.1.4.1 N-DCIS Safety-Related Design Bases Summary

The N-DCIS does not perform or support the performance of any safety-related function. It is classified as a nonsafety-related system, and has no safety-related design basis.

7.1.4.2 N-DCIS Nonsafety-Related Design Bases Summary

The nonsafety-related design bases for the N-DCIS include the following requirements to:

- Provide functional/operational independence of nonsafety-related components important to power generation;
- Perform closed loop control and system logic;

- Tolerate a single failure of an N-DCIS component without loss of power generation capability or challenge to a safety-related system;
- Receive selected signals from the Q-DCIS and send them to nonsafety-related devices;
- Collect and archive data for transient analysis, data trending, sequence of events recording, display of Safety Parameter Display System (SPDS) and accident monitoring information, and managing the annunciation of alarm conditions in the MCR;
- Provide secure data communication to all authorized external systems, including the technical support center (TSC), the emergency operating facility (EOF), and the emergency response data system (ERDS).
- Provide gateway interfaces to control and logic processing equipment supplied by parties other than the primary N-DCIS equipment supplier;
- Perform various PCF that include calculations, displays, and alarms;
- Provide for report generation; and
- Provide for a Plant Configuration Database (PCD).

7.1.4.3 N-DCIS Safety Evaluation Summary

The N-DCIS is used as the primary control, monitoring, and data communication system with power production applications. The N-DCIS is not required for safety-related purposes, nor is its operability required during or after any DBE. The system is required to operate in the normal plant environment and is relied on for data communications and power production applications. The N-DCIS provides an isolated alternate path for safety-related data to be presented to the plant operators. The N-DCIS network that supports the dual/triple, fault-tolerant digital controllers and communication scheme is diverse from the Q-DCIS network design in both hardware and software.

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. RMUs are typically located throughout the plant and auxiliary buildings. Computer equipment and peripherals are typically located mainly in the CB (MCR and Back Panel areas), Radwaste Building, TSC, EOF, and other auxiliary buildings.

The N-DCIS panels and components are designed to maintain structural integrity, during and after a DBE, and do not prevent any safety-related equipment in their area from performing its safety-related function.

Table 7.1-1 identifies the Q-DCIS systems and N-DCIS segments and the associated codes and standards applied, in accordance with the SRP. The following subsection summarizes N-DCIS conformance to regulatory requirements, guidelines, and industry standards.

7.1.4.4 N-DCIS Regulatory Requirements Conformance Summary

As shown in Table 7.1-1 and/or described in Subsection 7.1.6 the N-DCIS meets applicable portions of: .

- 10 CFR 50.55a(a)(1);
- 10 CFR 50.34(f)(2)(iii)[I.D.1];

- 10 CFR 50.34(f)(2)(iv)[I.D.2];
- 10 CFR 50.34(f)(2)(v)[I.D.3];
- 10 CFR 50.34(f)(2)(xv)[II.E.4.4];
- 10 CFR 50.34(f)(2)(xvii)[II.F.1];
- 10 CFR 50.34(f)(2)(xviii)[II.F.2];
- 10 CFR 50.34(f)(2)(xix)[II.F.3];
- 10 CFR 50.34(f)(2)(xxi)[II.K.1.22];
- 10 CFR 50.34(f)(2)(xxiv)[II.K.3.23];
- 10 CFR 50.34(f)(2)(xxvi)[III.D.1.1];
- 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3];
- 10 CFR 50.49;
- 10 CFR 50.62;
- 10 CFR 52.47(a)(21);
- 10 CFR 52.47(b)(1);
- 10 CFR 52.47;
- IEEE Std. 7-4.3.2, 338, 497, 518, 603, 828, 829, 830, 1008, 1012, 1028, 1050, 1074;
- ANSI/ISA 67.02.01 (RG 1.151) and 67.04.01 (RG 1.105);
- GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43, 63, and 64;
- SRM II.Q and II.T on SECY 93-087;
- RGs 1.89, 1.97, 1.100, 1.105, 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, and 1.209; and
- BTPs HICB-1, 10, 16, and 19.

7.1.4.5 N-DCIS Testing and Inspection Requirements Summary

The N-DCIS components and critical components of interfacing systems are tested to ensure that the specified performance requirements are satisfied. Factory, construction, and preoperational testing of the N-DCIS elements are performed before fuel loading and startup testing to ensure that the system functions as designed and that actual system performance is within specified criteria.

The N-DCIS controllers, displays, monitoring and input and output communication interfaces function continuously during normal power operation. Abnormal operation of these components can be detected during plant operation. In addition, the controllers are equipped with on-line diagnostic capabilities to identify and isolate failure of I/O signals, buses, power supplies, processors, and inter-processor communications. These on-line diagnostics can be performed without interrupting the normal operation of the N-DCIS.

7.1.4.6 N-DCIS Operator Interface Requirements Summary

The N-DCIS VDUs allow operator control and monitoring of the N-DCIS systems. However, they allow only monitoring of safety-related system data, through appropriate isolation. The VDUs are also segmented so that the network segments can be monitored and controlled independently. During normal operation the segments are not apparent to the operators. The N-DCIS supplies alarm and annunciation information to the operator and a permanent overview mimic display for important plant information.

7.1.4.7 N-DCIS System Boundaries

The N-DCIS includes no Q-DCIS components. The N-DCIS does not include the sensors or the sensor wiring to the RMUs or the RMU output wiring to the actuators.

7.1.4.8 N-DCIS Major Systems Description Summary

The N-DCIS systems and components are nonsafety-related entities of the DCIS. The N-DCIS major system summary descriptions follow.

7.1.4.8.1 GENE Systems Description Summary

The GENE network segment is a single channel of workstations, triple-redundant controllers, and dual-redundant controllers, that execute the following functions:

- Workstations:
  - 3D MONICORE, and
  - SPDS.
- Dual-Redundant Controllers:
  - RC&IS (includes Rod Server Processing Channel [RSPC], Rod Action and Position Information [RAPI], File Control Module [FCM], Signal interface unit [SIU]),
  - ATLM, and
  - Rod worth minimizer (RWM).
- Triple-Redundant Controllers:
  - DPS.

7.1.4.8.2 Plant Investment Protection Systems (Train A and Train B) Description Summary

The Plant Investment Protection (PIP) network segment comprises two channels (A and B) of dual-redundant controllers that execute the following functions:

- Control Rod Drive (CRD) System,
- Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) System,
- FAPCS,
- Nonsafety-related RSS,
- Reactor Component Cooling Water System (RCCWS),

- Plant Service Water System (PSWS),
- PSWS cooling towers,
- Nuclear Island Chilled Water System (NICWS),
- Drywell cooling nonsafety-related electrical systems,
- Instrument Air System (IAS),
- Nonsafety-related post accident monitoring (PAM) systems,
- Nonsafety-related LD&IS systems,
- PCCS Ventilation Fans,
- Ancillary and standby diesel generators,
- 6.9 KV plant electrical power system,
- Low voltage electrical system, and
- Nonsafety-related UPS.

The N-DCIS segments in PIP A and PIP B allow for operator control and monitoring from the MCR nonsafety-related VDUs and the RSS VDUs. The A and B segments can operate independently of one another.

During loss of offsite power events, the N-DCIS for PIP A and PIP B is powered by its respective nonsafety-related batteries for two hours and then by diesel generators and can therefore operate without offsite power.

7.1.4.8.3 Balance Of Plant Systems Description Summary

The balance of plant (BOP) network segments is a single channel of triple-redundant and dual-redundant controllers that execute the following functions:

- Triple-Redundant Controllers:
  - Steam Bypass and Pressure Control (SB&PC),
  - Feedwater Control System,
  - Feedwater Temperature Control System, and
  - Turbine-Generator Control System.
- Dual-Redundant Controllers
  - Turbine auxiliary;
  - Generator auxiliary controller;
  - Electrical system main transformer/Unit Auxiliary Transformer (UAT) controller;
  - Main condenser controller;
  - Electrical system Reserve Auxiliary Transformer (RAT) controller;
  - Normal heat sink controller;

- Condensate/Feedwater (FW)/drains/extraction controller, including extraction and level control;
- Water systems controller;
- Service air/containment inerting/floor drains controller; and
- Miscellaneous HVAC controller.

Segments in the BOP systems allow for operator control and monitoring from the MCR nonsafety-related VDUs.

7.1.4.8.4 Plant Computer Functions Description Summary

The PCF provide:

- Performance monitoring and control (PMC) functions, prediction calculations, visual display control, point log and alarm processing, surveillance test support, and automation;
- Core thermal power/flow calculations;
- The plant Alarm Management System (AMS) that alerts the operator to process deviations and equipment/instrument malfunctions;
- Fire Protection System (FPS) data through datalinks and gateways (if necessary);
- The Historian function, that stores data for later analysis and trending;
- Control of the main mimic on the MCR Wide Display Panel (WDP);
- Support functions for printers and the secure data communications to the TSC, EOF, ERDS, and potential links to the Simulator;
- Online procedures (OLP) to guide the operator during normal and abnormal operations, and to verify and record compliance;
- Transient recording;
- Nonsafety-related PAM displays;
- Report generators to allow the operator, technician, or engineer to create historical or real time reports for performance analysis and maintenance activities;
- The Plant Configuration Database (PCD) to document, manage, and configure components of the N-DCIS;
- Gateways to vendor-supplied nonsafety-related systems such as seismic, meteorological, and radiation monitoring; and
- Nonsafety-related process and area radiation monitoring.

PCF information display and control capability are provided by nonsafety-related VDUs in the MCR and RSS panels.

7.1.4.8.5 Nonsegment-Based Equipment

Equipment shared among segments are listed below:

- Nonsafety-related VDU/ Main Control Room Panel (MCRP) (the N-DCIS VDUs are connected to specific network segments to assure that the segment can be independently monitored and controlled should other segments fail; in the absence of such failures the VDUs are shared among the segments);
- Gateways;
- Datalinks; and
- Safety Parameter Display System (SPDS) logic.

7.1.5 N-DCIS Specifics

The N-DCIS data communication systems are embedded in the DCIS that performs the data communication functions that are part of and support the nonsafety-related systems described in Sections 7.2 through 7.8 and support the Q-DCIS to N-DCIS communications for the safety-related systems described in Sections 7.2 through 7.8. A simplified network functional diagram of the DCIS appears as Figure 7.1-1, and indicates the elements of the N-DCIS and the Q-DCIS.

The N-DCIS architecture, its relationships, and its acceptance criteria are further described in this subsection.

7.1.5.1 N-DCIS Design Bases

7.1.5.1.1 N-DCIS Safety-Related Design Bases

The N-DCIS does not perform or ensure any safety-related function. It is classified as a nonsafety-related system, and has no safety-related design basis.

7.1.5.1.2 N-DCIS Nonsafety-Related Design Bases

The N-DCIS is used as the primary control, monitoring, and data communication system for power production applications. The design bases for the N-DCIS include the requirements to:

- Segment the N-DCIS display and control of the two PIP Systems (A&B) and the BOP systems so they can operate independently of one other;
- Segment the major reactor control systems (FWCS, SB&PC System, TGCS and PAS) so they can operate independently of one another and from the DPS;
- Perform closed loop control and system logic independently of the MCR VDUs and Ethernet networks. Operability of the RSS panels, and their VDUs is independent of the operation or existence of the MCR displays;
- Ensure that no single failure of an N-DCIS component affects power generation;
- Provide a communication path for nonsafety-related data gathered and distributed throughout the plant, including datalink interfaces to control systems. The communication paths are redundant and include both the “native” control systems and “foreign”, vendor supplied or prepackaged control systems (condensate purification, offgas, radwaste, area radiation monitoring, and meteorological monitoring, for example);

- Reliably transfer to or from the plant areas, in digital format, analog or binary information that has been collected and digitized from nonsafety-related RMUs. The signals to the RMUs include transmitters, contact closures and other sensors or process activation signals, generated elsewhere for the control of remote devices such as pumps, valves or solenoids;
- Receive selected safety-related signals from the Q-DCIS through qualified safety-related isolation devices and datalinks to gateway devices or workstations and then transmit the signals to nonsafety-related VDUs and other nonsafety-related systems for control, monitoring and alarming purposes;
- Replace a majority of conventional, long-length, copper-conductor cables that connect components of the nonsafety-related plant I&C systems with fiber optic cable data networks to reduce cost and complexity;
- Provide an electrically noise-free transmission path for plant sensor data and control signals;
- Collect and archive data for transient analysis and data trending, sequence of events recording, display of SPDS and RG 1.97 information in the MCR, processing, and annunciation of alarm conditions to plant operational staff;
- Perform various PCF including PMC by providing Nuclear Steam Supply System (NSSS) performance and prediction calculations, visual display control, point log and alarm processing, surveillance test support, automation and the BOP performance calculations;
- Provide a permanent record and historical perspective for plant operating activities and abnormal events;
- Provide a secure communications interface with external computer and monitoring systems (one-way communication, no control capabilities). This includes the Plant Simulator (for training and for development and analysis of operational techniques), TSC, EOF, and the ERDS;
- Provide key-locked control equipment cabinet doors including door position switches. Electronic protection of control systems including password protection is provided in accordance with the LTRs, "ESBWR Cyber Security Program Plan," NEDO-33295, (Non- Proprietary); and "ESBWR Cyber Security Program Plan," NEDE-33295P, (Proprietary), (Reference 7.1-8);
- Provide reactor core performance information;
- Provide a SPDS of critical plant operating parameters. The parameters include reactor power, RPV water level, temperatures, pressures, flows, and the status of pumps and valves. The SPDS allows the MCR operators to follow the plant emergency operating procedures (EOPs) to shut down the reactor, maintain adequate core cooling, cool down the reactor to cold shutdown conditions and maintain containment integrity as required by 10 CFR 50.34(f)(2)(iv) TMI Action Item I.D.2. Specific SPDS displays are available in the MCR and SPDS parameters are available on the main plant mimic on the MCR WDP;

- Provide the MCR overview displays, navigational/top level displays, and system level displays;
- Provide TSC and EOF displays;
- Provide an AMS designed to alert the operator to an alarm condition, informing the operator of its priority, guiding the operator's response, and confirming whether the response was effective;
- Display normal, abnormal and EOPs on operator workstations and other workstations where display of operating procedures is permitted;
- Warn the operator to document that a Technical Specification limit, such as a limiting condition of operation (LCO), is being approached or violated when such conditions are detectable;
- Provide a 3D MONICORE system interface with the operator and with other systems;
- Provide time tagging of all measured points to facilitate transient recording and analysis (TRA), sequence of events recording, and first out determination;
- Provide real-time core thermal power and flow calculations from critical to 100% of rated power;
- Provide on-line diagnostics and monitoring of plant individual thermal heat cycle components, normalized to current plant conditions;
- Provide hard copy reports of current and historical plant operating data with pre-defined and custom formats to suit the needs of operations, maintenance, and engineering;
- Provide overall configuration management functions for the N-DCIS PCD;
- Provide manual and automatic DPS Selected Control Rod Run-in (SCRRI) initiation and Select Rod Insert (SRI);
- Provide the alternate rod insertion initiation (ARI) signal;
- Initiate Fine Motion Control Rod Drive (FMCRD) and Emergency Rod Insertion (ERI) condition signals;
- Acquire process measurement and equipment status signals from the process sensors and discrete monitors of the plant's nonsafety-related systems;
- Perform signal conditioning and A/D conversion for continuous process (analog) signals and perform signal conditioning and change-of-state detection for discrete signals;
- Provide data message formatting and data transmission from remote locations in the plant to the MCR through fiber optic cable and hardwired network connections;
- Receive command and control signals from the redundant controllers in the MCR area, and transmit the signals from the MCR area to remote locations in the plant where the N-DCIS distributes the signals to the final actuating devices;
- Provide datalink interfaces to all control and logic processing equipment supplied by parties other than the primary N-DCIS equipment supplier;

- Provide data support functions through a secure communications interface with the TSC, EOF, and the ERDS; and
- Provide operator aids from the PCF, such as safety parameter displays, transient data recording, analysis, archiving, alarm processing, and sequence of events processing.

7.1.5.1.3 N-DCIS Setpoint Methodology

To select I&C and to determine setpoints the design considers instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability. Adequate margin between limits and instrument setpoints is provided to allow for instrument error. The amount of instrument error is determined by test and experience. The setpoint is selected based on a known error; most of this error is in the transducer to the measurement channel and A/D converters of the RMU. The remaining equipment is microprocessor based with discrete setpoints that do not drift. The recommended test frequency is greater for instrumentation that demonstrates a stronger tendency to drift.

Ideally, the actual settings are determined by operating experience. However, in cases where operating experience is not available, settings are determined by conservative analysis. The settings are far enough from the values expected in normal operation to preclude inadvertent initiation of certain actions and far enough from the analyzed values to ensure that appropriate margins are maintained between the actual settings and analyzed values. The margin between the limiting system settings and the actual limits includes consideration of the maximum credible transient in the process being measured.

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

7.1.5.2 N-DCIS Description

The N-DCIS is segmented into parts that can work independently of one another if failures occur. The segments are not visible to the operator during normal operation. The N-DCIS uses hardware and software platforms that are diverse from the Q-DCIS. The N-DCIS network is dual redundant and at least redundantly powered so no single failure of an active component can affect power generation.

The individual N-DCIS segments are the:

- GENE network,
- PIP A network,
- PIP B network,
- BOP network, and
- PCF network.

Managed network switches are redundant per segment and provide monitoring and control of the N-DCIS networks while transmitting, data, alarms, recording and display information, and operator control information between segments and components. Managed network switches monitor and transmit data acquisition and control messages and displays associated with that segment. Each managed network switch has the capability to monitor and control unexpected and excessive traffic on its respective N-DCIS network segment. Each network switch can have up to several hundred "nodes" and several "uplink" ports that are connected to the other switches; all connections to these switches are through the fiber optic cable network. Fiber optic cables used for nonsafety-related applications are sheathed in material meeting IEEE Std. 383 that addresses fire propagation mitigation.

The switches allow the various controllers, data acquisition and displays associated with a segment to communicate with each other by almost instantaneous virtual connections that end when the communication is finished. The switches' "backbone" capacity determines how many simultaneous two-way connections can be made, but the capability is much higher than actually required.

These managed switches have security features that include identification of legal addresses, the capability to ignore or not uplink (to other segments) unexpected connections or their traffic, and the capability to alarm network traffic. Only when a switch determines that an information data packet is destined for a node on another switch is the information put on an uplink to another switch. The network switches learn and maintain their own forwarding tables containing a list of all the nodes and hosts on their respective network segment. When a network switch receives a data communication packet, it forwards only that particular data packet to the segment to which that receiving host is connected. This mechanism prevents data traffic between devices on the network from affecting devices on other segments of the network.

The uplink ports on the switches are connected together radially and in a ring because multiple interconnections increase reliability. Specifically the switches use a "spanning tree protocol" to automatically enable and disable ports so there is one path from the nodes of one switch to another. Should a path become disabled, the switches automatically reconfigure to establish another path through the remaining switches and fiber optic cable paths. Reconfiguration requires no operator input and is usually accomplished in seconds.

Each switch "node" (workstation, display, and controller) is connected to redundant switches of the segment. These connections support normal plant operation. The switches have mean times between failure (MTBF) of greater than 100,000 hours. Each switch has redundant power feeds and can work from either power source. The switches and connected controllers support extensive component and data self-diagnostics, and failures are alarmed.

The above text and Figure 7.1-1 show that the N-DCIS is not a single network. It is redundant and segmented to support the DCIS with very high reliability. A single failure of one of the redundant switches in a segment or multiple failures that involve no more than one switch per segment has no effect on plant operation or data. The failure is alarmed and can be repaired online. In the highly unlikely event of both switches of a segment simultaneously failing, that particular segment is lost. However, the remaining segments are unaffected and individual nodes connected to the failed switches can continue to function. The remaining switches then automatically reconfigure their uplink ports such that the remaining segments automatically find available data paths between each other.

The major N-DCIS functions are segmented as defined in Subsection 7.1.4.8.

7.1.5.2.1 Nonsafety-Related Shutdown Systems

Descriptions of nonsafety-related shutdown systems follow.

7.1.5.2.1.1 Remote Shutdown System

Each RSS panel has the ability to operate all of the nonsafety-related PIP equipment and the BOP equipment, either automatically or manually. Refer to Subsection 7.4.2 for additional information.

7.1.5.2.1.2 Reactor Water Cleanup/Shutdown Cooling System

The nonsafety-related RWCU/SDC system maintains reactor water purity during operation. It also provides normal shutdown cooling by taking suction from the RPV, pumping the flow through heat exchangers, and returning the cooled water to the vessel through the feedwater line. The system is segmented and allows the train A and B components to operate independently. Refer to Subsection 7.4.3 for additional information.

7.1.5.2.1.3 Fuel and Auxiliary Pools Cooling System

The nonsafety-related FAPCS maintains the fuel pool, spent fuel pool, suppression pool, auxiliary pools, and GDCS pools, by pumping pool water through heat exchangers and a water treatment unit (equipped with pre-filters and demineralizers) into two 100% cooling and cleaning trains. It also maintains suppression pool temperatures and cleanliness during operation. The FAPCS can also initiate a low pressure coolant injection (LPCI) mode following an accident and after the reactor has been depressurized to provide reactor makeup water for accident recovery. In this mode the FAPCS pump takes suction from the suppression pool and pumps it into the RPV through RWCU/SDC Loop B and Feedwater Loop A. The system is segmented and allows train A and B components to operate independently. Refer to Subsection 9.1.3 for additional information.

7.1.5.2.1.4 Control Rod Drive System

The nonsafety-related CRD system maintains the hydraulic control unit (HCU) accumulators at the pressure required to assure a successful scram, provides cooling water flow to the FMCRDs and to provide various high-pressure purge flows. The CRD system also provides a HP CRD injection mode capable of supplying inventory to the RPV at elevated pressures. While HP CRD injection is isolated upon a low level indication from the GDCS pools or drywell high pressure coincident with drywell high level, the isolation is bypassed by a failure of the GDCS to successfully inject (a scenario which is beyond design basis). The system is segmented and allows Train A and B components to operate independently. Refer to Section 4.6 as well as Subsections 7.1.2.8.8, 7.3.3, and 7.4.5 for additional information.

7.1.5.2.2 Nonsafety-Related Information Systems

Nonsafety-related information is provided by PRMS and ARMS.

7.1.5.2.2.1 Process Radiation Monitoring System

Nonsafety-related PRMS instrumentation monitors the main steam lines, the drywell, ventilation and stack discharges and liquid and gaseous effluent streams that might contain radioactive materials. The safety-related PRMS is discussed in Subsection 7.1.3.2.4.3. MCR display, recording, and alarm capabilities are provided along with controls that provide automatic trip inputs to the respective systems to prevent further radiation release. Refer to Subsection 11.5.3 for additional information.

7.1.5.2.2.2 Area Radiation Monitoring System

Nonsafety-related ARMS instrumentation continuously monitors the gamma radiation levels within designated areas of the plant. It provides early warning to operating personnel when predetermined dose rates are exceeded. Refer to Subsection 7.5.4 for additional information.

7.1.5.2.3 Control Systems

Descriptions of nonsafety-related control systems follow.

7.1.5.2.3.1 Nuclear Boiler System Instrumentation

Nonsafety-related NBS instrumentation provides indication of reactor coolant and vessel temperatures, RPV water level, and RPV pressure. Refer to Subsection 7.7.1 for additional information.

7.1.5.2.3.2 Rod Control and Information System

The nonsafety-related RC&IS is able to control reactor power level by controlling the movement of the control rods in the reactor core during manual, semi-automated, and automated modes of plant operations. The ATLM automatically enforces fuel operating thermal limits minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR) when reactor power is above the ATLM enable setpoint. Refer to Subsection 7.7.2 for additional information.

7.1.5.2.3.3 Feedwater Control System

The nonsafety-related FWCS has two sets of highly reliable and triple redundant controllers. The feedwater level controller automatically and manually regulates the flow of feedwater into the RPV. It maintains a predetermined water level for all modes of reactor operation, including heatup and cooldown. The feedwater temperature controller allows reactor power maneuvering without moving control rods. Refer to Subsection 7.7.3 for additional information.

7.1.5.2.3.4 Plant Automation System

The nonsafety-related PAS:

- Provides automatic startup/shutdown algorithms and controls;
- Regulates reactivity during criticality control;
- Provides heat up and pressurization control;
- Regulates reactor power; and
- Provides automatic power generation control during power operation. Refer to Subsection 7.7.4 for additional information.

The PAS is the plant-wide automation scheme implemented by the N-DCIS. The PAS coordinates the action of multiple systems using system-level controllers (with the capability to perform system-level automation) to automate the operation, maintenance, testing, and inspection functions. It uses automated program functions (APF) to coordinate the automatic power regulator (APR) and the power generation control system (PGCS).

The PAS provides the capability for supervisory control of the entire plant by supplying setpoint commands to independent nonsafety-related automatic control systems as changing load demands and plant conditions dictate. Safety-related systems are never controlled or tasked by the PAS. The automation system covers the tasks involved in criticality, heat-up and pressurization, turbine roll and synchronization, and plant power control.

The APR and PGCS automatically run the plant, with operator supervision from cold non-critical conditions to 100% rated temperature, pressure, and power and back to cold non-critical conditions.

The PAS establishes several broad automation sequences:

- Pre-startup check,
- Approach to criticality and reactor pressurization,
- Turbine-generator startup, increase to rated speed and synchronization,
- Power operations (increase turbine load to rated power), and
- One button shut down.

Prior to initiating any automation sequence including the turbine-generator startup, increase to rated speed and synchronization, prerequisite and continually operating equipment must be in a satisfactory pre-defined condition. There is a complete list of prerequisite conditions for each system. Some plant systems are never shut down, even during refueling outages and their operating conditions are independent of plant power.

7.1.5.2.3.5 Turbine Generator Control System

Functions of the TGCS include:

- Turbine speed/acceleration control (including ability to navigate 100% load rejection/ turbine island mode);
- Turbine over-speed protection;
- Turbine control interface with SB&PC System;
- Turbine load control;
- Turbine valve testing;
- Interfacing with the condensate/feedwater system;
- Related surveillance tests, checks, and inspections;
- Automatic response to alarm conditions, system faults, and plant transients;
- Related generator control functions; and
- Related turbine generator (TG) auxiliary support control functions.

7.1.5.2.3.6 Steam Bypass and Pressure Control System

A highly reliable and triple redundant nonsafety-related SB&PC System controls reactor pressure during plant startup, power generation, and the shutdown modes of operation. This is accomplished through control of the turbine control valves (TCV) and/or turbine bypass valves (TBV) so susceptibility to reactor trip, turbine generator trip, main steam isolation and safety relief valve opening is minimized. Refer to Subsection 7.7.5 for additional information.

7.1.5.2.3.7 Neutron Monitoring System - Nonsafety-related Systems

The nonsafety-related AFIP provides a signal proportional to the axial thermal neutron flux distribution at the radial core locations of the LPRM detectors. The signal facilitates fully automated, precise, reliable calculation of the LPRM gains. The signal also provides axial power measurement data for three dimensional core power distribution determinations. The nonsafety-related MRBM logic issues a control rod block demand to the RC&IS logic to prevent fuel damage. It assures that the MCPR and MLHGR do not violate fuel thermal limits. Refer to Subsection 7.7.6 for additional information.

7.1.5.2.3.8 Containment Inerting System

The nonsafety-related Containment Inerting System (CIS) establishes and maintains an inert atmosphere within containment. It operates during all plant operating modes, except during plant shutdown for refueling and/or equipment maintenance and during limited periods of time to permit access for inspection at low reactor power. Refer to Subsection 6.2.5.2 for additional information.

7.1.5.2.3.9 Diverse Instrumentation and Control Systems

Diverse I&C is provided to address BTP HICB-19 on defense-in-depth and diversity in digital computer-based I&C systems. This is in addition to the ATWS mitigation features, which provide alternate control rod insertion, boron injection, and feedwater runback. The nonsafety-related diverse I&C functions are implemented in the DPS. The DPS functions are implemented in a highly reliable triple redundant control system whose sensors, hardware and software are diverse from their counterparts on any of the safety-related I&C platforms.

The following diverse actuation functions are provided by the DPS:

- A set of protection logics that provide a diverse means to scram the reactor via control rod insertion using sensors, hardware and software that are separate from and independent of the primary RPS.
- A set of initiation logics that provide a diverse means to initiate certain ESF functions using sensors, hardware and software that are separate from and independent of the primary ESF systems.
- A set of redundant ARI signals that initiate associated logics (such as the FMCRD Run-in) and insertion of control rods through an alternate means by opening the three sets of ARI valves of the CRD system.

The DPS provides both manual and automatic initiation of the above functions. Refer to Subsection 7.8.1 for additional information.

7.1.5.2.3.10 Selected Control Rod Run-In / Select Rod Insert

The DPS processes the signals described by Subsection 7.8.1.1 to develop the automatic SRI and SCRRI command signals. The SRI and SCRRI can also be initiated manually from the MCR. The redundant N-DCIS SCRRI command signals are sent to the RC&IS in which each of the dual rod action and position information (RAPI) channels performs a two-out-of-three vote and initiates RAPI channel logic associated with accomplishing the SCRRI function. When activated, the SCRRI function inserts control rods using the FMCRD motors to pre-defined positions to reduce reactor thermal power to a target power level. This logic is implemented in a highly reliable redundant control system. The SCRRI command signal is also used in the ERI control logic of the N-DCIS, as discussed in Subsection 7.1.5.2.3.12.

The redundant SRI command signals are sent to the nonsafety-related scram timing test panel. This panel is electrically isolated from the divisional panels that contain the switches in the 120 VAC return from each HCU scram solenoid. When commanded to open (using two-out-of-three voting logic) for either a full DPS scram, a single HCU scram timing test or for predefined rod groups (SRI) the affected HCUs scram their associated control rods. Because the scram timing switches are in the HCU scram solenoid 120 VAC return, the RPS load drivers are in the solenoid 120 VAC supply, and the switches and solenoids are in a "series" circuit, there is no credible failure of the scram timing panel that can prevent or affect an RPS scram.

7.1.5.2.3.11 Alternate Rod Insertion

The N-DCIS performs two-out-of-three voting of the redundant ARI signals from the DPS to become the N-DCIS ARI initiation signal. Each of the RC&IS dual RAPI channels performs two-out-of-three voting of the redundant ARI initiation signals and initiates the RAPI channel logic associated with accomplishing the FMCRD Run-in logic.

When activated, ARI hydraulically inserts all operable control rods by depressurizing the scram air header to open the HCU scram valves. This logic is implemented in a highly reliable redundant control system.

As a backup means for the hydraulic scram function of the CRD system, the ARI command signal is also used in the ERI logic of the N-DCIS to insert all operable control rods to the full-in position using the FMCRD motors, as discussed in Subsection 7.1.5.2.3.12.

7.1.5.2.3.12 Emergency Rod Insertion

The N-DCIS combines the SCRRI/SRI command signal and ARI command signal by an "OR" function to become an FMCRD emergency insertion signal. Redundant FMCRD emergency insertion signals are sent to the ERI Control Panels (ERICPs) of the RC&IS for two-out-of-three voting. Associated emergency insertion condition signals in the ERICPs provide inputs to the induction motor controllers of the RC&IS.

For the SCRRI or ARI and FMCRD Run-in logic of the RC&IS equipment to be initiated, the ERI signals to the induction motor controllers must be concurrent with the RAPI logic SCRRI/SRI command related signal or ARI related command signals to the induction motor controllers. This logic is implemented in a highly reliable redundant control system.

7.1.5.2.4 Plant Computer Functions

All PCF are an integral part of the HFE process (Refer to Chapter 18). The allocation of functions accommodates human capabilities and limitations, fault detection and recovery capabilities are provided, and an acceptable operator workload is not exceeded. Additionally, PCF (like the plant controllers) are powered with UPS so that they are available to the operator for as long as the N-DCIS is powered.

The PCF increase the efficiency of plant performance by:

- Performing the functions and calculations necessary for the effective evaluation of nuclear power plant operation;
- Providing a permanent record and historical perspective for plant operating activities and abnormal events;
- Providing analysis, evaluation and recommendation capabilities for startup, normal operation, and plant shutdown;
- Providing the capability to monitor plant performance through presentation of video displays in the MCR and elsewhere throughout the plant and providing the ability to directly control certain nonsafety-related plant equipment through on-screen technology;
- Providing secure data communication with all external computer and monitoring systems (for example, one-way communication, no control capabilities) including the TSC, EOF, and ERDS; and
- Performing core thermal power and core coolant flow rate calculations from reactor heat balances. Iterative computational methods are used to establish a compatible relationship between the core coolant flow rate and core power distribution. The results are subsequently interpreted in the NSSS performance module as power in specified axial segments for each fuel bundle in the core.

The calculations performed by the N-DCIS include process validation and conversion, combination of points, NSSS performance calculations, and the BOP performance calculations.

The Performance Monitoring and Control Subsystem (PMCS) provides the NSSS performance and prediction calculations, visual display control, point log and alarm processing and BOP performance calculations.

7.1.5.2.4.1 Safety Parameter Display System

The SPDS provides critical plant operating parameters such as reactor power, RPV water level, temperatures, pressures, flows, and status of pumps and valves. The SPDS system allows the MCR operators to follow plant EOPs to shut down the reactor, maintain adequate core cooling, cool down the reactor to cold shutdown conditions and maintain containment integrity as required by 10 CFR 50.34(f)(2)(iv) TMI Action Item I.D.2. Specific SPDS parameters are available in the MCR and on the WDP plant mimic.

7.1.5.2.4.2 MCR Displays

The MCR panel equipment is part of the MCR Panels (MCRP) System. Information for the displays is presented with the following functional configuration arrangement:

- Level 0 is the integrated overview display.
- Level 1 is the navigational/top level display.
- Level 2 is the system level display.
- The integrated overview display (sometimes called the main plant mimic) is provided on the WDP.

- The fixed-position portion of the large display panel provides critical plant operating information, such as reactor power, RPV water level, temperatures, pressures, flows, status of major equipment, and availability of safety-related systems. There is a mimic in the MCR during plant normal, abnormal and emergency operating conditions. The dynamic display elements of the fixed-position displays are driven by dedicated microprocessor-based controllers that are independent of the N-DCIS.
- The large variable display portion of the WDP can indicate any display format available on a nonsafety-related VDU; the plant operator initiates the chosen format.
- Appropriately isolated safety-related information is available for display on the nonsafety-related integrated overview display and various nonsafety-related VDUs.
- The PCF provide navigational or top level displays which include:
  - Main menu;
  - Safety parameters;
  - PAM (RG 1.97) variables;
  - PGCS parameters;
  - Power generation control;
  - OLP;
  - Technical specification monitor/RPS monitor;
  - 3D MONICORE;
  - Historian function;
  - TRA;
  - Thermal performance monitor and diagnostic (TPM&D);
  - Report generator;
  - Bypass and inoperable status indication (BISI); and
  - System level displays (P&IDs, alarms).

The PCF control displays provide direct control and parameter monitoring of nonsafety-related equipment and systems through the use of the VDUs and various input devices, which are part of the MCR panels.

The RC&IS dedicated operator interface provides control and monitoring of the RC&IS and is described in Subsection 7.7.2.

7.1.5.2.4.3 Alarm Management System

The plant AMS is accessible via the MCR VDUs and RSS VDUs, and indirectly at the TSC and EOF.

The plant AMS is designed to alert the operator to a deviation from normal conditions. It informs the operator of the deviation's priority, guides the operator's response, and confirms whether or not the response was effective.

To fulfill these basic functions, the system must:

- Detect and, in some cases, predict the occurrence of changes in the plant; and
- Alert users to changes significant to the current operating situation, such that:
  - Only operationally relevant changes are alarmed,
  - The demands imposed on users' attention to recognize the changes are aggregated and considered with the demands of other concurrent control room tasks, and
  - Operators are alerted to additional plant information needed to understand and respond to changes.

To accomplish the above, the AMS design bases are to:

- Alert the operators to off-normal conditions which require them to take action;
- Reduce the number of alarms to be consistent with the total operator workload;
- Guide the operators to the appropriate response (linking alarms to alarm response procedures);
- Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions;
- Minimize distraction and unnecessary workload placed on the operators by the alarm system – especially during transient and accident conditions;
- Satisfy the dark panel concept: no alarm signal is shown to the operator under normal operating conditions;
- Determine system level alarms based on function and task analysis;
- Include the means to provide the operator with information in different views including sorting, filtering, and grouping of alarms;
- Generate basic alarms and high-level, composite, alarms. The generated alarms are subject to potential filtering, alarm suppression, and alarm prioritization techniques. The plant Historian maintains an alarm log whether or not alarms are presented to the operator. Alarms are then presented in the MCR either audibly (annunciator), visually (display), or both;
- Create temporary operator-defined alarms and associated alarm setpoints; and
- Integrate with other information systems, such as the OLP and TSM, to facilitate operator tasks; the AMS and TSM provide the suggested operator response to the various alarm and monitoring function events.

7.1.5.2.4.4 On Line Procedures

OLP provide for:

- Display of normal, abnormal, and emergency operating procedures on operator and other workstations;
- Display of operating procedures in logic, flowchart, and text formats;

- Hardcopy output of operating procedures from all workstation locations with the displayed format and content, considering potential alternative uses for study guides, and procedure maintenance;
- Maintenance (that is, addition, deletion, and modification) of operating procedures;
- Manual, semi-automated (selected procedures), or fully automated (selected procedures) implementation of operating procedures from the operator workstations;
- Access to controls from the displayed operating procedures;
- Continuous update of the display of parameters, to include embedded dynamic indication status (normal, warning, and alarm conditions), necessary for the plant operator to monitor and/or perform operating procedure steps;
- Confirmation of operator decisions and actions while retaining the operator as the final authority in the execution of procedures;
- Logs of the discrepancies between operator action and procedure execution options;
- Logs of the execution of sequences of steps (selected procedure sequences), not including actions taken by the operator to control components, to ensure that the proper status of components or systems is maintained (this might require manual operator input of steps that cannot be monitored by the N-DCIS); and
- Validation of each operating procedure using the plant Simulator.

7.1.5.2.4.5 Technical Specification Monitor

The TSM, when conditions are detectable, does the following:

- Monitors, displays and alarms all three safety-related platforms;
- Warns the operator when a technical specification limit, LCO, is being approached;
- Warns the operator when the LCOs are being violated;
- Determines the approach to an LCO based on equipment status information, core limits and margins and other data;
- Indicates appropriate action(s) to avoid violating the LCOs;
- Acquires and processes available information to determine the approach to and existence of an LCO;
- Automatically acquires required information;
- Determines, given available information, any automatic testing that could affect the LCOs;
- Indicates the action needed to recover from an LCO;
- Provides a log of LCO violations;
- Acquires or calculates as necessary, reactor and core parameters required for monitoring LCOs, such as thermal limit margins, power distribution, and heat generation rates;
- Shows the results of calculations of reactor and core parameters on operator displays;

- Provides manual input capability for LCOs that cannot be monitored automatically by the technical specification monitoring function;
- Sends alarms to the AMS, which provides for an acknowledgment function for alarm conditions;
- Shows the operator the availability status of the RPS and safety-related systems based on information from those systems' continuous self diagnostic checks;
- Provides RPS and safety-related System Monitoring (RPSM) as a sub-function;
- Monitors, through RPSM, support services (for example, voltages, cooling water, oil pressure and levels) that can affect the availability of the RPS and other safety-related systems;
- Monitors, through RPSM, the availability of the initiating equipment (sensors and control systems) and the implementing equipment (for example, pumps, and valves);
- Monitors, through RPSM, the availability of primary and backup sources of services;
- Monitors, through RPSM, process parameters (reactor pressure, water storage tank levels, and environmental conditions) that can affect the successful operation of the RPS or other safety-related systems; and
- Provides manual and automatic entry, through the RPSM, of the maintenance, calibration, and test data needed to establish RPS and other safety-related system operability.

7.1.5.2.4.6 Report Generator

The Report Generator is a report definition and execution utility program that allows the user to create reports within the PCF. It produces required custom output reports in the MCR and indirectly to the TSC, and EOF.

The data sources for the Report Generator include any measured or calculated data stored either in the Historian or in a real-time database (measured and calculated points) that enables the report program to locate and retrieve data for pre-configured reports used by operators, engineers and maintenance personnel.

The Report Generator can process algorithms to support plant-wide equipment logs and reports.

7.1.5.2.4.7 Plant Configuration Database

The PCD provides overall configuration and management functions for the N-DCIS at a PCF engineering workstation.

7.1.5.2.4.8 3D MONICORE

3D MONICORE provides core performance information. It has two major components, the Monitor and the Predictor. Both components use a three-dimensional core model code as the main calculation engine. 3D MONICORE provides the logic in the input preparation file that interfaces with the core model code that calculates the key reactor state information such as axial and radial power, moderator void and core flow distributions. From these calculations, other parameters such as the magnitude and location of minimum margin to thermal limits (such as

MCPR, peak fuel rod linear powers and average planar heat generation rates), fuel exposure and operating envelope data can be determined.

The 3D MONICORE Monitor periodically tracks current reactor parameters automatically with live plant data. Typically, the tracking interval is once per hour. Additionally, the 3D MONICORE system can be updated automatically by the PAS or ATLMs, or manually by the operator.

The 3D MONICORE Predictor runs upon user request with live data overlaid with user input. It predicts core parameters for reactor states either in steady or operational transient states other than the present one. This allows the user to study the effects of different rod patterns, core flows and fuel burnups before performing reactor maneuvers to support plant operation.

For accuracy improvement, 3D MONICORE has several adaptation modes, which use in-core neutron flux measurements and AFIP data to calculate nodal fit coefficients that can be input to later Monitor and Predictor cases. The choice of mode depends on the method used to adapt the results of the core model code to in-core detector measurements.

The 3D MONICORE function automatically provides data to other systems including the ATLM and RC&IS. The 3D MONICORE function provides APRM/LPRM calibration data to the PRNM, but only when the equipment is under specific rigorous administrative and manual control (for further information see the "Communications from N-DCIS to Q-DCIS [DCIS Time tagging and NMS calibration]" portion of Subsection 7.1.3.3). The data needed by these systems are detailed in their respective system specifications.

7.1.5.2.4.9 Historian

The Historian is the repository for all measured and calculated point data for the plant. It receives input from sources of point data, stores this data and presents it to the report generator, the display driver, and other applications needing historical point data. The Historian:

- Stores point data, plant operating activities, and abnormal event sequences, along with their time tags, for retrieval and analysis;
- Stores third-party generated data, such as 3D MONICORE data, in a format compatible with the display and report system;
- Stores values of RG 1.97 variables for current trending or later analysis; and
- Provides on-line data storage capability dependent on plant history and events that is nominally for one fuel cycle. The system warns the system operator about remaining disk storage space, giving the operator time for download to an off-line archiving device. The preferred archiving device uses optical disks.

7.1.5.2.4.10 Transient Recording and Analysis and Sequence of Events Recording

The N-DCIS clock provides the capability to time tag all cabinets' data on the N-DCIS, including Q-DCIS data sent to the N-DCIS (through properly isolated nonsafety-related gateways) at the millisecond level for TRA and the sequence of events recording. Time tagging is accomplished as closely as possible to the origin of the data. The required resolution of time tagging is based on the speed of the monitored process variable, the origin of the data (N-DCIS or Q-DCIS), and the available technology.

The capability of first-out determination and event analysis is provided by the combination of TRA, sequence of events (SOE), and the Historian.

Time tagging utilizes a pair of redundant, nonsafety-related, GPS-synchronized clocks to synchronize all stored data. These clocks (the N-DCIS clocks) provide the network time to all N-DCIS components.

The TRA utilities are largely reports of current point and historical point data. The TRA utilities can be used to analyze plant events and to support plant startup tests.

Some analysis functions are triggered by plant events and others are performed periodically based on the wall clock (for example hourly, shift, daily logs and reports).

7.1.5.2.4.11 Core Thermal Power and Core Flow Calculation

Real-time core thermal power from critical to 100% of rated power is calculated almost continuously. The calculation is supported by multiple, validated parameter measurements and eliminates "constants," previously used for some heat balance inputs, so bias in the calculation is eliminated. At low thermal power levels, the low flow control valve (LFCV) feedwater flow measurement increases accuracy. The core flow is calculated by the heat balance core flow methodology using the core inlet temperature measurement as input to determine core inlet enthalpy.

7.1.5.2.4.12 Thermal Performance Monitor and Diagnostic

The TPM&D provides an on-line diagnostic and monitoring program for the thermal heat cycle. It calculates the deviations of the calculated performance of individual system components from the actual measured performance when the plant is above some threshold power. The trends of the performance data can be used by utility personnel to identify components contributing to thermal efficiency loss.

The TPM&D is a plant model that is normalized to current plant conditions such as reactor power, core flow, reactor pressure and circulating water temperature. The output of the model is a detailed calculation (for example, flows, enthalpies, pressures, and temperatures) of the plant individual heat cycle components with predicted (design basis) and actual performance parameters under that condition. These actual and predicted parameters are compared, and their differences are used to calculate a figure of merit. An example is an equivalent system parameter such as normalized heat exchanger cleanliness.

7.1.5.2.5 N-DCIS Hardware

The flow of data in the N-DCIS is similar to that in the Q-DCIS. Data are acquired in the nonsafety-related RMUs, sent to nonsafety-related controllers, and then to workstations and displays for monitoring, alarming and recording purposes. The N-DCIS has the following major equipment.

- RMUs located throughout plant buildings such as the RB, CB, FB, Circulating Water System (CIRC) pump house, switchyard, Electric Building, Turbine Building, and Radwaste Building. The N-DCIS RMUs acquire and output the same signal types as the Q-DCIS RMUs but are nonsafety-related. The RMUs are connected directly to the controller cabinets appropriate to the segment and located in the Back Panel areas of the CB. The links are always by redundant fiber optic cable.

- Control processor cabinets housing the dual/triple redundant control processors, which process the control logic of nonsafety-related NSSS and most BOP systems. The control processor cabinets receive plant process data multiplexed at the RMUs and transmitted to the control processor. The control processor cabinets then transmit the resulting data to the RMUs where their output signals are used for control of nonsafety-related actuators. The control processor cabinets also provide data to the MCR VDUs for operator interface displays or plant-level applications. Note that closed loop control takes place within a network segment and within a controller cabinet and its connected RMUs such that this control is not dependent on signals routed from another network switch segment nor dependent on the operation of the N-DCIS networks.
- Network switch cabinets containing the redundant, managed switches for Ethernet switching and providing segmentation, and connection between the N-DCIS components connected to the redundant high-speed fiber optic cable networks.
- Workstation cabinets, depending on the application, supporting redundant or single workstations that, in turn support the VDUs. The workstations are used for dedicated logic functions where the use of a control processor is not appropriate, such as for the Historian, core thermal power or alarm management.
- The N-DCIS datalinks and gateways (when necessary) providing the N-DCIS communication with the Q-DCIS, vendor-supplied controllers, the secure communication with the TSC/EOF/ERDS, and other nonsafety-related packaged systems such as area radiation monitoring.
- Cabinets housing vendor-supplied control or monitoring systems such as seismic monitoring, area radiation monitoring, and integrated leak rate testing.
- Gateway cabinets that collect selected safety-related signals through isolated divisional interfaces for archiving and for nonsafety-related control and monitoring purposes. These gateways or workstations are always interconnected by fiber optic cable to support the electrical isolation requirements between the Q-DCIS and the N-DCIS components. The nonsafety-related (N-DCIS) systems have no control-related inputs to the safety-related (Q-DCIS) systems. For further details on gateways, their communication, and transmission of time tagging signals see Subsection 7.1.3.3.
- The MCR consoles and its MCR monitoring and control equipment that is the main operator interface with the various plant processes. Examples are flat panels with soft controls, or hard controls, page/party phone, meters, silence/acknowledge, recorders, main generator synchronizing inset, PAX phone, radio handsets, keyboards/trackballs.
- The display panels' components and functions that include alarm display, mimic, flat panel displays, Closed Circuit Television (CCTV) monitors, large variable display, and the components' associated computer processors.
- Signal isolators for RMU internal buses and the redundant fiber optic cable links in the field.
- I/O modules providing interfaces between process sensors/actuators.
- Fiber optic modems and media converters transmitting and receiving data through the redundant fiber optic cable links in the field to the redundant control processors.

- Computer peripherals, such as printers and plotters, providing output data capabilities.

7.1.5.2.6 N-DCIS Functions

The N-DCIS is not required to be operable during or after any DBE. The N-DCIS provides distribution and controls data communication networks that support the monitoring and control of interfacing nonsafety-related plant I&C systems. The N-DCIS also processes data from safety-related systems that are originally acquired by the Q-DCIS. Such data are always transmitted through qualified safety-related isolation devices via datalinks and fiber optic cable to provide the required isolation between the Q-DCIS and the N-DCIS.

Safety-related and nonsafety-related data, once acquired for any reason, are available for any other reason including monitoring, alarming, and recording. Data can be organized for displays and reports in any combination. This ability demonstrates that there are no “dedicated” data. For example, data for RG 1.97, SPDS, alarms, a specific system, or for the mimic are not dedicated. Data from all sources can be combined to form any coherent function.

N-DCIS controllers perform closed loop control and system automatic logic independently of operator inputs from the control room N-DCIS VDUs. RSS panels operate independently of the MCR displays.

The system includes electrical devices and circuitry such as RMUs, control processors, network switches, data communication paths, and interfaces. These connect field sensors, display devices, controllers, power supplies, and actuators, which are part of the nonsafety-related systems. The N-DCIS also includes any associated data acquisition and communications software, if required, that supports its data distribution and control function. The N-DCIS replaces most conventional, long-length, copper-conductor cables with a dual or triple redundant, fiber optic cable, data network. The fiber optic cable data network reduces the cost and complexity of cable runs and provides an electrically noise-free transmission path for plant sensor data and nonsafety-related control signals.

Triple redundant controllers and data acquisition systems are used for the DPS, FWC, SB&PC System, TGCS and PAS. As a minimum, dual redundant controllers and data acquisition are used for all power generation functions including non-control functions (such as 3D MONICORE) that support power generation and core thermal power and flow calculations. The nonsafety-related data from sensors are multiplexed at nonsafety-related RMUs and then transferred through the N-DCIS data network to components of the N-DCIS. Selected signals from the nonsafety-related instrumentation are transmitted to the N-DCIS input cabinets through dedicated hardwired connections as required for faster transmission rates of signals, such as SB&PC System to TGCS control. Similarly, output signals to actuators and controls that require faster transmission rates, such as manual turbine trip signals, also use dedicated hardwired connections. The RMUs and the data communication network for such nonsafety-related data processing and transmission are part of the N-DCIS.

Divisionally separated redundant isolated digital gateways provide one-way communications from safety-related systems to the N-DCIS. The electrical and data isolation functions are part of the Q-DCIS, and the gateway functions (data conversion and packaging) are part of the N-DCIS. The communications from nonsafety-related systems to the Q-DCIS are limited to communication from the 3D MONICORE function of the N-DCIS to the PRNM (LPRM and

APRM) function of the NMS and time tagging. For further detail on this communication and transmission of time tagging signals see Subsection 7.1.3.3.

The local N-DCIS RMUs perform signal conditioning and A/D signal conversion for continuous process signals. They also perform signal conditioning and change-of-state detection for discrete signals such as contact closures and openings. The RMU function performs both I/O signal-processing functions. The RMU formats the acquired signals into data messages and transmits the data through the data network to N-DCIS components for logic processing. The RMU with a system logic function receives logic commands, such as trip commands and control signals, from the data network N-DCIS logic processors. The RMU then provides terminal points for distributing the signals to the final actuating devices of the nonsafety-related systems.

Operator interfaces for control and display are realized through multiple, non-dedicated VDUs, each of which is connected to the segmented network switches.

The on-line diagnostic functions of the N-DCIS monitor transmission path quality and integrity. The dual redundant data communication paths are repairable on-line if one path fails. The N-DCIS failures are alarmed in the MCR. Periodic surveillance, using off-line tests with simulated input signals, verifies the overall system integrity.

The N-DCIS networks and components are distributed throughout the plant and are powered by redundant internal power supplies fed from two 120 VAC UPS. Some systems, such as the DPS, TGCS, FWCS, SB&PC System, and PAS, are triple redundant and are powered by three nonsafety-related UPS load groups.

7.1.5.3 N-DCIS Safety Evaluation

The N-DCIS is classified as nonsafety-related and is not required for safety-related purposes. Its operability is not required during or after any DBE. The N-DCIS is required to operate in the normal plant environment and is significant for power production applications. The N-DCIS does not perform any safety-related functions as a part of its design; however the N-DCIS does provide an isolated alternate path for safety-related data from Q-DCIS to N-DCIS that is presented in the MCR. The N-DCIS network that supports the dual/triple, fault-tolerant controllers of the process control systems uses a proven technique for high speed transfer of data different from Q-DCIS and thus provides diversity in design.

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. Specifically:

- RMUs are located throughout the plant and auxiliary buildings; and
- Computer equipment and peripherals are located mainly in the CB in the MCR and Back Panel areas. They are also located in other areas such as the EOF, Radwaste Building, TSC, Fuel Building, Fuel Building roof area, or alternate building designations specific to the plant design.

Most of the N-DCIS controller cabinets are located in two different rooms of the control building that are in separate fire areas. These rooms include the DPS equipment rooms and any of the Q-DCIS control building equipment rooms. The RMUs that support the N-DCIS controllers are located in most buildings of the power plant. Where the controllers support PIP A and PIP B systems, the controllers and RMUs are located in different fire areas. The DPS controllers are located in fire areas separate from the N-DCIS and Q-DCIS equipment rooms and the four DPS

RMUs are located in the reactor building. Two of the four RMUs are located in fire areas (quadrants) of the reactor building separate from the other two RMUs. The two RMUs of each pair are located in separate fire areas to separate the DPS RMUs that contain the series connected multiple load drivers used to operate solenoids and squib valves and will prevent inadvertent actuations affecting safe shutdown whether from hot shorts or fires in a single fire area. Finally, the input signals/sensors that provide DPS backup scram, isolation and ECCS functions, and the DPS squib/solenoid valve outputs are arranged such that half of the inputs/outputs are on each pair of RMUs such that a single event cannot lose more than two of the signals needed for the two-out-of-four logic or all DPS (output) actuation.

The N-DCIS panels and components are designed to retain their structural integrity during and after DBEs so that proximate safety-related equipment is not prevented from performing its safety-related function.

Table 7.1-1 identifies the N-DCIS elements and the associated regulatory requirements, guidelines, and codes and standards applied. The N-DCIS major subsystems are summarized in Subsection 7.1.4.8. The following subsections address I&C systems conformance to regulatory requirements, guidelines, and industry standards.

General DCIS conformance to regulatory requirements, guidelines, and industry standards is also addressed in Subsection 7.1.6.

7.1.5.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety, and 10 CFR 50.55a(h) Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The N-DCIS design complies with the above requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(iv)[I.D.2], Safety parameter display system:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxi)[II.K.1.22], Auxiliary Heat Removal Systems:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxiv)[II.K.3.23], Central Reactor Vessel Water Level Recording:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.49, Environmental Qualifications of Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The design has ATWS mitigation functions, as described in Section 7.8.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety-Related Issues:

- Conformance: The N-DCIS is nonsafety-related. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: Inspection, Test, Analyses, and Acceptance Criteria (ITAAC) for the N-DCIS are identified in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided within the design control document (DCD) conforms to this regulation.

10 CFR 52.47 (c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.1.5.3.2 General Design Criteria

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43, 63, and 64:

- Conformance: The N-DCIS design conforms to these GDCs. Refer to Subsections 3.1.2 and 3.1.3 for a general discussion of each GDC.

7.1.5.3.3 Staff Requirements Memorandum

SRM, SECY-93-087, Item II.Q, Defense Against Common Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: SRM on SECY 93-087, II.Q, states that if a postulated common mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
- The N-DCIS provides diverse functionality via the DPS and associated interface systems. The nonsafety-related portions of the systems that conform to this guidance are further discussed in Section 7.8 and in Reference 7.1-4.

SRM, SECY-93-087, Item II.T, Control Room Alarm Reliability:

- Conformance: The N-DCIS AMS follows guidance in the above document for redundancy, independence, and separation so that the "alarm system" is considered redundant, has its own redundant processors and uses signals from distributed and redundant controllers. Alarm points are sent through a dual network to redundant processors that have dual power feeds. The alarm processors are dedicated, redundant, and conservatively sized. The alarms can be displayed on multiple independent VDUs, each with dual power supplies. Alarms are driven by redundant data links to the AMS. There is one horn and one voice speaker. Test buttons test the horn and the lights.

7.1.5.3.4 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.97.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: RG 1.151 is not applicable to the N-DCIS. The N-DCIS receives signals from nonsafety-related sensors in various systems in the plant that are supplied by instrument sensing lines but, the N-DCIS itself does not contain instrument sensing lines.
- For details on conformance to the Regulatory Guides listed in subsection 7.1.4.4, refer to Subsection 7.1.6.4.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The N-DCIS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The N-DCIS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems

- Conformance: The N-DCIS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.1.5.3.5 Branch Technical Positions

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Conformance: The N-DCIS conforms to BTP HICB-1.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: N-DCIS conforms to BTP HICB-10. Details of design implementation are discussed in Section 7.5.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in this subsection (7.1.5) conforms to BTP HICB-16.

From the foregoing analyses, it is concluded that the N-DCIS meets its regulatory and industry design bases.

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

- Conformance: The nonsafety-related portions of the systems that conform to BTP HICB-19 are discussed in Section 7.8 and in Reference 7.1-4.

7.1.5.4 N-DCIS Testing and Inspection Requirements

Testing and inspection requirements for N-DCIS systems are presented as specific subsections in Chapter 7.

Channel check, channel functional test, logic system functional test, channel calibration, and response time test are required for some N-DCIS systems in support of technical specification surveillance requirements. The N-DCIS online diagnostic features described below support the technical specification surveillance requirements.

The N-DCIS controllers, displays, monitoring and I/O communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and alarmed. The N-DCIS controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the operability of I/O signals, buses, power supplies, processors, and inter-processor communications. On-line diagnostics are performed without interrupting the normal operation of the N-DCIS.

The N-DCIS components and critical components of interfacing systems are tested to ensure that the specified performance requirements are satisfied. Factory, construction, and preoperational testing of the N-DCIS is performed before fuel loading and startup testing to ensure that the system functions as designed and that tested system performance is within specified criteria.

The N-DCIS interfaces with the TSM for automatic cyclic comparison of channel outputs and monitoring of unacceptable deviations. The TSM provides a log of the results, and sends out-of-limits alarms to the AMS.

The N-DCIS uses diverse platforms for implementing nonsafety-related nuclear functions for 3D MONICORE, RC&IS, AFIP, MRBM, ATLM, and RWM. Self-diagnostic routines with alarms ensure operability.

- 3D MONICORE monitors the reactor core, by accepting signals from the AFIP and the LPRMs. The LPRMs are calibrated with respect to the AFIP signals. Failed sensor inputs are rejected so that they do not contribute to calculations. Subsection 7.1.5.2.4.8 provides a functional description of 3D MONICORE. There are two active redundant workstations, but only one is manually selected by the operator at any time to periodically send fuel thermal limits information to the two redundant ATLMs. The same information is also sent to the TSM to support channel check and channel functional test surveillances.

- The MRBM and the AFIP are subsystems of the NMS. AFIP signals are routed to the 3D MONICORE for calibrating the LPRM. Subsection 7.7.6.2.1 provides a functional description of the AFIP. The MRBM sends rod block signals to RC&IS to ensure that fuel thermal safety limits are not violated. Subsections 7.7.6.2.2 and 7.7.2.2.7.4 respectively provide a functional description of the MRBM and the rod block function.

- The ATLM and the RWM have two redundant channels that are subsystems of RC&IS, which ensures consistency between specific control rod pattern restrictions and the actual pattern of the rods in the reactor. Subsection 7.7.2 provides a functional description, and Figure 7.7-2 shows a block diagram of RC&IS.
- The ATLMs receive data from 3D MONICORE through message-authenticated data links. They interchange data and generate alarms on disagreements. They send rod block signals to RC&IS to prevent violation of fuel operating thermal limits. Subsection 7.7.2.2.7.7 provides a functional description of the ATLM. ATLM failure automatically generates a rod block and an alarm. Only one ATLM can be bypassed at any time, and so there is always an active ATLM in service; additionally automated plant operation is not possible without both ATLMs being in service.
- Fuel thermal limits and rod block signals from the ATLMs and the MRBM are periodically sent to the TSM to support Channel Check and Channel Functional Test surveillances.

As described above, the 3D MONICORE and ATLMs send fuel thermal limit information to the TSM to support channel check and channel functional test surveillances. The data downloads from the two systems are synchronized. The TSM conducts a check to compare the values, and generates alarms if the values are not comparable within acceptable limits.

Once per shift, in steady state operation, an automatic check of rod block capability is generated by the ATLM to close rod block contacts to RC&IS (this signal can also be sent by operator VDU command). The TSM detects the rod block command and generates an alarm. This routine tests the functionality of the output contacts for rod block, and will execute only after checking and confirming that the nuclear parameters as seen by 3D MONICORE are in steady-state.

Additional surveillance tests associated with RC&IS ensure control rod operability and control rod pattern control. The control rod separation switches are also checked for functionality during a refueling outage, along with individual scram time testing on all the rods. A physical coupling and decoupling of the control rod is carried out to actuate the corresponding separation switches and validate the rod block functionality.

7.1.5.5 N-DCIS Instrumentation and Control Requirements

7.1.5.5.1 Uninterruptible Nonsafety-Related AC Power Supply

The N-DCIS components and cabinets that are key to power generation are supplied with either dual redundant or triple redundant power supplies and power feeds. The sources of this power are three independent UPS inverters, supported by AC power under normal operating conditions. If off-site power fails and the diesel generators fail, the N-DCIS inverters receive power from three independent battery systems. All of these AC power feeds are well regulated and supply 120 ±10% VAC, 60 Hz. Inverter operation, frequency, voltages, currents, and battery and charger operation are monitored and alarmed. The N-DCIS panel is designed so that the loss of one power supply or incoming power source does not affect the N-DCIS or its functional or plant operation.

7.1.5.5.2 Lighting and Service Power System

The Lighting and Service Power System (LSPS) supplies 120 VAC power to the N-DCIS for lighting and maintenance equipment. This includes internal cabinet lighting and convenience outlets.

7.1.5.6 N-DCIS Major System Interfaces

The N-DCIS has interfaces with almost all of the I&C and electrical nonsafety-related plant systems. Safety-related system information acquired by the Q-DCIS is available to the N-DCIS through qualified safety-related isolation devices (CIMs) that are part of the Q-DCIS. System interfaces with nonsafety-related systems, or portions of systems, and systems acquiring Q-DCIS data through the isolation devices, datalinks, and gateways (when necessary) include:

- ARMS;
- Auxiliary Boiler System (ABS);
- Condensate and Feedwater System (C&FS);
- Chilled Water System (CWS);
- CIRC;
- Condensate Storage and Transfer System;
- CIS;
- CMS;
- Control Building HVAC System (CBVS);
- CPS;
- CRD system;
- DC Power Supply System;
- DPS;
- Drywell Cooling System (DCS);
- Electrical Power Distribution System (EPDS);
- Electric equipment building HVAC (EBVS);
- Equipment and Floor Drain System;
- Extraction System;
- FAPCS;
- FPS;
- Fuel Building HVAC System (FBVS);
- Fuel Transfer System (FTS);
- FWCS;

- GDCS;
- Generator;
- Generator Lube and Seal Oil System (GLSOS);
- Heater Drain and Vent System (HDVS);
- High Pressure Nitrogen Supply System (HPNSS);
- Hydrogen Gas Control System (HGCS);
- Hydrogen water chemistry;
- IAS;
- ICS;
- LD&IS;
- Lighting and Servicing Power Supply;
- Liquid Waste Management System (LWMS);
- Low Voltage Distribution System;
- Main condenser and auxiliaries;
- Main turbine;
- Makeup Water System;
- Medium Voltage Distribution System;
- Meteorological observation station;
- Moisture Separator Reheater System;
- NBS;
- NMS;
- Offgas System (OGS);
- Oil Storage and Transfer System;
- Oxygen Injection System (OIS);
- PAS;
- PCCS;
- PRMS;
- PSWS;
- Process Sampling System (PSS);
- The Q-DCIS;
- Radwaste Building HVAC System (RWVS);
- RC&IS;

- Reactor Building HVAC System (RBVS);
- RCCWS;
- RWCU/SDC;
- RPS;
- RSS;
- The SB&PC System;
- Service Air System (SAS);
- Service Building HVAC;
- Service Water Building HVAC;
- SLC system;
- Solid Waste Management System;
- SSLC/ESF;
- Standby on-site AC power supply;
- Stator Cooling Water System (SCWS);
- Turbine Auxiliary Steam System (TASS);
- Turbine Building Cooling Water System;
- Turbine Building HVAC System (TBVS);
- Turbine Bypass System (TBS);
- TGCS;
- Turbine Gland Seal System;
- Turbine Lube Oil System (TLOS);
- Turbine Main Steam System (TMSS);
- Uninterruptible AC Power Supply System;
- Yard Miscellaneous Drain System; and
- Zinc Injection System (ZNIS), an optional system.

7.1.6 General DCIS Conformance to Regulatory Requirements, Guidelines and Industry Codes and Standards

Table 7-1 of NUREG 0800 lists the Code of Federal Regulations (CFR) including GDC, SRM, RGs, and Instrumentation and Controls Branch Technical Positions (HICB) that provide acceptance criteria or guidelines for each subsection of Chapter 7. Additional acceptance criteria or guidelines are delineated in the (NUREG-0800) SRP Chapter 7 sections.

The specific regulatory acceptance criteria and guideline requirements applicable to each of these systems (safety-related or nonsafety-related but significant for plant operation) identified in the

SRP are tabulated in Table 7.1-1. The regulatory requirements and guidelines applicability matrix for Table 7.1-1 is followed in Sections 7.2 through 7.8 by a regulatory conformance discussion for each specific system. The degree of applicability and conformance, along with any clarifications or justification for exceptions, are presented in the safety evaluation sections for each specific system. Requirements and guidelines not applicable to the ESBWR design are delineated in Tables 1.9-7, 1.9-20, and 1A-1. General Q-DCIS and N-DCIS conformance is discussed in the following subsections.

7.1.6.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The Q-DCIS and N-DCIS designs comply with the above requirements.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The Q-DCIS design conforms to IEEE Std. 603.

10 CFR 50.34(f), Conformance to Three Mile Island (TMI) Action Plan Requirements:

- TMI-related requirements are generically addressed in Appendix 1A. Applicable TMI-related requirements are identified for the systems in Table 7.1-1. The applicable systems are designed to conform. Those TMI-related requirements that are not applicable are not included in Table 7.1-1. The relevant TMI-related requirements that are resolved by the ESBWR Q-DCIS and N-DCIS design are identified as follows:
  - II.K.3.18 - ADS Actuation. ADS is designed for automatic operation.
  - II.K.3.21 - Automatic Restart of LPCS and LPCI. There are no automatic restart requirements based on the ECCS design.

The TMI action items applicable to the I&C systems are:

- 10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design,
- 10 CFR 50.34(f)(2)(iv)[I.D.2], Safety parameter display system, (see Subsection 7.1.5.2.4.1),
- 10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication,
- 10 CFR 50.34(f)(2)(viii)[II.B.3], Compatibility to Promptly Obtain and Analyze Containment Atmosphere Samples,
- 10 CFR 50.34(f)(2)(x)[II.D.1], Relief and Safety Valve Test Requirements,
- 10 CFR 50.34(f)(2)(xi)[II.D.3], Direct Indication of Relief and Safety Valve Position in the Control Room,
- 10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions,
- 10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation,
- 10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation,
- 10 CFR 50.34(f)(2)(xiv)[II.E.4.2], Containment Isolation Systems,

- 10 CFR 50.34(f)(2)(xix)[II.F.3], Instruments for Monitoring Plant Conditions Following Core Damage,
- 10 CFR 50.34(f)(2)(xxi)[II.K.1.22], Auxiliary Heat Removal Systems,
- 10 CFR 50.34(f)(2)(xxiii)[II.K.2.10], Anticipatory Reactor Trip,
- 10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels,
- 10 CFR 50.34(f)(1)(x)[II.K.3.28], Automatic Depressurization System Functioning During/Following an Accident Situation.
- 10 CFR 50.34(f)(2)(xxiv)[II.K.3.23], Central Reactor Vessel Water Level Recording,
- 10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment,
- 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity, and
- 10 CFR 50.34(f)(2)(xxviii)[III.D.3.4], Control Room Habitability Problems Under Accident Conditions.

10 CFR 50.44(c)(4), Combustible Gas Control For Nuclear Power Reactors, Monitoring:

- Conformance: The SSLC/ESF and CMS design complies with this requirement.

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The Q-DCIS and N-DCIS design has ATWS mitigation functions, as described in Section 7.8.

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The Q-DCIS design conforms to these standards, as described in Sections 7.2, 7.3, and 7.4.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided within the DCD conforms to this regulation.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

10 CFR 50.49, Environmental Qualifications of Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The Q-DCIS systems are designed to meet the equipment qualification requirements set forth in 10 CFR 50.49. Details are discussed in Section 3.11

7.1.6.2 General Design Criteria

In accordance with Table 7.1-1, the following GDC are addressed for the Q-DCIS:

GDC 1, 2, 4, 10, 12, 13, 15, 16, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 33, 34, 35, 37, 41, 43, 44, 63, and 64.

- Conformance: The Q-DCIS design complies with these GDC. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.8.

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43, 63, and 64.

- Conformance: The N-DCIS design complies with these GDC. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.8.

7.1.6.3 Staff Requirements Memorandum

SRM on SECY 93-087 II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: To minimize exposure to common-mode failures, the digital I&C systems are designed for high reliability, with the application of quality assurance requirements as specified in 10 CFR 50.55a(a)(1). Additionally, the digital I&C is designed applying principles of defense-in-depth and diversity defense against common mode failures. Section 7.8 includes the description of the diverse I&C systems that specifically addresses the requirements of this SRM.

SRM on SECY 93-087 II.T, Control Room Annunciator/Alarm Reliability:

- Conformance: The AMS follows guidance in the above document for redundancy, independence, and separation because the "alarm system" is considered redundant. Alarm points are sent through dual networks to redundant message processors on dual power supplies. The processors are dedicated to only doing alarm processing. The alarms are displayed on multiple independent VDUs that each have dual power supplies. The alarm tiles, or their equivalent, are driven by redundant datalinks (with dual power). There are redundant alarm processors. There are no alarms that require manually controlled actions for safety-related systems to accomplish their function. Thus the requirements for safety-related equipment and circuits are not applicable.

7.1.6.4 Regulatory Guides

A discussion of the general conformance of the I&C equipment to RGs is provided below.

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: Safety-related systems have provision for periodic testing. Proper functioning of analog sensors is verified by channel cross-comparison and is done continuously by the PCF. 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 guidance of Paragraph D.4 (per BTP HICB-8) are discussed in the Safety Evaluation subsections within Sections 7.2 through 7.8.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance: Provisions are made to detect and monitor identified and unidentified leakage of reactor coolant consistent with the guidance of this RG.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: Bypass indications are designed to satisfy the guidance of IEEE Std. 603, Paragraph 5.8.3, and RG 1.47. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety-related systems status.

  Bypass indications use isolation devices that preclude the possibility of any adverse electrical effect of the bypass indication circuits on the plant safety-related system.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems:

- Conformance: The safety-related systems are organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy for the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related systems designs' conformance to the single-failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The applicable I&C systems are designed to comply with RG 1.62. Specific conformance of the I&C systems is addressed in Sections 7.2 through 7.4.

RG 1.75**,** Physical Independence of Electric Systems**:**

- Conformance: The safety-related system designs conform to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electronic Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The safety-related system design conforms to RG 1.89.

RG 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident:

- Conformance: The Q-DCIS and N-DCIS are designed to meet the guidance of RG 1.97. Details of design implementation are discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The Q-DCIS systems are designed to meet the guidance set forth in RG 1.100. Details are discussed in Section 3.11.

RG 1.105, Instrument Setpoints for safety-related Systems**:**

- Conformance: The Q-DCIS and N-DCIS are consistent with the guidance of RG 1.105. The applicable analytical or design basis limit (technical specification limit), as well as the nominal trip setpoint (instrument setpoint) and any "as-found tolerance," and "as left tolerance" are provided in separate documentation. These parameters are appropriately separated from each other based on instrument accuracy, calibration capability and design drift (estimated) allowance data. The setpoints are within the instrument best-accuracy range. The established setpoints provide margin to satisfy safety-related requirements and plant availability objectives.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: The I&C systems are consistent with the guidance of RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: The instrument sensing lines are designed to satisfy the guidance of RG 1.151. These lines are used to perform safety-related and nonsafety-related functions. There are four redundant, separate sets of instrument lines, each having safety-related instruments associated with one of the four electrical safety-related divisions. The RPS logic requires any two-out-of-four trip signals to scram. If a division 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 triple fault-tolerant digital controllers (FTDC) that use sensors separate from the safety-related sensors. Therefore, the systems are designed so that no single failure or two-division failure results in a plant condition requiring protective action and at the same time, prevents the remaining redundant protection divisions from providing the protective action. Sections of endorsed standard ANSI/ISA-67.02.01 on design practices for tubing, vents, and drains also apply to nonsafety-related instrumentation.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The guidelines of RG 1.152 are a basis for design procedures established for programmable digital equipment. As the principle RG for digital computers in safety-related systems in nuclear power plants, it endorses and refers to IEEE Std. 603 for specific criteria details. This RG also contains discussions on digital I&C equipment common mode failure issues. The concern is related to the possibility that a design error in the software in redundant divisions of a safety-related system could lead to common cause or common mode failure of the safety-related system function. It is possible for conditions to exist where some form of diversity is necessary that provides additional assurance beyond that which is provided by the design and quality assurance (QA) programs that incorporate software QA and V&V. The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense-in-depth can be applied as defense against common-cause failures. The justification for equipment diversity, or for the diversity of related system software such as a real-time operation system, must extend to equipment components to ensure that actual diversity exists. Claims for diversity based on different manufacturers are insufficient without consideration of the above. Other considerations such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity. The following sections are noted in IEEE Std. 7-4.3.2 as specifically addressed by the NRC in RG 1.152:

- The main text portions of IEEE Std. 7-4.3.2 are similar to those in the 1993 version, with more extensive requirements incorporated for software development, V&V, software configuration management, equipment qualification, self-diagnostics, independence, and reliability. There is no specific detail on diverse method requirements.
- Annex B, "Diversity Requirements Determination" is essentially unchanged from the 1993 version. This annex provides a methodology for determining the need for diversity. RG 1.152 does not endorse Annex B.
- Annex C, "Dedication of existing commercial computers" is similar to the 1993 version.
- Annex E, "Communication Independence" is similar to the annex in the 1993 version. The NRC does not endorse Annex E.
- Annex F, "Computer reliability" is similar to the annex in 1993 the version. The NRC states that quantitative reliability goals are not the only means, and does not endorse this method as the sole means of meeting the regulations for reliability of digital computers. The NRC acceptance is based on deterministic criteria.
- Safety I&C System compliance with IEEE Std. 7-4.3.2

Additionally, RG 1.152 includes guidance applicable to the Q-DCIS. Compliance is summarized as follows:

- Defense against software common mode failures: GEH has evaluated BTP HICB-19 guidelines including the acceptance criteria on defense-in-depth and diversity and defense against common mode failures, on the four echelons of defense against common mode failures. The four echelons are control systems, reactor trip system, Engineered Safety Features Actuation System (ESFAS), and monitoring and indicator functions. To fully address the guidelines of BTP HICB-19 on defense-in-depth and diversity and defense against common mode failures, the DPS backs up the primary safety-related I&C system protection functions. The DPS is implemented with hardware and software that is totally separate and independent from the primary safety-related I&C protection systems (RTIF, NMS, and SSLC/ESF). The DPS is implemented in addition to the ATWS/SLC system function. A detailed description of the DPS and the description of defense-in-depth and diversity and defense against common mode failure are included in Section 7.8.
- Software development process: The software development process of the Q-DCIS (including control systems key to plant operation) follows the guidelines of BTP HICB-14. Software development process plans for the DCIS design implementation include the Software Management Plan (SMP), Software Development Plan (SDP), Software Verification and Validation Plan (SVVP), Software Configuration Management Plan (SCMP), Software Safety Plan (SSP), as required by guidance in BTP HICB-14 and are described in Appendix 7B. Actual detailed hardware and software design implementation follows the guidelines specified by these plans as part of the design acceptance criteria process.
- Equipment qualification, self-diagnostics, independence, and reliability: IEEE Std. 603 states that these requirements are applicable to safety-related I&C system equipment.

The Q-DCIS meets the requirements of IEEE Std. 603, and the above requirements in areas applicable to digital computer-based equipment.

- Security: The security guidelines included in RG 1.152 are evaluated and incorporated as appropriate and necessary in the DCIS design, both on plant hardware security measures and software security measures. The software development process plans are developed with the security requirements incorporated for actual detailed design implementation.

RG 1.153, Criteria for Safety Systems:

- Conformance: Safety-related systems are designed to satisfy the requirements of IEEE Std. 603, as endorsed by RG 1.153.

RG 1.168, Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems of Nuclear Power Plants:

- Conformance: This RG endorses IEEE Std. 1012, IEEE Standard for SVVPs, 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-related systems. IEEE Std. 1028 is acceptable for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. Safety-related systems use the guidance in these standards, as discussed in Reference 7.1-10, to develop portions of the overall SDP and thus comply with RG 1.168.

RG 1.169, Configuration Management Plans For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.169 endorses IEEE Std. 828, IEEE Standard for SCMPs, 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-related systems. Safety-related systems use the guidance in these standards, as discussed in Reference 7.1-10, to develop portions of the overall SDP and thus comply with RG 1.169.

RG 1.170, Software Test Documentation For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: The guidance contained in IEEE Std. 829, IEEE Standard for Software Test Documentation, provides an acceptable approach for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety-related system software subject to the provisions in this guide. Safety-related systems use the guidance in these standards to develop portions of the overall SDP and thus comply with RG 1.170.

RG 1.171, Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.171 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. Safety-related systems use the guidance in this standard to develop, as discussed in Reference 7.1-10, portions of the overall SDP and, thus, comply with RG 1.171.

RG 1.172, Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.172 endorses IEEE Std. 830, Recommended Practice for Software Requirements Specifications, as amended in the Regulatory Position. This standard describes current practices for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety-related applications; however, it does provide guidance on the development of software requirements specifications that exhibit characteristics important for developing safety-related system software. This is consistent with the goal of ensuring high-integrity software in reactor safety-related systems. Safety-related systems use the guidance in this standard, as described in the References 7.1-10 and 7.1-12, to develop portions of the overall software development plan and thus comply with RG 1.172.

RG 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.173 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 is used in conjunction with guidance from other appropriate RGs, standards, and software engineering literature. Safety-related systems use the guidance in this standard, as described in References 7.1-10 and 7.1-12, to develop portions of the overall SDP and thus comply with RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: Electrical and electronic components in the I&C safety-related systems are qualified for anticipated levels of EMI at their as-installed locations. EMC of I&C equipment is verified through factory testing and site-specific testing for both individual equipment and interconnected systems to meet EMC requirements for protection against the following:

  – EMI,

  – RFI,

  – Electrostatic discharge, and

  – Electrical surge.

  EMI qualifications, including methods of evaluating EMI operating envelopes, follow the requirements defined in Mil Std. 461E and IEC 61000-4. Q-DCIS equipment is qualified to perform continuously within specified ranges even when exposed to EMI environmental limits at the hardware mounting location. To that end, EMI qualifications for safety-related systems meet the proposed requirements of RG 1.180, Rev 1

"Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems."

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The surge withstanding capability of the safety-related I&C design conforms with IEEE Std. 1050. See Subsection 8A.1.2 for detailed information about the lightning protection system and conformance to RG 1.204.

RG 1.209, Guidelines For Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The safety-related system design conforms to RG 1.209.

7.1.6.5 Branch Technical Positions

BTPs that are applicable to the DCIS systems are identified relative to the I&C systems in Table 7.1-1. BTPs that are not applicable to the I&C design are identified in Table 1.9-7. BTPs are guidance documents; the DCIS is generally designed to conform to the BTPs. The degree of conformance, along with any clarifications or exceptions, is discussed in the safety evaluation subsections of Sections 7.1 through 7.8.

The following BTPs are not applicable to the ESBWR design:

BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service. Reactor coolant pumps are not used in the design and Position B.1 does not apply.

BTP HICB-6, Guidance on Design of Instrumentation and Controls Provided to Accomplish changeover from Injection to Recirculation Mode. No recirculation pumps and ECCS pumps are used in the design.

BTP HICB-13, Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors. RTDs are not used in safety-related applications.

The following BTPs are applicable:

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System. The GDCS and PIP A/B segment of N-DCIS design conforms to BTP HICB-1.

BTP HICB-8, Guidance on Application of RG 1.22. The Q-DCIS is fully functional during reactor operation and is tested in conjunction with the SSLC/ESF. Therefore, the Q-DCIS design conforms to BTP HICB-8. The DPVs, SRVs, and squib valves are not tested during reactor operation.

BTP HICB-9, Guidance on Requirements for RPS Anticipatory Trips. The Q-DCIS conforms to BTP HICB-9.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97. The Q-DCIS and N-DCIS design conforms to BTP HICB-10. Details of design implementation are discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices. The Q-DCIS design conforms to BTP HICB-11.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints. The Q-DCIS design conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-based I&C Safety Systems. Refer to Subsections 7.1.2.4, Reference 7.1-10 and 7.1-12 discussions. The Q-DCIS design conforms to BTP HICB-14.

The Q-DCIS and N-DCIS follow a development process that is in accordance with BTP HICB-14. As part of the Certification activity, the software development process plans require NRC review and approval.

Safety-related I&C systems (RTIF, NMS and SSLC/ESF) use computers for their logic functions. A description of the Q-DCIS design, together with the description of the DPS is included in Section 7.8, and specifically addresses the issues of defense-in-depth and diversity and defense against common mode failures.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52. BTP HICB-16 is applicable to all sections of Chapter 7 of the Design Control Document and all sections conform to it.

BTP HICB-16 states that the application should:

- Describe the resolution of unresolved and generic safety issues applicable to the I&C systems;
- Describe the interface requirements to be met by portions of the plant for which the application does not seek certification and which are necessary to ensure proper functioning of the I&C system; and
- Identify and describe the validation of innovative means of accomplishing I&C system safety-related functions.

Applications that propose the use of computers for systems with safety-related uses should describe the computer system development process. Applications that propose the use of computers for RTS and ESFAS functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity requirements.

The I&C design has no unresolved or generic safety-related issues applicable to I&C systems. In Section 1.11, unresolved and generic safety-related issues are discussed. There are several new generic issues that are related to I&C systems, such as failure of protective devices on safety-related equipment, electromagnetic pulse, identification of protection system instrument sensing lines, and protection system testability. These issues either are not applicable to safety-related I&C systems or are addressed by the safety-related I&C design. Within the scope of the DCD submitted for certification application, there are no interface requirements described here that fall into this category.

The design uses the voluminous data available from operating plants and from the testing and licensing efforts performed to license the predecessor designs and individual plants. The I&C design does not use innovative means for accomplishing safety functions.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based I&C Systems. Refer to Subsection 7.2.1.3.5 and 7.3.4.3 discussions. The Q-DCIS design conforms to BTP HICB-17.

BTP HICB-18, Guidance on Use of Programmable Logic Controllers in Digital Computer-based I&C System. The Q-DCIS design conforms to BTP HICB-18.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087). The Q-DCIS, DPS and associated N-DCIS interfacing systems design conform to BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance. The Q-DCIS design conforms to BTP HICB-21.

7.1.6.6 Industry Standards

The safety evaluation subsections throughout Chapter 7 address the RGs identified by the SRP. The IEEE standards that are endorsed by RGs are not addressed separately.

Some codes or standards that are not mentioned in the SRP are used in specific system applications. These are identified in the system description and the corresponding reference section. In accordance with the SRP format, the following IEEE standards applicable to the I&C equipment are addressed in other chapters.

IEC 61000-4 series. The design conforms to this series of standards.

IEEE Std. 323, "Qualifying safety-related Equipment for Nuclear Power Generating Stations." Safety-related systems are designed to meet the requirements of IEEE Std. 323. Environmental qualification is addressed in Section 3.11.

IEEE Std. 344, "Recommended Practices for Seismic Qualification of Safety-related Equipment for Nuclear Power Generating Stations". Safety-related I&C equipment is classified as Seismic Category I and designed to withstand the effects of the safe shutdown earthquake (SSE). It remains functional during normal and accident conditions. Qualification and documentation procedures used for Seismic Category I equipment and systems satisfy the provisions of IEEE Std. 344 as indicated in Section 3.10.

IEEE Std. 379, "IEEE Standard for the Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems." The Q-DCIS platforms, RTIF-NMS, SSLC/ESF, ATWS/SLC logic controllers, HP CRD isolation bypass logic controllers, and Vacuum Breaker Isolation Function (VBIF) logic controllers, are organized into four physically and electrically isolated divisions that use principles of redundancy and independence to conform to the single failure criterion.

IEEE Std. 383, "IEEE Standard for Type Test of Safety-related Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations." Electric cable conforms to this standard. Fiber optic cable insulation/covering/jacketing also conforms to the requirements for flame tests in IEEE Std. 383.

IEEE Std. 384, "IEEE Standard Criteria for Independence of Safety-related Equipment and Circuits". See the discussion of RG 1.75 in Subsection 7.1.6.4.

IEEE Std. 497, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." Accident monitoring instrumentation is discussed in Section 7.5.

IEEE Std. 518, "IEEE Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources". The design conforms to IEEE Std. 518.

IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations". Conformance to IEEE Std. 603 is discussed in Subsection 7.1.6.6.1.

IEEE Std. 1050, "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations". The design conforms to IEEE Std. 1050.

7.1.6.6.1 IEEE Std. 603 – IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

The scope of IEEE Std. 603 includes safety-related I&C systems that are described in Sections 7.1 through 7.8. IEEE Std. 603 does not directly apply to nonsafety-related systems, other than to require independence between nonsafety-related systems and safety-related systems. IEEE Std. 603 provides design criteria for safety systems. ESBWR divides safety systems into two parts: the Q-DCIS platforms, and the subsystems that contain the sensors and actuators used by the Q-DCIS platforms. This section describes how the IEEE Std. 603 criteria are allocated to the different Q-DCIS platforms and subsystems. For convenience, some of these requirements may also be adopted as design bases for some nonsafety-related I&C components and systems such as for accident monitoring instrumentation, in accordance with RG 1.97. Compliance with the requirements of IEEE Std. 603 is also identified as compliance with the requirements and guidance contained within the federal regulations, GDC, SRM, and RGs, as described throughout Section 7.1. The safety-related I&C design comprises the Q-DCIS which includes the equipment in the RTIF, NMS, and SSLC/ESF cabinets. The design conforms to IEEE Std. 603. ITAACs are provided for the major attributes for compliance with IEEE Std. 603 and are not intended to limit the scope of compliance.

When the IEEE Std. 603 design criteria are applied to platforms relying on the use of software to perform their safety-related functions, additional criteria from IEEE Std. 7-4.3.2, which augments the IEEE Std. 603 criteria, also apply to the platform as described under the applicable IEEE Std. 603 criterion. The evaluation of Q-DCIS platforms for compliance with IEEE Std. 603 and IEEE Std. 7-4.3.2 criteria includes the examination of the effects that the associated sensors and actuators have on the performance of the safety-related function.

In accordance with the software development process described in Appendix 7B and the defense-in-depth and diversity strategy described in Section 7.8, the protection systems are executed as software projects on particular Q-DCIS platforms. The software projects are named RTIF, NMS, SSLC/ESF, VBIF, ATWS/SLC, and HP CRD.

Table 7B-1 shows the relationship between the Q-DCIS platforms and their corresponding software projects. As shown, the RTIF-NMS platform has two software projects: RTIF and NMS. The SSLC/ESF platform has one software project: SSLC/ESF. The Independent Control Platform has three software projects: VBIF, ATWS/SLC, and HP CRD.

7.1.6.6.1.1 Safety System Designation (IEEE Std. 603, Section 4, et al)

IEEE Std. 603, Section 4, requires that a specific basis be established for the design of each safety-related system. The designs of the Q-DCIS platforms are based on the abnormal events in Table 15.0-2.

Criterion 4.1 requires identification of the DBEs applicable to each mode of operation of the plant along with the initial conditions and allowable limits of plant conditions for each such event. Table 1.3-1 defines the reactor system design characteristics. Tables 15.0-3, 15.0-4, 15.0-5, and 15.0-6 define the safety-related analysis acceptance criteria for the AOOs, infrequent events, special events, and accidents. Table 15.1-2 defines the ESBWR operating modes for the entire operating envelope. Table 15.1-3 defines the ESBWR abnormal events with applicable operating modes. Table 15.2-1 defines the input parameters, initial conditions, and assumptions for AOO events and infrequent events. Table 15.5-2 defines the initial conditions and bounding limits for ATWS events. Credited systems, interlocks, and functions for each DBE are described in Sections 15.2, 15.3, 15.4, and 15.5. Additional details about the specific safety-related or nonsafety-related interfacing system design bases, interlocks, and functions are found in Sections 4.6, 5.2, 5.4, 6.2, 6.3, 8.3, 9.1, 9.3, 9.4, 10.2, 10.3, and 10.4. Information provided for each design basis item enables the detailed design of the system to be carried out. Safety-related system design basis descriptions are included in the various sections of this chapter as indicated below.

- Reactor Trip System;
  - RPS (Subsection 7.2.1),
  - NMS (Subsection 7.2.2), and
  - Suppression Pool Temperature Monitoring (Subsection 7.2.3).
- SSLC/ESF (Subsection 7.3.5);
  - ECCS (Subsection 7.3.1):
    - ADS (Subsection 7.3.1.1),
    - GDCS (Subsection 7.3.1.2),
    - ICS (Subsection 7.4.4), and
    - SLC system (Subsection 7.4.1).
- PCCS (Subsection 7.3.2);
- LD&IS non-MSIV functions (Subsection 7.3.3) (MSIV functions of the LD&IS are located in the RTIF cabinets);
- CRHS (Subsection 7.3.4);
- RSS (Subsection 7.4.2);
- RWCU/SDC (Subsection 7.4.3);
- PAM system (Subsection 7.5.1);
- CMS (Subsection 7.5.2);
- PRMS (Subsection 7.5.3);
- ATWS/SLC (7.8.1);
- CRHS (7.5.2); and
- VB isolation function (7.3.6).

Criterion 4.2 requires identification of the safety-related functions and corresponding protective actions of the execute features for each event evaluated in the Nuclear Safety Operational Analysis (NSOA). Table 15.1-5 defines the execute systems required to respond to each event. Table 15.1-6 defines the automatic safety-related instrument trips in response to each event. Additionally, safety-related design bases for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

Criterion 4.3 requires identification of the permissive conditions for each operating bypass capability that is to be provided. Additionally, the permissive conditions for each operating bypass for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

Criterion 4.4 requires identification of the variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured. The minimum list of such variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18. The variables and combinations of variables that are associated with each event are discussed in the relevant subsection describing the event as defined in Table 15.1-7.

Criterion 4.5 requires identification of (1) the points in time and the plant conditions during which manual control is allowed, (2) the justification for permitting initiation or control subsequent to initiation solely by manual means, (3) the range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations are performed, and (4) the variables identified by Criterion 4.4 that are displayed for the operator to use in taking manual action, for each action identified by Criterion 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. The minimum list of variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18.

Criterion 4.6 requires identification of the minimum number and locations of sensors required for protective purposes for those variables identified by Criterion 4.4 that have spatial dependence. The minimum list of variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18. The variables and combinations of variables that have spatial dependence are described within each applicable subsection of this chapter.

Criterion 4.7 requires identification of the range of transient and steady-state conditions of both motive and control power and the environment during normal, abnormal, and accident circumstances throughout which the safety system performs. Safety-related mechanical equipment and electrical equipment (which comprises electrical power and instrumentation and controls equipment) is qualified in accordance with the equipment qualification program described in Section 3.11. Environmental conditions for the zones where qualified equipment is located are calculated for normal, AOO, test, accident and post-accident conditions and are documented in Appendix 3H, Equipment Qualification Environmental Design Criteria.

Criterion 4.8 requires identification of the conditions having the potential for functional degradation of safety system performance and for which provisions are incorporated to retain the capability for performing the safety functions. Safety-related mechanical equipment and electrical equipment (which comprises electrical power and instrumentation and controls equipment) is qualified in accordance with the equipment qualification program described in Sections 3.9 through 3.11. Environmental conditions for the zones where qualified equipment is located are calculated for normal, AOO, test, accident and post-accident conditions and are documented in Appendix 3H, Equipment Qualification Environmental Design Criteria.

Criterion 4.9 requires identification of the methods to be used to determine that the reliability of each safety system design is appropriate and any qualitative or quantitative reliability goals that may be imposed on the system design. The ESBWR Design Reliability Assurance Program (D-RAP) is a program utilized during detailed design and specific equipment selection phases to assure that the important ESBWR reliability assumptions of the Probabilistic Risk Assessment (PRA) are addressed throughout the plant life. The D-RAP is described in Section 17.4.

Criterion 4.10 requires identification of the critical points in time or the plant conditions, after the onset of a design basis event, including: (1) the point in time or plant conditions for which the protective actions of the safety system are initiated, (2) the point in time or plant conditions that define the proper completion of the safety function, (3) the point in time or the plant conditions that require automatic control of protective actions, and (4) the point in time or the plant conditions that allow returning a safety system to normal. The relevant points in time and plant conditions associated with each event, except for the allowable conditions for returning a plant to normal, are discussed in the relevant subsection describing the event as defined in Table 15.1-7. The allowable conditions for returning a plant to normal (i.e., return to service conditions) will be developed as part of the procedure development process described in Section 18.9.

Criterion 4.11 requires identification of the equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The safety-related systems are designed to accomplish their safety-related functions in accordance with the single-failure criterion, IEEE Std. 603, Section 5.1. Failure modes and effects analyses are performed on the safety-related system final design to ensure that no equipment protective provisions preclude correctly performing any safety-related function.

Criterion 4.12 requires identification of any other special design basis that may be imposed on the system design (e.g., diversity, interlocks, regulatory agency criteria). The design bases for each subsystem (including bases for diversity, interlocks, regulatory agency criteria) are identified within each applicable subsection of this chapter.

7.1.6.6.1.2 Single Failure Criterion (IEEE Std. 603, Section 5.1)

The safety-related system designs are organized into four physically and electrically isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally the design meets N-2 conditions (see Subsection 7.1.3.3.6).

The safety-related control systems include sufficient redundancy and independence to fulfill their intended safety function even when degraded by any single credible failure. The RTIF - NMS, SSLC/ESF, and independent control platform implement the single failure criterion of IEEE Std. 603 Section 5.1 using four independent and redundant channels, which are provided in two-out-of-four trip logic. This ensures no single failure of or within any division prevents the system from performing its safety function or causing either an inadvertent reactor scram or an ECCS actuation. Redundancy begins with the sensors monitoring the variables and continues through the signal processing, output devices, and actuators.

Independence is implemented as described in Subsections 7.1.6.6.1.7 and 7.1.6.6.1.20.

Failure modes and effects analyses (FMEA) complying with IEEE Std. 379 are used to confirm the safety-related system designs' conformance to the single-failure criterion.

The FMEA is consistent with the failure modes detectable by the self-diagnostic features of the hardware/software platforms and those detected by periodic surveillance.

Equipment is provided in accordance with a prescribed quality assurance plan as described in Subsection 7.1.6.6.1.4.

7.1.6.6.1.3 Completion of Protective Action (IEEE Std. 603, Sections 5.2 and 7.3)

After initiation by either automatic or manual means, the protective actions go to completion in conformance to IEEE Std. 603, Section 5.2. They go to completion by using one of the following: seal-in logic, non-resettable squib valves, manually reset valves, diverse functions, or a combination of logic, valves and functions. Deliberate operator action is required to reset the safety-related systems. Additionally, completion of protective actions for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.4 Quality (IEEE Std. 603, Section 5.3)

The Quality criterion requires that the Q-DCIS be consistent with minimum maintenance requirements and low failure rates and be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Q-DCIS meets this requirement through the application of the ESBWR Quality Assurance Program described in Chapter 17.

IEEE Std. 7-4.3.2 has additional quality assurance requirements related to software. Refer to LTRs "ESBWR Software Management Program Manual," NEDE-33226P (Reference 7.1-12), and "ESBWR Software Quality Assurance Program Manual," NEDE-33245P (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software quality assurance requirements.

- IEEE Std. 7-4.3.2, Criterion 5.3.1, Software Development. The quality of software development activities is assured in accordance with the Software Quality Assurance Plan (SQAP).
- IEEE Std. 7-4.3.2, Criterion 5.3.2, Software Tools. Software tools are controlled in accordance with the Software Configuration Management Plan (SCMP).
- IEEE Std. 7-4.3.2, Criterion 5.3.3, Verification and Validation (V&V). Software V&V is performed in accordance with the Software V&V Plan (SVVP).
- IEEE Std. 7-4.3.2, Criterion 5.3.4, Independent V&V (IV&V). Software IV&V is performed in accordance with the Software V&V Plan (SVVP).

- IEEE Std. 7-4.3.2, Criterion 5.3.5, Software Configuration Management. Software configuration is controlled in accordance with the Software Configuration Management Plan (SCMP).
- IEEE Std. 7-4.3.2, Criterion 5.3.6, Software Project Risk Management: Software project risk management is managed in accordance with the Software Management Plan (SMP).

Safety-related equipment is provided under the GEH 10 CFR 50, Appendix B quality assurance program. The NRC-accepted GEH Quality Assurance Program with its implementing procedures, constitutes the Quality Assurance system that is applied to the Q-DCIS design. It satisfies all applicable requirements of the following: 1) 10 CFR 50 Appendix B; 2) ANSI/ASME NQA-1; and 3) ISO 9001. Safety-related I&C systems employing digital computers, software, firmware, and software tools conform to the quality requirements in IEEE Std. 7-4.3.2 as described in References 7.1-10 and 7.1-12.

7.1.6.6.1.5 Equipment Qualification (IEEE Std. 603, Section 5.4)

The Equipment Qualification criterion requires the referencing platform to be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that the safety-related system is capable of meeting the performance requirements specified in the design basis. The Q-DCIS meets the Equipment Qualification requirements through the application of the Equipment Qualification program that is described in Sections 3.9 through 3.11. Refer to Table 3.11-1 for a list of electrical and mechanical equipment and conformance criteria for Equipment Qualification.

IEEE Std. 7-4.3.2 has additional Equipment Qualification requirements related to Structures, Systems, or Components (SSCs) using software. Refer to LTRs "ESBWR Software Management Program Manual," NEDE-33226P (Reference 7.1-12), and "ESBWR Software Quality Assurance Program Manual," NEDE-33245P (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software equipment qualification requirements.

- IEEE Std. 7-4.3.2, Criterion 5.4.2, Qualification of existing commercial computers is performed in accordance with the commercial-off-the-shelf dedication process in accordance with the Software Development Plan.
- IEEE Std. 7-4.3.2, Criterion 5.4.1, The referencing platform qualification testing is performed with the referencing system functioning with software and diagnostics that are representative of those used in actual operation in accordance with the Software Test Plan.

7.1.6.6.1.6 System Integrity (IEEE Std. 603, Section 5.5)

The System Integrity criterion requires that the referencing platform's features be adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment enumerated in the design basis. The Q-DCIS meets this requirement through the application of the Equipment Qualification program described in Sections 3.9 through 3.11, and Subsection 7.1.6.6.1.5.

IEEE Std. 7-4.3.2 has additional system integrity requirements related to SSC using software. Refer to LTRs "ESBWR Software Management Program Manual," NEDE-33226P

(Reference 7.1-12), and "ESBWR Software Quality Assurance Program Manual," NEDE-33245P (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software system integrity requirements:

- IEEE Std. 7-4.3.2, Criterion 5.5.1, Design for computer integrity: The referencing system is designed to perform its safety-related function when subjected to design basis conditions.
- IEEE Std. 7-4.3.2, Criterion 5.5.2, Design for test and calibration: The referencing system is designed to perform its safety-related function when undergoing test and calibration in accordance with the Software Development Plan.
- IEEE Std. 7-4.3.2, Criterion 5.5.3, Fault detection and self-diagnostics: Fault detection and self-diagnostics (as performed by platform self-test features) do not adversely affect the capability of the referencing system to perform its safety-related functions in accordance with the Software Development Plan.

The Q-DCIS systems are required to accomplish their safety-related functions under the full range of applicable conditions enumerated in the design bases. Other areas addressed as requirements include adequate system real-time performance for digital computer-based systems to ensure completion of protective action, evaluation of hardware integrity and software integrity (software safety-related analysis, as part of BTP HICB-14 requirements), failure to a safe state upon loss of energy or adverse environmental conditions, and the requirements for manual reset.

The Q-DCIS meets the integrity requirements described in IEEE Std. 603, Section 5.5. The RTIF – NMS platform functions fail to the tripped state. The SSLC/ESF platform and the independent control platform fail to a state where the actuated component remains "as-is" to prevent a control system induced LOCA. Hardware and software failures detected by self-diagnostics cause a trip signal to be generated in the RPS division in which the failure occurs and no trip signal is generated if the failure occurs in a SSLC/ESF or independent control platform division. Single failures of hardware and software do not inhibit manual initiation of protective functions.

7.1.6.6.1.7 Independence (IEEE Std. 603, Section 5.6)

The required independence between redundant portions of a safety-related system, between safety-related systems and the effects of DBEs, and between safety-related systems and other systems is defined. Three aspects of independence are addressed in each case: physical independence, electrical independence, and communication independence. The Q-DCIS design meets these requirements.

Each division is sufficiently independent from the other divisions so that no one division is dependent on information, timing data, or communication from any other division to initiate a safety-related trip signal. The failure of a single division does not prevent the initiation of a safety-related trip. Each safety-related logic evaluates the data from its own division's sensors and continuously broadcasts the result of its evaluation to the other divisions as either a "trip" or "no trip" signal.

A safety-related trip is initiated whenever any two divisions sense conditions that require a safety-related trip. Each division receives input data from its own separate set of sensors connected to the same process source and separately transmits trip signals to the other divisions. The trip actuators go to their trip state whenever they receive concurrent, like parameter trip signals from any two safety-related logic transmissions. The signal isolators are qualified to withstand all credible faults, such as short circuits or high voltage, so that faults cannot propagate and degrade the performance of any safety-related control function.

Physical Independence

The Q-DCIS systems have four redundant and independent divisions that are physically independent and separated and that have independent electrical power sources applied to them. Except where fiber optic cable is used, there are no common switches shared by the four divisions. The sensors used for each of the four divisions, are independent and physically separated from one another. All wiring and electrical components are physically separated via isolation barriers or spacing. Refer to Subsection 7.1.3.3.1.

Electrical Independence

Independence between safety-related systems is achieved through proper equipment qualification and isolation. Safety-related systems are totally separated and independent from nonsafety-related systems. When system interfacing is required, electrical isolation is provided via isolation devices (qualified per IEEE Std. 384) and by the use of fiber optic cables.

Communication Independence

Communication between redundant safety channels is limited to a minimum, such as trip signals and bypass status signals, and is through proper isolation devices. In accordance with IEEE Std. 379, communication between redundant divisions or between safety-related control systems and nonsafety-related control systems is electrically isolated and one-way. (Refer to Subsection 7.1.3.3.) In addition, loss of communication or communication upsets are contained within a single channel and cannot inhibit the ability of redundant channels to perform their functions. Optical couplers and fiber optic cable provide the route for communications.

Communication between safety-related systems and nonsafety-related systems is carried out via fiber optic cable through the required qualified safety-related signal isolation devices (CIMs), and data pathways such as datalinks and gateways (when necessary). Communication from nonsafety-related systems to safety-related systems is prohibited, with the exception of time tagging and NMS calibration data. Additional discussion on this subject is included in Subsection 7.1.3.3. The RTIF, NMS, and SSLC/ESF protection functions have priority over data transmissions, so that data transmissions do not interfere with the RTIF, NMS, or SSLC/ESF protection functions. .

7.1.6.6.1.8 Capability for Testing and Calibration (IEEE Std. 603, Section 5.7)

The capability for testing and calibration of safety-related system equipment is provided during power operation and duplicates the performance of the safety-related function as closely as practicable, as discussed in Sections 7.2 through 7.8. Tests are capable of being performed in overlapping segments when testing one safety-related function. Maintenance bypasses of individual functions are provided in the safety-related system channels to enable testing during power operation. For example, the safety-related functions of each safety-related division can be tested on-line with the tested division bypassed from the two-out-of-four voting trip logic. The I&C equipment has built-in self-diagnostic functions to identify critical failures such as loss of power and data errors. The Q-DCIS meets the requirements outlined in this section. Refer to Subsections 7.1.3.3.6, 7.1.3.3.7, 7.1.3.4 and 7.1.3.5.

Safety-related sensors are designed with the capability for test and calibration during reactor operation. Additionally, any exceptions for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.9 Information Displays (IEEE Std. 603, Section 5.8)

The Information Displays criterion requires that information displays for the referencing platform be designed to be accessible to the operators, display variables for manually controlled actions, display system status information, provide indication of bypasses, and display post-accident monitoring variables in accordance with the HFE process. The Q-DCIS information displays, including displays for manually controlled actions, meet this requirement by the application of the HFE design process described in Chapter 18. This process includes the steps to ensure compliance with regulatory requirements. The information display design conforms to the guidance offered in RG 1.47 for bypassed and inoperable status indication.

System Status Indication: The safety-related and nonsafety-related I&C systems are provided with system status information that meets the requirements of IEEE Std. 603, Section 5.8. All pertinent system trip/logic status, parameter data values, equipment functional status and ESF actuator status are displayed to the operator upon request. For safety-related systems, this information is available for each division. Certain information, key to plant operation and status monitoring, is permanently displayed on the large WDP in the MCR. Alarm and annunciation indications are also available in the MCR in accordance with system design requirements. All information available within a division, including post accident monitoring information, can be viewed in a safety-related manner on the VDUs associated with that division. The same divisional information and all nonsafety-related information can be viewed on the nonsafety-related VDUs and WDP.

Indication of Bypasses: For safety-related system protection functions, bypass status is continuously displayed to the operator.

Locations of Displays: Displays in the MCR are either on the main control console or on the large WDP visible and accessible to the operator. The man-machine interface system design includes design requirements and specifications for the classification of locations of displays in the MCR. More detailed descriptions of requirements for the locations of displays are included in Chapter 18.

7.1.6.6.1.10 Control of Access (IEEE Std. 603, Section 5.9)

Administrative control is used to implement access control to vital areas of the plant, including the MCR. Physical security and electronic security devices are provided to ensure only authorized and qualified plant personnel are allowed to have access to the Q-DCIS cabinets and consoles. Physical security is described in Section 13.6. In addition to the plant physical security, the Q-DCIS equipment has its own access control devices. Q-DCIS cabinets have doors with keylocks and position switches. Q-DCIS components within the cabinets have keylock switches that are used to control access to special functions (such as, the INOP/OP switch).

Keys, passwords, and other security devices (following the guidance of RG 1.152) are used to control access to specific rooms; open specific equipment cabinets; obtain permission for access to enter specific electronic instruments for calibration, testing, and setpoint changes; and, gain access to safety-related system software and data. Safety-related software is not routinely changed at the plant site.

Opening a Q-DCIS cabinet door produces an alarm in the MCR.

There is no access to safety-related system equipment and control through the network from nonsafety-related system equipment. Computer-related access controls and authorization are part of the cyber security program plan, which is described in the LTRs, "ESBWR Cyber Security Program Plan," NEDO-33295, (Non-Proprietary); and "ESBWR Cyber Security Program Plan," NEDE-33295-P, (Proprietary), (Reference 7.1-8).

7.1.6.6.1.11 Repair (IEEE Std. 603, Section 5.10)

The Q-DCIS systems provide timely recognition of location, replacement, repair, and adjustment of malfunctioning equipment. Periodic self-diagnostic functions locate the failure to the component level. Through individual division bypassing, the failed component is replaced or repaired on line without affecting the safety-related system protection function. During repairs the trip logic is two-out-of-three so that the single failure criterion is still met.

7.1.6.6.1.12 Identification (IEEE Std. 603, Section 5.11)

The Q-DCIS system equipment conforms to the identification requirements specified in IEEE Std. 603, Section 5.11. Color-coding is used as one of the major methods of identification. Safety-related equipment is distinctly marked in each redundant division of a safety-related system. Hardware component or equipment units have an identification label or nameplate. See Subsection 8.3.1.3 for additional details. For digital computer-based system equipment, versions of computer hardware, programs, and software are distinctly identified. Configuration management formalizes system component and software identification.

IEEE Std. 7-4.3.2 has additional identification requirements related to SSC using software. Refer to LTRs "ESBWR Software Management Program Manual," NEDE-33226P (Reference 7.1-12), and "ESBWR Software Quality Assurance Program Manual," NEDE-33245P (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 requirement for the identification and retrieval of software identification using software maintenance tools.

7.1.6.6.1.13 Auxiliary Features (IEEE Std. 603, Section 5.12)

Safety-related I&C system auxiliary supporting features conform to IEEE Std. 603, Section 5.12 where applicable and maintain the supported safety-related system performance at an acceptable level.

The Q-DCIS is supported by four divisions of safety-related uninterruptible power as described in Subsection 8.3.2. DC batteries supply power if there is a loss of off-site and on-site AC power.

HVAC, whether active or passive is a key auxiliary supporting system that maintains the necessary environmental conditions for both the safety-related and nonsafety-related I&C equipment. Under normal operating conditions when offsite power is available or when diesel generators are running, HVAC systems control the temperature and humidity of all I&C equipment. Under a loss of power condition, including Station Blackout (SBO), batteries provide continuous safety-related I&C operation for 72 hours, and continued operation of the nonsafety-related I&C equipment for two hours. However, during a loss of power condition, active HVAC is not available to the safety-related CB or RB equipment, except in the CRHA as noted below.

The Q-DCIS and its safety-related battery-operated support equipment remain powered and the heat generated is removed passively (except possibly by small chassis mounted fans); the Q-DCIS and support equipment is qualified to the worst case anticipated temperature rise. Battery-backed N-DCIS equipment is only powered for two hours if offsite and diesel generator power is lost; during that interval the batteries supplying the N-DCIS also power nonsafety-related HVAC in the CRHA. If the nonsafety-related redundant HVAC is not available, safety-related temperature sensors with two-out-of-four logic trip the control room power that feeds predefined components of the nonsafety-related I&C and other predefined nonsafety-related heat loads. The safety-related I&C that remains operable is qualified for the resulting temperature rise with passive heat removal. This scheme protects the equipment and maximizes operator comfort. Additional description of the HVAC design, including the use of room coolers powered by the ancillary diesel generators is included in Chapter 8, Chapter 9, and Appendix 19A.

7.1.6.6.1.14 Multi-Unit Stations (IEEE Std. 603, Section 5.13)

The multi-unit station criteria do not apply to the standard single unit plant design submitted for NRC certification.

7.1.6.6.1.15 Human Factors Considerations (IEEE Std. 603, Section 5.14)

The I&C system design includes a HFE design process that is consistent with the requirements outlined in NUREG-0711, "Human Factors Engineering Program Review Model." The HFE process defines a comprehensive, iterative design approach for the development of a human-centered control and information infrastructure and is described in Chapter 18.

7.1.6.6.1.16 Reliability (IEEE Std. 603, Section 5.15)

The degree of redundancy, diversity, testability, and quality of the safety-related I&C design achieves the necessary functional reliability. Safety-related equipment is provided under GEH's 10 CFR 50 Appendix B quality program. The BTP HICB-14 and IEEE 7.4.3.2 (as endorsed by RG 1.152) guidance followed for software development processes achieves reliable software design and implementation. The Design Reliability Assurance Program (D-RAP) described in Section 17.4 confirms that any quantitative or qualitative reliability goals established for the protection systems have been met. To achieve defense against common mode failure, the design includes defense-in-depth and diversity measures including the incorporation of the DPS described in Section 7.8. Reference 7.1-4 provides specific information on the redundancy and diversity used in safety-related I&C systems. The Q-DCIS is included in the consideration of the probabilistic risk assessment (PRA). (Refer to Chapter 19.)

7.1.6.6.1.17 Automatic Control (IEEE Std. 603, Sections 6.1 and 7.1)

The RTIF-NMS, and ATWS/SLC logic automatically initiates reactor trip and the RTIF for LD&IS (non-MSIV), SSLC/ESF and VBIF logic automatically actuates the ESF that mitigate the consequences of DBEs. These automatic protection actions are implemented through two-out-of-four voting logic whenever one or more process variables reach their actuation setpoint. Variables are monitored and measured by each of the RTIF - NMS, ATWS/SLC, SSLC/ESF, and VBIF divisions.

Plant-specific setpoint analyses determine the protection systems' instrument setpoints using the methodology described in Reference 7.1-9. The GEH setpoint methodology uses plant-specific setpoint analyses to ensure that the combination of characteristics of the instruments such as range, accuracy and resolution provide the required high probability that the analytical limits in Chapter 15 analyses are not exceeded for the safety-related control system components and systems of the safety-related I&C. The response times of the I&C systems are assumed in the safety-related analyses and verified by plant specific surveillance testing or system analyses. The Q-DCIS application software, hardware processing rates, and internal and external communication system design ensures that the real-time performance of the safety-related control systems is deterministic.

7.1.6.6.1.18 Manual Control (IEEE Std. 603, Sections 6.2 and 7.2)

Each protective action can be manually initiated at the system level, in conformance to RG 1.62, and at the division level in conformance to IEEE Std. 603, Sections 6.2 and 7.2. The manual initiation satisfies divisional rules for independence and separation. Two manual actions, each in a separate division, are required in order to satisfy the two-out-of-two system logic or the two-out-of-four division logic that initiates a reactor trip in the RPS and ESF functions in the SSLC/ESF systems.

The operator can manually initiate the ESF functions by performing the appropriate action in two-out-of-four divisions; thus, satisfying the two-out-of-two system initiation logic. The ESF functions that use squib valves use a redundant two-step arm and fire sequence. This prevents single failures from firing or from inhibiting the firing of the squib valves. The squib valves are the GDCS pool injection valves, the suppression pool injection valves, the GDCS deluge valves, the ADS DPV, and the SLC injection valves. To manually initiate the GDCS short-term and long-term injection systems, a low-pressure signal must be present in the RPV. This prevents inadvertent manual initiation of the system during normal reactor operation.

The operator can manually initiate reactor emergency shutdown, reactor trip, with control rods by using any of three different methods using redundant or diverse controls. The manual reactor trip occurs independently of the automatic trip logic and sensor status.

The two manual scram switches, the Reactor Mode Switch, and the four divisional manual trip switches (per protective system) are located in the MCR and are easily accessible to the operator.

The two MCR manual scram switches, the RSS manual scram switches share no equipment with the automatic controls and require no software for their operation, and the DPS manual scram switches share a minimum of equipment with the automatic controls. The MCR and RSS manual scram switches are directly connected to the power feed for the load drivers that are, in turn, connected directly to the scram pilot valve solenoids. The DPS can manually scram by controlling both the HCU scram solenoid valves (by interrupting the current in the 120 VAC return from the solenoid) and the ARI scram air header dump valves.

After manual initiation, the protective actions go to completion in conformance to IEEE Std. 603, Section 5.2 as described in Subsection 7.1.6.6.1.3. The manual initiation of a protective action performs all actions carried out by automatic initiation.

In the Q-DCIS design, there are no protective actions that have not been selected of automatic control. There are also no manual actions necessary to maintain safe conditions after the completion of protective actions for 72 hours after a DBE.

The manual controls are designed so that the information provided, display content and location are taken into consideration for easy operator access and action in the MCR. Further information about the design of manual controls and HFE considerations, as well as plant manual operation procedure requirements, are included in Chapter 18. Additionally, manual controls for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.19 Interaction Between the Sense and Command Features and Other Systems (IEEE Std. 603, Section 6.3)

The Q-DCIS protection systems are totally separate and independent from the nonsafety-related control systems, in accordance with GDC 24. Any failure of nonsafety-related systems does not affect safety-related protection systems or prevent them from performing their safety-related functions. If one safety-related division fails, any nonsafety-related control system can be isolated from the failure by using data validation techniques to select a valid control input from the three other remaining divisions. The communication path broadcasts one way - from the protection system to the N-DCIS. A failure of communication does not affect the protection function. Therefore, providing additional redundancy to isolate the protection system from communication failure is not required and not applied. For further detail on communication between the Q-DCIS and the N-DCIS (including transmission of time tagging signals) see Subsection 7.1.3.3.

Sensors used by safety-related I&C systems are not shared with nonsafety-related control systems. Calculated safety-related signals such as APRMs can be used, after isolation, by nonsafety-related control systems.

7.1.6.6.1.20 Derivation of System Inputs (IEEE Std. 603, Section 6.4)

To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables. An example of an indirect measurement is the loss of feedwater flow in the RPS scram logics. The loss of the feedwater flow variable is represented by the loss of the power generation bus signal. When the power to the feedwater pump motor is lost, the feedwater flow is also immediately lost. The use of loss of power generation bus signals to represent the loss of feedwater flow signal meets the requirements of the safety-related analysis of Chapter 15, because it is the only credible way that all feedwater flow can be lost. Additionally, derivation of system inputs for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.21 Capability for Testing and Calibration (IEEE Std. 603, Section 6.5)

The operational availability of the protection system sensors can be checked by perturbing the monitored variables, by cross-checking between redundant channels that have a known relationship with each other and that have read-outs available, or by introducing and varying a substitute input to the sensor of the same nature as the measured variable. The four-division RTIF-NMS, SSLC/ESF, and independent control platform logic provides at least two valid divisions for crosschecking of monitored variables. The third division also has the capability to be available for crosschecking, depending on the maintenance bypass status. When one division is placed into maintenance bypass mode, the condition is alarmed in the MCR and the division logic automatically becomes a two-out-of-three voting scheme. Most sensors and actuators are provisioned for actual testing and calibration during power operation with the exceptions described in Sections 7.2 through 7.8. See Subsections 7.1.3.3.5, 7.1.3.3.6, 7.1.3.3.7, and 7.1.3.5 for additional details.

In the Q-DCIS design a 24 month calibration periodicity is implemented to ensure accuracy and integrity of signal development, transmission and processing. Digital I&C equipment utilized in the I&C design is qualified for the environment in which it is located so that it retains its calibration during the post accident time period. Additionally, capability for testing and calibration for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.22 Operating Bypasses (IEEE Std. 603, Sections 6.6 and 7.4)

Operating bypasses are implemented in the Q-DCIS. One example of such operating bypasses is associated with the trip function dependence on reactor operating mode. The requirements of IEEE Std. 603 are met by the safety-related I&C operating bypass design. Specific descriptions of safety-related system operating bypasses are included in Subsections 7.2.1.5 and 7.3.5.2. Operating bypasses are automatically removed as described in Subsections 7.2.1.5 and 7.3.5.2. Additionally, operating bypasses for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.23 Maintenance Bypass (IEEE Std. 603, Sections 6.7 and 7.5)

Maintenance bypass capability is incorporated in the design of the Q-DCIS. This permits equipment maintenance, testing, and repair of one individual division with the plant operating and without initiating any protection functions. The single failure criterion is met under this bypass condition. Although it is possible to bypass only one division at a time, the Q-DCIS design is able to supply its safety-related functions even with a two-division failure. Maintenance bypass is always alarmed or indicated in the MCR. Maintenance bypass for safety-related I&C systems is typically applied through a joystick bypass switch with exclusive logic that allows only one division, out of four, to be bypassed at any given time. Maintenance bypasses are initiated manually by the plant operator per administrative control. Additionally, maintenance bypasses for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.24 Setpoints (IEEE Std. 603, Section 6.8)

For automatic protective devices, safety-related setpoints and setpoints having significant safety functions for the Technical Specification required limiting safety system settings are determined by the methodology described in Reference 7.1-9. The GEH setpoint methodology uses plant-specific setpoint analyses to ensure that the instruments' range, accuracy, and resolution meet the performance requirements assumed in the safety-related analyses in Chapter 15 for the safety-related control system components and systems. This methodology meets the requirements of

IEEE Std. 603, Section 6.8. The response times of the I&C systems assumed in the safety-related analyses are verified by plant specific surveillance testing or system analyses.

7.1.6.6.1.25 Electrical Power Sources (IEEE Std. 603, Section 8.1)

The Q-DCIS protection system cabinets and components are supported by two independent power sources. Each division of safety-related I&C is powered by two UPS that can supply 120 VAC from either offsite power, diesel generator power, or safety-related batteries (for 72 hours). Either of the two power sources allows Q-DCIS operation. These power sources comply with IEEE 603 as described in Subsection 7.1.6.6.1. See Subsection 7.1.3.3.7 for additional description. Descriptions of safety-related system power sources are included in Chapter 8.

7.1.6.6.1.26 Non-electrical Power Sources (IEEE Std. 603, Section 8.2)

If a non-electrical power source is required for a safety function, then the source of the power is classified as safety-related and complies with IEEE 603 as described in Subsection 7.1.6.6.1. Additionally, non-electrical power sources for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.27 Maintenance Bypass (IEEE Std. 603, Section 8.3)

The Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies appropriate to their division with battery backup (per division) for at least 72 hours. The UPS have a manual maintenance switch and either supply (per division) can operate its Q-DCIS division. Using the inverter's manual bypass and shutting down either the associated batteries, chargers or inverters technically makes the division inoperable but, in fact the division remains fully functional, losing only the ability to operate for 72 hours should offsite or diesel power be lost (it operates for approximately 36 hours under those circumstances). Operation of the Q-DCIS when one of its power supplies is in maintenance bypass is appropriately alarmed. In the very unlikely event that an entire division is without power the failsafe RTIF-NMS platform interprets the condition as a trip (unless bypassed) and neither the SSLC/ESF platform nor the ICP assumes a trip. Because only two divisions are necessary to satisfy the safety requirements, no functionality is lost. The condition of a division without power triggers an alarm. Refer to the discussion of GDC 18 in DCD Subsection 8.3.1.2.1 for maintenance provisions of safety-related power supplies. Further discussion of the safety-related power supplies is provided throughout Chapter 8.

A single non-electrical redundant power source (e.g., one of two parallel accumulators, one of two squibs) may be taken to "maintenance bypass" (i.e., isolated) without adversely impacting the safety function of any system.

For those non-electrical power sources having a degree of redundancy of one, taking it to maintenance bypass does not adversely impact the reliability of any safety-related system to perform its safety functions. Additionally, manual bypassing of power sources for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.28 Cyber Security (IEEE Std. 7-4.3.2)

The security measures included in RG 1.152 are evaluated and incorporated in the Q-DCIS design and include plant hardware and software security measures. The software development process plans are developed with the security measures.

The comprehensive cyber security program plan (Reference 7.1-8) identifies security risks and outlines appropriate procedures. The plant ensures that hardware, controls, and data networks comprising the control network cannot be disrupted, interrupted, or negatively affected by unauthorized users or external systems. Reference 7.1-8 documents the design commitments, which meet the applicable guidance of RG 1.152, Section C.2, and Positions 2.1 through 2.9.

Inspections, tests, analyses, and acceptance criteria (ITAAC) associated with the cyber security program plan are provided in Tier 1 together with the SDP.

7.1.7 COL Information

None.

7.1.8 References

7.1-1 (Deleted)

7.1-2 (Deleted)

7.1-3 (Deleted)

7.1-4 GE Hitachi Nuclear Energy, "ESBWR I&C Diversity and Defense-In-Depth Report." NEDO-33251, Class I (Non-proprietary), Revision 2, May 2009.

7.1-5 (Deleted)

7.1-6 (Deleted)

7.1-7 (Deleted)

7.1-8 [*GE Hitachi Nuclear Energy, "ESBWR Cyber Security Program Plan," NEDE-33295P, Class III (Proprietary), Revision 0, October 2007, and NEDO-33295, Class I (Non-Proprietary), Revision 0, October 2007.*]*

7.1-9 GE-Hitachi Nuclear Energy, "GEH ABWR/ESBWR Setpoint Methodology," NEDE-33304P, Class III (Proprietary), Revision 1, November 2008, and NEDO-33304, Class I (Non-proprietary), Revision 1, November 2008.

7.1-10 [*GE Hitachi Nuclear Energy, "ESBWR Software Quality Assurance Program Manual (SQAPM)," NEDE-33245P, Class III (Proprietary), Revision 3, July 2008, and NEDO-33245, Class I (Non-Proprietary), Revision 3, July 2008.*]*

7.1-11 GE Nuclear Energy, "General Electric Instrument Setpoint Methodology," NEDC-31336P-A, Class III (Proprietary), September 1996, and NEDO-31336-A, Class I (Non-proprietary), September 1996.

7.1-12 [*GE Hitachi Nuclear Energy, "ESBWR - Software Management Program Manual (SMPM),"* NEDE-33226P, Class III (Proprietary) Revision 4, May 2009, and *NEDO-33226, Class I (Non-proprietary), Revision 4, May 2009.*]*

7.1-13 (Deleted)

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)[6]	CMS (includes SPTM)[6]	NBS[6]	CRD[6]	NMS	SSLC/ESF[3]	LD&IS (non-MSIV)[1][6]	PRMS	CMS[6]	NBS (includes ADS)[6]	GDCS	ICS	SLC[6]	CBVS[2]	CRD[5][6]	VBIF	ATWS/SLC[4][6]	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
10 CFR																								
50.55a(a)(1)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
50.55a(h)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
50.34(f)(1)(v) [II.K.3.13]								X				X	X	X										
50.34(f)(1)(x) [II.K.3.28]												X												
50.34(f)(2)(iii) [I.D.1]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
50.34(f)(2)(iv) [I.D.2]																					X			
50.34(f)(2)(v) [I.D.3]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				X
50.34(f)(2)(viii) [II.B.3]								X			X													
50.34(f)(2)(x) [II.D.1]								X			X													
50.34(f)(2)(xi) [II.D.3]								X				X												
50.34(f)(2)(xiv) [II.E.4.2]	X		X					X	X															

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
50.34(f)(2)(xv) [II.E.4.4]								X	X														X	
50.34(f)(2)(xvii) [II.F.1]								X		X	X													X
50.34(f)(2)(xviii) [II.F.2]							X	X				X												X
50.34(f)(2)(xix) [II.F.3]								X		X	X	X												X
50.34(f)(2)(xxi) [II.K.1.22]	X	X						X						X								X		
50.34(f)(2)(xxiii) [II.K.2.10]		X						X						X										
50.34(f)(2)(xxiv) [II.K.3.23]																								X
50.34(f)(2)(xxvi) [III.D.1.1]								X	X															X
50.34(f)(2)(xxvii) [III.D.3.3]								X		X	X													X
50.34(f)(2)(xxviii) [III.D.3.4]								X		X						X								
50.44(c)(4)								X			X													

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)[6]	CMS (includes SPTM)[6]	NBS[6]	CRD[6]	NMS	SSLC/ESF[3]	LD&IS (non-MSIV)[1][6]	PRMS	CMS[6]	NBS (includes ADS)[6]	GDCS	ICS	SLC[6]	CBVS[2]	CRD[5][6]	VBIF	ATWS/SLC[4][6]	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
50.49	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																							
50.62							X	X						X					X		X	X	X	
50.63	X	X	X			X		X	X				X	X		X								
52.47(a)(21)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(b)(1)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(a)(25)	N/A																							
52.47	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(c)(2)	N/A																							
GENERAL DESIGN CRITERIA																								
1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 7.1-1
I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
10	X	X					X																	
12	X	X					X														X			
13	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
15	X		X					X	X			X												
16	X		X					X	X									X						
19	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
20	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
21	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
22	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
23	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
24	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
25	X	X					X														X			
26	X	X				X	X												X		X			
27	X	X				X	X												X		X			
28																	X				X			
29	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
30								X	X			X												
33								X				X	X	X								X		
34								X						X										
35								X				X	X	X	X				X					
37								X				X	X	X	X				X					

Table 7.1-1
I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)[6]	CMS (includes SPTM)[6]	NBS[6]	CRD[6]	NMS	SSLC/ESF[3]	LD&IS (non-MSIV)[1][6]	PRMS	CMS[6]	NBS (includes ADS)[6]	GDCS	ICS	SLC[6]	CBVS[2]	CRD[5][6]	VBIF	ATWS/SLC[4][6]	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
38																						X		
41								X			X												X	
42																							X	
43								X			X												X	
44														X										
63								X																X
64								X		X	X													X
SRM on SECY 93-087																								
II.Q	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
II.T								X													X			X
Regulatory Guides (RG)																								
1.22	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
1.45								X	X	X	X													
1.47	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.53	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.62	X	X	X					X	X			X	X	X		X		X	X	X				
1.75	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.89	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																							
1.97(10)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.100	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																							
1.105	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
1.118	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.151 (8)		X		X	X	X			X		X	X	X	X	X				X	X		X	X	
1.152(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
1.153	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.168(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.169(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.170(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.171(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.172(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.173(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.180(9)	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																							
1.204	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.209	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																							
Branch Technical Positions (BTP)																								
BTP HICB-1								X					X									X		

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)[6]	CMS (includes SPTM)[6]	NBS[6]	CRD[6]	NMS	SSLC/ESF[3]	LD&IS (non-MSIV)[1][6]	PRMS	CMS[6]	NBS (includes ADS)[6]	GDCS	ICS	SLC[6]	CBVS[2]	CRD[5][6]	VBIF	ATWS/SLC[4][6]	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
BTP HICB-3	N/A																							
BTP HICB-6	N/A																							
BTP HICB-8	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-9	X	X				X																		
BTP HICB-10[10]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
BTP HICB-11	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-12	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-13	N/A																							
BTP HICB-14[7]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-16	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
BTP HICB-17[7]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-18[7]	X	X					X	X										X	X	X				

Table 7.1-1

I&C Regulatory Requirements Applicability Matrix

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform			Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)[6]	CMS (includes SPTM)[6]	NBS[6]	CRD[6]	NMS	SSLC/ESF[3]	LD&IS (non-MSIV)[1][6]	PRMS	CMS[6]	NBS (includes ADS)[6]	GDCS	ICS	SLC[6]	CBVS[2]	CRD[5][6]	VBIF	ATWS/SLC[4][6]	HP CRD Isolation Bypass Function	GENE	PIP A/B	BOP	PCF
BTP HICB-19[7]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
BTP HICB-21[7]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Notes:

(1) LD&IS (non-MSIV) controls the safety-related actuators (for the isolation valves and dampers) associated with the following nonsafety-related systems: RWCU/SDC, FAPCS, EFDS, CIS, CWS, CMS, HPNSS, RBVS, and FBVS. RWCU/SDC provides safety-related sensor inputs to LD&IS (non-MSIV). The regulatory requirements associated with these actuators and sensors are addressed as part of LD&IS.

(2) CBVS includes the CRHS and Control Room Habitability Area HVAC Subsystem (CRHAVS) and EFUs.

(3) SSLC/ESF includes RSS, MCRP and safety-related VDUs.

(4) Includes the NBS sensors associated with ATWS/SLC.

(5) SSLC/ESF platform column for CRD includes safety-related sensors associated with control rod separation detection.

(6) The following safety-related systems have logic implemented on multiple platforms in support of their protective functions: CMS, CRD, LD&IS, NBS and SLC. Refer to DCD Sections 7.2, 7.3, 7.4, and 7.5 for detailed descriptions of the system functions.

(7) These criteria are addressed with digital computer-related functions of the Q-DCIS and N-DCIS.

(8) Sections of the ANSI/ISA standard that are not specific to safety-related systems, but provide guidance on design practices for tubing, vents and drains apply to the systems associated with the N-DCIS network segments.

(9) Hardware associated with the N-DCIS network segments uses industrial methods for EMI/EMF/RFI/EMC compliance.

(10) The ESBWR I&C conforms to RG 1.97 and applies the guidance in IEEE std. 497. RG 1.97 endorses IEEE Std. 497 (with clarifications and exceptions stated in RG 1.97) and the use of the HFE development process to determine the human actions during and following accident scenarios. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																			
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM		
		RTIF						NMS													
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)	HP CRD Isolation Bypass Function
4.1	Design basis events	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.2	Safety-related functions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.5.5.3.1	7.1.6.6.1.1 7.5.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.3	Permissive conditions for operating bypasses	7.1.6.6.1.1	7.1.6.6.1.1 7.2.1.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.2.3.3.1	7.1.6.6.1.1 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.2.2.3.1	7.1.6.6.1.1 7.3.5.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.5.3.3.1	7.1.6.6.1.1 7.5.2.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.1.2.3.1	7.1.6.6.1.1 7.4.4.3.1	7.1.6.6.1.1 7.4.1.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.6.3.1	7.1.6.6.1.1	7.1.6.6.1.1
4.4	Monitored variables, and associated analytical limits	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.5	Minimum criteria for manual actions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.6	Spatially dependent variables	7.1.6.6.1.1	7.1.6.6.1.1 7.2.1.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.2.3.3.1	7.1.6.6.1.1 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.2.2.3.1	7.1.6.6.1.1 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.5.3.3.1	7.1.6.6.1.1 7.5.2.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.1.2.3.1	7.1.6.6.1.1 7.4.4.3.1	7.1.6.6.1.1 7.4.1.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.6.3.1	7.1.6.6.1.1	7.1.6.6.1.1
4.7	Range of transient and steady-state conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.8	Adverse environmental conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.9	Reliability methods	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.10	Abnormal Event critical times / conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.11	Equipment protective provisions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.12	Special design basis	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																			
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM		
		RTIF						NMS													
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)	HP CRD Isolation Bypass Function
5.1	Single failure criterion	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2
5.2	Completion of protective action	7.1.6.6.1.3	7.1.6.6.1.3 7.2.1.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.2.3.3.1	7.1.6.6.1.3 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.2.2.3.1	7.1.6.6.1.3 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.5.3.3.1	7.1.6.6.1.3 7.5.2.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.3.1.2.3.1	7.1.6.6.1.3 7.4.4.3.1	7.1.6.6.1.3 7.4.1.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3 7.3.6.3.1	7.1.6.6.1.3	7.1.6.6.1.3
5.3	Quality	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4
5.4	Equipment qualification	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5
5.5	System Integrity	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6
5.6	Independence	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7
5.7	Capability for test and calibration	7.1.6.6.1.8	7.1.6.6.1.8 7.2.1.3.1	7.1.6.6.1.8 7.3.3.3.1	7.1.6.6.1.8 7.2.3.3.1	7.1.6.6.1.8 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.8	7.1.6.6.1.8 7.2.2.3.1	7.1.6.6.1.8 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.8 7.3.3.3.1	7.1.6.6.1.8 7.5.3.3.1	7.1.6.6.1.8 7.5.2.3.1	7.1.6.6.1.8	7.1.6.6.1.8 7.3.1.2.3.1	7.1.6.6.1.8 7.4.4.3.1	7.1.6.6.1.8 7.4.1.3.1	7.1.6.6.1.8	7.1.6.6.1.8	7.1.6.6.1.8 7.3.6.3.1	7.1.6.6.1.8	7.1.6.6.1.8
5.8	Information displays	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9
5.9	Control of Access	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10
5.10.	Repair	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11
5.11	Identification	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12
5.12	Auxiliary features	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13
5.13	Multi-unit stations	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14
5.14	Human factors considerations	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15
5.15	Reliability	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16
6.1	Automatic Control	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																			
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM		
		RTIF						NMS													
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)	HP CRD Isolation Bypass Function
6.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18 7.2.1.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.2.3.3.1	7.1.6.6.1.18 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.2.2.3.1	7.1.6.6.1.18 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.5.3.3.1	7.1.6.6.1.18 7.5.2.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.3.1.2.3.1	7.1.6.6.1.18 7.4.4.3.1	7.1.6.6.1.18 7.4.1.3.1	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.6.3.1	7.1.6.6.1.18	7.1.6.6.1.18
6.3	Interaction between the sense and command features and other systems	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19
6.4	Derivation of system inputs	7.1.6.6.1.20	7.1.6.6.1.20 7.2.1.3.1	7.1.6.6.1.20 7.3.3.3.1	7.1.6.6.1.20 7.2.3.3.1	7.1.6.6.1.20 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.20	7.1.6.6.1.20 7.2.2.3.1	7.1.6.6.1.20 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.20 7.3.3.3.1	7.1.6.6.1.20 7.5.3.3.1	7.1.6.6.1.20 7.5.2.3.1	7.1.6.6.1.20	7.1.6.6.1.20 7.3.1.2.3.1	7.1.6.6.1.20 7.4.4.3.1	7.1.6.6.1.20 7.4.1.3.1	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20 7.3.6.3.1	7.1.6.6.1.20	7.1.6.6.1.20
6.5	Capability for testing and calibration	7.1.6.6.1.21	7.1.6.6.1.21 7.2.1.3.1	7.1.6.6.1.21 7.3.3.3.1	7.1.6.6.1.21 7.2.3.3.1	7.1.6.6.1.21 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.21	7.1.6.6.1.21 7.2.2.3.1	7.1.6.6.1.21 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.21 7.3.3.3.1	7.1.6.6.1.21 7.5.3.3.1	7.1.6.6.1.21 7.5.2.3.1	7.1.6.6.1.21	7.1.6.6.1.21 7.3.1.2.3.1	7.1.6.6.1.21 7.4.4.3.1	7.1.6.6.1.21 7.4.1.3.1	7.1.6.6.1.21	7.1.6.6.1.21	7.1.6.6.1.21 7.3.6.3.1	7.1.6.6.1.21	7.1.6.6.1.21
6.6	Operating bypasses	7.1.6.6.1.22	7.1.6.6.1.22 7.2.1.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.2.3.3.1	7.1.6.6.1.22 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.2.2.3.1	7.1.6.6.1.22 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.5.3.3.1	7.1.6.6.1.22 7.5.2.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.3.1.2.3.1	7.1.6.6.1.22 7.4.4.3.1	7.1.6.6.1.22 7.4.1.3.1	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22 7.3.6.3.1	7.1.6.6.1.22	7.1.6.6.1.22
6.7	Maintenance bypass	7.1.6.6.1.23	7.1.6.6.1.23 7.2.1.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.2.3.3.1	7.1.6.6.1.23 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.2.2.3.1	7.1.6.6.1.23 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.5.3.3.1	7.1.6.6.1.23 7.5.2.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.3.1.2.3.1	7.1.6.6.1.23 7.4.4.3.1	7.1.6.6.1.23 7.4.1.3.1	7.1.6.6.1.23	7.1.6.6.1.23	7.1.6.6.1.23 7.3.6.3.1	7.1.6.6.1.23	7.1.6.6.1.23
6.8	Setpoints	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24
7.1	Automatic Control	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17

Table 7.1-2

I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference

		Q-DCIS																			
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM		
		RTIF						NMS													
IEEE Std. 603 Section	Functions (1)	RTIF	RPS	LD&IS (MSIV Only) (6)	CMS (includes SPTM) (6)	NBS (6)	CRD (6)	NMS (3)	SSLC/ESF (4)	LD&IS (Non-MSIV) (2)&(6)	PRMS	CMS (6)	NBS (includes ADS) (6)	GDCS	ICS	SLC (6)	CBVS (7)	CRD (6)	VBIF	ATWS / SLC (5),(6)&(7)	HP CRD Isolation Bypass Function
7.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18 7.2.1.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.2.3.3.1	7.1.6.6.1.18 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.2.2.3.1	7.1.6.6.1.18 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.5.3.3.1	7.1.6.6.1.18 7.5.2.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.3.1.2.3.1	7.1.6.6.1.18 7.4.4.3.1	7.1.6.6.1.18 7.4.1.3.1	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.6.3.1	7.1.6.6.1.18	7.1.6.6.1.18
7.3	Completion of protective action	7.1.6.6.1.3	7.1.6.6.1.3 7.2.1.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.2.3.3.1	7.1.6.6.1.3 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.2.2.3.1	7.1.6.6.1.3 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.5.3.3.1	7.1.6.6.1.3 7.5.2.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.3.1.2.3.1	7.1.6.6.1.3 7.4.4.3.1	7.1.6.6.1.3 7.4.1.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3 7.3.6.3.1	7.1.6.6.1.3	7.1.6.6.1.3
7.4	Operating bypass	7.1.6.6.1.22	7.1.6.6.1.22 7.2.1.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.2.3.3.1	7.1.6.6.1.22 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.2.2.3.1	7.1.6.6.1.22 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.5.3.3.1	7.1.6.6.1.22 7.5.2.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.3.1.2.3.1	7.1.6.6.1.22 7.4.4.3.1	7.1.6.6.1.22 7.4.1.3.1	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22 7.3.6.3.1	7.1.6.6.1.22	7.1.6.6.1.22
7.5	Maintenance bypass	7.1.6.6.1.23	7.1.6.6.1.23 7.2.1.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.2.3.3.1	7.1.6.6.1.23 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.2.2.3.1	7.1.6.6.1.23 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.5.3.3.1	7.1.6.6.1.23 7.5.2.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.3.1.2.3.1	7.1.6.6.1.23 7.4.4.3.1	7.1.6.6.1.23 7.4.1.3.1	7.1.6.6.1.23	7.1.6.6.1.23	7.1.6.6.1.23 7.3.6.3.1	7.1.6.6.1.23	7.1.6.6.1.23
8.1	Electrical power sources	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25
8.2	Non-electrical power sources	7.1.6.6.1.26	7.1.6.6.1.26 7.2.1.3.1	7.1.6.6.1.26 7.3.3.3.1	7.1.6.6.1.26 7.2.3.3.1	7.1.6.6.1.26 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.26	7.1.6.6.1.26 7.2.2.3.1	7.1.6.6.1.26 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.26 7.3.3.3.1	7.1.6.6.1.26 7.5.3.3.1	7.1.6.6.1.26 7.5.2.3.1	7.1.6.6.1.26	7.1.6.6.1.26 7.3.1.2.3.1	7.1.6.6.1.26 7.4.4.3.1	7.1.6.6.1.26 7.4.1.3.1	7.1.6.6.1.26	7.1.6.6.1.26	7.1.6.6.1.26 7.3.6.3.1	7.1.6.6.1.26	7.1.6.6.1.26
8.3	Maintenance Bypass	7.1.6.6.1.27	7.1.6.6.1.27 7.2.1.3.1	7.1.6.6.1.27 7.3.3.3.1	7.1.6.6.1.27 7.2.3.3.1	7.1.6.6.1.27 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.27	7.1.6.6.1.27 7.2.2.3.1	7.1.6.6.1.27 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.27 7.3.3.3.1	7.1.6.6.1.27 7.5.3.3.1	7.1.6.6.1.27 7.5.2.3.1	7.1.6.6.1.27	7.1.6.6.1.27 7.3.1.2.3.1	7.1.6.6.1.27 7.4.4.3.1	7.1.6.6.1.27 7.4.1.3.1	7.1.6.6.1.27	7.1.6.6.1.27	7.1.6.6.1.27 7.3.6.3.1	7.1.6.6.1.27	7.1.6.6.1.27

Notes:

(1) The IEEE Std. 603 criteria apply to the safety-related portions of the systems identified in this table.

(2) LD&IS (non-MSIV) controls the safety-related actuators (for the isolation valves and dampers) associated with the following nonsafety-related systems: RWCU/SDC, FAPCS, EFDS, CIS, CWS, CMS, HPNSS, RBVS, and FBVS. RWCU/SDC provides safety-related sensor inputs to LD&IS (non-MSIV). The regulatory requirements associated with these actuators and sensors are addressed as part of LD&IS.

(3) NMS has Q and N parts. The Q parts are SRNM, LPRM, APRM, and OPRM. The N parts are AFIP and MRBM.

(4) SSLC/ESF includes the RSS, MCRP, and safety-related VDUs.

(5) Includes the NBS sensors associate with ATWS/SLC.

(6) The following safety-related systems have logic implemented on multiple platforms in support of their protective functions: CMS, CRD, LD&IS, NBS and SLC. Refer to DCD Sections 7.2, 7.3, 7.4, and 7.5 for detailed descriptions of the system functions.

(7) CBVS includes the CRHS and CRHAVS subsystems and EFUs.

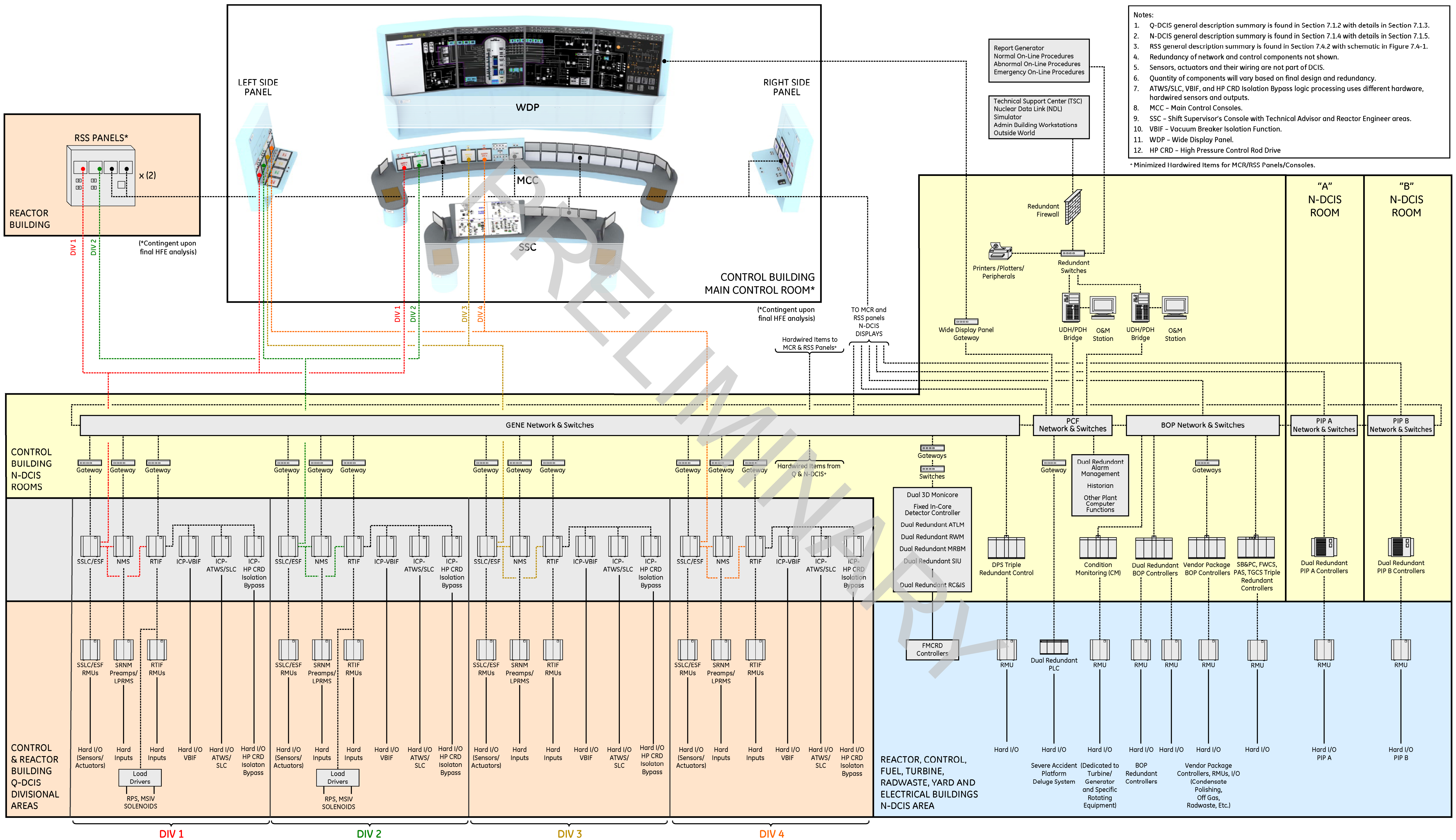
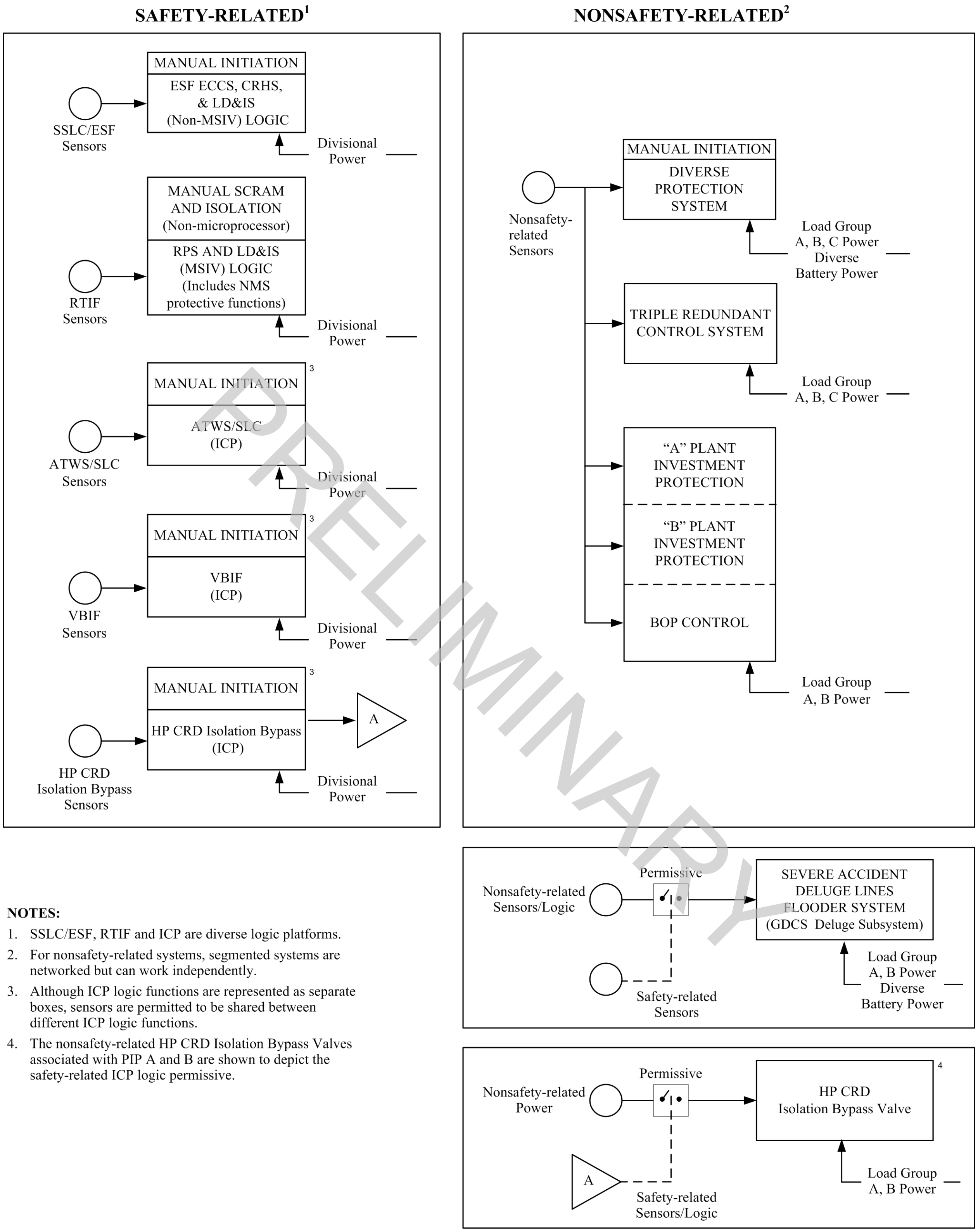


Figure 7.1-1. Simplified Network/Functional Diagram of DCIS

Figure 7.1-2. Deleted



NOTES:

1. SSLC/ESF, RTIF and ICP are diverse logic platforms.
2. For nonsafety-related systems, segmented systems are networked but can work independently.
3. Although ICP logic functions are represented as separate boxes, sensors are permitted to be shared between different ICP logic functions.
4. The nonsafety-related HP CRD Isolation Bypass Valves associated with PIP A and B are shown to depict the safety-related ICP logic permissive.

Figure 7.1-3. ESBWR Distributed Power-Sensor/Logic Diversity Diagram

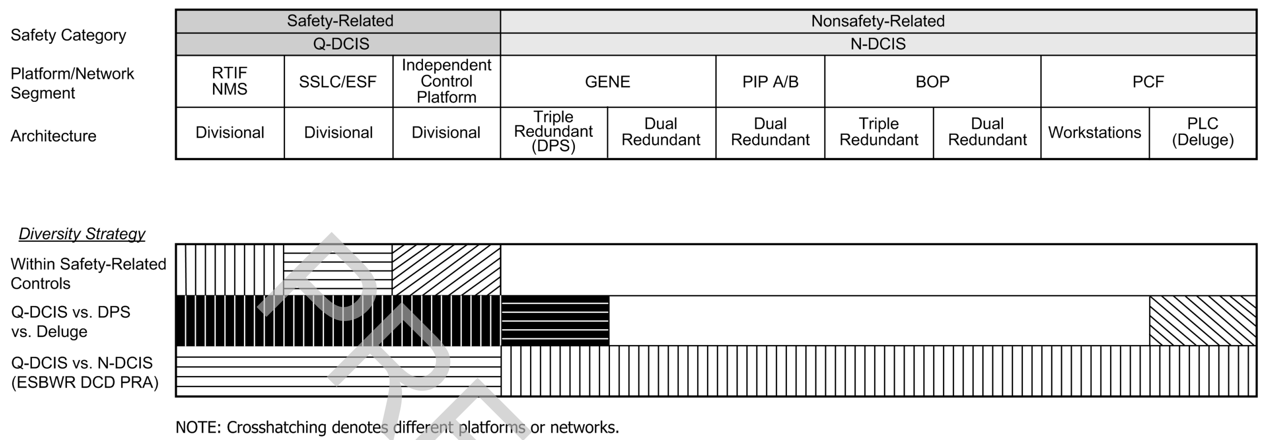


Figure 7.1-4. ESBWR Hardware/Software (Architecture) Diversity Diagram

7.2 REACTOR TRIP SYSTEM

The Reactor Trip System includes the Reactor Protection System (RPS), the Neutron Monitoring System (NMS), and the Suppression Pool Temperature Monitoring (SPTM) functions. These systems are discussed below in Subsections 7.2.1, 7.2.2 and 7.2.3, respectively.

7.2.1 Reactor Protection System

7.2.1.1 System Bases

The RPS safety-related design bases are the following:

- To initiate an automatic safe shutdown of the reactor (also known as reactor trip) by means of rapid hydraulic insertion of all control rods (scram) when:
  - Anticipated operational occurrences (AOO) (transient) anomalous states occur, which potentially impair reactor safety; and
  - Errors in operation take place resulting in transients that potentially impair reactor safety.
- To initiate reactor power reduction and safe shutdown of the reactor by means of rapid hydraulic insertion of a predefined group of the control rods when necessary for rapid reactor power reduction. Several groups can be defined and scrammed in sequence. This feature is called Select Rod Insert (SRI) and is initiated by reliable signals from the Diverse Protection System (DPS).
- To provide timely protection against the onset and effects of conditions threatening the integrity of the reactor fuel barriers, the reactor coolant pressure boundary (RCPB), or containment vessel pressure boundary. This limits the uncontrolled release of radioactive materials from the fuel assembly or the RCPB. Also to provide such protection against conditions that threaten important plant equipment integrity.
- To initiate an automatic reactor trip whenever monitored process variables exceed or fall below their specified trip setpoints based on values determined by AOO, accident analyses, and instrument setpoint calculation methodology.
- To provide control switches for initiation of manual reactor scram by the plant operator when necessary.
- To provide reactor mode selection for enabling the appropriate instrument channel trip functions required in a particular mode of plant operation. Mode selection also provides for bypassing instrument channel trip functions that are not required and for establishing other necessary interlocks associated with the major plant operating modes.
- To provide selective automatic and manual operational trip bypasses, as necessary, to permit proper plant operations. These bypasses allow for protection requirements depending upon specific existing or subsequent reactor operating conditions.
- To provide seal-in of specific trip logic paths after trip conditions have been satisfied and to inhibit the trip reset, as necessary, to ensure subsequent required protective action sequences are completed.

- To provide manual reset capability permitting restoration of the RPS and other affected systems to their normal operational status following seal-in of any trip logic path or after a full reactor scram.
- To provide isolated outputs to other systems sharing instrument channel signals with the RPS, using trip signals generated by the RPS, or requiring other indications of specific RPS status for their inputs.
- To provide isolated outputs to appropriate warning, trip, or bypass alarm annunciators to operator displays (for example, flat panel or cathode ray tube [CRT] displays) and to the plant computer functions (PCF) of the Nonsafety-related Distributed Control and Information System (N-DCIS).
- To provide means for calibration and adjustment of trip function setpoints and to provide sufficient controls to permit surveillance and post-maintenance testing of RPS equipment.

The following bases ensure that the RPS is designed with sufficient reliability:

- Single failures, bypasses, repairs, calibration, or adjustments do not impair the normal protective functions of the RPS and do not result in inadvertent reactor scram or insertion of control rods. The RPS is capable of accomplishing its protection functions in the presence of any single failure within the RPS (with any three of the four divisions of safety-related power available), any failures caused by a single failure, and any failure caused by any design basis event requiring RPS protective action.
- The RPS is designed to cause reactor scram even during system shutdown and loss of electrical power sources.
- The RPS fails into a safe state if conditions such as disconnection of the system (or portions of the system), loss of electrical power, or adverse environment are experienced.
- Loss of a single power source directly associated with RPS equipment and protection functions does not cause instrument channel trips, division trips, or scram solenoid de-energization resulting in full reactor scram or insertion of any control rod.
- Once initiated, RPS protective actions continue in their intended sequence until completion of hydraulic control rod insertion. The RPS trip is sealed-in and can only be reset manually. All manual resets are automatically inhibited for 10 seconds to allow sufficient time for scram completion.
- The RPS has built-in redundancy in its design that fulfills the reliability and availability requirements of the system.
- The RPS has bypass capability for failed portions of each division's equipment without degrading operability.
- A separate and diverse manual trip function is provided through the use of two manual-trip switches. Actuation of both manual-trip switches is required for a full reactor scram.
- Physical separation and electrical isolation between redundant divisions of the RPS are provided by separate process instrumentation, separate racks, and separate or independent panels and cabling. Separate equipment rooms in the Control Building (CB) perform this function.

The following features reduce the probability that RPS operational reliability is degraded by operator error.

- Access to trip settings, calibration controls, test points, and other terminal points are under the control of Operations supervisory personnel.
- Manual bypass of components is under the control of the main control room (MCR) operator. Any bypass of safety-related parts of the system is continuously alarmed in the MCR. The design does not allow more than one division to be bypassed at a time.
- Selective automatic and manual trip bypasses are provided to permit proper plant operation.
- Controls for manual initiation of reactor scram by the plant operator are provided.
- A Reactor Mode Switch is provided to select the plant operation mode. This switch sends bypass and interlock signals to the RPS, instruments, and hardware.

7.2.1.2 System Description

7.2.1.2.1 Reactor Protection System Identification

The RPS is the overall complex of instrument channels, trip logics, trip actuators, manual controls, and scram logic circuitry. This complex initiates rapid insertion of control rods to shut down the reactor when situations and circumstances arise that could result in unsafe reactor operating conditions. The RPS also establishes appropriate interlocks for different reactor operating modes and provides status and control signals to other systems and alarms.

To accomplish its overall function, the RPS interfaces with the:

- Safety-Related Distributed Control & Information System (Q-DCIS),
- Safety System Logic and Control / Engineered Safety Features (SSLC/ESF),
- NMS,
- Nuclear Boiler System (NBS),
- Control Rod Drive (CRD) System,
- Containment Monitoring System (CMS) (including the SPTM function),
- Rod Control and Information System (RC&IS),
- Leak Detection and Isolation System (LD&IS),
- Isolation Condenser System (ICS),
- Steam Bypass and Pressure Control System (SB&PC System),
- Plant Automation System (PAS),
- MCR panels,
- N-DCIS,
- DPS,

- Uninterruptible Alternating Current (AC) Power Supply System, and
- Raceway System.

The RPS hardware/software platform is diverse from SSLC/ESF and DPS. RPS has a separate set of sensors from SSLC/ESF, and a diverse set of sensors from DPS (note that RPS is contained within the RTIF cabinets).

A simplified RPS functional block diagram is provided in Figure 7.2-1; a more detailed diagram representing the RPS data flow and configuration is provided in Figures 7.2-11a and 7.2-11b. A simplified RPS interfaces and boundaries diagram is provided in Figure 7.2-2.

7.2.1.2.2 Reactor Protection System Classification

The RPS is classified as a safety-related system. The functions and components of the RPS are safety-related unless otherwise indicated. The RPS electrical equipment also is classified as Seismic Category I and as IEEE electrical category safety-related.

7.2.1.2.3 Power Sources

AC electric power required by the four divisions of RPS logic is supplied from four pairs of physically separate, electrically independent, uninterruptible, safety-related 120 VAC buses. Either UPS of the divisional power source supports the RPS division. Two divisions of the safety-related 120 VAC also are used as the power sources for the solenoids of the scram pilot valves.

7.2.1.2.4 Reactor Protection System Equipment Design

The RPS is designed to provide reliable, single-failure proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. The RPS satisfies the single-failure criterion even when one entire division of sensors is bypassed and/or when one of the four automatic RPS trip logic systems is out of service (with any three of the four divisions of safety-related AC power available). This is accomplished through the combination of fail-safe equipment design, redundant sensor division trip decision logic, and redundant two-out-of-four trip systems output scram logic. The dual two-out-of-four arrangement used in the RPS design ensures that the single-failure criterion is incorporated.

Equipment within the RPS is designed to fail into a trip-initiating state upon loss of power, loss or disconnection of any input signal, or loss of any internal or external device-to-device connection signal. The failure does not affect trip bypass logic signals or trip bypass permissive logic signals.

The design of the RPS includes two operator-controlled bypasses: the “division of sensors” and the “division of logic (division-out-of-service)” bypasses. These are independently controlled by separate fiber optic “joystick” switches allowing the operator to insert the bypass into only one division at a time. There is no combination of operator bypasses that can reduce the redundancy of the RPS system below the requirements of IEEE Std. 603 Sections 6.7 and 7.5. The system always is able to scram the reactor if any two like and un-bypassed parameters exceed their trip values. The required scram capability is maintained even if the RPS back panel chassis are keylock-disabled (not an operator function).

7.2.1.2.4.1 Arrangement

The RPS-related equipment is divided into four redundant divisions of sensor (instrument) channels, trip logics, and trip actuators as well as two divisions of manual scram controls and scram logic circuitry. The sensor channels, divisions of trip logic, divisions of trip actuators, and associated portions of the divisions of scram logic circuitry together constitute the RPS automatic scram and backup scram initiation logic. The divisions of manual scram controls and associated portions of the divisions of scram logic circuitry together constitute the RPS manual scram and backup scram initiation logic.

The automatic and manual scram initiation logics are independent of each other and use diverse methods and equipment to initiate a reactor scram. A functional equipment arrangement is shown in Figure 7.2-1.

Sensor Channels: Equipment within a sensor channel consists of sensors (transducers or switches), a Digital Trip Module (DTM), and multiplexers. The sensors within each channel detect abnormal operating conditions and send analog (or discrete) output either directly to the RPS cabinets or to the Reactor Trip and Isolation Function (RTIF) Remote Multiplexer Units (RMUs) within the associated division of the Q-DCIS. The RMU within each division performs signal processing including analog to digital conversion, then sends the digital or digitized analog output values of the monitored variables to the DTM for trip determinations within the associated RPS sensor channel in the same division. The DTM in each sensor channel compares individual monitored variable values with trip setpoint values. For each variable the DTM sends a separate trip/no trip output signal to the functional Trip Logic Units (TLU) in the four divisions of trip logic. DTM signals sent from one division to other divisions are isolated optically using fiber-optic cables. The DTMs and TLUs are microprocessor-based modules of the RPS.

The software associated with RPS channel trip and trip system coincident logic decisions installed in these modules is RPS unique. The number of sensors used in the functional performance of the RPS is shown in Table 7.2-1.

Q-DCIS equipment within a single division of sensor channels is powered from the safety-related power source of the same division. However, different pieces of equipment are powered from separate low-voltage DC power supplies within the panels belonging to the same division. Within a sensor channel, the sensors themselves are components of the RPS or components of an interfacing system. Signal conditioning and distribution performed by the RMUs are functions of the Q-DCIS.

Components within each of the four RPS sensor channels are separated physically and are independent from components of other sensor channels. The RPS equipment is independent and physically separated from other safety-related or nonsafety-related systems fulfilling the requirements of IEEE Std. 603, Section 5.6.

Any signal communication between the RPS and other systems is through the required safety-related isolation devices (the safety-related fiber optic communication interface modules [CIMs]). There are no signal inputs from other systems affecting the safety function of the RPS. The application of this nonsafety-to-safety interface is described in Subsection 7.1.3.3. The transfer of data between the safety-related system and nonsafety-related system is one-way.y

Divisions of Trip Logic: Equipment within an RPS division of trip logic consists of TLUs, manual switches, Bypass Units (BPUs), and Output Logic Units (OLUs).

The TLUs perform the automatic scram initiation logic checking for two-out-of-four coincidence of trip conditions in any set of instrument channel signals coming from the four divisions of DTMs, or when a NMS-isolated digital trip signal (voted two-out-of-four in the NMS TLU) is received. The automatic scram initiation logic for any trip is based on the reactor operating mode switch status, channel trip conditions, NMS trip input, and bypass conditions. Each TLU, in addition to receiving the signals described above, also receives digital input signals from the BPU and other control interfaces in the same division. Signals from one RPS division to another RPS division are isolated optically using fiber optic cables.

The various manual switches provide the operator with the means to enforce interlocks within RPS trip logic for special operation, maintenance, testing, and system reset. The BPUs perform bypass and interlock logic for the division of channel sensors bypass and the division of logic bypass. Each RTIF BPU sends its divisional sensor bypass signal to the TLU of the same division and an isolated divisional sensor bypass signal to the TLUs of the other three divisions. Each RTIF BPU sends its divisional logic bypass signal to the OLUs of the same division and an isolated divisional logic bypass signal to the OLUs of the other three divisions.

The OLUs perform division trip, seal-in, reset, and trip test functions. Each OLU receives bypass inputs from the RTIF BPU and trip inputs from the TLU of the same division. Each OLU provides trip outputs to the trip actuators.

Equipment within a division of trip logic is powered from the same division of safety-related power source. However, different pieces of equipment are powered from separate low-voltage DC power supplies in the same division.

Divisions of Trip Actuators: Equipment within a division of trip actuators includes load drivers for automatic primary scram and initiation of backup scram. The RPS includes two physically separate and electrically independent divisions of trip actuators receiving inputs from the four divisions of the OLU. The load drivers are isolated, solid-state, current-interrupting devices with fast response times and are used for the primary scram actuators. The primary scram actuators are powered by 120 VAC and can tolerate the high current levels associated with Hydraulic Control Unit (HCU) scram solenoid operation.

The operation of the load drivers is such that a trip signal on the input side creates a high impedance current-interrupting condition on the output side. The output side of each load driver is isolated electrically from its input signal. The load driver outputs are arranged in the primary scram logic circuitry between the scram solenoids and scram solenoid 120 VAC power source. When in a tripped state, the load drivers cause the scram solenoids (scram initiation) to de-energize. The load drivers within a division interconnect with the OLU of all other divisions to form a special arrangement (connected in series and in parallel in two separate groups) that results in two-out-of-four scram logic. Reactor scram occurs if load drivers associated with any two or more divisions receive trip signals from the OLUs (Refer to Figure 7.2-1).

Output contactors are used for backup scram actuators, scram–follow initiation, and scram reset permissive actuators. When in a tripped state, the output contactors for backup scram cause the valve solenoids to energize. The output contactors of the backup scram are arranged in a two-out-of four configuration similar to that described above for the primary scram load drivers. Backup scram is separate and independent in power source and function from primary scram.

Divisions of Manual Scram Controls: Equipment within a division of manual scram controls includes manual switches, contactors, and relays providing an alternate, diverse, manual means to initiate a scram and backup scram. Each division's manual scram function controls the power sources to the same division of scram logic circuitry for scram initiation and division of scram logic circuitry for backup scram initiation.

Divisions of Scram Logic Circuitry: The two divisions of primary scram logic circuitry are powered from independent and separate power sources. One of the two divisions of scram logic circuitry distributes Division 1 safety-related 120 VAC power to the A solenoids of the HCUs. The other division of scram logic circuitry distributes Division 2 safety-related 120 VAC power to the B solenoids of the HCUs. The HCUs (including the scram pilot valves and the scram valves) are components of the CRD System. A full scram of control rods associated with a particular HCU occurs when both A and B solenoids of the HCU are de-energized. The arrangement of equipment groups within the RPS from sensors to actuator loads is shown in Figure 7.2-1. The RPS interfaces and boundaries with other systems are shown in Figure 7.2-2.

7.2.1.2.4.2 Initiating Circuits

The RPS logic initiates a reactor scram in the individual sensor channels when any one or more of the conditions listed below exist. The system monitoring the associated process condition is found in the system indicated in parentheses. These conditions are:

- High drywell pressure (CMS),
- Turbine stop valve (TSV) closure (RPS),
- Turbine control valve (TCV) fast closure (RPS),
- NMS-monitored SRNM and APRM conditions exceed acceptable limits (NMS),
- High reactor pressure (NBS),
- Low reactor pressure vessel (RPV) water level (Level 3) decreasing (NBS),
- High RPV water level (Level 8) increasing (NBS),
- Main steam line isolation valve (MSIV) closure (Run mode only) (NBS),
- Scram accumulator charging water header pressure – low-low (CRD),
- High suppression pool temperature (CMS),
- High condenser pressure (RPS),
- Power generation bus loss (Loss of all feedwater [FW] flow)(Run mode only) (RPS),
- High simulated thermal power (FW temperature biased) (NBS and NMS),
- Feedwater temperature exceeding allowable simulated thermal power vs. FW temperature domain (NBS),
- Operator-initiated manual scram (RPS), and

- Reactor Mode Switch in Shutdown position (RPS).

With the exception of the NMS outputs, the MSIV closure, TSV closure and TCV fast-closure, loss of all FW flow due to a power generation bus loss, main condenser pressure high, and manual scram outputs, systems provide sensor outputs through the RTIF RMU.

The MSIV Closure, TSV closure and TCV fast-closure, loss of all FW flow due to a power generation bus loss, manual scram output, and main condenser pressure high signals are provided to the RPS through hardwired connections. The NMS trip signal is provided to the RPS through fiber optic cable. The systems and equipment providing trip and scram initiating inputs to the RPS for these conditions are discussed in the following subsections.

Neutron Monitoring System

The separate and isolated NMS digital Startup Range Neutron Monitor (SRNM) trip signals, and Average Power Range Monitor (APRM) trip signals from each of the four divisions of the NMS equipment are provided to their divisions of RPS trip logic as shown on Figure 7.2-1.

SRNM Trip Signals: The safety-related SRNM subsystem provides trip signals to the RPS to cover the range of plant operation from source range through startup range (more than 10% of reactor rated power). Three SRNM conditions, monitored as a function of the NMS, comprise the SRNM trip logic output to the RPS. These conditions are:

- SRNM upscale (high count rate),
- Short (fast) period, and
- SRNM inoperative.

The three trip conditions from every SRNM associated with a NMS division are combined into a single SRNM trip signal for that division. The specific condition causing the SRNM trip output state is identified by the NMS, and is not detectable within the RPS. The SRNM trip functions are summarized in Table 7.2-2. SRNM trip signals are summarized in Table 7.2-3.

APRM Trip Signals: The APRM trip signals cover the range of plant operation from a few percent of reactor rated power to greater than rated power. Three APRM conditions, monitored as a function of the NMS, comprise the APRM trip logic output to the RPS. These conditions are:

- APRM high thermal neutron flux,
- High simulated reactor thermal power, and
- APRM inoperative.

The APRM trip functions are summarized in Table 7.2-4.

Within the safety-related APRM subsystem there is the Oscillation Power Range Monitor (OPRM) function, which is capable of generating a trip signal in response to core thermal neutron flux oscillation conditions, and thermal-hydraulic instability fast enough to prevent cladding thermal limit violation and fuel damage. This OPRM trip signal is combined with the other three APRM trip signals to form the final APRM trip signal to the RPS. The NMS also provides the RPS with a simulated reactor thermal power signal to support the load rejection bypass algorithm.

Nuclear Boiler System

Reactor Pressure: Reactor pressure is measured by four physically separate pressure transmitters mounted on separate divisional local racks in the safety envelope within the Reactor Building (RB). Each transmitter is on a separate instrument line and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate RTIF DTM in one of the four RPS divisional sensor channels. The four pressure transmitters and associated instrument lines are components of the NBS.

Reactor Pressure Vessel Water Level: RPV water level is measured by four physically separate level (differential pressure) transmitters mounted on separate divisional local racks in the safety envelope within the RB. Each transmitter is on a separate pair of instrument lines and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate DTM in one of the four RPS divisional sensor channels. The four separate level transmitters and associated instrument lines are components of the NBS.

Main Steamline Isolation Valve Closure: Each of the four Main Steam Lines (MSLs) can be isolated by closing either its inboard or outboard isolation valve. Position (limit) switches are mounted on both isolation valves of each MSL. These switches provide output to the appropriate DTM or RMU in one of the four RPS divisional trip channels using hard-wired connections. On each MSL, two position switches are mounted on each inboard isolation valve and each outboard isolation valve. Each of the two position switches on any one MSL isolation valve is associated with a different RPS divisional sensor channel. A reactor scram is initiated by either the inboard or outboard valve closure on two or more of the MSLs. The eight MSIVs and the 16 position switches supplied with these valves (for RPS use) are components of the NBS.

Feedwater Temperature Biased Simulated Thermal Power: FW temperature is measured by four separate temperature sensors mounted on each FW line in the MSL tunnel area within the RB. Each sensor is connected to a separate channel and is associated with a separate RPS electrical division. Each sensor provides a temperature signal to the RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate RTIF DTM. The eight temperature sensors (four on each FW line) are components of the NBS. The RPS uses FW temperature from NBS to develop a Simulated Thermal Power high setpoint that is a function of FW temperature.

Simulated Thermal Power Biased Feedwater Temperature: The RPS uses the Simulated Thermal Power signal from NMS and feedwater temperature from NBS as described in the paragraph above to generate a high/low feedwater temperature setpoint that is a function of Simulated Thermal Power. The RPS initiates a scram when the FW temperature further departs from the area allowed by the thermal power vs. FW temperature domain.

Control Rod Drive System

Locally mounted pressure transmitters measure the scram accumulator charging water header pressure at four physically separate locations. Each transmitter is associated with a separate RPS division and is on a separate instrument line. Each transmitter provides an analog output signal to the RMU, which digitizes and conditions the signal before sending it to the appropriate DTM (in one of the four RPS divisional trip channels). The four pressure transmitters and associated instrument lines are components of the CRD System. This is an anticipatory scram because it initiates a scram before the scram accumulators have time to depressurize.

Reactor Protection System

Turbine Stop Valve Closure: TSV closure is detected by separate valve stem position switches on each of the four valves. Each position switch provides an open/close contact output signal through hard-wired connections to the DTM in one of the four RPS divisional trip channels. The TSV closure trip occurs in each division of trip logic when any two or more position switches detect the TSV closure. The TSVs are components of the main turbine. The position switches are components of the RPS.

Turbine Control Valve Fast Closure: Low oil pressure in the hydraulic trip system, which is indicative of TCV fast-closure, is detected by separate pressure transmitters on each of the four TCV hydraulic mechanisms. Each pressure transmitter provides a 4 - 20 mA signal through hard-wired connections to the DTM in each of the four RPS divisional trip channels. The TCV closure trip occurs in each division of trip logic when any two or more sensor channels detect low oil pressure in the hydraulic trip system. The TCV hydraulic mechanisms are components of the main turbine. The pressure transmitters are components of the RPS.

Turbine Bypass Valve Position: The Turbine Bypass Valves (TBV) provide position limit switch inputs to the RPS as a permissive to inhibit reactor trip on TSV closure or TCV fast closure if the TBVs open to their 10% position within a defined period of time. One switch with four sets of contacts is mounted on each valve. Each contact is associated with one of the four RPS divisions to permit two-out-of-four logic. The position switches are components of the RPS.

High Condenser Pressure: High condenser pressure is detected by separate pressure transmitters mounted on the main condenser. Each pressure transmitter provides an analog output signal through hard-wired connections to the DTM in each of the four RPS divisional trip channels. The pressure transmitters are components of the RPS. The reactor scram at high condenser pressure shuts off steam flow to the main condenser and protects the main turbine. This is an anticipatory scram in that high condenser pressure also trips the main turbine and prevents TBV operation.

Power Generation Bus Loss (Loss of All Feedwater Flow Event): The plant electrical system has four power generation buses operating at 13.8 kV. Although all four buses are normally energized, the loads on these buses are arranged such that any three of the four buses can support the necessary FW pumps required for power generation. Specifically, these buses supply power for the FW pumps and circulating water pumps. In the Run mode at least three of the four buses must be powered.

If the sensor (one per division) on each bus detects a low voltage, indicating that less than three buses are operating, the two-out-of-four logic initiates a scram after a preset delay time. This delay time (less than one second) is to allow the auto transfer from the Unit Auxiliary Transformer (UAT) feed to the Reserve Auxiliary Transformer (RAT) feed to restore normal bus voltages. Loss of more than one power generation bus is indicative of loss of the FW pumps and flow. It is also indicative of loss of condenser vacuum from the loss of the circulating water pumps.

This is an anticipatory scram on loss of the power generation buses to mitigate the RPV water level drop to Level 1 following the loss of FW pump function. This scram terminates additional steam production within the RPV before Level 3 is reached.

Manual Scram: Two manual scram switches and the Reactor Mode Switch provide diverse means to initiate manually a reactor scram independent of conditions within the sensor channels, divisions of trip logic, and trip actuators. When the Reactor Mode Switch is placed in the shutdown position, power to the circuits affected by each manual scram pushbutton is interrupted resulting in a full scram. Each of the manual scram switches is associated with one of the two divisions of actuator load power. Both manual scram switches have to be actuated simultaneously to result in a full manual scram. Because the non-software-based manual scram capability of the RPS system operates directly on the scram solenoid power, only Divisions 1 and 2 are involved. If either of those two divisions is out of service (including maintenance), a half-scram results; depressing the other division manual scram pushbutton then results in a full scram. If either of the two divisions is out of service for non-power issues the manual scram capability remains unaffected. The operability of Divisions 3 and 4 has no effect on the RPS manual scram capability.

Manual scram switches also are provided in the Remote Shutdown System (RSS) panels to achieve hot shutdown for the reactor from outside the MCR. There is a separate manual switch in each of the four divisions providing a means to manually trip all actuators in that division. An alternative manual scram can be accomplished by activating any two (or more) of the four manual divisional trip switches.

Reset Logic: A reset switch is provided to reset the manual scram in both (1 and 2) divisions of manual scram controls. A separate manual switch associated with each division of trip actuators provides the means to reset the seal-in at the input of all trip actuators in the same division. The reset does not have any effect if the conditions that caused the division trip have not cleared when a reset is attempted. All manual resets are automatically inhibited for 10 seconds to allow sufficient time for scram completion. The switch used to reset the manual scram circuitry permits resetting of the several scram groups in sequence, so re-energization of only one-half of the scram solenoids is performed at one time.

After a full scram the scram accumulator charging water header pressure drops below the trip setpoint, resulting in a trip initiating input to all four divisions of trip logic. While this condition exists, the four divisions of trip logic cannot be reset until the scram accumulator charging water header pressure trip is manually bypassed in all four divisions, and all other trip-initiating conditions have been cleared.

Containment Monitoring System

Drywell Pressure: Containment (drywell) pressure is measured at four physically separate locations by pressure transmitters located on separate divisional local racks in the safety envelope within the RB. Each transmitter is on a separate instrument line and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the RMU, which digitizes and conditions the signal before sending it to the appropriate DTM in the four RPS divisional trip channels. The four pressure transmitters and associated instrument lines are components of the CMS.

Suppression Pool Temperature: Four channels of safety-related divisional suppression pool temperature signals, each formed by the average value of a group of 16 thermocouples installed uniformly (both vertically and azimuthally) inside the suppression pool, provide the suppression pool temperature data for automatic scram initiation. For the suppression pool temperature high signal to be considered valid, 12 of the 16 assigned thermocouples are required to be operable. When the established limits of high temperature are exceeded in two of the four divisions, scram initiation is generated.

Each temperature sensor provides an analog output signal to the RMU, which digitizes and conditions the signal before sending it to the appropriate DTM. The temperature sensors and associated instrument lines are components of the CMS. The suppression pool water level signals also are provided. When water level drops below any of the temperature sensors, the exposed sensors are logically bypassed, so only the sensors below water level are used to determine the averaged temperature signal to the RPS.

7.2.1.2.4.3 Reactor Protection System Outputs to Interfacing Systems

Scram Signals to the CRD System: Reactor trip conditions existing in any two or more of the four RPS automatic trip channels and/or in both RPS manual trip channels cause power to the output circuits of the RPS (normally supplying power to the solenoids of the scram pilot valves of the CRD system) to be disconnected, resulting in insertion of all control rods and reactor shutdown.

When the scram pilot valve solenoids are disconnected from power by the RPS trip signals, the two backup scram valves of the CRD system are actuated by the RPS trip signals to exhaust the air from the scram air header, resulting in backup scram action.

RPS Status Outputs to the NMS: Two types of RPS status condition signals (four combined signals each, one per division) are provided to the NMS by the RPS. Isolated output signals, indicating that the Reactor Mode Switch is in the Run position, are provided to the four divisions of the NMS whenever the mode switch is in that position. These signals are used by the NMS to bypass the NMS SRNM alarm and trip function, whenever the Reactor Mode Switch is in the Run position.

Scram Follow Signals to the RC&IS: Upon the occurrence of any full reactor scram condition the RPS provides isolated output signals to the RC&IS. This enables automatic rod run-in (scram-follow) logic in the RC&IS to cause full insertion (or "run-in") of the fine motion control rod drives subsequent to scram. The RPS also provides the RC&IS with both scram test switch status, indicating the start of a rod pair scram test and the position of the Reactor Mode Switch.

Rod Block Signals to the RC&IS: Rod withdrawal inhibit signals (one for each channel) are provided by the RPS via isolated output signals sent to the RC&IS whenever there is a "Scram Accumulator Charging Water Header Pressure - Low" trip signal or when any scram accumulator charging water header pressure trip bypass switch is in the Bypass position.

Outputs to the LD&IS: The Reactor Mode Switch status signals from each division are provided to the LD&IS for RCPB isolation function. The RPS also provides an interlock to the LD&IS for bypassing the MSIV isolation (when the Reactor Mode Switch is not in the Run position) that otherwise would result from high main condenser vacuum-pressure and/or low inlet-pressure to the turbine during startup and shutdown.

Outputs to Main Control Room Panels:

Safety-related status and alarm signals are sent from the RPS to the MCR console.

Displays: Instrument channel sensor checks are capable of being performed at the MCR console. Displays exist for readout and comparison of the current values of the variables or separate processes being monitored for each set of four (one per division). The minimum set of signals included in displays related to RPS scram variables are:

- Reactor vessel pressure,
- RPV water levels,
- Containment drywell pressures,
- Scram accumulator charging water header pressures,
- Suppression pool (local or bulk) temperatures,
- Power generation bus voltages,
- FW temperature,
- TSV position,
- Hydraulic Trip System oil pressure,
- MSIV position,
- Main condenser pressure, and
- NMS outputs.

The values of all scram parameters are continuously sent through the required safety-related isolation to the N-DCIS where displays of the scram parameters from all divisions are integrated to allow easy comparison between divisions. Additionally, the PCF and alarm systems alarm if any divisional parameter value differs from the value in the other three divisions by more than a predetermined amount. The intent is that channel sensor checks be performed continuously.

Alarms: Alarms are provided at the MCR console by the trip condition of any of the four sensor trip channels, by the trip condition of each automatic or manual trip system, and when bypassing a scram function. The alarm function is provided through the required safety-related isolation to the PCF.

The provided alarms / indications related to RPS status are:

- RPS NMS trip (generated in NMS),
- Reactor vessel pressure high,
- RPV water level low (≤ Level 3),
- RPV water level high (≥ Level 8),
- Containment (drywell) pressure high,
- MSIV closure trip,
- TSV closure,

- TCV fast closure,
- Main condenser pressure high,
- Power generation bus loss (loss of all FW flow),
- FW temperature biased Simulator Thermal Power trip,
- Scram accumulator charging water header pressure - low,
- Suppression pool temperature high,
- RPS divisional automatic trip (auto-scram) (each of the four: Div. 1, 2, 3, 4 automatic trip),
- RPS divisional manual trip (each of the four: Div. 1, 2, 3, 4 manual trip),
- Manual scram trip (two: both Manual A and Manual B),
- Reactor Mode Switch in Shutdown position,
- Shutdown mode trip bypassed,
- Non-coincident NMS trip mode in effect (in NMS),
- NMS trip mode selection switch still in non-coincident position, with Reactor Mode Switch in Run position (in NMS),
- Division in which channel A (B, C, or D) sensors are bypassed (four),
- Trip conditions in Channel A (B, C, or D) and Channel A (B, C, or D) sensors bypassed (four),
- Division 1 (2, 3, or 4) TLU out-of-service bypass (four),
- Scram accumulator charging water header pressure - low-low trip bypass,
- Any scram accumulator charging water header pressure trip with bypass switch still in bypass position and the Reactor Mode Switch in Startup or Run mode,
- Auto-scram test switch in test mode (manual trip of automatic logic) (four),
- TSV closure trip bypassed,
- TCV fast closure trip bypassed,
- MSIV closure trip bypassed,
- NMS SRNM trip bypassed with the Reactor Mode Switch in Run position,
- Non-coincident NMS trip bypassed with the Reactor Mode Switch in Run position,
- RPV water level high trip bypassed,
- Condenser pressure high trip bypassed,
- FW temperature biased Simulated Thermal Power Trip (STPT) bypassed,
- Special MSIV operation bypassed, and

- Power generation bus loss trip bypassed..

The above RPS displays and alarms meet the information display requirements of IEEE Std. 603, Section 5.8.

Outputs to Nonsafety-Related DCIS (Plant Computer Functions): The PCF maintains logs of the tripped, bypassed, and reset conditions of the RPS instrument channels, divisions of logic, divisions of trip actuators, and scram logic circuitry as well as tripped and reset conditions of RPS automatic and manual trip systems from the RPS through the required safety-related isolation to the N-DCIS. For conditions causing reactor trip the N-DCIS identifies the specific trip variable, the affected divisional channel identity, and the specific automatic or manual trip system. These signals also are provided to the sequence of events (SOE) function of the PCF.

Outputs to the Isolation Condenser System: Reactor Mode Switch status (that is, Run/Not Run indications) from the four divisions is provided by the RPS to the ICS to be used as automatic operation signal permissives or inhibits. Automatic operation signal permissives are generated whenever the Reactor Mode Switch is placed in the Run position, and automatic operation signal inhibits are generated whenever the Reactor Mode Switch is placed in any of its remaining three positions.

Outputs to the Plant Automation System: The RPS provides the PAS with separate signals to indicate the position of the Reactor Mode Switch. The RPS also provides the auto scram signal from the OLU to the PAS.

Uninterruptible AC Power Supply: The AC electric power required by the four divisions of RPS logic is delivered from four pairs of physically separate and electrically independent uninterruptible safety-related 120 VAC buses. The power circuits of the "A" and "B" solenoids of the scram pilot valves are powered from two of the four divisional pairs of 120 VAC UPS.

7.2.1.2.4.4 System Logic Architecture and Redundancy

The basic system architecture of the RPS ensures reliable processing of sensed plant variables by employing four independent trip logic systems in four separate divisions of safety-related protection equipment. Figure 7.2-1 illustrates the basic RPS functional arrangement.

Each divisional trip system processes the trip decisions of plant sensor inputs from the four divisions using two-out-of-four coincidence to confirm the final trip state for each variable in each division. Automatic reactor trip outputs from each system to the final actuators are also confirmed by two-out-of-four coincidence of division trip outputs. A separate and diverse manual trip method is provided in the form of two independent manual trip channels. Actuation of both manual trip systems is required for a full reactor scram. Availability is enhanced because any one division can be bypassed at one time to allow online repair without degrading operability. This satisfies the repair requirement of IEEE Std. 603, Section 5.10 while maintaining plant availability.

The RPS consists of four redundant divisions identical in design and independent in operation. Although each division constitutes a separate trip system, normally each division can make two-out-of-four trip decisions with or without a division of sensors being bypassed. There are four instrument channels provided for each process variable being monitored, one for each RPS division. Four sensors, one per division, are provided for each variable. When more than four sensors are required to monitor a variable the outputs of the sensors are combined into only four instrument channels. The logic in each division does not depend on absolute time of day and is asynchronous with respect to the other divisions. No division depends on the correct operation of another division. There is no combination of MCR-initiated bypasses that can unacceptably degrade the RPS.

Figures 7.2-1, 7.2-11a, and 7.2-11b provide a more detailed view of the RTIF (which includes the RPS) configuration and communication paths.

The RTIF is implemented with two communication methodologies: "point-to-point" optical fiber interdivisional communication and a shared memory ring network. Point-to-point communication is limited to trip and bypass information and any necessary message authentication. Point-to-point fiber is also used for TLU to OLU, RTIF to NMS and RTIF to SSLC/ESF communication. Since the RTIF is "fail safe" the loss of any communication or fiber will be interpreted as a trip. The other communication methodology uses a shared memory ring network that extends between the various RPS system chassis. The processors of each chassis ("nodes") connected to the ring can read the entire shared memory on the communications (CIM) card and write only to a designated portion of the CIM card. The data on the ring are actively transported between one chassis transmitter and another's receiver until all nodes have been updated. To increase reliability, another ring (forming a counter-rotating ring) is provided with the data going in the opposite direction, this scheme allows both rings to be broken between two nodes and all data still gets to all nodes; no single failure will prevent data transmission.

There are two "counter rotating" rings within each division of RTIF. The upper ring on Figure 7.2-11a interconnects the RMU, DTM, TLU and Q-CIM which are the only chassis needed to support the RTIF safety functions. This is the (redundant) path by which the RMUs transfer data to the DTMs and, in turn to the TLUs as described above. Note that the BPU is not on the shared memory ring because the BPU is implemented in hardware logic.

There is a second redundant ring that interconnects the above chassis and additionally nonsafety-related "operator" and "maintenance" VDUs in the RTIF and RMU cabinets and on the safety surveillance panel in the MCR (the safety-related function of this VDU is Seismic Category II). Additionally on this ring are two nonsafety-related N-CIM (RTIF N-CIM A and RTIF N-CIM B), each of which has access to the equivalent rings of the other three divisions, and therefore all RTIF divisional data.

The VDUs may be used at any time to monitor RTIF signals and internal diagnostics; however, they cannot input to any of the RTIF chassis for calibration or maintenance purposes unless the chassis or RTIF division has been made "INOP" by a keylock switch. INOP corresponds to a trip unless the division has been bypassed. The INOP status is alarmed.

7.2.1.3 Safety Evaluation

Table 7.1-1 identifies the RPS and the associated codes and standards applied, in accordance with the Standard Review Plan NUREG-0800. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.2.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The RPS conforms to these standards.

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The RPS conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the RPS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.2.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are discussed in Sections 7.2.1.1, 7.2.1.2.4, and 7.2.1.5.2.1.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to the RPS.
  - Section 5.2 (Completion of Protective Actions): See Subsections 7.2.1.1 and 7.2.1.3.4.
  - Section 5.7 (Capability for Test and Calibration): Subsections 7.2.1.4.1 and 7.2.1.4.2 describe testing of the RPS. Additional information can be found in Subsections 7.2.1.3.4, 7.2.1.5.2.2, and 7.2.1.5.11.
  - Section 6.2 and 7.2 (Manual Control): See Subsections 7.2.1 1 and 7.2.1.3.4 for discussion of RPS manual control.
  - Section 6.4 (Derivation of System Inputs): The two RPS sensing inputs that are not direct measures of the variables are the RPV water level and the loss of feedwater flow in the RPS scram logics. The RPV water level is measured by the differential pressure derived from the sensing line with a reference point. This method is a proven technology in the boiling water reactor (BWR) applications. The loss of the feedwater flow variable is represented by the loss of the power generation bus signal. When the power to the feedwater pump motor is lost, the feedwater flow is also immediately lost. The use of loss of power generation bus signals to represent the loss of feedwater flow signal meets the requirements of the safety-related analysis of Chapter 15, because it is the only credible way that all feedwater flow can be lost.
  - Section 6.5 (Capability of Test and Calibration): Subsections 7.1.2.1.4.1 and 7.2.1.4.2 describe testing of the RPS. Additional information can be found in subsections 7.2.1.3.4, 7.2.1.5.2.2, and 7.2.1.5.11.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the RPS are described in Subsections 7.2.1.2.4.1 and 7.2.1.5.2.1.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the RPS are described in Subsections 7.2.1.2.4 and 7.2.1.5.2.2.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the RPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the RPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The RPS design conforms to these requirements.

10 CFR 50.34(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The RPS design of bypass and inoperable status indication conforms to these requirements and is consistent with the conformance of the RPS design to RG 1.47.

10 CFR 50.34(f)(2)(xxi)[II.K.1.22], Auxiliary Heat Removal Systems:

- Conformance: The RPS conforms to these requirements.

10 CFR 50.34(f)(2)(xxiii)[II.K.2.10], Anticipatory Reactor Trip:

- Conformance: The reactor will trip in response to a Loss of All Feedwater Flow Event. This is an anticipatory trip actuated on a power generation bus loss event. The reactor will also trip on a turbine trip only if an insufficient number of bypass valves opens within a prescribed time period.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The RPS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The RPS conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the RPS within the DCD documents conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.2.1.3.2 General Design Criteria

GDC 1, 2, 4, 10, 12, 13, 19, 20, 21, 22, 23, 24, 25, 26, 27 and 29:

- Conformance: The RPS design conforms to these GDC.

7.2.1.3.3 Staff Requirements Memorandum

Item II.Q of SECY-93-087, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The Reactor Trip (Protection) System design conforms to Item II.Q of SECY-93-087 NRC Branch Technical Position (BTP HICB-19) by the implementation of an additional Diverse Instrumentation and Control System described in Section 7.8.

7.2.1.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions - This includes conformance to BTP HICB-8:

- Conformance: The system is capable of being tested, from sensor device to final actuator device, during plant operation. The tests must be performed in overlapping stages so an actual reactor scram would not occur as a result of the testing.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems**:**

- Conformance: Automatic indication that a system is out of service is provided in the MCR. Indicators show which part of a system is not operable and which division is bypassed. Annunciator test switches are provided in the MCR.

  Individual indicators are arranged together in the MCR to indicate which function of the system is out of service, bypassed, or otherwise inoperable. These automatic indicators remain available, and cannot be cleared until the function is operable.

  A manual switch or push button is provided for manual bypass actuation, which annunciates out-of-service conditions.

  These display provisions serve to supplement administrative controls and aid the operator in assessing the availability of component and system-level protective actions. These displays do not perform a safety-related function.

  System out-of-service alarm circuits are electrically isolated from the plant safety-related systems to prevent adverse effects.

  Testing is included on a periodic basis when equipment associated with the display is tested.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems:

- Conformance: The RPS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy for the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related systems designs' conformance to the single-failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: Means are provided for manual initiation of reactor scram through the use of two control switches and the Reactor Mode Switch. Reactor scram is accomplished by operation of both pushbutton switches, or by placing the Reactor Mode Switch in the Shutdown position. These controls are located on the MCR console.

The common equipment required for initiation of both manual scram and automatic scram is limited to actuator load power sources, actuator loads, and cabling between the two. There is no shared trip or scram logic equipment for manual scram and automatic scram. No single failure in the manual, automatic, or common portions of the protection system would prevent initiation of reactor scram by manual or automatic means.

Manual initiation of reactor scram, once initiated, goes to completion as required by IEEE Std. 603, Section 5.2.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The RPS design complies with the criteria set forth in IEEE Std. 603, Section 5.6, and RG 1.75. Safety-related circuits and safety-related associated circuits are identified and separated from redundant and nonsafety-related circuits. Isolation devices are provided where an interface exists between redundant safety-related divisions and between safety-related or safety-related associated circuits and nonsafety-related circuits. See Subsection 8.3.1.4.1 for RPS separation requirements.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The RPS initiation setpoints are consistent with this guide. Reference 7.2-1 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection System:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118. The RPS is designed so its individual elements can periodically and independently be tested to demonstrate system reliability is being maintained. Safety-related RPS equipment allows for inspection and testing during periodic shutdowns and refueling.

RG 1.151, Instrument Sensing Lines:

- Conformance: NBS provides the measurement inputs to RPS. The NBS instrument sensing lines conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design complies with RG 1.152. The hardware and software for the RPS function and other safety-related systems are developed in compliance with RG 1.152, which endorses IEEE Std. 7-4.3.2. The structured development plan for the RPS includes conformance to all software standards referenced in IEEE Std. 7-4.3.2. Hardware and software are integrated into a final assembly validated by testing against input requirements.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The RPS design conforms to 10 CFR 50.55a(h) as implemented on the RTIF platform.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.168 as implemented on the RTIF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.169 as implemented on the RTIF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.170 as implemented on the RTIF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.171 as implemented on the RTIF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.172 as implemented on the RTIF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.173 as implemented on the RTIF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The RPS design conforms to RG 1.180 as implemented on the RTIF platform. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The RPS design conforms to RG 1.209 as implemented on the RTIF platform. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.2.1.3.5 Branch Technical Positions

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The RPS design conforms to BTP HICB-8.

BTP HICB-9, Guidance on Requirements for RPS Anticipatory Trips:

- Conformance: Hardware used to provide trip signals in the RPS is designed in accordance with IEEE Std. 603, Section 5.4 and is considered safety-related and meets the design requirements of BTP HICB-9.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The RPS design conforms to this position as implemented on the RTIF platform. The RPS logics use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

  Certain diverse and hardwired portions of RPS may use coil-to-contact isolation of relays or contactors. This is acceptable according to BTP HICB-11 when the application is analyzed or tested per the guidelines of RG 1.75 and RG 1.153.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The RPS design conforms to BTP HICB-12 as implemented on the RTIF platform. The nominal setpoints are calculated based on the GEH instrument setpoint methodology (Reference 7.2-1). The setpoints are established based on instrument accuracy, calibration capability, and estimated design drift allowance data, and are within the instrument best accuracy range.

- The digital RPS trip setpoints do not drift and any changes are reported to the N-DCIS as alarms. The analog-to-digital converters are self-calibrating, and the RPS uses self-diagnostics, all of which are reported to the N-DCIS through the required safety-related isolation. It is expected that all of the variability in the parameter channel will be attributable to the field sensor. The established setpoints provide margin to fulfill both safety requirements and plant availability objectives.

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

- Conformance: Development of software for the safety-related system functions within RPS conforms to the guidance of BTP HICB-14. Discussion of software development is included in the LTRs [*"ESBWR Software Management Program Manual (SMPM)," NEDO-33226, NEDE-33226P, and "ESBWR Software Quality Assurance Program Manual (SMPM)," NEDO-33245, NEDE-33245P (References 7.2-3 and 7.2-4). Safety-related software (to be embedded in the memory of the RPS logics) is developed according to a structured plan as described in References 7.2-3 and 7.2-4. These plans follow the software life cycle process described in BTP HICB-14.*]*

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in the RPS section content conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The RPS logics conform to BTP HICB-17. Discussions on self-test and surveillance tests of RPS are provided in Subsection 7.2.1.4.

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

- Conformance: Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance of BTP HICB-18. The Q-DCIS is built and qualified specifically for ESBWR applications as safety-related and not as commercial grade programmable logic controllers (PLCs). The embedded and operating system software meet the acceptance criteria contained in BTP HICB-14, for safety-related applications.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087):

- Conformance: The Reactor Trip (Protection) System designs conform to BTP HICB-19 by implementation of an additional diverse instrumentation and control (I&C) system described in Section 7.8 as the DPS.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The real-time performance of RPS in meeting the requirements for safety-related system trip and initiation response conforms to BTP HICB-21 as implemented on the RTIF platform. The real-time performance of the safety-related control system is deterministic based on the Q-DCIS internal and external communication system design and the RPS logic design. Timing signals are neither exchanged between divisions of independent equipment nor between logics within a division.

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7.2.1.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for Chapter 7 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3] and 10 CFR 50.34(f)(2)(xxiii)[II.K.2.10] apply to the RPS and are addressed in Subsection 7.2.1.3.1. TMI action plan requirements are generically addressed in Table 1A-1 of Appendix 1A.

7.2.1.4 Testing and Inspection Requirements

7.2.1.4.1 System Testing: Operational Verifiability

The RPS is designed so its individual operating elements are tested periodically and independently to demonstrate that RPS reliability is maintained.

The RPS design and the design of other systems providing the RPS with instrument channel inputs permit verification of the operational availability of each input sensor used by the RPS with a high degree of confidence even during reactor operation. Channel checks are continuously performed by the PCF.

The instrument channels are calibrated periodically and adjusted to verify that the necessary precision and accuracy are being maintained. Such periodic checking and testing during plant operation is possible without loss of scram capability and without causing an inadvertent scram.

Safety-related sensors are designed with the capability for test and calibration during reactor operation, with the following two exceptions in the RPS:

- MSIV limit switches, and
- TSV limit switches.

These limit switches are not accessible during reactor operation. While they are tested/checked for operability during reactor operation, they cannot be calibrated until the reactor is shutdown.

Safety-related RPS equipment is designed to allow inspection and testing during periodic shutdowns of the nuclear reactor and during refueling shutdowns.

7.2.1.4.2 Surveillance Testing and In-Service Testing

The RPS equipment testing includes:

- Preoperational, startup and refueling/outage inspection testing; and
- In-service and operational surveillance testing.

The RPS is designed to permit testing of an emergency reactor shutdown by methods simulating actual plant operation and duplicating, as closely as possible, the performance of protective actions even during reactor operation. These test methods support in-service verification of scram capability with high reliability. The RPS components and testing strategies are designed so that identifiable failures are detectable. Test methods are designed to facilitate recognition and location of malfunctioning component to allow for the replacement, adjustment, or repair of the component.

In-service testing of the RPS is performed periodically to verify operability during normal plant operation and to ensure that each tested channel can perform its intended design function. The surveillance tests include: (a) instrument channel checks, (b) functional tests, (c) verification of proper sensor and channel calibration, (d) verification of applicable functions in the division of trip logic and division of actuators, and (e) response time tests.

7.2.1.5 Instrumentation and Control Requirements

7.2.1.5.1 Automatic Scram Variables

Refer to Subsection 7.2.1.2.4.2 for discussions of the automatic scram initiating circuits and the systems that apply to them.

7.2.1.5.2 Automatic and Manual Bypass of Selected Scram Functions

7.2.1.5.2.1 Operational Bypasses

Manual or automatic bypass (take out of service) of certain scram functions permits the selection of suitable plant protection conditions during different conditions of reactor operation. These RPS operational bypasses inhibit actuation of those scram functions not required for a specific state of reactor operation.

The conditions of plant operation requiring automatic or manual bypass of certain reactor trip functions are described below.

- Main steam TSV closure and steam governing TCV fast closure trip bypasses: These permit continued reactor operation at low power levels when the TSVs or TCVs are closed. The main steam TSV closure and the steam governing TCV fast closure scram trip functions are automatically bypassed when the APRM simulated thermal power of the NMS is below 40% of the rated thermal power output.

  The TSV closure and TCV fast closure trips are automatically bypassed if a sufficient number of the bypass valves are opened. This bypass occurs if a sufficient number of TBVs open to at least 10% within a preset time limit following the TCV fast closure or TSV closure signal to inhibit reactor trip. The NMS system provides the RPS with an analog simulated thermal power signal used to determine both the low power bypass and the required number of TBV needed to open for a post turbine trip or for full load rejection conditions. The low power bypass is automatically removed and both scram trip functions are enabled at reactor power levels above the bypass setpoint. The bypass permits the RPS to remain in its normal energized state under the specified conditions. This bypass condition is indicated in the MCR.

- Scram accumulator charging water header pressure - low-low bypass**:** This bypass is allowed only when the Reactor Mode Switch is in either the Shutdown or Refuel position. If a bypass of a scram trip is required for scram accumulator charging water header pressure - low-low after a scram has occurred (indicated operational bypass), four administratively controlled trip bypass switches in the MCR permit scram reset.

When the reactor is in the shutdown or refuel mode the scram accumulator charging water header pressure – low-low trip can be bypassed manually in each division of trip logic by separate, manual scram accumulator charging water header pressure trip bypass switches. Control of this bypass is achieved through administrative means using manual bypass switches. This bypass allows RPS reset after a scram, while scram accumulator charging water header pressure is below the trip setpoint. The scram accumulator charging water header pressure – low-low condition would persist until the scram valves are re-closed. Each division of trip logic sends a separate rod withdrawal block signal to the RC&IS when this bypass exists in the division. This operational bypass condition is indicated in the MCR.

The bypass is automatically removed whenever the Reactor Mode Switch is put in either the Startup or Run mode, regardless of whether the scram accumulator charging water header pressure trip bypass switches are in their bypass positions. However, a separate alarm would result in the MCR if any of the switches were left in the bypass position when the Reactor Mode Switch is in either the Startup or Run mode.

- MSIV closure for MSIV bypass (indicated operational bypass): The scram trip for MSIV closure is automatically bypassed in each division whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position - with reactor pressure in the associated sensor channel less than a predetermined setpoint. This bypass condition is alarmed in the MCR and permits plant operation when the MSIVs are closed during low power operation. The bypass is automatically removed if the Reactor Mode Switch is moved to the Run position. This bypass permits the RPS to be placed in its normal energized state for operation at low power levels with the MSIVs either closed or not fully open.
- Special MSIV operational bypass (indicated operational bypass): Four manually-operated bypass switches are made available in the MCR to permit the bypass of trip signals from closed MSIVs on any one of the four main steam lines. This bypass permits continued reactor operation at reduced reactor power and steam flow when one steam line must be isolated for a prolonged period of time. This operational bypass is indicated in the MCR.
- Power generation bus loss trip bypass (indicated operational bypass): The Power Generation Bus Loss (Loss of All Feedwater Flow Event) scram trip function is automatically bypassed whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position. This bypass condition is indicated in the MCR and is automatically removed if the Reactor Mode Switch is moved to the Run position.
- Reactor Mode Switch in Shutdown position bypass (indicated operational bypass): The RPS scram trip caused by the Reactor Mode Switch being placed in the Shutdown position is automatically bypassed after a time delay of approximately 10 seconds. This operational bypass condition permits resetting of the trip actuators and re-energization of the scram pilot valve solenoids and is alarmed in the MCR.
- NMS SRNM scram trip functions with Reactor Mode Switch in the Run position bypass: Whenever the Reactor Mode Switch is in the Run position, SRNM reactor scram trip

functions are automatically bypassed. However, this bypass is not alarmed because it is the normal condition with the Reactor Mode Switch in the Run position. This bypass condition is indicated in the MCR. The SRNM rod block functions also are disabled when the Reactor Mode Switch is in the Run position.

- Non-coincident NMS scram trips in Run mode bypass: Whenever the Reactor Mode Switch is in the Run position it forces the NMS logic to the coincident mode (regardless of the coincident/non-coincident NMS switch position). If any of the coincident/non-coincident NMS trip switches are in the non-coincident position when the Reactor Mode Switch is in the Run position there is an alarm in the MCR. This logic is an NMS function.

  The coincident trip mode is required during reactor startup. The non-coincident NMS trip function is required during initial fuel loading and subsequent refueling operations. During such operations the Reactor Mode Switch is in the Refuel position (or for certain testing conditions, in the Shutdown or Startup positions). A non-coincident NMS trip occurs in each division of trip logic when any single SRNM trip signal is present in the NMS if the coincident/non-coincident manual switch in the division is in the non-coincident position. This logic is an NMS function.

- RPV water level high trip bypass (indicated operational bypass): The RPV water level high trip function is automatically bypassed whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position. This bypass condition is indicated in the MCR and is automatically removed if the Reactor Mode Switch is moved to the Run position.

- Condenser pressure high trip bypass (indicated operational bypass): The condenser pressure high trip function is automatically bypassed whenever the Reactor Mode Switch is in the Shutdown, Refuel, or Startup position. This bypass condition is indicated in the MCR and is automatically removed if the Reactor Mode Switch is moved to the Run position.

- APRM, OPRM, and SRNM scram trips bypasses: These have manual bypass capabilities within the NMS, not the RPS.

7.2.1.5.2.2 Maintenance Bypasses

Manual bypass capability is provided to allow certain portions of RPS-related equipment to be taken out of service for maintenance, repair, or replacement. Maintenance bypasses reduce the degree of redundancy of RPS channels but do not affect or eliminate any scram function. Protective functions are available while any RPS equipment is in maintenance bypass. Except where indicated otherwise, any maintenance bypass generates a status alarm at the MCR operator's console.

The following maintenance bypasses are provided**.**

- Detector inputs (division of sensors) bypass (indicated maintenance bypass): A manually operated bypass switch with interlock capability (for example, a joystick-type switch) is installed in the MCR to bypass (take out of service) the division of sensors trip of one RPS division at a time. Once a bypass of one sensor channel has been established, bypasses of any of the remaining three sensor channels are inhibited. Whenever a division of sensors bypass switch is placed in the bypass position, there is an alarm in the

MCR indicating the bypassed sensor division. The effect of the division of sensors bypass is to convert the two-out-of-four trip to two-out-of-three trip logic. A division of sensors bypass in any division bypasses all trip-initiating input signals from the bypassed division at the DTM trip input to the TLU. Bypassing a division of sensors allows each of the four divisions to determine a two-out-of-three trip. Loss of communication with a bypass switch is interpreted as a “no bypass” signal.

This bypass permits any one of the safety-related RPS components of the input sensor channels of one division to be repaired, replaced, or maintained off-line.

- TLU output (division-out-of-service) bypass (indicated maintenance bypass): A manually-operated bypass switch with interlock capability (for example, a joystick-type switch) is installed in the MCR to bypass the RPS trip output logic of one RPS electrical division at a time. This bypass is effective at the TLU trip input to the OLU and permits the RTIF TLU of the associated division to be repaired, replaced, or maintained off-line. Loss of communication with the bypass switch is interpreted as a “no bypass” signal.

  The interlock ensures that the output signals of only one TLU (of one division) can be bypassed at any one time. Once a bypass of one division of trip logic has been established, bypasses of any of the remaining three division trip logics are inhibited. When a division-out-of-service bypass switch is placed in the bypass position, there is an alarm in the MCR indicating which division is out of service. With a division-out-of-service bypass in effect, the operator still is able manually to trip that division.

- The division-of-sensors maintenance bypass function and the division-out-of-service maintenance bypass function are independent. Thus, bypassing one division of sensors (taken out of service at the sensor channels level) and, simultaneously removing from service the same division or any other division at the RPS trip system level is allowed. In all cases, the RPS system remains able to trip the reactor if any two (or more) un-bypassed parameters exceed their trip values.

7.2.1.5.3 Requirements for Manual Controls

Operator action by means of manual controls is limited to:

- Initiation of scram by manual scram switches;
- Reactor Mode Switch operation (results in scram if placed in the Shutdown position);
- Reset of automatic trip systems after trip input signals clear;
- Reset of manual trip systems (preferably after reset of the automatic trip systems) ;
- Manual bypasses for conditions that are specifically permitted; and
- Manual initiation of selected trip systems or trip actuators using trip logic test switches.

7.2.1.5.4 Reactor Mode Switch

A multi-function, multi-bank, control switch placed on the MCR console provides mode selection for the necessary interlocks associated with the various plant modes: Shutdown, Refuel, Startup, and Run. This Reactor Mode Switch provides both electrical and physical separation between the components associated with each of the four separate divisions. The mode switch positions and their related bypass and trip/reset functions are as follows.

- Shutdown Position:
  - Initiates a reactor scram,
  - Enables NMS non-coincident trip mode,
  - Enables a manual scram accumulator charging water header pressure trip bypass,
  - Enables automatic bypass of the TCV fast closure trip,
  - Enables automatic bypass of the TSV closure trip,
  - Enables automatic bypass of the MSIV closure trip, and
  - Enables automatic bypass of the power generation bus loss (Loss of All FW Flow) trip.
- Refuel Position:
  - Enables NMS non-coincident trip mode,
  - Enables the manual scram accumulator charging water header pressure trip bypass,
  - Enables automatic bypass of the TCV fast closure trip,
  - Enables automatic bypass of the TSV closure trip,
  - Enables automatic bypass of the MSIV closure trip, and
  - Enables automatic bypass of the Power Generation Bus Loss (Loss of All FW Flow) trip.
- Startup Position:
  - Enables NMS non-coincident trip mode,
  - Disables the manual scram accumulator charging water header pressure trip bypass,
  - Enables the automatic bypass of the MSIV closure trip,
  - Enables automatic bypass of the TCV fast closure trip,
  - Enables automatic bypass of the TSV closure trip, and
  - Enables automatic bypass of the power generation bus loss (Loss of All FW Flow) trip.
- Run Position:
  - Disables all trip bypasses enabled by any of the other three modes, and
  - Bypasses NMS SRNM trips.

7.2.1.5.5 Manual Scram Switches

Two manual scram switches permit initiation of a scram, independent of conditions within other RPS equipment (sensor channels, divisions of trip logic, or divisions of trip actuators). Each manual scram switch is associated with one of the two divisions of actuator load power. Both manual scram switches are located on the MCR console and do not require any microprocessor functionality; duplicate switches are included in the RSS panels.

7.2.1.5.6 Manual Divisional Trip Switches

Each of the four RPS automatic trip systems has manual trip capability provided by four divisional trip switches located in positions easily accessible for optional use by the plant operator. Each switch, when momentarily put into its trip position, trips the actuators that normally would be tripped by a scram condition for that division. Momentarily operating any two of the four manual divisional trip switches results in a full reactor scram.

7.2.1.5.7 Trip Reset Switches

Up to five trip-reset switches will reset any of the four automatic and two manual-scram trip systems that have been tripped and sealed-in, as follows.

- One trip reset switch resets both manual trip systems. The switch circuitry staggers the re-energization of the four groups of scram pilot valve solenoids so only two groups of "A" and "B" solenoids are re-energized simultaneously.
- Four separate switches comprise the trip-reset function for resetting the sealed-in, automatic trip logic outputs in the four divisions. Thus, physical separation of the four electrical divisions is maintained.

7.2.1.5.8 Operational Bypass Switches

Requirements for operational bypass switches for RPS safety-related functions are addressed in Subsection 7.2.1.5.2.1. Operational bypass switches are under administrative control.

7.2.1.5.9 Reactor Mode Switch In Shutdown Position Scram Bypass Switches

Two manual control switches are used to bypass the scram signal when moving the Reactor Mode Switch to its Shutdown position. This bypass only would be permitted during an outage condition when the reactor already is shutdown.

7.2.1.5.10 Maintenance Bypass Switches

Requirements for RPS-related maintenance bypass switches are addressed in Subsection 7.2.1.5.2.2. The maintenance bypasses are:

- Four division-of-sensor maintenance bypass switches; and
- Four division-out-of-service maintenance bypass switches.

7.2.1.5.11 Test Switches

Test switches to aid in surveillance testing during reactor operations are provided in the RPS design.

7.2.2 Neutron Monitoring System

The NMS monitors reactor core thermal neutron flux from the startup source range to beyond rated power and provides trip signals initiating reactor scrams under excessive neutron flux or excessive rates of change in neutron flux (short period) conditions.

7.2.2.1 System Design Bases

The subsystems comprising the NMS are:

- Startup Range Neutron Monitor (SRNM),
- Power Range Neutron Monitor (PRNM),
- Automatic Fixed In-Core Probe (AFIP), and
- Multi-Channel Rod Block Monitor (MRBM)

The PRNM subsystem includes the Local Power Range Monitor (LPRM), APRM functions, and the OPRM.

The SRNM and PRNM subsystems are safety-related and are discussed below. The nonsafety-related AFIP subsystem and the MRBM are addressed in Subsection 7.7.6. The application of this non-safety to safety interface is described in Subsection 7.1.3.3 The CIM uses a one-way fiber optic communication data link and provides required safety-related isolation when passing data from nonsafety-related systems to safety-related systems.

7.2.2.1.1 Startup Range Neutron Monitor Subsystem

7.2.2.1.1.1 Trip Functions

The SRNM scram trip functions are discussed in Subsection 7.2.1.2.4.2, and rod block trip functions are discussed in Subsection 7.7.2.2. The SRNM channels also provide trip bypass. The trip setpoints are adjustable. The SRNM trip functions are shown in Table 7.2-2. A short period signal (the period withdrawal permissive) inhibits continuous control rod withdrawal, thereby avoiding a reactor scram (due to the short reactor period caused by excessive rod withdrawal).

- The trip signals provided in the SRNM design are shown in Table 7.2-3.
- SRNM trips are active only when the Reactor Mode Switch is not in the Run position. When the NMS coincident/non-coincident switch is in the non-coincident position any one of the SRNM can generate trips. When the Reactor Mode Switch is in the Run position, the NMS trips are automatically put into the coincident mode and, if any of the coincident/non-coincident switches are still in the non-coincident position, an alarm will be generated. For each division, the three SRNM scram trip signals are combined to form a divisional SRNM trip signal that is separately sent with the divisional APRM trip signal to the RPS.
- Trips dependent upon signal magnitude have setpoints adjustable in the instrument range.
- The SRNM internal algorithms modify the response time of the period and upscale rod blocks and scrams as a function of count rate and power with a longer response time allowed for initially lower flux.

- A short-period warning signal (Period Withdrawal Permissive) is provided to inhibit rod withdrawal to avoid an inadvertent scram due to excessive rod withdrawal.
- An SRNM interlock signal "ATWS Permissive" is established and sent to the Anticipated Transients Without Scram / Standby Liquid Control (ATWS/SLC) logic as a permissive signal to allow the initiation of liquid boron injection by the SLC system.
- The period trip is active in the coincident and non-coincident mode.
- An instrument inoperative alarm is provided to signal that an SRNM channel is out of service.
- An SRNM channel is considered inoperative if any of the following conditions occur. Its Calibrate-Operate switch is not in the Operate mode, and
  - Any interlock in the channel is open,
  - The unit self-test function detects critical failures, or
  - The detector polarizing (excitation) voltage falls below a preset level.

7.2.2.1.1.2 Safety-Related Design Bases

The general SRNM safety-related functional requirements follow.

- The SRNM is designed as a safety-related system. The SRNM generates a high neutron flux trip signal or a short-period trip signal used to initiate a reactor scram in time to prevent fuel damage resulting from AOOs or infrequent events.
- The SRNM and its preamplifier are qualified to operate under design basis accident (DBA) and abnormal environmental conditions.
- The independence and redundancy incorporated in the SRNM functional design are consistent with the safety-related design basis of the RPS.
- The system is designed to produce a safety-related permissive signal to the ATWS/SLC system logic.

The SRNM is designed as a safety-related subsystem generating trip signals to prevent fuel damage in the event of any abnormal reactivity insertion transients (while operating in the startup power range). The trip signal results either from an excessively high neutron flux level or an excessive rate of neutron flux increase (a short reactor period).

The setpoints of these trips are such that under the worst reactivity insertion transients fuel integrity is always protected. Under the worst bypass condition, where one SRNM from each division is bypassed, the monitoring and protection functions still are adequately provided. The independence and redundancy requirements are incorporated into the design of the SRNM and are consistent with the safety-related design bases of the RPS.

7.2.2.1.1.3 Nonsafety-Related Design Bases

Neutron sources and neutron detectors together provide a signal count rate of at least 3 cps with the control rods fully inserted in a cold non-irradiated core.

The SRNM is designed to perform the following nonsafety-related functions:

- Indicate measurable increases in output signals, with the maximum permitted number of SRNM channels out of service during normal reactor startup operations.
- Provide continuous thermal neutron flux monitoring over a range of 10 decades (approximately 1×10^3 to 1.5×10^{13} neutrons/cm^2/sec).
- Provide continuous measurement of time rate-of-change of neutron flux (reactor period) over the range from approximately -100 seconds to (-) infinity and (+) infinity to approximately +10 seconds.
- Generate interlock signals to block control rod withdrawal if the neutron flux is greater-or-less-than a preset value, or if defined electronic failures occur.
- Generate rod block (inhibit control rod withdrawal) whenever the reactor period decreases below a preset value.
- Maintain the monitoring and alarming functions of the available monitors upon the loss of a single power bus.

7.2.2.1.2 Local Power Range Monitor

7.2.2.1.2.1 Safety-Related Design Bases

The general safety-related functional requirements are as follows.

- To provide a sufficient overall number of LPRM signals to fulfill the APRM safety-related design bases.
- To design the LPRM as a safety-related system to fulfill the APRM safety-related design bases.
- To qualify the LPRM to operate under design basis accidents and abnormal environmental conditions.

The LPRM is designed to monitor the local power level and to provide a sufficient number of LPRM signals to the APRM system to fulfill the safety-related design basis for the APRM. The LPRM itself has no safety-related design basis. However, it is qualified to safety-related standards.

7.2.2.1.2.2 Nonsafety-Related Design Bases

The LPRM performs the following nonsafety-related functions.

- Provides signals to the APRM that are proportional to the local neutron flux at various locations within the reactor core.
- Provides signals to alarm high or low local thermal neutron flux.
- Provides signals proportional to the local neutron flux to drive indicators and displays, and for the PCF to be used for operator evaluation of power distribution, etc.
- Provides signals proportional to the local neutron flux for use by other interface systems such as the RC&IS for the rod block monitoring function.

7.2.2.1.3 Average Power Range Monitor

7.2.2.1.3.1 Safety-Related Design Bases

The general APRM safety-related functional requirements are as follows.

- To design the system to safety-related standards. The general functional requirements specify that, under the worst permitted input LPRM bypass conditions, the APRM is capable of generating a timely trip signal in response to excessive average neutron flux increases to prevent fuel damage. The independence and redundancy incorporated into the design of the APRM is consistent with the safety-related design bases of the RPS.
- To design the system to produce a safety-related simulated thermal power signal to the RPS to allow that system to support reactor power scram bypass requirements.
- To provide information for monitoring the average power level of the reactor core in the power range. The APRM is capable of generating a timely trip signal to scram the reactor in response to an excessive and unacceptable neutron flux increase to prevent fuel damage. Such a trip signal includes a trip from the simulated thermal power signal, representing the APRM flux signal through a time constant representing the actual fuel time constant. The resulting simulated thermal power signal accurately represents core thermal (as opposed to neutron flux) power and the heat flux through the fuel.
- To assure scram functions when the minimum LPRM input requirement to the APRM is fulfilled. If this requirement cannot be met an inoperative channel trip signal is generated. Independence and redundancy requirements are incorporated into the design and are consistent with the safety-related design basis of the RPS.

7.2.2.1.3.2 Nonsafety-Related Design Bases

The APRM performs the following nonsafety-related functions.

- Provides continuous indication of average reactor power (neutron flux) from 1% to 125% of rated reactor power, which overlaps with the SRNM range. Such signals are made available as core power information to other interfacing systems.
- Provides interlock signals for blocking further rod withdrawal to avoid an unnecessary scram actuation.
- Provides a simulated thermal power signal derived from each APRM channel, which approximates the heat dynamic effects of the fuel.
- Provides a continuously available LPRM/APRM display for detection of any neutron flux oscillation in the reactor core.

7.2.2.1.4 Oscillation Power Range Monitor

7.2.2.1.4.1 Safety-Related Design Bases

The general OPRM safety-related functional requirements are as follows.

- Design the OPRM to safety-related standards. The general functional requirements specify that, under the worst permitted input LPRM bypass conditions, the OPRM is capable of generating a timely trip signal in response to core neutron flux oscillation conditions and thermal-hydraulic instability to prevent violation of the thermal safety limit. The independence and redundancy incorporated into the design of the OPRM is consistent with the safety-related design bases of the RPS.

- Provide OPRM monitoring and protection function for core-regional and core-wide neutron flux oscillation monitoring using the LPRM signals sent to the associated APRM channel in which the OPRM channel resides. The OPRM is capable of generating a timely trip signal to scram the reactor in response to an excessive and unacceptable neutron flux oscillation to prevent fuel damage. Scram functions are ensured when the minimum LPRM input requirement to the OPRM is fulfilled. Independence and redundancy requirements are incorporated into the design and are consistent with the safety-related design basis of the RPS.

7.2.2.1.4.2 Nonsafety-Related Design Bases

The OPRM provides core neutron flux oscillation information for the PCF and MCR display, and alarms when the OPRM is inoperative or has an insufficient number of LPRM inputs.

7.2.2.2 System Description

The safety-related functions of the NMS consist of the SRNM and PRNM subsystems. (The LPRM, APRM, and OPRM collectively are called the PRNM subsystem.) The nonsafety-related AFIP subsystem of the NMS and the MRBM are discussed in Subsection 7.7.6.

7.2.2.2.1 System Identification

The purpose of the NMS is to monitor reactor power generation and, for the safety-related aspects of the NMS, to provide trip signals to the RPS initiating a reactor scram whenever there is an excessive neutron flux (and thermal power) level, excessive neutron flux oscillation, or excessive rate of change in neutron flux (short period). In addition, it provides power information to the PCF and the Automated Thermal Limit Monitor (ATLM) in the RC&IS, for control of the rod withdrawal block and FW temperature control valve one-way block functions. The operating range of the various detectors is shown in Figure 7.2-3. A functional block diagram (Figure 7.2-4) shows a typical SRNM division. A functional block diagram (Figure 7.2-5) shows a typical PRNM division.

7.2.2.2.2 Neutron Monitoring Subsystem Safety Classification

The SRNM, LPRM, APRM, and OPRM perform safety-related functions and are designed to meet the applicable design criteria. The system classification is shown in Section 3.2. The safety-related subsystems are qualified in accordance with Sections 3.10 and 3.11.

The AFIP Subsystem of the NMS and the MRBM are nonsafety-related and are discussed within Subsection 7.7.6.

7.2.2.2.3 Power Sources

The safety-related NMS equipment is powered by redundant 120 VAC divisional safety-related UPS. The power sources for each system are discussed in the individual subsystem descriptions.

7.2.2.2.4 Startup Range Neutron Monitor Subsystem

7.2.2.2.4.1 General Description

The SRNM monitors neutron flux from the source range (approximately 1×10^3 neutrons/cm^2/sec) to approximately 1.5×10^{13} neutrons/cm^2/sec. The SRNM subsystem has 12 SRNM channels, each having one fixed in-core regenerative fission chamber sensor.

7.2.2.2.4.2 Power Sources

SRNM channels are powered as listed below:

- A, E, J: 120 VAC Div. 1 UPS,
- B, F, K: 120 VAC Div. 2 UPS,
- C, G, L: 120 VAC Div. 3 UPS, and
- D, H, M: 120 VAC Div. 4 UPS.

Each SRNM cabinet is powered by two redundant divisional 120 VAC UPS in the appropriate division; either source of power can support system operation.

7.2.2.2.4.3 Physical Arrangement

The 12 SRNM detectors are located at a fixed elevation about the mid-plane of the fuel region and are uniformly distributed throughout the core. The SRNM detector locations in the core, together with the neutron source locations, are shown in Figure 7.2-6. Each detector is contained within a pressure barrier dry tube inside the core with signal output exiting the bottom of the dry tube under-vessel. Detector cables are routed separately to the appropriate containment penetration according to divisional assignment. They are connected to their designated preamplifiers located in the respective divisional quadrants of the RB.

The SRNM preamplifier signals are transmitted to the SRNM digital processing equipment units, which provide algorithms for signal processing and calculations to provide neutron flux, power, period trip margin, and period. Additionally, they provide outputs for local and control console displays and recorders and to the PCF. The individual SRNM channel trips are combined to form a SRNM divisional trip in the NMS TLU function (as shown in Figure 7.2-4). This SRNM divisional trip is sent to the RPS through a safety-related network interface. (This is the logic in the coincident mode. Further discussion of SRNM trip logic is included in Subsection 7.2.2.5.)

Alarm and trip outputs also are provided for both high neutron flux and short period trip or alarm conditions. Such outputs include the instrument inoperative trip. The electronics for the SRNM and their designated bypass units are located in four separate cabinets, one in each of the four divisional RB quadrants, and in each of the CB divisional equipment room locations. The SRNM satisfies the IEEE Std. 603, Section 5.1 single-failure criterion because the failure of any individual SRNM channel does not affect the protection function of the SRNM through channel bypasses discussed in Subsection 7.2.2.2.4.6 (with any three of the four divisions of safety-related power available). It also satisfies the IEEE Std. 603, Section 5.6 independence requirement.

7.2.2.2.4.4 Signal Processing

Over the 10-decade power monitoring range two monitoring methods are used: (1) the counting method for the lower counting range (approximately 1×10^3 neutrons/cm^2/sec) to approximately 1×10^9 neutrons/cm^2/sec, and (2) the Campbelling technique Mean Square Voltage (MSV) for the higher range, from 1×10^8 neutrons/cm^2/sec to 1×10^{13} neutrons/cm^2/sec of neutron flux.

In the counting range, after pre-amplification, the discrete pulses produced by the sensors are applied to a discriminator. The discriminator, together with other digital noise-limiter features, separates the neutron pulses from gamma radiation and other noise pulses. The neutron pulses are counted. The reactor thermal power is proportional to the count rate.

In the MSV range, where it is difficult to distinguish among the individual pulses, a DC voltage signal proportional to the mean square value of the input signal is produced. The reactor power is proportional to this MSV. In the mid-range overlapping region, where both methods apply, the SRNM calculates a neutron flux value based on a weighted interpolation of the two flux values as calculated by each method. A continuous and smooth flux reading transfer is achieved in this manner. In addition, there is the calculation algorithm for the period-based trip circuitry generating a trip margin setpoint for the period trip protection function.

7.2.2.2.4.5 Trip Functions

The SRNM scram trip functions are discussed in Subsection 7.2.2.1.1.1, and rod block trip functions are discussed in Subsection 7.2.2.1.1.3. The SRNM channels also provide trip bypass. The trip setpoints are adjustable. The SRNM trip functions are shown in Table 7.2-2. A short period signal (the period withdrawal permissive) inhibits continuous control rod withdrawal to avoid a reactor scram (due to a shorter reactor period caused by excessive rod withdrawal).

7.2.2.2.4.6 Bypasses and Interlocks

The 12 SRNM channels are divided two ways; there are three SRNMs per division assigned as previously described and the 12 SRNMs are additionally divided into core quadrants with three SRNMs per quadrant such that each quadrant has three separate divisions. The quadrants/SRNMs are arranged into four bypass groups of three SRNMs each; a joystick type bypass switch ensures that no more than one SRNM in a quadrant can be simultaneously bypassed. Therefore, a maximum of four SRNM channels can be bypassed at any one time. This scheme assures that each quadrant will always have at least two unbypassed SRNMs for startup range flux monitoring. There is no additional SRNM bypass capability at the divisional level. However, it is possible to bypass all three SRNMs belonging to the same division. When this is required, a divisional bypass is generated that allows that division's NMS DTM to be bypassed. For SRNM calibration or repair, the bypass can be performed for each individual channel separately through these SRNM bypasses without putting the whole division out of service. The SRNM subsystem satisfies the repair requirement of IEEE Std. 603, Section 5.10. Note that bypassing any of the SRNM sensors within a division does not affect the ability of the NMS to perform two-out-of-four trip determinations using the trip decisions from the SRNM divisions (with any three of the four divisions of safety-related power available). The SRNM subsystem satisfies the IEEE Std. 603, Section 5.1 single-failure criterion.

The SRNM bypass switches are mounted on the MCR panel. Bypass functions for the SRNM and the APRM in the NMS are separate. There is no single NMS divisional bypass affecting both the SRNM and the APRM. No APRM bypass forces a SRNM bypass. Also, all NMS bypass logic control functions are located within the NMS, not in the RPS.

The SRNM has several major interlock logics. The SRNM trip functions are in effect when the Reactor Mode Switch is not in the Run position. The SRNM upscale trip is only active in the NMS non-coincident mode (Table 7.2-2). The SRNM ATWS permissive signals are sent to the ATWS/SLC system to control initiation of SLC system boron injection and associated functions (such as FW runback).

7.2.2.2.4.7 Redundancy and Diversity

The signal outputs from the 12 SRNM channels are arranged so each of the four divisions includes a different set of designated SRNM channels covering different regions of the core. The SRNM monitoring and protection function is provided by each individual channel. Failure of an un-bypassed single SRNM channel causes an inoperative trip to only one of the four divisions, whereas a full scram requires divisional trips in two-out-of-four divisions within the NMS. Bypassing a single SRNM channel does not cause a trip output to the related SRNM division and does not prevent the remaining SRNM channels from performing their safety-related functions.

7.2.2.2.4.8 Environmental Considerations

The wiring, cables, and connectors located within the drywell are designed for continuous duty in the environmental conditions described in Appendix 3H.

The SRNM instruments are designed to operate under the expected environmental conditions. Environmental qualification is discussed in Section 3.11.

7.2.2.2.5 Local Power Range Monitor

7.2.2.2.5.1 General Description

The LPRM monitors local neutron flux in the power range. The LPRM provides input signals to the APRM (Subsection 7.2.2.2.6), the RC&IS (Subsection 7.7.2), and the PCF of the N-DCIS (Subsection 7.1.5).

7.2.2.2.5.2 Uninterruptible Power Supply

Alternating current power for the LPRM circuitry is supplied by four pairs of redundant divisional 120 VAC UPS buses corresponding to the four safety-related divisions. The cabinets can perform their functions with either of their redundant power sources. Each division supplies power to one-fourth of the detectors. Each LPRM detector is provided with a DC power supply, housed in the designated divisional APRM instrument furnishing the detector polarizing potential.

7.2.2.2.5.3 Physical Arrangement

A single division of LPRMs consists of a total of 64 detectors - one detector from each LPRM assembly (from a total of 64 assemblies in the core). There are a total of 256 LPRM detectors in the core. Each assembly consists of four LPRM fission chamber detectors uniformly spaced at four axial positions in the fuel bundle vertical direction. The 64 assemblies are distributed uniformly throughout the whole core. Within the core, for each square fuel region of four-by-four fuel bundles, LPRM assemblies are located at the four corners.

The LPRM assembly locations in the core are illustrated in Figure 7.2-7. The LPRM detector axial positions in the fuel bundle vertical direction are illustrated in Figure 7.2-8. The LPRM detector at the lowest position is designated LPRM A. Detectors above A are designated B and C, with the uppermost detector designated D.

The LPRM detector is a fission chamber with a polarizing potential of approximately 100 VDC. The four detectors comprising a detector assembly are contained in a common tube also housing the AFIP sensors (Subsection 7.7.6). The enclosing housing tube is perforated to promote reactor coolant flow for detector cooling.

In addition, the LPRM assembly contains a set of two thermocouples mounted inside its lower portion (at an elevation below the core plate). The thermocouple sensors provide core inlet temperature data to be used by the PCF of the N-DCIS for core flow determination using the heat balance method. A pair of thermocouple sensors is mounted on all 64 LPRM assemblies (at the same elevation). Figure 7.2-8 shows the relative elevations of the fixed in-core probe sensors and the thermocouples.

The LPRM cables are grouped by associated APRM trip channel under the RPV and routed to the RB in conduit to maintain separation. The LPRMs provide inputs to each of the four APRM channels. The four APRM channels are mounted in separate bays with complete physical separation. This arrangement and wiring practice provides the required electrical isolation and physical separation to fulfill the independence requirement of IEEE Std. 603, Section 5.6.

7.2.2.2.5.4 Signal Processing

At the under-vessel pedestal region the LPRM detector outputs from the assembly are connected to respective coaxial cables routed through the containment penetrations and to the signal conditioning units in the RB. In the signal conditioning units the signals are processed, amplified, converted to digital data, and transmitted by fiber optic cable to the CB NMS cabinets located in the safety-related equipment rooms.

The amplified signal is proportional to the local neutron flux level. The LPRM signals are averaged and normalized to reactor power by the APRM logic, to produce an APRM signal (Refer to Subsection 7.2.2.2.6). Individual LPRM signals also are transmitted (with proper electrical isolation) through dedicated interface units in the APRM from other systems such as the RC&IS and the PCF to provide local power information.

7.2.2.2.5.5 Trip Functions

The LPRM channels provide trip and status signals indicating when an LPRM is upscale, downscale, or bypassed.

7.2.2.2.5.6 Bypasses and Interlocks

Each LPRM channel is capable of being individually bypassed. When the maximum allowed number of bypassed LPRMs for each APRM has been exceeded an inoperative trip is generated by the affected APRM channel.

7.2.2.2.5.7 Redundancy

The LPRM detectors are arranged in four divisional APRM channels with 64 LPRM detector signals in each. The redundancy criteria are met, ensuring (in the event of a single failure under permissible APRM bypass conditions) the safety-related protection function is performed as required (with any three of the four divisions of safety-related power available).

7.2.2.2.5.8 Environmental Considerations

The LPRM detector and detector assembly are designed to operate up to a gauge pressure of approximately 8.62 MPa (1250 psig) and at an ambient temperature of approximately 315°C (511°F). The wiring, cables, and connectors located within the drywell are designed for continuous duty at drywell ambient conditions. The LPRMs are capable of functioning during and after DBEs. (Refer to Sections 3.10 and 3.11).

7.2.2.2.6 Average Power Range Monitor

7.2.2.2.6.1 General Description

The APRM performs a safety-related function. There are four APRM channels, one per division. Each APRM channel receives 64 LPRM signals as primary inputs (from the RB) through fiber optic cables. Each APRM channel then averages the inputs and normalizes the result to provide an APRM value corresponding to the average core thermal power signal. One APRM channel is associated with each division of the RPS.

7.2.2.2.6.2 Power Sources

APRM channels are powered as listed below:

- A: Redundant 120 VAC Div. 1 UPS,
- B: Redundant 120 VAC Div. 2 UPS,
- C: Redundant 120 VAC Div. 3 UPS, and
- D: Redundant 120 VAC Div. 4 UPS.

Either of the two redundant divisional power sources supports APRM operation. The bypass units and LPRM detectors associated with each APRM channel receive power from the same power sources as the APRM channel.

7.2.2.2.6.3 Physical Arrangement

The APRM subsystem consists of four independent and separate instrument channels. Each APRM channel receives 64 LPRM signal inputs. The assignment of individual LPRM sensors to each of the four APRM channels is performed, ensuring that an even and uniform selection of LPRM sensors from the whole core is allocated to each APRM channel. In this manner, the average value of the 64 LPRM signals from the entire core represents the average core power value. The LPRM signals within the APRM channel are averaged and normalized to form an average core power APRM signal. The LPRM assignment to APRM channels is shown in Figure 7.2-9.

7.2.2.2.6.4 Signal Conditioning

The APRM channel electronic equipment averages the output signals from 64 LPRM detectors to form an APRM signal for this channel. The averaging circuit automatically corrects for the number of un-bypassed LPRM input signals. The APRM channel electronics unit includes the capabilities for LPRM and APRM calibrations and diagnostics. The APRM has communication interface modules (CIMs) to send signals to other systems. A simplified PRNM block diagram is shown in Figure 7.2-5. Individual APRM channel trips are routed to the RPS directly. The APRM satisfies the IEEE Std. 603, Section 5.1 single-failure criterion, because the failure of any individual APRM channel does not affect the protection function of the APRM through channel bypasses, as discussed in Subsection 7.2.2.6.6 (with any three of the four divisions of safety-related power available). It also satisfies the IEEE Std. 603, Section 5.6, independence requirement, because the redundant portions of the NMS equipment are independent of (and physically separated from) each other, and the NMS equipment is separated from other systems.

7.2.2.2.6.5 Trip Function

The APRM scram trip function is discussed in Subsection 7.2.1.2.4.2. The APRM rod block trip function is discussed in Subsection 7.7.2.2. The APRM channels also provide trip and status signals indicating when an APRM channel is upscale, downscale, bypassed, or inoperative. The trip setpoints are adjustable. APRM system trip functions are summarized in Table 7.2-4.

7.2.2.2.6.6 Bypasses and Interlocks

Bypass of one APRM channel out of four channels is allowed at any one time for repair during plant operation while maintaining the required APRM functions. This satisfies the repair requirement of IEEE Std. 603, Section 5.10. When one APRM channel is bypassed, the trip logic in the NMS becomes two-out-of-three instead of two-out-of-four (with any three of the four divisions of safety-related power available).

The bypass of APRM channels is accomplished with a joystick-type switch having mutually exclusive positions. The APRM bypass switch is located on an MCR panel. Access to the panel and the switch is under administrative control. When a bypass is active, the input from the bypassed APRM/OPRM channel (APRM or OPRM trip function) will be bypassed by removing it from the vote. The remaining signals are voted with a two-out-of-three logic, thus retaining the ability to withstand a single-channel failure.

The final check of the signals, performed independently by each voter channel, ensures that no single failure causes an inadvertent bypass. The bypass function uses physical means and independent logic to ensure that no more than one channel is bypassed at a given time.

There are no automatic bypasses for the APRM trip function. The APRM trip setpoint is automatically changed to a lower value (setdown) when the manually operated Reactor Mode Switch is not in the Run position. When any APRM (or OPRM) channel output is bypassed, the bypass is indicated on the plant operator's panel. The same channel bypass bypasses both the OPRM and APRM channels.

The APRM ATWS permissive signals are sent to the ATWS/SLC system as permissive signals for the ADS initiation inhibit function. The ATWS permissive value for ADS initiation is provided in Table 7.2-4.

7.2.2.2.6.7 Redundancy

Four independent channels of the APRM monitor neutron flux. Each channel is associated with one NMS division, with its optically isolated trip signal sent to the other three NMS divisions. The redundancy criteria are met ensuring (in the event of a single failure under permissible APRM bypass conditions) the safety-related protection function is performed as required (with any three of the four divisions of safety-related power available).

7.2.2.2.6.8 Environmental Considerations

Chapter 3 describes the APRM operating environments. The APRM is capable of functioning during and after the DBE in which continued APRM operation is required (Sections 3.10 and 3.11).

7.2.2.2.7 Oscillation Power Range Monitor

7.2.2.2.7.1 General Description

The OPRM consists of four independent safety-related channels. The OPRM channel uses the same set of LPRM signals used by the associated APRM channel in which the OPRM channel resides. Each OPRM receives identical LPRM signals from the corresponding APRM channel as inputs and forms OPRM cells to monitor the thermal neutron flux behavior in all regions of the core. Assignment of LPRMs to the four OPRM channels is shown in Figure 7.2-10.

The OPRM channel consists of OPRM cells formed by grouping LPRM inputs (maximum of four). The OPRM cell signal is the average of all grouped LPRM input signals and is used for detecting thermal hydraulic instability of the reactor core. The LPRM signals assigned to each cell are summed and averaged to provide an OPRM signal for that cell. The OPRM trip protection algorithm detects thermal hydraulic instability (flux oscillation with unacceptable amplitude and frequency) and provides a trip output if the trip setpoint is exceeded.

7.2.2.2.7.2 Power Sources

The OPRM function resides in the APRM equipment and is supplied with the same redundant APRM 120 VAC power.

7.2.2.2.7.3 (Deleted)

7.2.2.2.7.4 Trip Function

The OPRM trips are combined with the APRM trips of the same APRM channel and sent to the RPS. When there is an insufficient number of operating OPRM cells the OPRM function generates an alarm signifying an inoperative OPRM channel. If the number of operating LPRM inputs to an OPRM cell is less than the minimum required, the cell is considered to be inoperative. Similarly, the channel is inoperative if it does not have enough operating cells. Any cell can cause an OPRM channel alarm or trip condition.

The OPRM channel monitors OPRM cell signal responses and provides alarm and trip signals based on the oscillation detection algorithm defined in a detailed hardware and software design specification document. Any cell can cause an OPRM channel alarm or trip condition.

The OPRM channel trips are sent to the RPS. The OPRM function does not generate an inoperative trip but does generate an alarm signifying an inoperative OPRM channel when there is an insufficient number of operating OPRM cells. (An inoperative OPRM cell is a cell having an insufficient number of operating LPRM inputs).

A summary of OPRM trip functions is provided in Table 7.2-6.

7.2.2.2.7.5 Bypasses and Interlocks

The OPRM alarms and trips are bypassed in all reactor operation modes except Run and when operating below a preset power level. The OPRM bypass is controlled by the APRM channel in which it resides. Bypass of the APRM channel also bypasses the OPRM trip function within this APRM channel.

7.2.2.2.7.6 Redundancy

The OPRM has the same redundancy design as the APRM. The redundancy criteria are met such that, in the event of a single failure under permissible APRM/OPRM bypass conditions, the safety-related protection function is performed as required (with any three of the four divisions of safety-related power available).

7.2.2.2.7.7 Environmental Conditions

The OPRM is subject to the same environmental conditions as the APRM.

7.2.2.3 Safety Evaluation

This evaluation covers the safety-related SRNM, LPRM, APRM, and OPRM functions of the NMS.

The evaluation of the trip inputs from the NMS to the RPS is discussed in Subsection 7.2.1.

The AFIP subsystem and the MRBM are nonsafety-related subsystems of the NMS, and are evaluated in Subsection 7.7.6.

Table 7.1-1 identifies the NMS and the associated codes and standards applied, in accordance with the Standard Review Plan NUREG-0800. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.2.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The NMS design conforms to these standards.

10 CFR 50.55a(h), "Protection and Safety Systems," compliance with ANS/IEEE Std. 603:

- Conformance: The NMS conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the NMS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsections 7.2.2.1.1.2, 7.2.2.1.2.1, 7.2.2.1.3.1, and 7.2.2.1.4.1.

- – Section 4.3 (Permissive Conditions for Operating Bypasses): See Subsections 7.2.2, Tables 7.2-2 and 7.2-4 for a description of the NMS system Operating Bypasses and Permissive Conditions.
- – Section 4.6 (Spatially Dependent Variables): See Subsections 7.2.2.2.4.3, 7.2.2.2.5.3, 7.2.2.2.6.3, and Tables 7.2-6 through 7.2-10 for a description of the NMS system sensor and location information.
- – Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.
- – Section 5.7 (Capability for Test and Calibration): See Subsections 7.2.2.4.1 through 7.2.2.4.2.4 for NMS Test and Calibration Capability.
- – Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable to NMS.
- – Section 6.4 (Derivation of System Inputs): The NMS derives its sense and command features from direct measurements.
- – Section 6.5 (Capability of Test and Calibration): See Subsections 7.2.2.4.1 through 7.2.2.4.2.4 for NMS Test and Calibration Capability.
- – Section 6.6 and 7.4 (Operating Bypasses): See Section 7.2.2, Tables 7.2-2 and 7.2-4 for a description of the NMS system Operating Bypasses and Permissive Conditions.
- – Section 6.7 and 7.5 (Maintenance Bypasses): See Subsections 7.2.2.2.4.6, 7.2.2.2.5.6, 7.2.2.2.6.6, 7.2.2.2.7.5 for a description of NMS Maintenance Bypasses.
- – Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the NMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- – Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the NMS power sources are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The NMS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The NMS design of bypass and inoperable status indication conforms to this requirement, consistent with conformance of the NMS design to RG 1.47.

  The 12 SRNM channels are divided into four divisions and are independently assigned to four bypass groups such that bypass of up to four SRNM channels at any one time is allowed while still providing the required monitoring and protection capability (with any three of the four divisions of safety-related power available).

10 CFR 50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: The LPRM assemblies contain thermocouples that are available for monitoring core cooling. The discussion of the thermocouples for LPRM is addressed in Subsection 7.2.2.2.5.3.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The NMS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The NMS conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the NMS within the DCD documents conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.2.2.3.2 General Design Criteria

GDC 1, 2, 4, 10, 12, 13, 19, 20, 21, 22, 23, 24, 25, 26, 27, and 29:

- Conformance: The NMS design complies with these GDC.

7.2.2.3.3 Staff Requirements Memorandum

Item II.Q of SECY-93-087, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems):

- Conformance: The NMS design, as part of the safety-related system, minimizes the likelihood of common mode failures, and conforms to this requirement by the implementation of additional Diverse Instrumentation and Control System capabilities, described in Section 7.8.

7.2.2.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: The NMS design conforms to RG 1.22.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The NMS design conforms to RG 1.47.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The NMS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The NMS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The NMS design conforms to RG 1.105. Reference 7.2-1 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation and Control Portions of Safety Systems:

- Conformance: The NMS design conforms 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.168 as implemented on the NMS platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.169 as implemented on the NMS platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.170 as implemented on the NMS platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.171 as implemented on the NMS platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.172 as implemented on the NMS platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.173 as implemented on the NMS platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The NMS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The NMS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.2.2.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The NMS design conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance for Application and Qualification of Isolation Devices:

- Conformance: The NMS design conforms to BTP HICB-11. The NMS equipment uses safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices to meet the requirements of RG 1.75 and RG 1.153.

BTP HICB-12, Guidance for Establishing and Maintaining Instrument Setpoints:

- Conformance: The analytical limits of the safety-related setpoints of the NMS are determined from safety analyses for each reactor fuel cycle to ensure the reactor core is protected from any rising neutron flux potentially exceeding these values. The nominal setpoints are calculated to be consistent with the GEH standard setpoint methodology (Reference 7.2-1), which conforms to RG 1.105. The setpoint margin calculated by this method also has considered additional uncertainties with the calibration interval. Therefore, the NMS meets BTP HICB-12.

  Most of the uncertainty associated with safety-related NMS trip setpoints is associated with the various neutron sensors because the digital electronics in the NMS do not drift, the setpoints are monitored and alarmed by the PCF of N-DCIS.

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

- Conformance: [*Development of software for the safety-related system functions within NMS conforms to the guidance of BTP HICB-14 as discussed in the LTRs "ESBWR Software Management Program Manual (SMPM)," NEDO-33226, NEDE-33226P, and "ESBWR Software Quality Assurance Program Manual (SQAPM)," NEDO-33245, NEDE-33245P (References 7.2-3 and 7.2-4.) Safety-related software to be embedded in the memory of the NMS logics is developed according to a structured plan described in References 7.2-3 and 7.2-4. These plans follow the software life cycle process described in BTP HICB-14.*]*

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The NMS section content conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The safety-related subsystems of the NMS are designed to support the required periodic testing. (Refer to Subsection 7.2.2.4.) The NMS system equipment features a self-test design operating in all modes of plant operations. This self-test function does not interfere with the safety-related functions of the system. The NMS design conforms to BTP HICB-17.

BTP HICB-18, Guidance of Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems:

- Conformance: Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance of Branch Technical Position HICB-18. Q-DCIS is built and qualified specifically for ESBWR applications as safety-related and not as commercial grade PLCs. The embedded and operating system software meet the acceptance criteria contained in BTP HICB-14, for safety-related applications.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems:

- Conformance: The NMS design conforms to BTP HICB-19 by implementation of an additional diverse instrumentation and control system described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The SRNM/APRM digital subsystems (and the OPRM digital subsystem) are designed to respond in real time to ensure that specified fuel limits are not exceeded, and core power oscillations are detected and suppressed. The NMS conforms to BTP HICB-21.

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7.2.2.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for Chapter 7, and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)(I.D.3) applies to the NMS and is addressed in Subsection 7.2.2.3.1.

TMI action plan requirements are generically addressed in Table 1A-1 of Appendix 1A.

7.2.2.4 Testing and Inspection Requirements

7.2.2.4.1 General Requirements

NMS instruments (not including sensors) outside the containment are designed so they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram and with easy access for the service personnel.

NMS instrument modules, including SRNM and APRM, are designed with the capability of being tested for normal performance, trip performance, and calibration function through either an automated or manual process. Routine surveillance functions, including periodic tests and calibration, are automated with minimum operator involvement.

Detailed NMS instrument test function requirements, including periodic tests and calibration durations for each instrument, are included in the detailed NMS hardware and software system specification document.

For microprocessor-based instruments an instrument unit self-test function is provided.

7.2.2.4.2 Specific Requirements

7.2.2.4.2.1 Startup Range Neutron Monitor Testability and Calibration

Each SRNM channel is tested and calibrated using the procedures listed in the SRNM instruction manual. Each SRNM channel is checked when the reactor mode switch is not in "Run" to ensure that the SRNM high flux scram function and short period scram function are operable. Portions of the required testing may be performed in other operating Modes. See Subsection 7.2.2.4 for a description of SRNM inspection and testing requirements.

7.2.2.4.2.2 Local Power Range Monitor Testability and Calibration

LPRM channels are calibrated using data from the AFIP subsystem and based on PCF three-dimensional core power distribution calculations. The calibration follows procedures in the applicable instruction manual.

7.2.2.4.2.3 Average Power Range Monitor Testability and Calibration

APRM channels are calibrated using data from the PCF reactor heat balance calculation. The calibration follows procedures in the applicable instruction manual. Each APRM channel is checked individually (by introduction of test signals) for operability of the APRM high neutron flux scram and rod-blocking functions.

7.2.2.4.2.4 Oscillation Power Range Monitor Testability and Calibration

Each OPRM channel can be checked individually (by introduction of test signals) for operability of the OPRM trip protection algorithm.

7.2.2.5 Instrumentation and Control Requirements

7.2.2.5.1 Instrumentation Requirements

The design of NMS instruments primarily is based on digital I&C practices with digital electronics-based programmable and memory units. The NMS instruments follow a modular design concept so each modular unit or its subunit is easily replaceable. Each instrument has a flexible interface design to accommodate either metal wire or fiber optic communication links.

NMS instruments are provided with necessary operator-interface functions based on adequate NMS man-machine interface (MMI) requirements.

The NMS displays provided in the MCR, as a minimum, include:

- SRNM reactor period, power level, and count rate (12);
- SRNM upscale/INOP trip and reactor period trip status;
- SRNM upscale rod block, reactor period rod block, and downscale rod block status,
- SRNM channel bypass status;
- SRNM period based permissive;
- SRNM ATWS permissive status;
- LPRM bypass status, LPRM upscale alarm, and LPRM downscale alarm status (256 each);
- Number of bypassed LPRMs per APRM channel;
- APRM power level (4);
- APRM bypass status (4);

- APRM divisional reactor upscale/INOP trip, upscale rod block, and downscale rod block status;
- APRM simulated thermal power level (4);
- APRM simulated thermal power upscale trip status;
- APRM ATWS permissive status (4);
- OPRM divisional trip status;
- MRBM main channel bypass status;
- MRBM main channel rod block status; and
- AFIP system operability status.

The alarms in the MCR include:

- SRNM non-coincident upscale trip,
- SRNM non-coincident upscale rod block,
- SRNM downscale rod block,
- SRNM short period trip, short period rod block,
- SRNM inoperative trip,
- SRNM period withdrawal permissive alarm,
- LPRM upscale, downscale alarm,
- APRM upscale trip,
- APRM upscale rod block, downscale rod block,
- APRM simulated thermal power upscale trip,
- APRM simulated thermal power rod block,
- APRM system inoperative trip,
- MRBM upscale rod block, downscale, inoperative rod block,
- AFIP inoperative, and
- OPRM trip.

The above NMS displays and alarms fulfill the information display requirements of the IEEE Std. 603, Section 5.8.

7.2.2.5.2 Basic Control Logic Requirements

The control logic of the safety-related subsystems in the NMS is "fail-safe." That is, a trip signal is initiated if the control logic device fails due to critical hardware failure, power failure, or loss of communication failure.

The NMS controls located in the MCR panel include:

- SRNM channel bypass controls (one for each bypass group) (hardware);
- APRM channel bypass control (one for each division) (hardware); and
- Coincident/non-coincident switch. In the non-coincident position (not in Run mode), any single SRNM channel trip condition sends a trip signal to the RPS and causes a reactor scram.

Each SRNM, LPRM, OPRM, or APRM channel can be individually bypassed. Restrictions on the total number and distribution of bypassed channels (at one time) are followed to avoid a reactor trip due to inoperative NMS channels.

Each of the 12 SRNM channels belongs to one of the four bypass groups. Each group has one "multiple position" selector switch so only one SRNM channel in each group is capable of being bypassed at a time. The SRNM channel bypassed status is displayed on the NMS user interface.

The APRM equipment allows the operator to bypass any one of the four APRM channels during normal plant operation. The APRM channel bypassed status is displayed on the NMS user interface. The trip logic at the NMS becomes two-out-of-three instead of two-out-of-four.

There are separate bypass functions for the SRNM and APRM in the NMS. (There is no single NMS divisional bypass affecting both the SRNM and the APRM.) An APRM bypass does not force an SRNM bypass. The SRNM and APRM bypasses are separate logics to NMS. All NMS bypass logic control functions are located within NMS but none are located in the RPS. Use of SRNM and APRM bypasses does not adversely affect the ATWS permissive and ADS inhibit output functions.

Individual LPRM channels are bypassed by first confirming, for a given APRM channel, that the minimum LPRM input requirement is still met after the bypasses are completed. The operator has to input the LPRM designator to be bypassed, then switch it into bypass. The LPRM channel bypassed status is displayed on the NMS user interface. If the maximum allowed number of bypassed LPRMs associated with any APRM channel is exceeded an inoperative trip is automatically generated by that APRM channel.

A failure that causes a channel to become inoperative causes a channel trip output to the NMS.

When the Reactor Mode Switch is in the Run position, the NMS is in a "Coincident" mode. SRNM trips are active only when the Reactor Mode Switch is not in the Run position. If the manual coincident/non-coincident switch is in the "non-coincident" position when the Reactor Mode Switch is placed in the run position an alarm is generated in the MCR. When the NMS is in non-coincident mode, any one of the SRNMs channel trips can cause a reactor scram; in the coincident mode, at least two-out-of-four divisions must be tripped in order to activate the reactor scram.

7.2.2.5.3 Basic Instrument Arrangement Requirements

NMS instruments and equipment are located in appropriate areas in the CB and RB with appropriate divisional physical and electrical separation.

Figures 7.2-4 and 7.2-12 provide a more detailed view of the NMS configuration and communication paths.

The NMS is implemented with two communication methodologies: "point-to-point" optical fiber interdivisional communication and a shared memory ring network. Point-to-point communication is limited to trip and bypass information and any necessary message authentication. Point-to-point fiber is also used NMS to RTIF and NMS to SSLC/ESF communication. Since the NMS is "fail safe" the loss of any communication or fiber will be interpreted as a trip. The other communication methodology uses a shared memory ring network that extends between the various NMS system chassis. The processors of each chassis ("nodes") connected to the ring can read the entire shared memory on the communications (CIM) card and write only to a designated portion of the CIM card memory. The data on the ring are actively transported between one chassis transmitter and another's receiver until all nodes have been updated. To increase reliability, another ring (forming a counter-rotating ring) is provided with the data going in the opposite direction, this scheme allows both rings to be broken between two nodes and all data still gets to all nodes; no single failure will prevent data transmission.

There are two "counter rotating" rings within each division of NMS. The upper ring on Figure 7.2-12 interconnects the RMU, DTM, TLU and Q-CIM which are the only chassis needed to support the NMS safety functions. This is the (redundant) path by which the RMUs transfer data to the DTMs and, in turn to the TLUs as described above Note that the BPU is not on the shared memory ring because the BPU is implemented in hardware logic.

There is a second redundant ring that interconnects the above chassis and additionally nonsafety-related "operator" and "maintenance" VDUs in the NMS and RMU cabinets and on the safety surveillance panel in the MCR (the safety-related function of this VDU is Seismic Category II). Additionally, on this ring are two nonsafety-related N-CIM (NMS N-CIM A and NMS N-CIM B), each of which has access to the equivalent rings of the other three divisions and therefore all NMS divisional data.

The VDUs may be used at any time to monitor NMS signals and internal diagnostics; however, they cannot input to any of the NMS chassis for calibration or maintenance purposes unless the chassis or NMS division has been made "INOP" by a keylock switch. INOP corresponds to a trip unless the division has been bypassed. The INOP status is alarmed.

7.2.3 Suppression Pool Temperature Monitoring

The SPTM function of the CMS, is classified as safety-related.

7.2.3.1 System Design Bases

7.2.3.1.1 Safety-Related Design Bases

The safety-related functional requirement of the SPTM is to prevent the suppression pool temperature from exceeding established limits. It does this by providing the inputs necessary for automatic reactor scram initiation, which limits heat addition to the suppression pool.

The SPTM function is physically implemented by the safety-related four-divisional subsystem, designed for Seismic Category I requirements.

The SPTM function also provides:

- Safety-related inputs to the MCR for indication.

7.2.3.1.2 Nonsafety-Related Design Bases

The nonsafety-related SPTM functional requirements are:

- To provide input for automatic suppression pool cooling mode initiation, and
- To provide input for data display, alarm, and recording on the MCR panels.

7.2.3.2 System Description

7.2.3.2.1 General

The SPTM function provides suppression pool temperature data for automatic scram and automatic suppression pool cooling initiation when established high temperature limits are exceeded. In addition, the SPTM function provides suppression pool temperature data for operator information and recording, and for post-accident conditions of the suppression pool. The SPTM function outputs to other systems are shown in Table 7.2-5.

7.2.3.2.2 Power Sources

The SPTM hardware is powered by the appropriate dual divisional redundant 120 VAC UPS - either of which can support the SPTM function.

7.2.3.2.3 Equipment Design

The SPTM function comprises four independent safety-related instrumentation divisions, each containing 16 sensors spatially distributed around the suppression pool. The sensor locations are established to:

- Provide four-divisional, redundant measurements of suppression pool local and bulk-mean temperatures under normal plant operating conditions and under postulated accident and post-accident conditions;
- Implement the divisional separation of sensors in the azimuthal directions, with redundancy and separation of sensors realized in four divisions and with sensors appropriately covering the different elevations of the pool; and
- Locate sensors away from jet paths of SRV quenchers, horizontal vent discharges, and Passive Containment Cooling System (PCCS) vent line discharges. This limits the temperature differences between local and bulk-mean values.

The sensor electrical wiring, encapsulated in pliable, grounded sheathing, is terminated in Wetwell-sealed, moisture-proof junction boxes for easy sensor replacement or maintenance during a plant outage. The temperature sensor wiring from the Wetwell junction boxes is directed through the suppression pool divisional instrument penetrations to the four-divisional Q-DCIS RMUs.

7.2.3.2.4 Signal Processing

The SPTM function supports measurement and calculation of bulk average suppression pool temperatures for both normal operation and DBA conditions. A minimum number of thermocouples per division is required to be operational. The SPTM logic automatically compensates for inoperable thermocouples. If less than the required number of thermocouples is available a trip signal is generated in that division. These signals are transmitted through the divisional Q-DCIS to the RPS. Safety-related protective actions are generated by the RPS. Abnormal status alarms, data display, and recording are provided.

7.2.3.3 Safety Evaluation

Table 7.1-1 identifies the SPTM function and the associated codes and standards applied, in accordance with the Standard Review Plan, NUREG-0800. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.2.3.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The SPTM function complies with these standards

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The SPTM function conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the SPTM function conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.2.3.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable to the SPTM function.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency requirements of the SPTM function are described in Subsection 7.2.1.2.4.2.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): Subsection 7.2.3.4 describes testing requirements specific to the SPTM function.
  - Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable to the SPTM function.
  - Section 6.4 (Derivation of System Inputs): SPTM inputs are derived from direct measures.
  - Section 6.5 (Capability of Test and Calibration): Subsection 7.2.3.4 describes testing requirements specific to the SPTM function.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses are not applicable to the SPTM function.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the SPTM function are adequately described in Subsection 7.1.6.6.1.24.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the SPTM function are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.

– Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the SPTM function are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The SPTM function conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The SPTM function complies by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The SPTM function conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the SPTM function within the DCD documents conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.2.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, and 29:

- Conformance: The SPTM function complies with these GDC.

7.2.3.3.3 Staff Requirements Memorandum

Item II.Q, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems):

- Conformance: The SPTM function conforms to item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of diverse instrumentation and control described in Section 7.8.

7.2.3.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Function:

- Conformance: The SPTM function conforms to RG 1.22.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System:

- Conformance: The SPTM function conforms to RG 1.47.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The SPTM is organized into four physically and electrically-isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The SPTM function conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5..

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for safety-related Instrumentation:

- Conformance: The SPTM function conforms to RG 1.105. Reference 7.2-1 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection System:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: The SPTM function conforms to RG 1.151.

RG 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.152.

RG 1.153, Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The SPTM function conforms to10 CFR 50.55a(h).

RG 1.168, Verification, Validation Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.168 as implemented on the RTIF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.169 as implemented on the RTIF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.170 as implemented on the RTIF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.171 as implemented on the RTIF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.172 as implemented on the RTIF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.173 as implemented on the RTIF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The SPTM function conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The SPTM function conforms to RG 1.209 See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.2.3.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The SPTM function conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The SPTM function conforms to BTP HICB-11. RTIF logic controllers for the SPTM use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The SPTM function conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The SPTM function conforms to BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The SPTM function conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The SPTM function conforms to BTP HICB-17.

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

- Conformance: The SPTM function conforms to BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The SPTM function conforms to BTP HICB-21.

7.2.3.3.6 TMI Action Plan Requirements

In accordance with the SRP for Section 7.2 and with Table 7.1-1, only I.D.3 applies to the SPTM function. This is addressed in Subsection 7.2.3.3.1 for 10 CFR 50.34(f)(2)(v). TMI action plan requirements are generically addressed in Table 1A-1 of Appendix 1A.

7.2.3.4 Testing and Inspection Requirements

Proper functioning of analog temperature sensors is verified by channel cross-comparison during the plant normal operation mode. The bulk pool temperatures are continuously compared between divisions and alarmed (for inconsistency) by the PCF.

Each of four SPTM safety-related divisions is testable during plant normal operation to determine the operational availability of the system. Each safety-related SPTM division has the capability for testing, adjustment, and inspection during a plant outage.

7.2.3.5 Instrumentation and Controls Requirements

The I&C requirements related to SPTM are addressed in Subsections 7.2.3.1 and 7.2.3.2.

7.2.4 COL Information

None.

7.2.5 References

7.2-1 GE-Hitachi Nuclear Energy, "GEH ABWR/ESBWR Setpoint Methodology," NEDE-33304P, Class III (Proprietary), Revision 1, November 2008, and NEDO-33304, Class I (Non-proprietary), Revision 1, November 2008.

7.2-2 (Deleted)

7.2-3 [*GE Hitachi Nuclear Energy, "ESBWR - Software Management Program Manual (SMPM),"* NEDE-33226P, Class III (Proprietary) Revision 4, May 2009, and *NEDO-33226, Class I (Non-proprietary), Revision 4, May 2009*.]*

7.2-4 [*GE Hitachi Nuclear Energy, "ESBWR - Software Quality Assurance Program Manual (SQAPM),"* NEDE-33245P, Class III (Proprietary), Revision 3, July 2008, and *NEDO-33245, Class I (Non-proprietary), Revision 3, July 2008.*]*

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

Table 7.2-1

Sensors Used in Functional Performance of RPS

Sensor Description	Number of Sensors
NMS (LPRM)	256
NMS (SRNM)	12
NBS reactor vessel pressure	4
Drywell pressure	4
RPV narrow range water level	4
Scram accumulator charging water header pressure	4
MSIV position switches	16
TSV position switches	4
TCV hydraulic trip system oil pressure	4
TBV position switches	48
Power generation bus voltage (Loss of All FW flow)	4
Condenser pressure	12
Suppression pool temperature	64
Feedwater temperature	8

Table 7.2-2

SRNM Trips and Rod Blocks

Trip/Block Description	Trip/Block Value[1]	Function	Comments
SRNM Short Period Trip	10 seconds	Scram	Bypassed in RUN mode Coincident and non-coincident modes [2]
SRNM Short Period Alarm	20 seconds	Rod Block	Bypassed in RUN mode Coincident and non-coincident modes
SRNM Period Withdrawal Permissive	55 seconds	Rod Block	Bypassed in RUN mode Coincident and non-coincident modes Signal is a permissive for automated rod motion
SRNM Inoperable (INOP)	Critical SRNM fault, module interlock disconnect; HV (excitation) voltage low	Scram and Rod Block	Bypassed in RUN mode Coincident and non-coincident modes
SRNM Downscale Alarm	3 cps	Rod Block	Bypassed in RUN mode Coincident and non-coincident modes
SRNM Upscale Flux Trip	5E+5 cps	Scram	Bypassed in RUN mode Non-coincident mode only Count rate range only

Table 7.2-2

SRNM Trips and Rod Blocks

Trip/Block Description	Trip/Block Value[1]	Function	Comments
SRNM Upscale Flux Alarm	1E+5 cps	Rod Block	Bypassed in RUN mode Non-coincident mode only Count rate range only
SRNM ATWS Permissive	6% power	Permissive signal to ATWS/SLC system (all modes)	Coincident and non-coincident modes

1. Instrument setpoint accuracy is determined by safety analyses using GEH instrument setpoint methodology (Reference 7.2-1).
2. Coincident and non-coincident modes controlled by plant procedures.

Table 7.2-3

SRNM Trip Signals

			Indicator Type		
Condition [1, 5]	**Rod Block**	**N-DCIS**	**Alarm**	**Indication**	**Reactor Trip[4]**
Upscale Trip [2]		X	X	X	X
Upscale Alarm	X	X	X	X	
Period Trip [3]		X	X	X	X
Period Alarm	X	X	X	X	
Period Withdrawal Permissive	X	X	X	X	
Inoperative	X	X	X	X	X
Downscale Alarm	X	X	X	X	
Channel Bypass		X		X	

1. No trips are active in Run mode or for a bypassed channel; however, they are active in other operating modes.
2. This trip is operable in the non-coincident mode.
3. For trip conditions, see Subsection 7.2.2.1.1.1.
4. This refers to channel/division trip signal provided to RPS.
5. These signals are all sent to N-DCIS for monitoring, alarming and recording. They are also available on safety-related displays.

Table 7.2-4

APRM Trip Function Summary

Trip Function	Analytical Limit For Trip Setpoint [1]	Action
APRM Upscale Flux Trip	125% power 15% power	Scram (only in Run) Scram (not in Run)
APRM Upscale Flux Alarm	108% power 12% power	Rod Block (only in Run) Rod Block (not in Run)
APRM Upscale Simulated Thermal Power Trip	115% power	Scram
APRM Inoperative	1. LPRM inputs too few; 2. Module interlocks disconnect	Scram & Rod Block Scram & Rod Block
APRM ATWS Permissive	6% power	ADS Permissive signal to SSLC system (all modes)
APRM Downscale	5% power	Rod Block (only in Run)

1. Instrument setpoint accuracy is determined by safety analyses using GEH instrument setpoint methodology of Reference 7.2-1.

Table 7.2-5

Outputs from SPTMs to Other Systems

Signal	Utilization
Sixteen divisional suppression pool local temperature signals to each safety-related DCIS RMU (in each of 4 divisions).	Input for divisional scram initiation and temperature status display within SSLC/ESF and RPS. Input for non-divisional suppression pool cooling mode initiation (FAPCS). Input for non-divisional suppression pool temperature data display, alarm and recording (within N-DCIS & MCR).

Table 7.2-6

OPRM Trip Function Summary

Trip Function	Analytical Limit For Trip Setpoint [1]	Action
OPRM Inoperative	LPRM inputs too few	OPRM Cell/Channel Alarm
OPRM Oscillation Detection	Per TRACG developed setpoint tables and ESBWR core stability curves	Channel Trip
OPRM Oscillation Detection	Per TRACG developed setpoint tables and ESBWR core stability curves	Channel Alarm
OPRM Bypass	N/A	Controlled by APRM bypass

1. Instrument setpoint accuracy is determined by safety analyses using GEH instrument setpoint methodology of Reference 7.2-1.

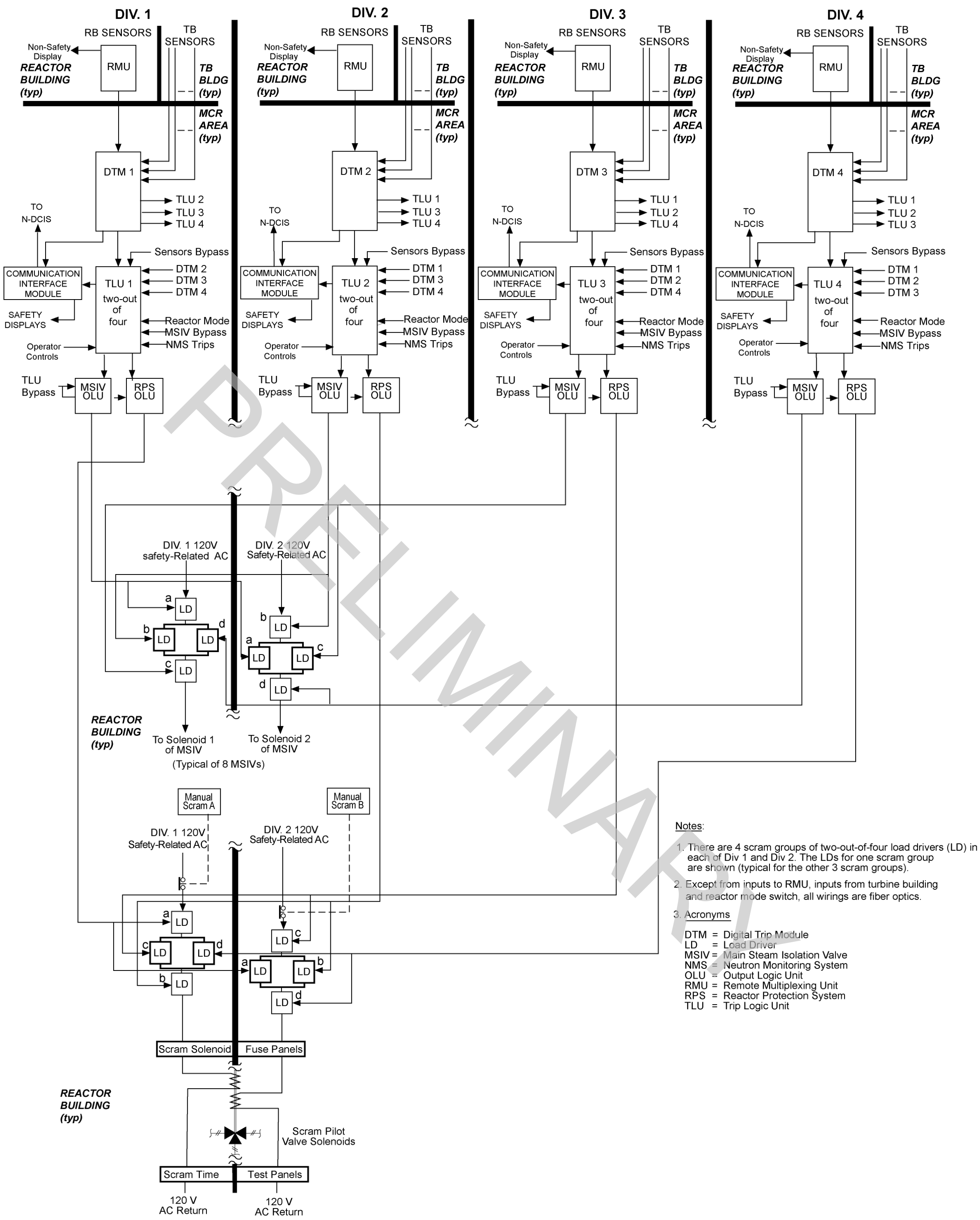
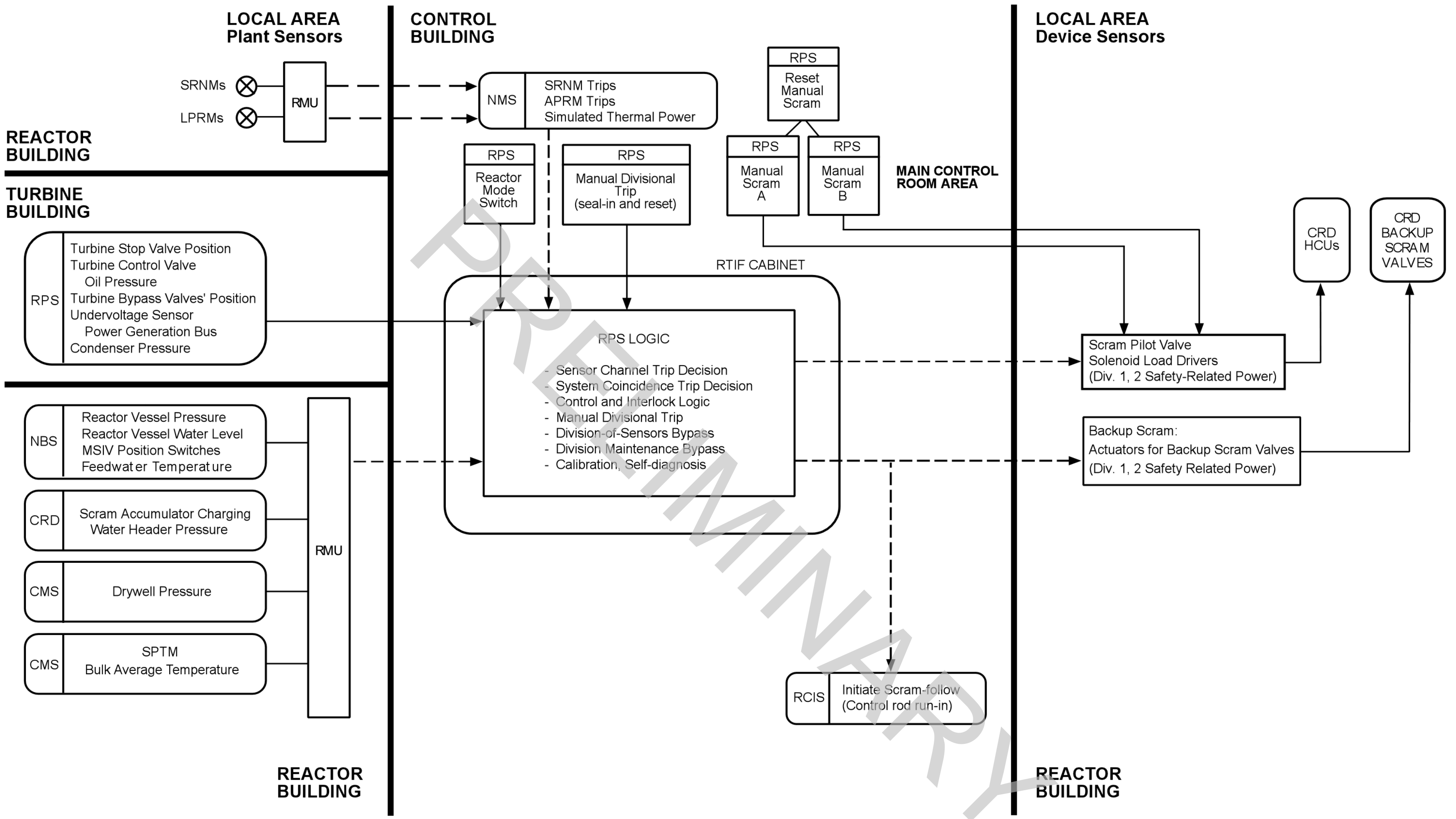


Figure 7.2-1. RPS Functional Block Diagram



1. Optical Signals on Fiber Optic Cable
2. Electrical Signals on Metallic Cable

Figure 7.2-2. RPS Interfaces and Boundaries Diagram

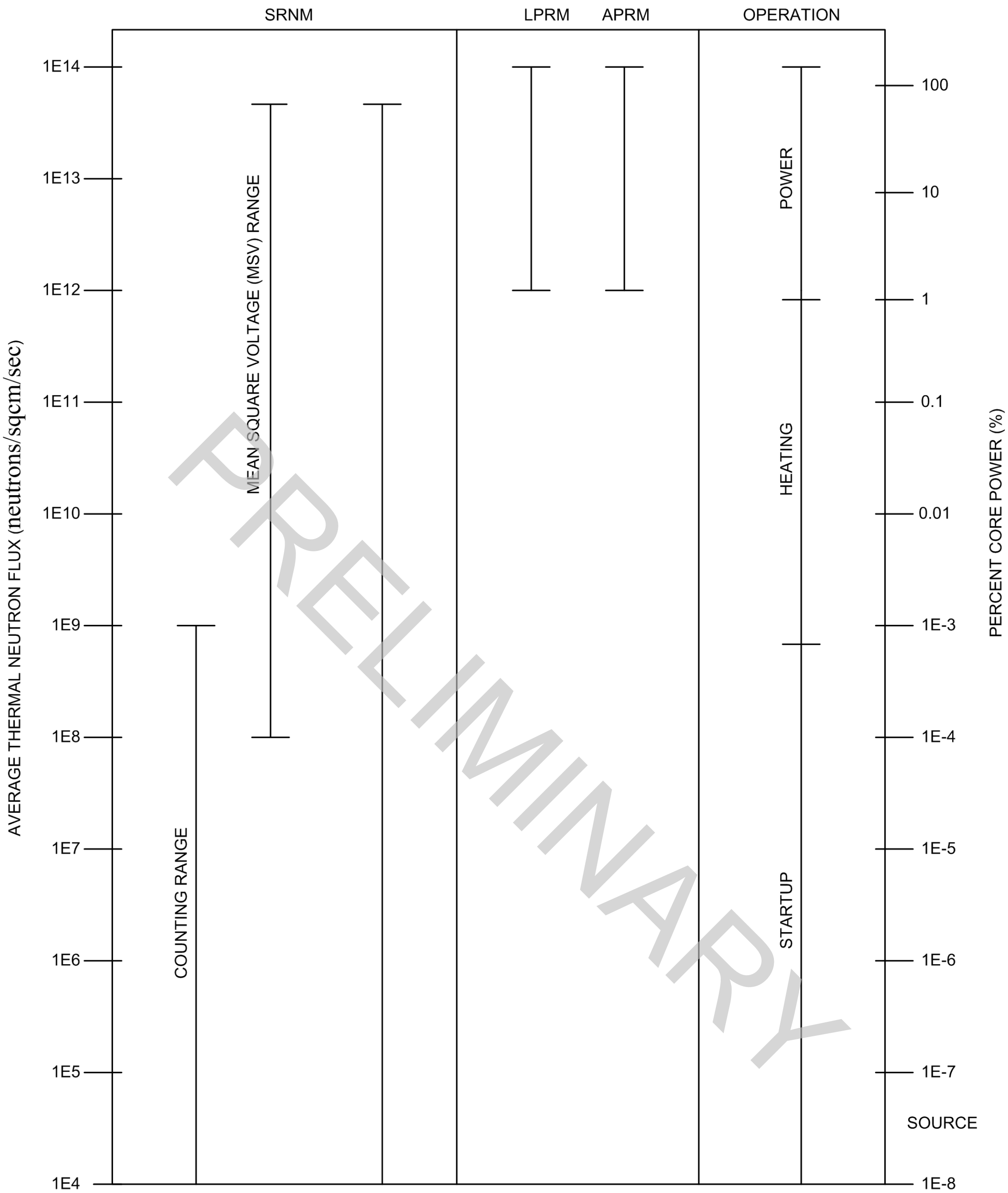


Figure 7.2-3. Neutron Flux Monitoring Ranges

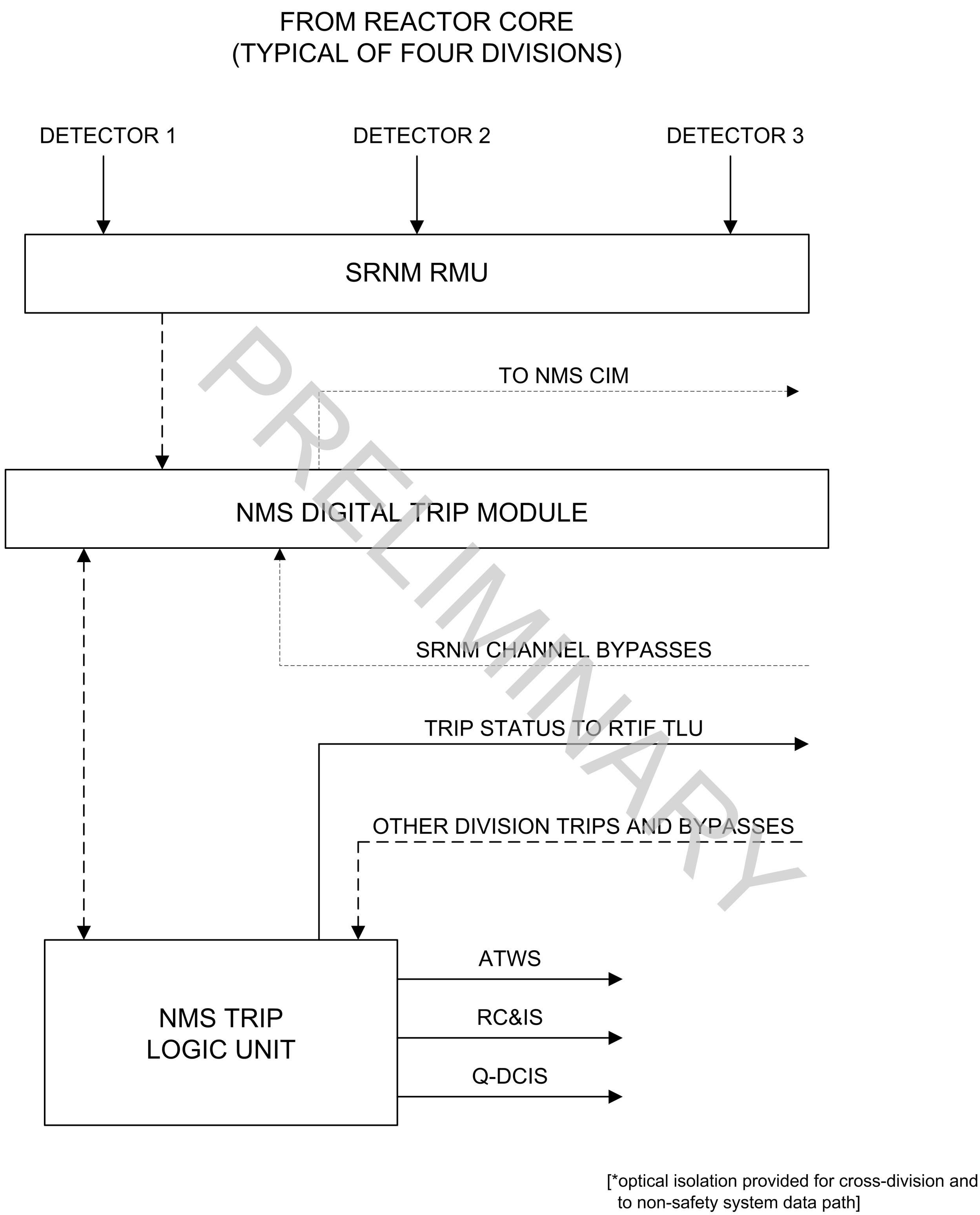


Figure 7.2-4. Basic Configuration of a Typical SRNM Subsystem

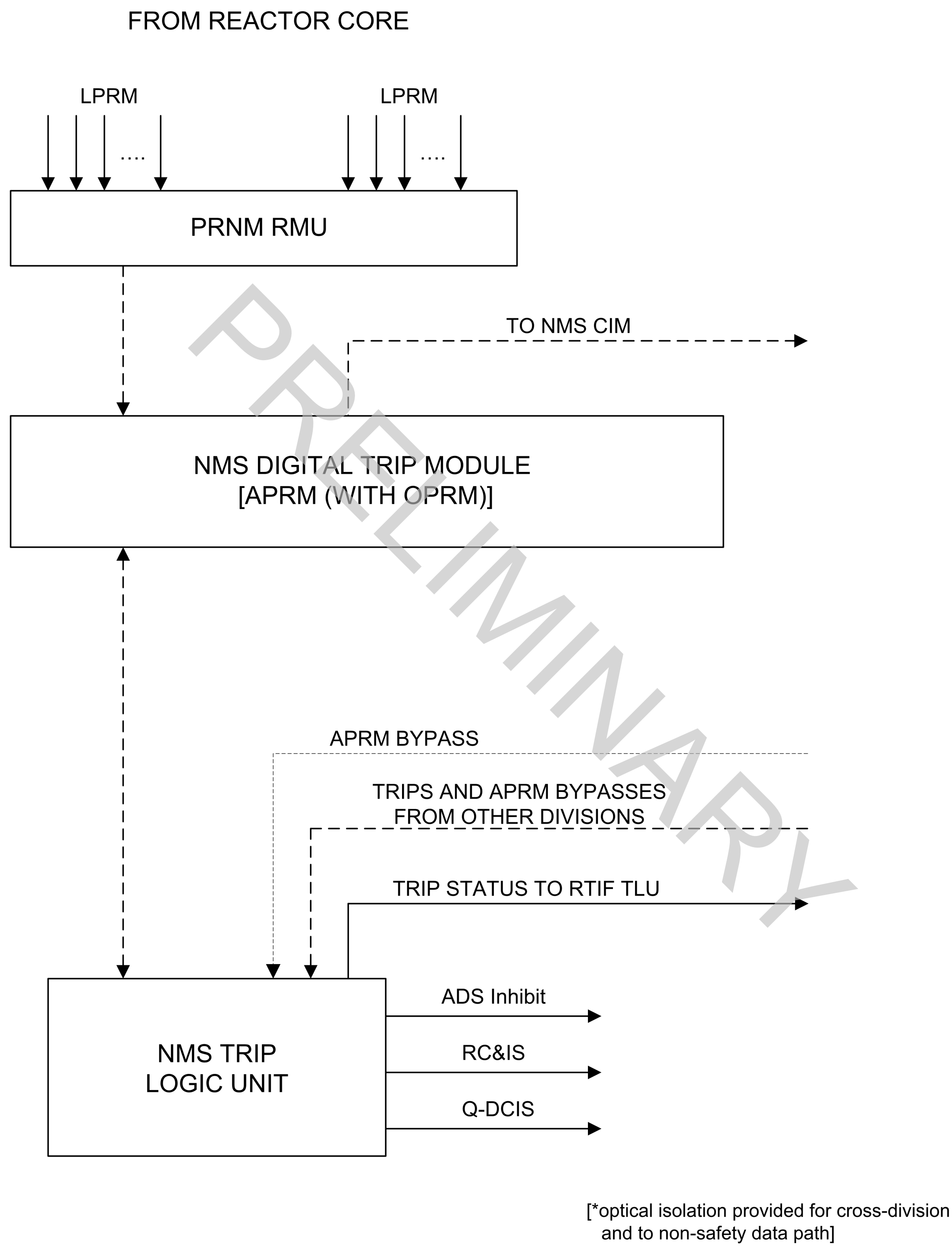


Figure 7.2-5. Basic Configuration of a Typical PRNM Subsystem

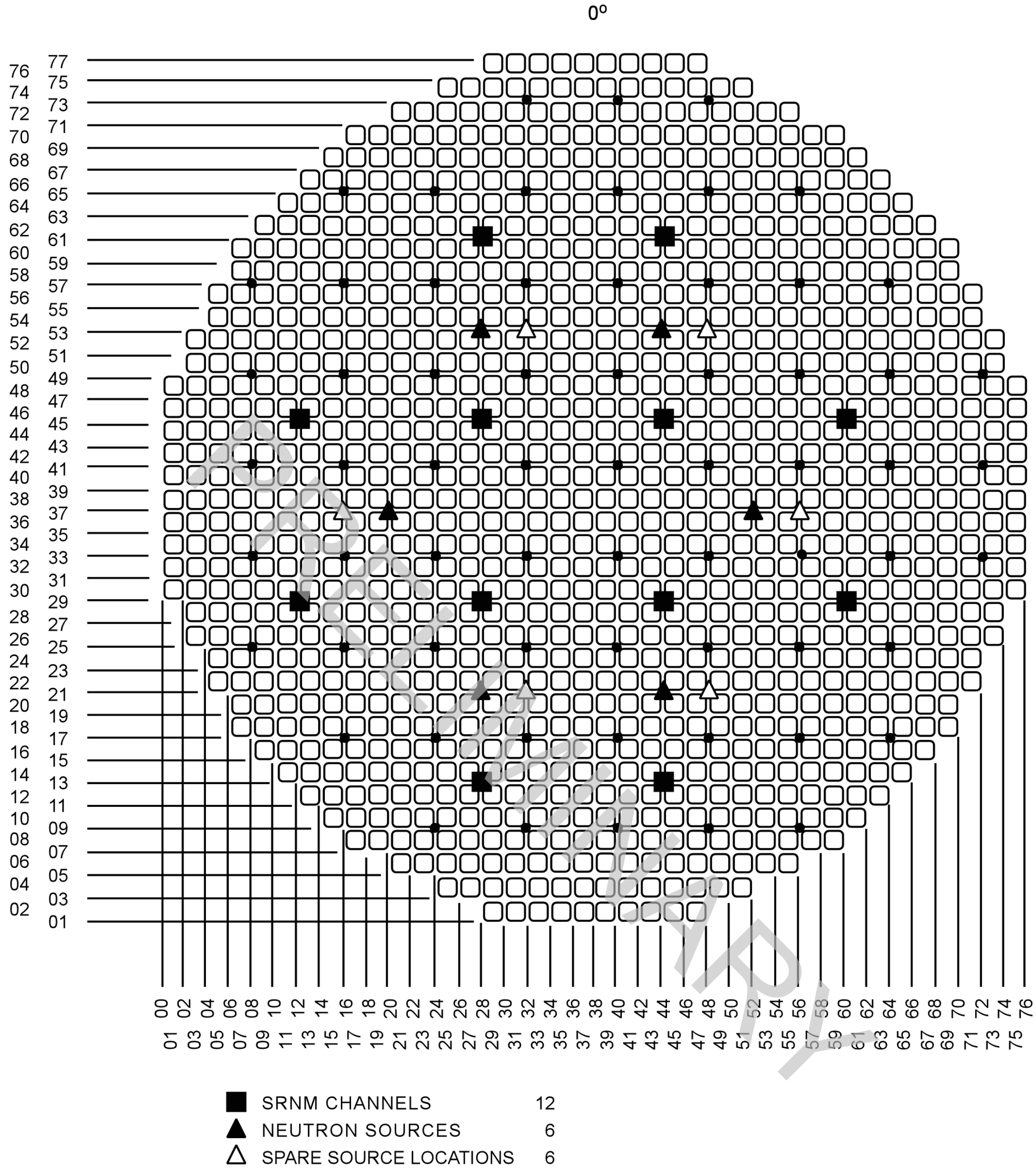
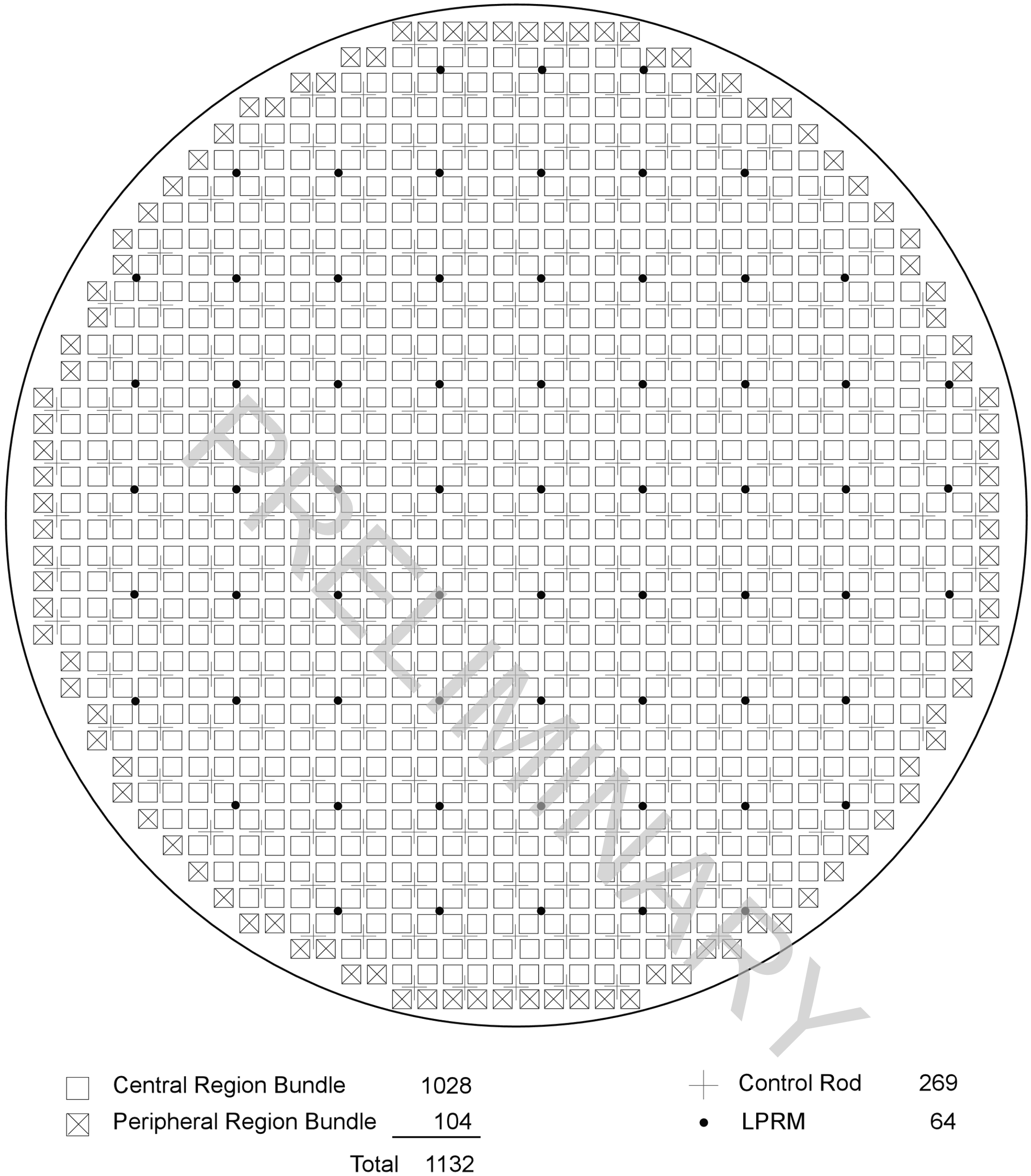


Figure 7.2-6. SRNM Detector Locations



ESBWR Core Map

Figure 7.2-7. LPRM Locations in the Core

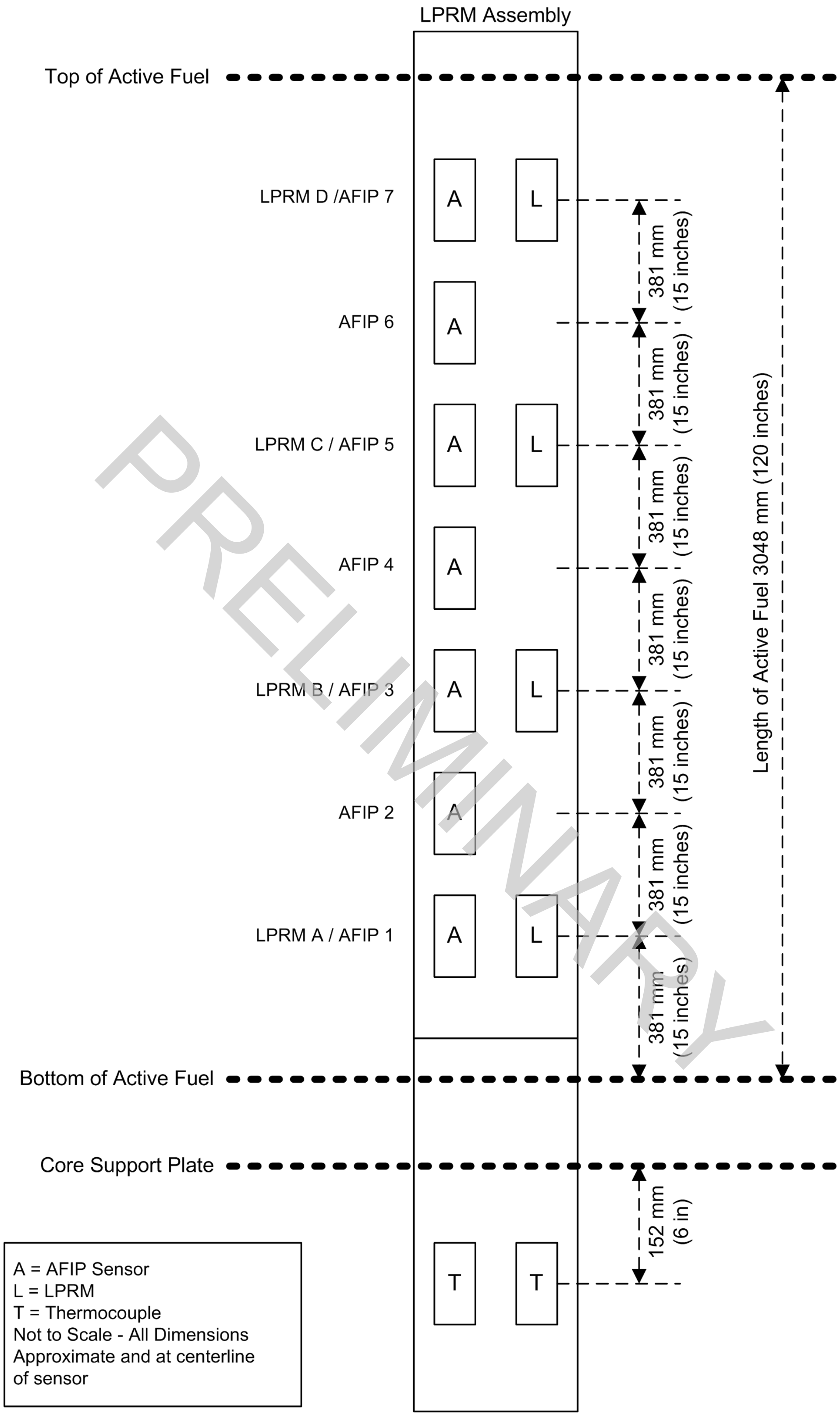


Figure 7.2-8. Axial Distribution of LPRM Detectors

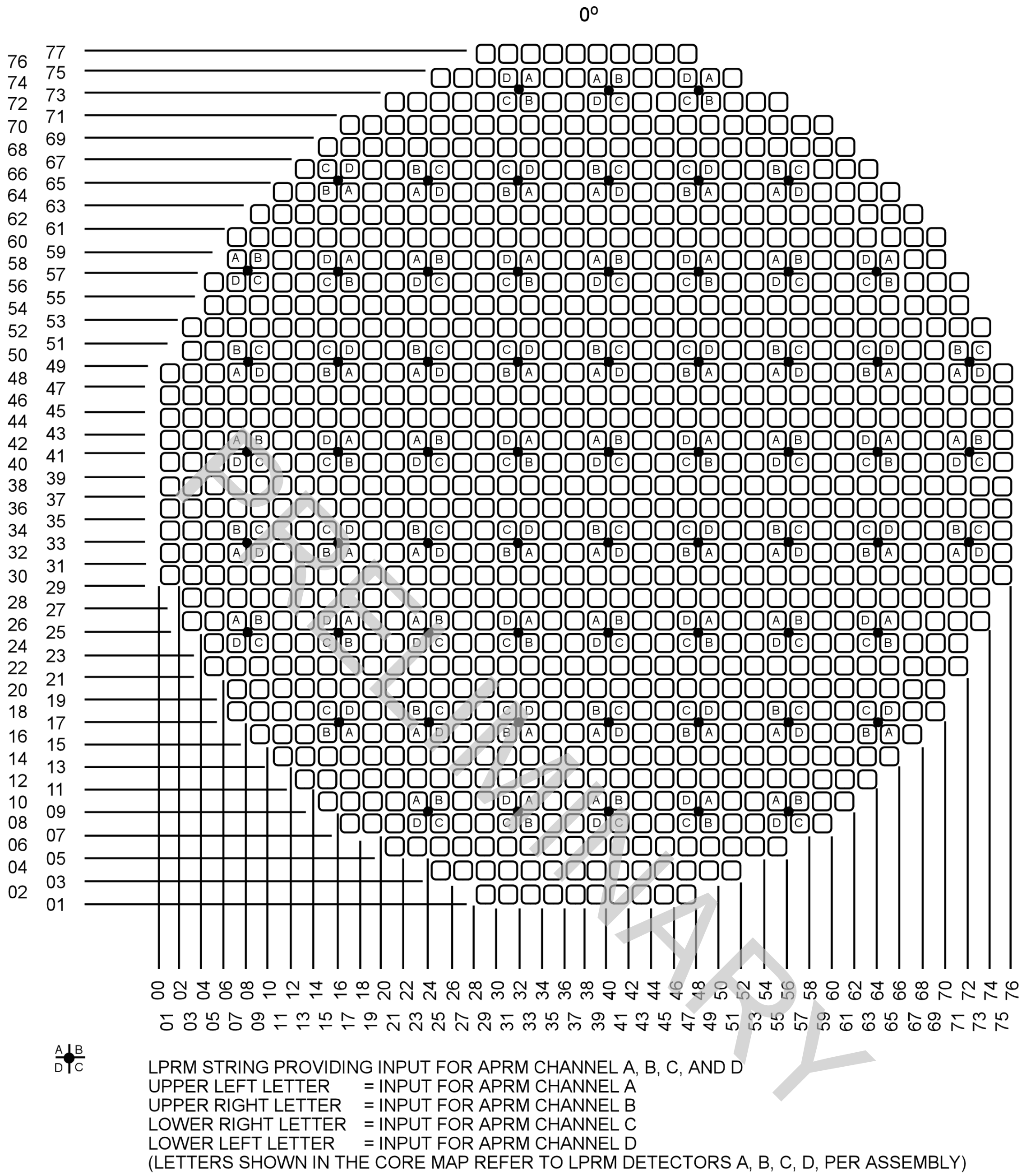
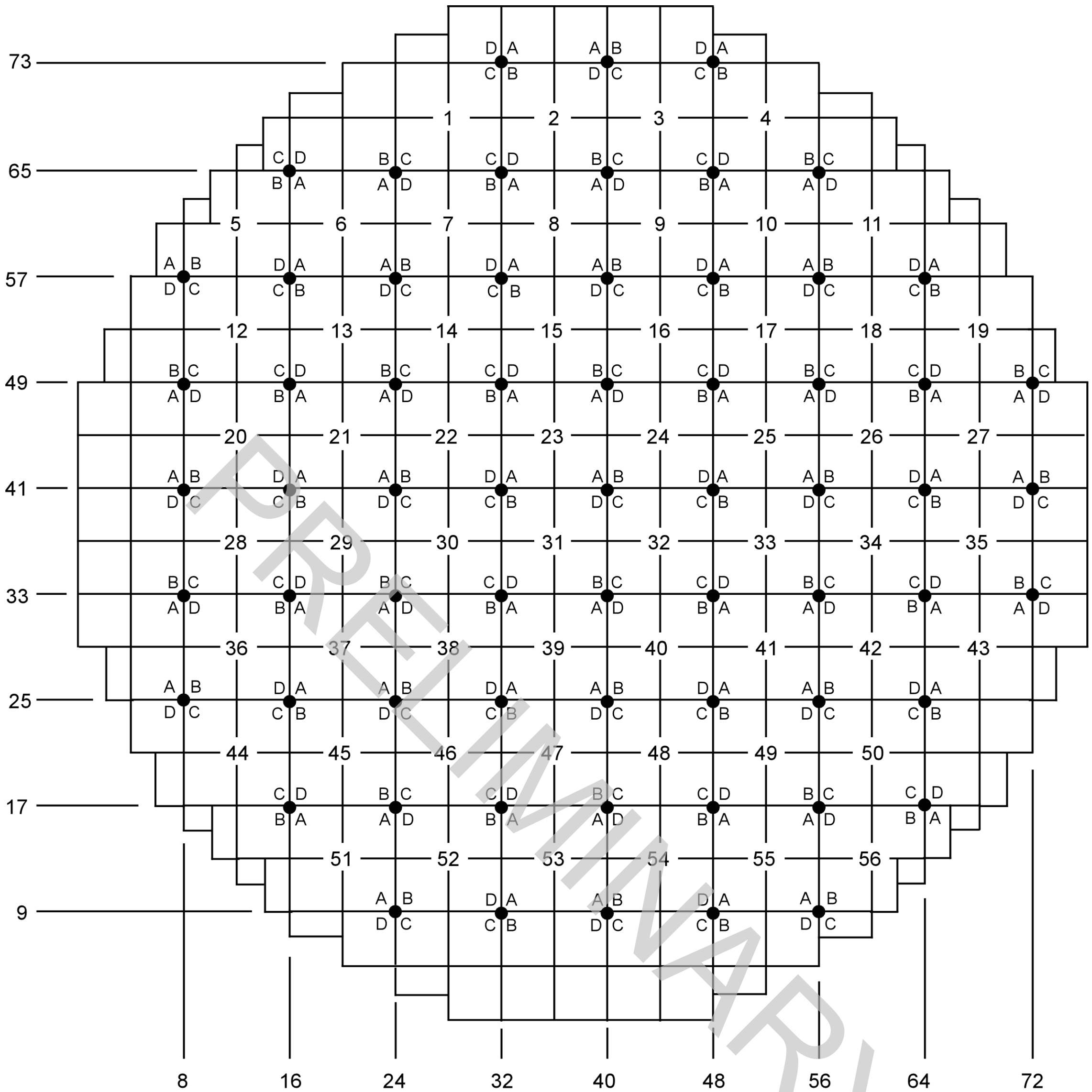


Figure 7.2-9. LPRM Assignments to APRM Channels



A B / D C LPRMs PROVIDING INPUT TO OPRM CHANNELS A, B, C, AND D

UPPER LEFT LETTER = INPUT FOR OPRM CHANNEL A
UPPER RIGHT LETTER = INPUT FOR OPRM CHANNEL B
LOWER RIGHT LETTER = INPUT FOR OPRM CHANNEL C
LOWER LEFT LETTER = INPUT FOR OPRM CHANNEL D
(LETTERS IN THE MAP REFER TO LPRM DETECTORS A, B, C, D PER ASSEMBLY)

Figure 7.2-10. LPRM Assignment to OPRM Channels

(Typical of four divisions)

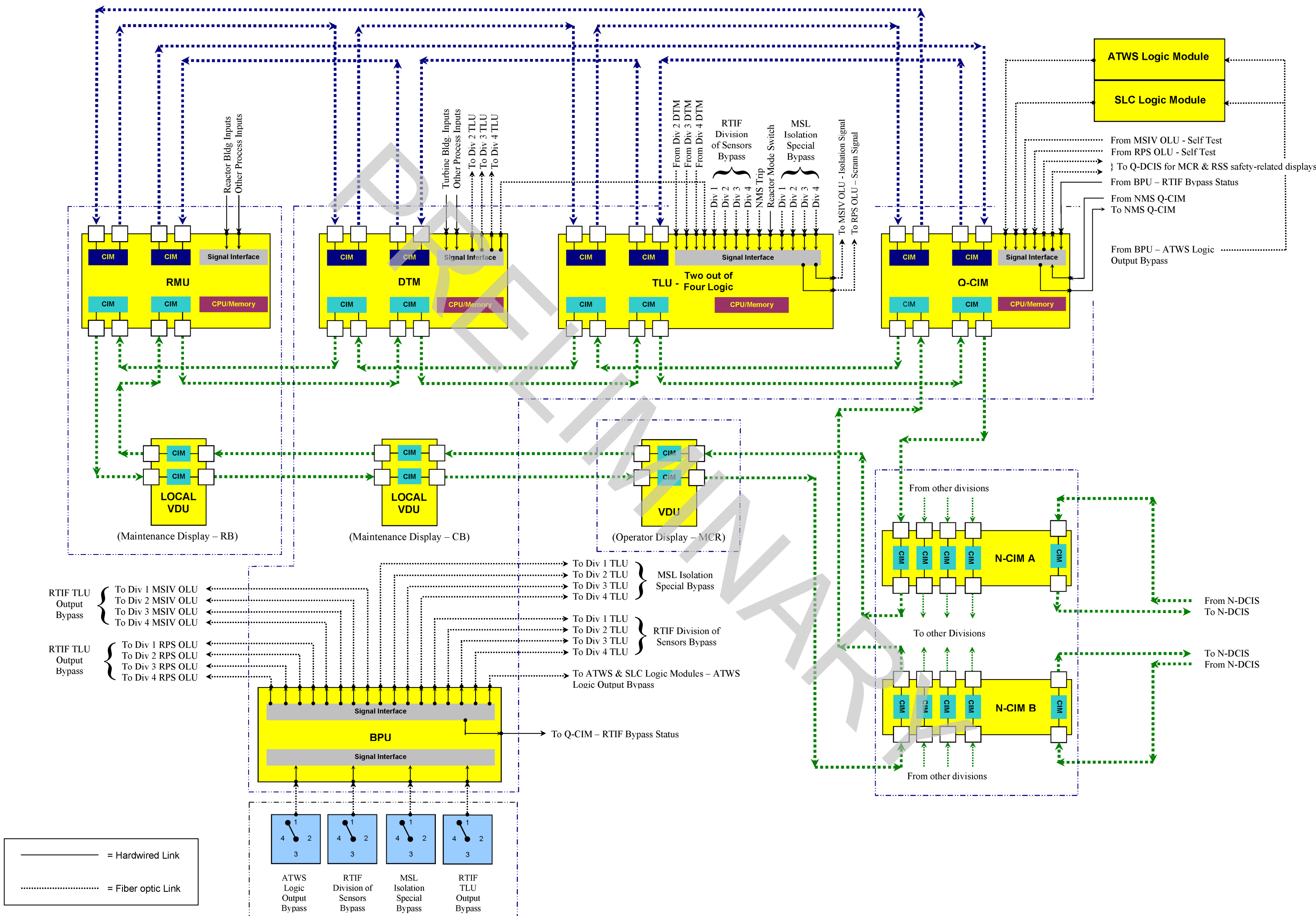


Figure 7.2-11a. Reactor Trip and Isolation Function (RTIF) Functional Block Diagram

(Four Divisions Shown)

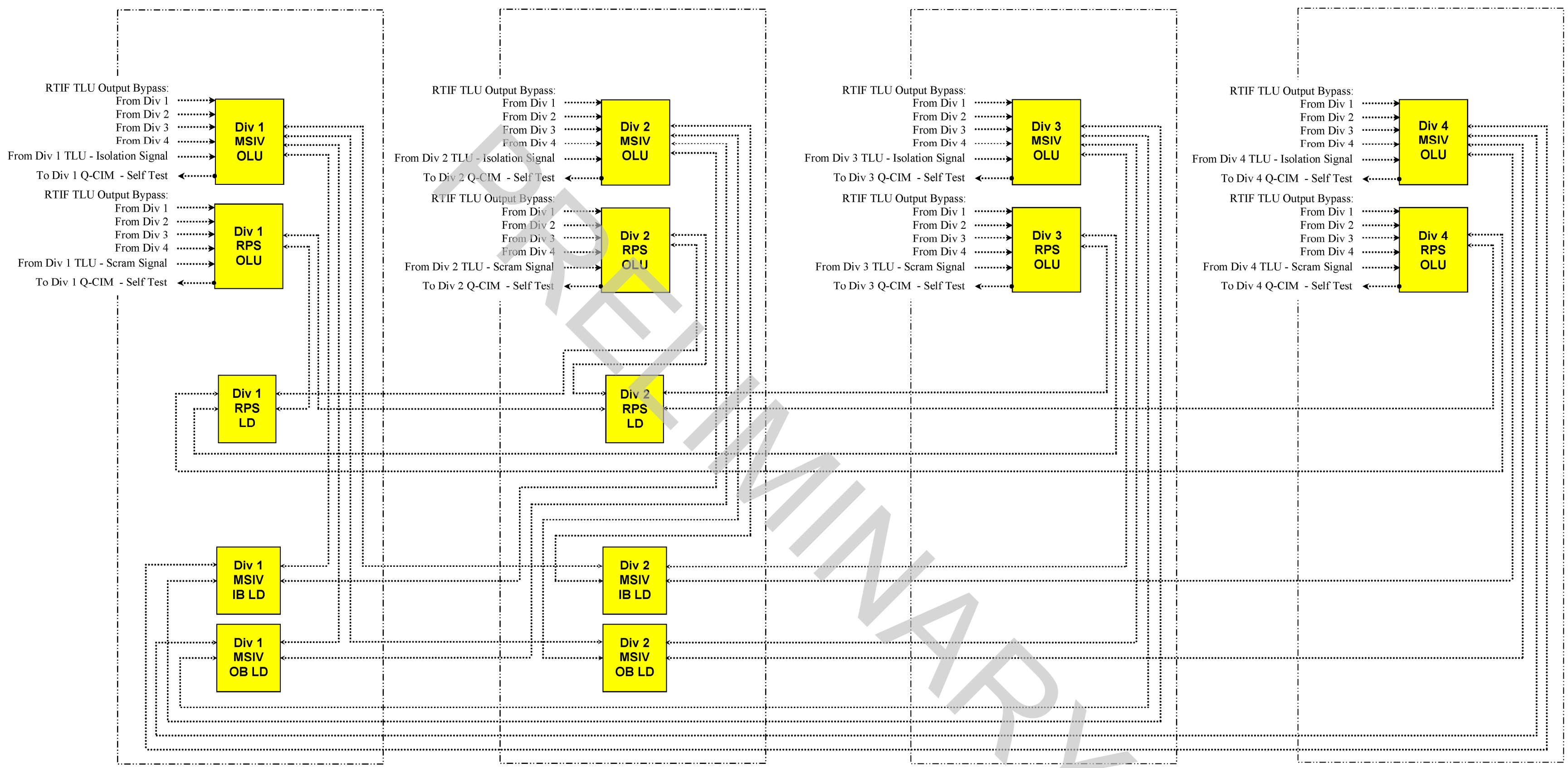


Figure 7.2-11b. Reactor Trip and Isolation Function (RTIF) Functional Block Diagram – Output Logic Unit Detail

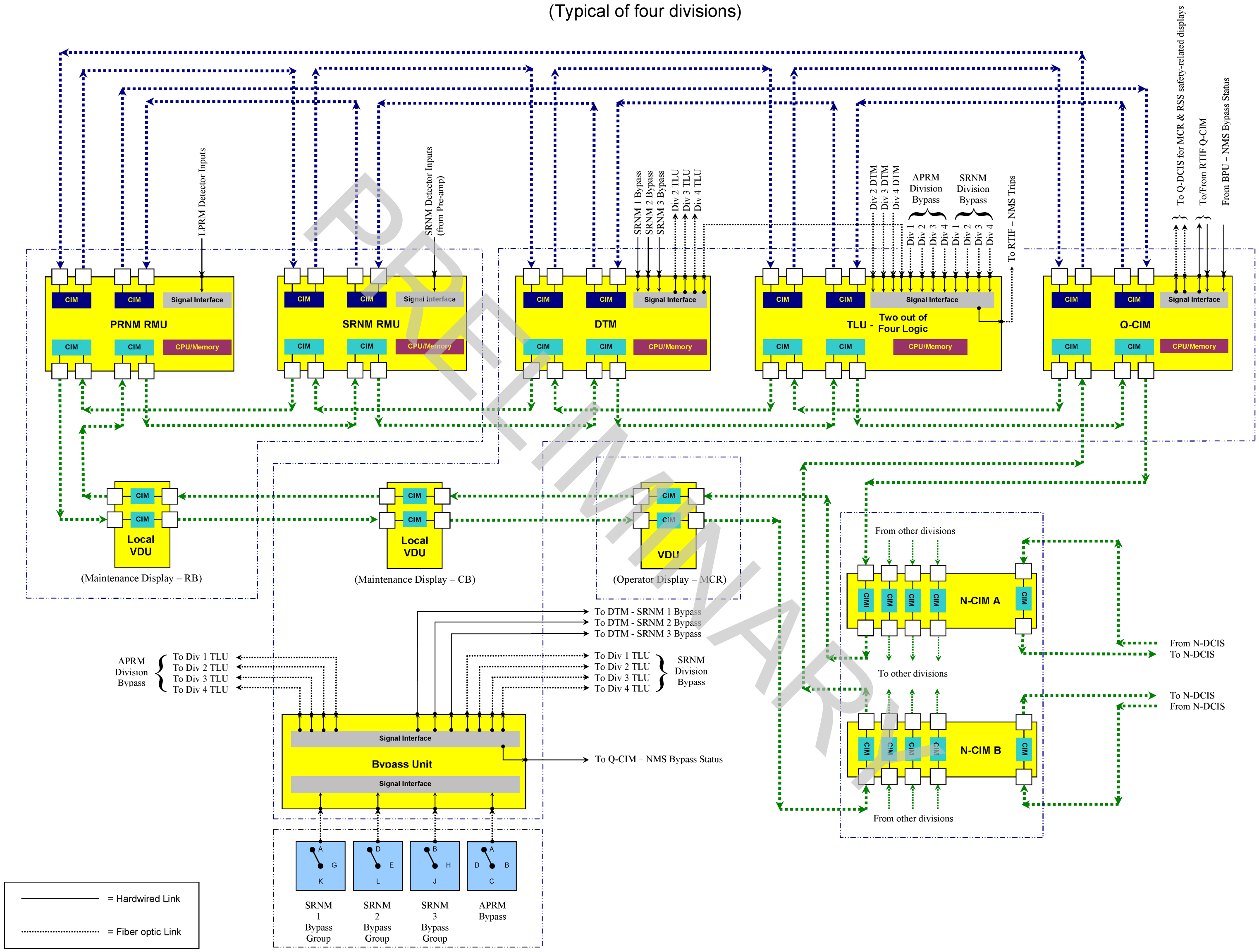


Figure 7.2-12. Neutron Monitoring System (NMS) Functional Block Diagram

7.3 ENGINEERED SAFETY FEATURES SYSTEMS

The Engineered Safety Features (ESF) systems are part of a group of systems collectively called the Safety-Related Distributed Control and Information System (Q-DCIS). A simplified network functional diagram of the DCIS is included as Figure 7.1-1. This diagram indicates the relationships of the ESF systems with their safety-related peers and with nonsafety-related plant data systems collectively called the Nonsafety-Related Distributed Control and Information Systems (N-DCIS). Section 7.1 contains a description of these relationships.

7.3.1 Emergency Core Cooling System

The Emergency Core Cooling System (ECCS) comprises the Automatic Depressurization System (ADS), the Gravity-Driven Cooling System (GDCS), the Isolation Condenser System (ICS) (Subsection 7.4.4), and the Standby Liquid Control (SLC) System (Subsection 7.4.1).

7.3.1.1 Automatic Depressurization System

The ADS resides within the Nuclear Boiler System (NBS). It depressurizes the reactor so that the low-pressure GDCS can provide make up coolant to the Reactor Pressure Vessel (RPV).

7.3.1.1.1 System Design Bases

The ADS instrumentation and controls (I&C) safety-related requirements are to:

- Detect reactor low water level, RPV Level 1 (see Subsection 7.7.1.2 and Figure 7.7-1 for more information on the definition of water levels),
- Automatically actuate the Safety Relief Valves (SRVs) and Depressurization Valves (DPVs) after RPV Level 1 is reached or drywell pressure high is detected,
- Actuate the SRVs and DPVs sequentially and in groups to achieve the required depressurization characteristics,
- Render no more than one valve inoperative for any single failure,
- Ensure physical and electrical separation and isolation between safety-related divisions and from nonsafety-related circuits and equipment, and
- Indicate the status of SRV and DPV in the Main Control Room (MCR).

The ADS I&C meet the nonsafety-related requirements that:

- No single I&C failure inadvertently opens an SRV or a DPV, and
- ADS-parameter alarms are provided in the MCR.

7.3.1.1.2 System Description

The ADS is a subsystem of the NBS and comprises 10 SRVs, eight DPVs, and the associated I&C. The SRVs are nitrogen operated solenoid actuated relief valves. The DPVs are electrically operated squib valves. The SRVs and DPVs are divided into groups, and lift in sequence when required, and are described in detail in Subsection 5.2.2 and Subsection 6.3.2, respectively.

The NBS functional components (including the ADS) are shown on Figure 5.1-2. The mechanical aspects of the ADS functions within the ECCS are discussed in Subsection 6.3.3. Typical SRV and DPV logic and control are shown on Figures 7.3-1a and 7.3-1b, respectively.

Automatic Operation

Actuation of ADS equipment is controlled automatically, without need for operator action. Capability for manual actuation also is provided (IEEE Std. 603, Sections 6.2 and 7.2).

Automatic actuation of the ADS occurs when the RPV water reaches Level 1, which is detected by four wide range RPV water level transmitters. ADS is also initiated on drywell pressure high (using four pressure transmitters). These transmitters are separate from those used for Reactor Protection System (RPS) functions and diverse from the Diverse Protection System (DPS) wide range level transmitters.

When a sustained RPV Level 1 is detected for 10 seconds or sustained drywell pressure high is detected for 60 minutes, five SRVs (group 1) are opened to start RPV pressure reduction, followed by the remaining five SRVs (group 2) after a time delay. See Table 7.3-2 for the time delay parameters. The sequence continues with groups of DPVs, each opening after further successive time delays. See Table 7.3-3 for the DPV groups and time delay parameters. This sequential operation minimizes the water loss as a result of liquid swell in the RPV when its pressure is rapidly reduced. See Table 5.2-2 for the SRV and DPV settings and/or capacities.

Automatic initiation of ADS is inhibited by the ATWS/SLC system logic as described in Subsection 7.8.1.1.1.2. The ADS Inhibit signal inhibits the sequenced start logic for the SRV and DPV valves.

Additionally, as discussed in Subsection 7.8.1.2, the DPS has the ability to open independently the same SRVs and DPVs using the same logic, but using diverse hardware/software equipment and a diverse set of reactor-level and drywell pressure sensors For the ADS, the DPS can actuate a fourth, nonsafety-related solenoid on each of the SRVs, and a fourth squib initiator on each of the DPVs.

Manual Operation

The safety-related Video Display Units (VDUs) in the MCR provide a display format allowing the operator to manually open each SRV and each DPV independently, using the primary Safety System Logic and Control/ESF (SSLC/ESF) platform. Each nonsafety-related VDU in the MCR provides a display format allowing the operator to manually open each SRV independently, using the DPS logic function. Each display uses an "arm/fire" configuration requiring at least two deliberate operator actions. Operator use of the "arm" portion of the display triggers a plant alarm. The two manual opening schemes from SSLC/ESF and from DPS are diverse.

Each safety-related VDU provides a display with an "arm/fire" switch (one per division) to manually initiate ADS as a system, rather than initiating each valve individually (IEEE Std. 603, Sections 5.8, 6.2 and 7.2). If the operator uses any two of the four "arm/fire" switches, the ADS sequence seals in and starts the ADS valve opening sequence. This requires at least four (two arm and two fire) deliberate operator actions.

MCR controls are provided to manually inhibit the ADS under ATWS conditions (as described in Subsection 7.8.1.1.1.2).

Actuation Logic

See Figure 7.3-1a for typical SRV actuation logic, and Figure 7.3-1b for typical GDCS and DPV actuation logic.

The ADS actuation logic is implemented in four SSLC/ESF divisions, each of which can make a RPV Level 1 or drywell pressure high trip vote. Each of the divisional trip votes is shared with the other divisions. Normally, each of the four divisions makes a two-out-of-four trip decision from the four divisional votes; however, the entire SSLC/ESF system has a bypass control such that any single division of sensors can be removed from the two-out-of-four decision process, so that the remaining three divisions operate with a two-out-of-three trip decision. Only one division at a time can be bypassed, and used to facilitate either maintenance or calibration activities. Divisional bypasses are alarmed in the MCR.

Each division of SSLC/ESF is configured such that all functions (like the DTM function or 2/4 voter function) are implemented in triply redundant processors, to support the requirement that single divisional failures cannot result in inadvertently opening any ADS valve (SRV or DPV). (See Figures 7.3-1a, 7.3-1b.) The four divisional sensor signals and their trip setpoints are continuously monitored for consistency by the N-DCIS plant computer functions (technical specification monitor). An inconsistency results in an alarm. RPV level within each division is measured independently by three separate A/D converters in the RMU and sent by three redundant paths to the triply redundant processors in the SSLC/ESF. The triply redundant logic in each division will issue an RPV Level 1 trip signal if the measured RPV water level drops below the Level 1 setpoint. Similarly the triply redundant measurements and logic will issue a Drywell Pressure High trip signal if measured drywell pressure exceeds the high drywell pressure setpoint.

The RPV Level 1 and Drywell Pressure High signal actuates the timers in the triply redundant processors (see Tables 7.3-2 and 7.3-3). If the trip signal resets (as, for example, from an instrument column transient), the timer resets and restarts when the next trip signal is received. If the RPV Level 1 trip signal sustained for 10 seconds, the logic seals in and issues an RPV Level 1 signal. The RPV Level 1 signal is also used to start ECCS subsystems in sequence. The SSLC/ESF platform is described in Subsection 7.3.5. The RPV Level 1 signal specifically actuates five timers in the triply redundant ADS logic. If the drywell pressure high trip signal sustained for 60 minutes, the logic seals in and issues a Drywell Pressure High signal. The Drywell Pressure High signal also actuates the five timers in the triply redundant logic. The Drywell Pressure High signal is also used to actuate GDCS injection valve timer operation as described in Subsection 7.3.1.2.

Divisional separation is maintained by using optical isolators and separate raceway, conduit, and penetration wiring to each SRV or DPV. Trip signals from any two divisions can open all of the ADS valves.

The actual firing circuit for the various squib initiators and SRV solenoids consists of two (solenoid) or three (squib initiator) load driver/discrete output circuits, followed by a continuity monitor and a disable/test switch all arranged in series, and located in two (per division) safety-related or DPS RMUs in the Reactor Building (RB); the two RMUs associated with the firing circuit are located in different fire areas. Because there is the division of sensors bypass and the logic is implemented in a triply redundant controller and multiple load drivers/discrete outputs are used, no additional division of trip logic bypass is implemented in the SSLC/ESF logic. It is undesirable to perform this level of bypass activity with the RMU electrically connected to the valve. The disable/test switch described below provides the bypass function required. In addition to the usual RMU self-diagnostics, means are provided to indicate that each of the series load driver/discrete output circuits can be "closed" (the circuits can be exercised one at a time from the MCR) and to indicate that both have closed.

The disable/test switch (Figure 7.3-1b) that disables the firing circuit affects one valve and does not interact with the other valves allocated to that RMU. Operation of any disable/test switch triggers an MCR alarm indicating that the firing circuit is out of service. Although the load driver/discrete output checks can be done online (one at a time) without causing valve operation, opening the firing circuit with the disable/test switch allows the continuity monitor to be tested, and allows online surveillance and maintenance activities to be done, with the assurance that a valve is not opened inadvertently. The operation of a disable/test switch in any one division does not disable the SRV or DPV because it maintains the ability to be opened by its other divisional solenoid/squib initiator. Additionally it is not possible to lose single failure inadvertent actuation protection by any operator or disable/test switch action.

The ADS design parameters shown in Table 7.3-1 ensure that no single failure of an ADS division logic, SRV actuation pilot, or DPV igniter circuit can prevent successful system operation as long as any three of the four divisions of safety-related power are available. This satisfies the single failure criterion.

Supporting systems for the ADS include the instrumentation, logic, control, and motive power sources. The instrumentation and logic power is supplied by the corresponding divisional safety-related power sources. The actual SRV solenoid and DPV squib initiator power also is supplied by the corresponding divisional safety-related or nonsafety-related load group power sources (See Subsection 8.3.1.1.3). The motive power for the electrically operated pneumatic pilot solenoid valves on the SRVs is from accumulators located near the SRVs, and supplied with nitrogen by the High Pressure Nitrogen Supply System (HPNSS).

7.3.1.1.3 Safety Evaluation

Chapter 15 and Section 6.3 evaluate the individual and combined capabilities of the ECCS systems, including the ADS. For the entire range of reactor coolant system break sizes, the ECCS systems ensure that the reactor core always is submerged.

SSLC/ESF initiating instrumentation, including the ADS, responds to the potential inadequacy of core cooling regardless of the location of the breach in the reactor coolant pressure boundary (RCPB). Detection of RPV low water level, which is completely independent of breach location, is used to initiate the ADS.

The redundancy of the control and monitoring equipment for the ADS is consistent with the redundancy of the four divisions of ADS.

No single failure in the ADS initiation circuitry can prevent the ADS from depressurizing the RPV, or cause an inadvertent actuation of the ADS. This satisfies the single failure criterion of IEEE Std. 603, Section 5.1.

The ADS has no equipment protective interlocks that could interrupt automatic system operation.

The ADS instrumentation and logic, and the SRV and DPV initiation circuitry is powered by divisionally separated safety-related power sources.

Table 7.1-1 identifies the ADS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.1.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The ADS design complies with 10 CFR 50.55a(a)(1).

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The ADS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the ADS design conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.3.1.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses See Subsection 7.3.1.1.2.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to ADS.
  - Section 5.2 (Completion of Protective Actions): See Subsection 7.3.1.1.2.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 7.3.1.1.2.
  - Section 6.2 and 7.2 (Manual Control): See Subsection 7.3.1.1.2.
  - Section 6.4 (Derivation of System Inputs): Derivation of System Inputs for the DPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.20.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 7.3.1.1.2.
  - Section 6.6 and 7.4 (Operating Bypasses): See Subsection 7.3.1.1.2.
  - Section 6.7 and 7.5 (Maintenance Bypasses): See Subsection 7.3.1.1.2.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the DPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the DPS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.34(f)(1)(x)[II.K.3.28], Automatic Depressurization System Functioning During/Following an Accident Situation:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.34 (f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The ADS design complies with 10 CFR 50.34 (f) (2) (v) [I.D.3].

10 CFR 50.34(f)(2)(x)[II.D.1], Relief and Safety Valve Test Requirements:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.34(f)(2)(xi)[II.D.3], Direct Indication of Relief and Safety Valve Position in the Control Room:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: NBS provides the reactor water level measurement (temperature compensated) inputs to ADS. The reactor water level instrumentation errors due to non-condensable gases in instrument reference legs are addressed in Subsection 7.7.1.2.2.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instruments for Monitoring Plant Conditions Following Core Damage:

- Conformance: The ADS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The ADS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the ADS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.1.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 15, 19, 20, 21, 22, 23, 24, 29, 30, 33, 35, and 37:

- Conformance: The ADS design complies with these GDCs.

7.3.1.1.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: Implementation of a Diverse I&C System, the DPS, is described in Section 7.8.

7.3.1.1.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: Components are tested periodically during refueling outages every two years. The ADS design conforms to RG 1.22 with the clarification that for the DPVs, periodic testing is interpreted to mean testing of the squib initiators in a laboratory after removal from the squib valves.

  Because the DPVs are squib-actuated and cannot be closed once they are opened, there is no practicable system design to allow testing during reactor operation without creating an unacceptable breach of the RCPB. The SRVs are tested with the reactor at low power and at, or near, rated pressure. Both the squib wires and the SRV solenoids are continuously monitored for electrical continuity, as indicated in Subsection 7.3.1.1.4.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The ADS design conforms to RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The ADS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The ADS design conforms to RG 1.62. Manual actuation of ADS requires the operator to actuate at least two dual action switches. This ensures that manual initiation of the ADS is a premeditated act.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The ADS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints used to initiate the ADS are consistent with RG 1.105. Because the discrete setpoints in the ADS logic do not drift, most of the variation is expected to be in the process transmitters. Setpoints are continuously monitored and alarmed by the PCF. Reference 7.3-2 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118. A full functional test of the ADS is not practical, because a LOCA results if the non-reclosable DPVs are opened. Acceptable reliability of equipment operation is demonstrated by alternate test methods. System logic is periodically self-tested, and initiating circuits are continuously monitored. DPV valve initiators periodically are removed and test-fired in a laboratory. RPV level transmitters are located outside containment, so calibration verification can be performed during plant operation.

RG 1.151, Instrument Sensing Lines:

- Conformance: NBS provides the measurement inputs to ADS. The NBS instrument sensing lines conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The ADS design conforms to 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The ADS design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The ADS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The ADS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.1.1.3.5 Branch Technical Positions

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: BTP HICB-8 calls for the identification of the actuated equipment not tested during reactor operation, and for a discussion of how each conforms to the justification criteria of Paragraph D.4 of RG 1.22. The ADS design conforms to RG 1.22 with the clarification that for the DPVs, periodic testing is interpreted to mean testing of the squib initiators in a laboratory after removal from the squib valves.

- Because the DPVs are squib-actuated and cannot be closed once they are opened, there is no practicable system design to allow testing during reactor operation without creating an unacceptable breach of the RCPB. The SRVs are tested with the reactor at low power and at, or near, rated pressure. Both the squib wires and the SRV solenoids are continuously monitored for electrical continuity, as indicated in Subsection 7.3.1.1.4.

  The SRVs and DPV initiators can be tested when the reactor is shut down.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The ADS design conforms to BTP HICB-11.

  ADS logic is controlled by the SSLC/ESF system. SSLC/ESF logic controllers for the ADS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices. The Q-DCIS provides the communication functions for SSLC/ESF. See Subsections 7.1.2, 7.1.3.2 and 7.1.3.3 for a description of the Q-DCIS communication system design.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The ADS design conforms to BTP HICB-12. See Reference 7.3-2.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The ADS design conforms to BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the ADS within the DCD conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The ADS design conforms to BTP HICB-17.

BTP HICB-19, Guidance on Evaluation of Defense-in-Depth and Diversity in digital Computer-based Instrumentation and Control Systems:

- Conformance: The ADS design conforms to BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The ADS design conforms to BTP HICB-21.

7.3.1.1.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3] apply to the ADS. The ADS complies with the requirements as indicated above. TMI action plan requirements are addressed in Appendix 1A.

7.3.1.1.4 Testing and Inspection Requirements

The ADS voter logic units (VLU function) continuously self-tests. A very low current is used to test the continuity of the SRV pilot solenoids and the bridge wires within the DPV squib valve actuating circuitry. The test current is continuously applied, and triggers an alarm if the circuit is interrupted. Testing of ADS equipment is conducted during refueling outages. Refer to Subsection 6.3.2.8.4 for a discussion of mechanical tests performed on the ADS. The same continuity test also is applied to the GDCS squib valves described in Subsection 7.3.1.2.

7.3.1.1.5 Instrumentation and Control Requirements

System status during normal plant operation and ADS performance monitoring in an accident relies on the following MCR indications (additional discussion on the ADS instrumentation is contained in Subsection 7.3.1.1.2):

- Status indication of the SRVs and DPVs;
- SRV discharge line temperature alarm;
- RPV pressure indication;
- Suppression pool high/low level alarm;
- GDCS pool low level alarm;
- Water level indication for the GDCS pools, suppression pool, and RPV; and
- Alarms for the following ADS parameters in the MCR:
  - Manual arming of ADS,
  - Manual actuation of ADS,
  - Two-out-of-four ADS Level 1 signals,
  - Automatic ADS initiation,
  - Aborted ADS initiation,
  - SRV solenoid loss of continuity,
  - DPV squib firing circuit loss of continuity,
  - Inconsistent wide range divisional RPV water level alarms,
  - Any inconsistency in divisional input information from the four SSLC/ESF platform divisions to each Voter Logic Unit (VLU), as compared at the VLU,
  - Any single load driver/discrete output trip in the firing circuit of a DPV or SRV,
  - Two-out-of-four ADS Drywell Pressure High signals,

– Divisional RPV Level 1 trip, and

– Divisional Drywell Pressure high trip.

Safety-related ADS instrumentation located in the drywell is designed to operate in the environment resulting from a Loss of Coolant Accident (LOCA). Safety-related instruments located outside the containment also are qualified for the environment in which they must perform their safety function.

7.3.1.2 Gravity-Driven Cooling System

The basic components of the GDCS are within the containment. The GDCS pools, piping and valves are in the drywell. The suppression pool is on the outer periphery of the drywell within the containment envelope.

7.3.1.2.1 System Design Bases

The GDCS I&C are designed to meet the following safety-related requirements and 10 CFR 50.2, Design Bases:

- Automatically initiate the GDCS to prevent fuel-cladding temperatures from reaching the limits of 10 CFR 50.46.
- Respond to a need for emergency core cooling following reactor depressurization, regardless of the physical location of the malfunction or break causing the need.
- Be completely automatic in operation. Manual initiation of GDCS is possible at any time, provided protective interlocks have been satisfied.
- Prevent the inadvertent actuation of the deluge valves thus preventing inadvertent draining of the GDCS pools.
- Prevent any single control logic and instrumentation failure from inadvertently opening a GDCS injection valve or equalizing valve.
- Display GDCS valve positions and GDCS pool levels on a mimic of the system in the MCR.

7.3.1.2.2 System Description

The GDCS system comprises the GDCS injection and equalization functions as well as the deluge subsystem. The injection and equalization functions are used to cool the core in the event of a LOCA. The deluge system is used to flood the containment floor in the event of a core breach.

The GDCS injection and equalization functions are implemented by four injection lines from the three GDCS pools to the RPV and four equalization lines from the suppression pool to the RPV. There are two valves on each injection line, with four squib initiators per valve (three divisional initiators and one from the DPS [see Section 7.8]), for a total of eight GDCS injection valves and 32 squib initiators. There is one squib valve on each of the four equalizing lines and four squib initiators per valve (three divisional initiators and one from the DPS [see Section 7.8]), for a total of four equalizing valves and 16 squib initiators. The equalizing valves are used after reactor core decay heat has boiled away sufficient vessel inventory added by the GDCS to again begin lowering the RPV water level. With three divisional initiators per valve, the system can be without two divisions of power and still perform its intended function.

The GDCS pools are located within the drywell at an elevation above the top of active fuel (TAF) and provide core cooling water by the force of gravity. The suppression pool is located within the drywell, with its equalization lines located above the TAF.

Redundant safety-related and nonsafety-related level transmitters - four for each pool - continuously monitor the GDCS pool water level. These values are continuously shown on the safety-related and nonsafety-related displays. Both high and low pool levels result in alarms from the PCF (part of N-DCIS).

The overall design of the system assures that, when needed, all eight injection valves and all four equalizing valves are fired - even with a complete failure of any two divisions. However, no squib is fired inadvertently as a result of any single failure.

Automatic Operation

Actuation of the GDCS injection function is performed automatically, without need for operator action. The signal to open the GDCS injection valves is given after a time delay (Table 7.3-4) When the RPV water level drops below Level 1 sustained for 10 seconds, the GDCS time delay is initiated . For certain LOCA events where RPV water level does not drop below Level 1, GDCS injection valve time delay is also initiated on drywell pressure high signal, sustained for 60-minutes. With three divisional initiators per valve, the system can tolerate the complete loss of two divisions of power (one in bypass and one failure) and still perform its intended function.

Actuation of the GDCS equalizing function is performed automatically, without need for operator action. The GDCS equalizing valves initiation occurs automatically following a sustained RPV Level 1 signal, for 10 seconds, plus Table 7.3-4 time delay, and only after the RPV water level decreases below RPV Level 0.5 (1m above TAF). This action results in the actuation of the four equalizing squib valves mounted on the suppression pool equalizing lines. With three divisional initiators per valve, the system can tolerate the complete loss of two divisions (one bypass and one failure) of power and still perform its intended function.

GDCS injection and equalize subsystem initiation is inhibited automatically under ATWS conditions as described in Subsection 7.8.1.1.1.2.

Manual Operation

Each safety-related VDU provides a display with an “arm/fire” switch (one per division, for a total of four) to manually initiate the GDCS sequence as a system. If the operator uses any two of the four switches, the GDCS sequence seals in and starts the GDCS valve sequencing. This manual actuation also is interlocked with RPV pressure. This requires four deliberate (two-arm and two-fire) operator actions. For all of the manual initiations, operator use of the “arm” portion of the display triggers a plant alarm.

The safety-related VDUs in the MCR provide a display format allowing the operator to manually open each GDCS injection valve independently, using the primary SSLC/ESF logic function. Likewise, each nonsafety-related VDU in the MCR provides a display format allowing the operator to individually open each GDCS injection valve independently, using the DPS logic function. Each display uses an “arm/fire” configuration (interlocked with a low reactor pressure signal) requiring at least two deliberate operator actions. Operator use of the “arm” portion of the display triggers a plant alarm. The two manual opening schemes from the SSLC/ESF (primary) and the DPS (backup) are diverse.

In addition the safety-related VDUs in the MCR provide a display format allowing the operator manually to open each GDCS equalizing valve independently, using the primary SSLC/ESF logic function. Likewise, each nonsafety-related VDU in the MCR provides a display format allowing the operator to individually open each GDCS equalizing valve independently, using the DPS logic function. Each display uses an "arm/fire" configuration requiring at least two deliberate operator actions (interlocked with a low reactor pressure signal). Operator use of the "arm" portion of the display triggers a plant alarm. The two manual opening schemes from the SSLC/ESF (primary) and the DPS (backup) are diverse.

Actuation Logic

The logic elements providing controls for the actuation of the GDCS injection and equalizing squib valves are contained in the SSLC/ESF platform within Q-DCIS, outside the drywell containment. The RPV level transmitters and the drywell pressure sensors used to initiate GDCS, are located on racks outside the drywell.

The GDCS injection and equalizing valve logic includes the SSLC/ESF "division of sensors" bypass switch, two-out-of-four trip decisions, and single-failure proof actuation logic - with any three of the four divisions of safety-related power available. The valve logic also is single-failure proof against inadvertent actuation, meaning each division of logic has three load drivers each of which must operate for the associated squib valves to fire.

The wide range level and drywell pressure transmitters that are used for the ADS logic and fuel zone range RPV water level transmitter are also used for the GDCS equalizing valve logic; these are separate and independent from the transmitters used for RPS functions and diverse from those used by the DPS. Both sets of RPV water level transmitters belong to the NBS.

The generation of the RPV-Level 1 or Drywell Pressure High signal for the GDCS is described above (Automatic Operation). The logic for all squib initiators is similar. The signals are acquired per division by RMUs of the same division. The data are sent via fiber optic cables to the SSLC/ESF cabinets located in the corresponding divisional I&C equipment rooms in the Control Building (CB). Each division's logic compares the measured parameters to setpoints. If the measured parameter is at or past the setpoint, a divisional sensor trip is generated and sent both to its own division and to each of the other divisions by appropriately isolated fiber optic cables.

Each division has access to all four divisional sensor trip signals, and performs a redundant two-out-of-four vote on the four sensor trip signals. (The vote is two-out-of-three if one division is bypassed, because no more than one division can be bypassed at any one time.)

Each division uses triply redundant logic to perform the two-out-of-four vote on the four divisional sensor trip signals. The effect is that any two divisions sensing the appropriate trip conditions results in all divisions providing a trip signal.

The existence of the multiple logic trips per division is necessitated by the requirement that no injection or equalizing squib valve inadvertently be fired as the result of a single failure.

For the eight GDCS injection squib valves logic, when a sustained RPV Level 1 is detected for 10 seconds or a sustained drywell pressure high is detected for 60 minutes, adjustable timers will be activated at a preset time delay (as specified in Table 7.3-4). After the time delay, a trip signal is output to the GDCS squib load drivers/discrete outputs. There are eight injection squib valves, each with three divisional squib initiators, and one DPS squib initiator.

Within the RMU, for each equalizing valve squib initiator, there is a series circuit of divisional power, three load drivers/discrete outputs in series, a current monitor, and a normally closed disable/test switch. The triply redundant logic in the main SSLC/ESF processors must transmit separate close signals to each of the three load driver/discrete outputs. The effect is that two of the three triply redundant processors must separately command all of the load drivers/discrete outputs to fire the divisional squib initiator, making the design single failure proof against inadvertent actuation. Because each GDCS injection squib valve always has three squib initiators, powered by three different divisions, the design is also single-failure proof if required to operate all eight valves, and even will initiate with the loss of two divisions of power.

The current monitor continuously verifies squib electrical continuity, and the disable/test switch is used when performing maintenance or surveillance testing, or testing the current monitor. If the disable/test switch opens the circuit, an alarm signal is sent to the MCR, indicating that the squib initiator (not the valve) is inoperable.

For diversity, the DPS also is able to fire its squib electrical initiator on each of the eight GDCS injection squib valves, using single-failure proof logic (both to operate and to avoid inadvertent operation). This is accomplished using a completely separate squib initiator connected to the DPS system (see Figures 7.3-1b 1and 7.3-1c). The DPS system uses diverse (from the SSLC/ESF) sensors, hardware, and software to operate the GDCS injection valves. Figure 7.3-2 shows the initiation logic of a typical equalizing squib valve.

Within the RMU, for each squib initiator, there is a series circuit of divisional power, three load drivers/discrete outputs in series, a current monitor, and a normally closed disable/test switch. To fire the equalizing valve squib initiator, the triply redundant logic in the SSLC/ESF must time out the post GDCS initiation signal permissive, acquire at least two of four fuel zone range signals, determine that the measured value is at or below Level 0.5 and two-out-of-four vote the resulting divisional sensor trips and transmit separate close signals to each of the three load driver/discrete outputs. The effect is that two of the three triply redundant processors must separately command all of the load drivers/discrete outputs to fire the divisional squib initiator, making the design single failure proof against inadvertent actuation.

Because each equalizing valve always has three divisional squib initiators powered by three different divisions, the design is also single-failure proof whenever required to operate all four valves, with any three of the four divisions of safety-related power available. The equalizing valves are needed for the long term, so they are not automatically operated by the DPS system. The equalizing valves are included in the manually initiated GDCS valve logic, and also have capability to be fired individually from safety-related VDU displays or nonsafety-related VDU displays.

Deluge System

The severe accident deluge (GDCS subsystem) is designed to flood the containment floor in the event of a core breach that results in molten fuel on the containment floor. This system is made up of two individual and identical trains both of which contain an automatic actuation and manual actuation ability. There are 12 deluge valves each with four squib initiators (each train has a manual and automatic initiator). Each of these valves feeds the Basemat-Internal Melt Arrest Coolability (BiMAC) deluge system, which floods the containment floor following a severe accident. The BiMAC system is described in more detail in Subsection 6.2.1. A typical squib deluge valve is shown in Figure 6.3-2. The logic for the deluge valves is executed in a pair of dedicated nonsafety-related PLCs and a pair of dedicated safety-related temperature switches.

Automatic actuation of the deluge valves is accomplished in concert with lower drywell high temperature. The containment floor area is divided into 30 cells, with two thermocouples installed in each cell. One thermocouple from each cell is monitored in one PLC, while the other thermocouple from each cell is monitored in a second PLC. When measured temperatures exceed the setpoint (see Table 7.3-4) at one set of thermocouples coincident with setpoints being exceeded at a second set of thermocouples in an adjacent cell, a trip signal is generated in each PLC.

The trip signal in each PLC starts an adjustable deluge squib valve non-bypassable timer. At the end of the deluge squib valve set time delay, each of the two timers outputs a trip signal to the respective deluge valve squib load driver/discrete output. The timer outputs are wired in series so each of the two timers must transmit a temperature trip signal to the corresponding series load driver/discrete output. Additionally, a pair of dedicated safety-related temperature switches monitor the drywell temperature below the RPV. Each temperature switch uses a capillary and bulb action to close a contact wired in series with the PLC timer outputs. The effect is that both PLC timer outputs and both temperature switch outputs must operate to fire the squib initiator. The temperature switches serve as permissives for the deluge logic. These temperature switches are safety-related to prevent inadvertent actuation of the deluge system, which could needlessly drain the GDCS pools.

The deluge logic is completely separate from and independent of the Q-DCIS and the N-DCIS, and is powered by dedicated pair of batteries supported by battery chargers operating on nonsafety-related power. In the event that this nonsafety-related power is lost, deluge logic power is supplied from dedicated batteries for 72 hours. The deluge valves also are powered by a pair of dedicated batteries supported by battery chargers operating on nonsafety-related power. In the event that this nonsafety-related power is lost, deluge valve power is supplied from each pair of dedicated batteries for 72 hours.

The batteries for the deluge valves are separate from and independent of the batteries for the deluge logic. Each of these batteries can fire all 12 deluge valve squibs. All of the deluge valve batteries are separate from and independent of the other plant batteries.

The logic elements providing the controls for the actuation of the deluge valves are contained within a separate pair of dedicated nonsafety-related PLCs and a pair of dedicated safety-related temperature switches. The only safety-related function of the deluge logic is prevention of inadvertent actuation. The deluge logic is independent from all the other plant controls, and also is located outside containment.

Temperature indications and alarms, as well as continuity alarms and valve open/close indications for each squib valve are available in the MCR. Each valve has a normally closed disable/test switch available for maintenance purposes.

Two control switches are furnished in the MCR, to allow the operator manually to open the 12 deluge valves. These switches are of the “arm/fire” type, and are wired in series such that four deliberate operator actions (two for "arm" and two for "fire") and the safety-related temperature switches are required to operate the valves. These switches actuate the squib initiator on each deluge valve. Operator use of the "arm" portion of the switch triggers a plant alarm in the PCF.

7.3.1.2.3 Safety Evaluation

Section 6.3 evaluates the individual and combined capabilities of ADS and GDCS. For the entire range of nuclear process system break sizes, the ADS and GDCS ensure that the reactor core is always submerged.

Instrumentation initiating the ADS and GDCS injection and equalizing functions must respond to the potential inadequacy of core cooling regardless of the location of the breach in the RCPB. Such a breach inside or outside the containment is sensed by RPV low water level. This signal is completely independent of breach location, and is therefore used to initiate the GDCS injection and equalizing functions.

No operator action is required to initiate the correct response of the GDCS. If the system fails to initiate, the MCR operator manually accomplishes GDCS initiation through controls and displays in the MCR. Sufficient alarms and indications in the MCR allow the operator to assess the performance of the GDCS. Specific instrumentation is addressed in Subsection 7.3.1.2.5.

The redundancy of the control and monitoring equipment for the GDCS injection and equalizing functions is consistent with the redundancy of the four divisions of the GDCS. Control and monitoring equipment is located in the MCR and is under the supervision of the MCR operator.

The initiation scheme for the GDCS injection and equalizing functions is designed such that no single failure in the initiation circuitry, with any three of the four divisions of safety-related power available, can prevent the GDCS from providing the core with adequate cooling. This is assured by the redundancy of the components in the four divisions of the GDCS.

The GDCS has no equipment protective interlocks that could interrupt automatic system operation. To initiate the GDCS injection and equalization systems manually, a RPV low-pressure signal must be present. This prevents system initiation while the reactor is at operating pressure. The GDCS injection and equalizing functions are designed to operate from safety-related power. The system instrumentation is powered by divisionally separated safety-related power. The injection squib valve, and the equalizing squib valve logic and initiation circuitry is powered by divisionally separated, safety-related power (Refer to Section 8.3). The mechanical aspects of the GDCS are discussed in Subsection 6.3.2.

The two deluge system temperature switches and related contacts are safety-related only to prevent the inadvertent actuation of the deluge valves. No single failure within the deluge system control and monitoring equipment causes an inadvertent actuation of the deluge system. This is to protect against inadvertently draining the GDCS pools, thereby preventing the injection and equalizing systems from performing their safety functions.

Table 7.1-1 identifies the GDCS and the associated codes and standards applied in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards. Any exceptions or clarifications are so noted.

7.3.1.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The GDCS design complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The GDCS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the GDCS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.3.1.2.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the GDCS system.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to GDCS.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions is not applicable beyond that discussed in subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsection 7.3.1.2.4.
  - Section 6.2 and 7.2 (Manual Control): See Subsection 7.3.1.2.2.
  - Section 6.4 (Derivation of System Inputs): The GDCS derives its sense and command features from direct measurements.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 7.3.1.2.4.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the GDCS are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the GDCS are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the GDCS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the GDCS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels,

- Conformance: The GDCS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design,

- Conformance: The GDCS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The GDCS design complies by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The GDCS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The GDCS conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the GDCS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.1.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, 33, 35, and 37:

- Conformance: The GDCS design complies with these GDCs.

7.3.1.2.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The GDCS design conforms to these criteria by providing diverse I&C, as described in Section 7.8.

7.3.1.2.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Function:

- Conformance: System logic is tested continually as described in Subsection 7.3.1.2.4. Components are tested periodically during refueling outages. The GDCS design complies with RG 1.22. In the GDCS, the squib valves are not actuated during reactor operation, because their actuation would adversely affect the operation of the plant by resulting in a reactor shutdown.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety:

- Conformance: The GDCS design complies with RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The GDCS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The GDCS design complies with RG 1.62. Each division of the GDCS has a manual actuation switch in the MCR. Initiation of the system requires actuation of two switches to ensure that manual initiation is a premeditated act. There is an interlock between the manual initiation switches and a low reactor-pressure signal. This interlock prevents manual initiation of the system if the RPV is not depressurized.

RG 1.75, Physical Independence of Electric Systems:

- The GDCS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints used to initiate GDCS are established consistent with RG 1.105. Reference 7.3-2 provides a detailed description of the GEH methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: NBS provides the measurement inputs to GDCS. The NBS instrument sensing lines conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.152.

RG 1.153, Criteria for Power, I&C Portions of Safety Systems:

- Conformance: The GDCS design complies with 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The GDCS design conforms to RG 1.169 as implemented on the SSLC/ESF platform..

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The GDCS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The GDCS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.1.2.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the GDCS:

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Conformance: Because the portion of the GDCS downstream of the squib valves connected to the RPV has a design pressure equivalent to the reactor operating pressure, and the low pressure portion of the GDCS upstream of the squib valves is open to the GDCS pools, there is no need for over-pressure protection of the low pressure portion. A high-pressure interlock is provided to prevent inadvertent manual initiation of the GDCS.

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: BTP HICB-8 requires the identification of actuated equipment not tested during reactor operation and a discussion of how each conforms to the provision of Paragraph D.4 of RG 1.22. In the GDCS, the squib valves are not actuated during reactor operation, because their actuation would adversely affect the operation of the plant by resulting in a reactor shutdown.
  - Given the GDCS system requirements for zero RCPB leakage over the 60-year life of the plant, the only practical solution is for the system actuation valve to be non-reclosing with a metal diaphragm seal that is ruptured to initiate system flow.
  - The GDCS is designed to provide adequate inventory make-up to the core in the event of a LOCA. The system has sufficient redundancy and reliability that core-cooling requirements are met in the event of a LOCA.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: SSLC/ESF logic controllers for the GDCS comply with BTP-HICB-11. SSLC/ESF logic controllers for the GDCS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: GDCS logic resides within the SSLC/ESF conforming to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The GDCS design conforms to BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR 52:

- Conformance: The GDCS design conforms to BTP HICB-16

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The GDCS design conforms to BTP HICB-17.

BTP HICB-19, Guidance on Evaluation of Defense-in-Depth and Diversity in digital Computer-based Instrumentation and Control Systems:

- Conformance: The GDCS design conforms to BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The GDCS design conforms to BTP HICB-21.

7.3.1.2.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for Section 7.3 and Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3] (addressed above) apply to the GDCS. The GDCS design complies with these requirements. TMI action plan requirements are generically addressed in Appendix 1A.

7.3.1.2.4 Testing and Inspection Requirements

The GDCS TLUs are self-tested continually at preset intervals. The TLUs of each logic division, and the timers for the automatic logic, can be tested during plant operation. GDCS equipment inside containment is tested during refueling outages. Refer to Subsection 6.3.2.7.4 for a discussion of mechanical tests performed on the GDCS.

7.3.1.2.5 Instrumentation and Control Requirements

The performance and effectiveness of the GDCS in a postulated accident is verified by observing the following MCR indications (additional discussion on the GDCS instrumentation is contained in Subsection 7.3.1.2.2 and in Subsection 6.3.2.7.5):

- Status indication of locked-open maintenance valves;
- Status indication and alarm of the squib-actuated valves;
- Position indication of the GDCS check valves;
- Drywell and RPV pressure indication;
- Suppression pool high/low level alarm;
- GDCS pool high/low level alarm;

- Water level indication for the GDCS pools, suppression pool and RPV; and
- Squib valve open alarm.

The safety-related GDCS instrumentation is designed to operate in a drywell environment resulting from a LOCA. The thermocouples that initiate the deluge valves are qualified to operate in a severe accident environment. Safety-related instruments, located outside the drywell, are qualified for the environment in which they must perform their safety-related functions.

7.3.2 Passive Containment Cooling System

The Passive Containment Cooling System (PCCS) consists of condensers that are an integral part of the containment pressure boundary. The PCCS heat exchanger tubes are located in the Isolation Condenser/Passive Containment Cooling System (IC/PCCS) pool outside the containment. Containment (drywell) pressure above the suppression pool (wetwell) pressure, similar to the situation during a loss of reactor coolant into the drywell, forces flow through the PCCS condensers. Condensate from the PCCS drains to the GDCS pools. As the flow passes through the PCCS condensers, heat is rejected to the IC/PCCS pool, thereby cooling the containment atmosphere. This action occurs automatically, without the need for actuation of components. The PCCS does not have instrumentation, control logic, or power-actuated valves, and does not need or use electrical power for its operation in the first 72 hours after a LOCA. For long-term effectiveness of the PCCS, the vent fans are manually initiated by operator action. Other information on the PCCS is given in Subsection 6.2.2 and leak rates are discussed in Subsection 16B.3.3.

7.3.3 Leak Detection and Isolation System

The primary function of the Leak Detection and Isolation System (LD&IS) is to detect and monitor leakage from the RCPB and to initiate the appropriate safety action to isolate the source of the leak. The system is designed to automatically initiate the isolation of certain designated process lines penetrating the containment, to prevent release of radioactive material from the RCPB. The initiation of the isolation functions closes the appropriate containment isolation valves. The LD&IS functions are performed in two separate and diverse safety-related platforms. The Main Steam Isolation Valve (MSIV) isolation logic functions are performed in the Reactor Trip and Isolation Function (RTIF) platform, while all other containment isolation logic functions are performed in the SSLC/ESF platform. The non-safety monitoring functions of LD&IS are performed in the N-DCIS.

7.3.3.1 System Design Bases

The following safety-related system design criteria are applicable to the design of the LD&IS.

- The LD&IS is engineered as a safety-related system, Seismic Category 1, and conforms to the regulatory requirements, guidelines, and industry standards listed in Table 7.1-1 for this system.
- The MSIV function of LD&IS logic design is fail-safe, such that loss of electrical power to the logic of one LD&IS division initiates a channel trip. The containment isolation

function of LD&IS logic design is fail as-is such that loss of power to the logic of one division does not result in a trip.

- Isolation is initiated with precision and reliability once leakage has been detected from the RCPB.
- Once isolation is initiated, the action continues to completion. Deliberate operator action is required to reopen the isolation valves.
- The LD&IS design meets the single failure criterion because no single failure within the system, with any three of the four divisions of safety-related power available, initiates inadvertent isolation or prevents isolation when required.
- Automatic isolation is initiated by coincidence of any two-out-of-four channel trips, as appropriate for each monitored variable.
- Electrical communication and physical independence is maintained between safety-related divisions and between safety-related and nonsafety-related equipment.
- The LD&IS design incorporates provisions to permit bypass of a single division of sensors at any one time.
- LD&IS instrumentation uses a diversity of sensed parameters and redundant channels for initiation of containment isolation.
- Manual isolation capability is provided for diversity from the automatic logic.
- The containment leak detection methods described in RG 1.45 are adopted in the LD&IS system design.
- Identified and unidentified leakages within the containment are monitored separately to quantify the flow rates.
- The LD&IS provides different divisional isolation signals to the containment isolation valves.

7.3.3.2 System Description

The LD&IS is a four-division system designed to detect and monitor leakage from the RCPB, and isolate the source of the leak by initiating closure of the appropriate containment isolation valves. The LD&IS control and isolation logic uses two-out-of-four coincidence voting channels for each plant variable monitored for containment isolation. Various plant variables are monitored, such as flow, temperature, pressure, RPV water level, and radiation level. These are used in the logic to initiate alarms and the required control signals for containment isolation. Two or more diverse leakage parameters are monitored for each specific isolation function. The LD&IS logic functions reside in the framework of the RTIF and the SSLC/ESF platforms, where trip signals are generated, initiating the isolation functions of the LD&IS.

In addition to containment isolation after a LOCA event, safety-related control and isolation functions are implemented by the LD&IS for:

- Main steam lines and drain lines,
- ICS process lines,

- Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) System process and sampling lines,
- Fuel and Auxiliary Pools Cooling System (FAPCS) suction lines and discharge from the GDCS pools,
- Chilled water system lines to drywell coolers,
- Drywell sumps liquid drain lines,
- Containment purge and vent lines,
- RB area air supply and exhaust ducts,
- Feedwater lines,
- Fission products sampling lines, and
- Isolation of high pressure makeup water injection to the RPV.

The nonsafety-related detected and monitored sources or indications of leakage are:

- Condensate flow from the upper and lower drywell air coolers,
- Leakage to the drywell from valves equipped with leak-off lines between the two valve stem packings,
- Fission product leakages into the drywell detected by the Process Radiation Monitoring System (PRMS),
- RPV head flange pressure seal leakage,
- Drywell floor drain and drywell equipment drain sump level change (sump levels and flow rates are used to quantify identified and unidentified leakages),
- Drywell temperature,
- SRV discharge line temperature,
- RB equipment and floor drain sump pump activity,
- Equipment areas temperature, and
- RCCWS intersystem leakage radiation.

The LD&IS control functions initiating automatic isolation functions are classified safety-related, and these functions use redundant divisional channels satisfying both the mechanical and electrical separation criteria as well as the single failure criterion. This system operates continuously during normal reactor operation, and during plant abnormal and accident conditions.

The system design is configured as shown in Figure 7.3-3. The LD&IS interfacing sensor parameters are listed in Table 7.3-5. A detailed description of detection methods, monitored plant parameters, and the monitoring instrumentation is included in Subsection 5.2.5.

7.3.3.3 Safety Evaluation

The LD&IS control and isolation functions, including the sensors and channel instrumentation, are a safety-related system, and qualified environmentally and seismically for continuous operation during plant normal, abnormal, and accident conditions. The system design conforms to the design bases described in Subsection 7.3.3.1. The LD&IS system design uses measurements and redundant instrument channels to detect and monitor reactor coolant leakage in (and external to) the containment, and to detect and isolate the source of the leak, thereby preventing radioactive releases to the environs. The isolation logic uses four redundant divisional channels to monitor a leakage parameter and uses the two-out-of-four coincidence voting logic technique for initiation of the isolation function. This design technique improves system availability to perform safety-related functions, satisfies the single failure criterion, and permits channel bypass for maintenance and repair during normal plant operation. Loss of one channel due to failure or power loss does not cause inadvertent isolation.

The four redundant divisions of the MSIV isolation function of the LD&IS comprise a fail-safe design. The isolation logic is energized under normal conditions and de-energized to initiate the isolation function on indication of abnormal leakage. The four redundant divisions of the containment isolation feedwater isolation and HP CRD isolation functions of the LD&IS use fail as-is designs and energized-to-trip logic.

The signals used to isolate the feedwater lines by closing the feedwater isolation valves (FWIVs) are:

- Feedwater lines differential pressure high coincident with high drywell pressure,
- Drywell pressure high coincident with drywell water level high,
- RPV water level 0.5 with time delay,
- RPV water level 8, or
- Drywell pressure high-high.

The signals provided to stop the feedwater pumps by opening the feedwater pump Adjustable Speed Drive (ASD) controller power circuit breakers are:

- Feedwater lines differential pressure high coincident with high drywell pressure,
- Drywell pressure high coincident with drywell water level high,
- RPV water level 0.5 with time delay, and
- RPV water level 9.

For certain LOCA events, High Pressure Makeup Water Injection needs to be isolated to ensure that containment pressure remains within design limits. The signals used to terminate the HP CRD flow by closing the HP CRD isolation valves are:

- Low level in two-of-three GDCS pools; and
- Drywell pressure high coincident with drywell water level high.

Feedwater isolation on drywell pressure high-high is inhibited automatically under ATWS conditions as described in Subsection 7.8.1.1.1.2. The feedwater isolation logic can also be inhibited manually under ATWS conditions.

The LD&IS logic is designed to seal-in the isolation signal once the trip has been initiated. The isolation signal overrides any control action to trigger the opening of isolation valves. Reset of the isolation logic is required before any isolation valve can be opened manually. Manual valve override capability is provided for valves that are required to operate following an abnormal event on a valve-by-valve or line-by-line basis. The valve override requires at least two deliberate operator actions and is under administrative controls. The override status is alarmed in the MCR.

The system logic design incorporates provisions to permit bypass of a single division of sensors at one time for repair and maintenance without affecting system capability to perform its safety-related functions. With one division of sensors in the bypass mode, no other division of sensors simultaneously can be bypassed.

Manual control switches and associated logic are provided in the design of the LD&IS to give the operator the capability to perform manual control functions for initiation of isolation, logic reset, channel bypass and test functions.

The instrumentation for the drywell Low Conductivity Waste (LCW) and High Conductivity Waste (HCW) sump levels is designed to meet the leakage rate requirements for identified and unidentified sources. The LD&IS includes isolation logic using drywell pressure high and low RPV water level for the isolation of the drain lines transferring waste from the sumps to the liquid radwaste system. Additional information on LD&IS operation is contained in Subsection 5.2.5.

Table 7.1-1 identifies the LD&IS function and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.3.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The LD&IS design complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The LD&IS conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the LD&IS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-Related Functions): See Subsection 7.3.3.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the LD&IS system.
  - Section 4.6 (Spatially Dependent Variables): See Subsection 5.2.5.2.1.
  - Section 5.2 (Completion of Protective Actions): See Subsection 7.3.3.3.

- Section 5.7 (Capability for Test and Calibration): See Subsection 7.3.3.4 for LD&IS (MSIV), Subsection 7.3.5.4 for Non-MSIV, & 7.4.3.4 for RWCU/SDC.
- Section 6.2 and 7.2 (Manual Control): See Subsections 7.3.3.3, 7.3.3.1 for LD&IS (MSIV), and 7.3.5.1 for non-MSIV.
- Section 6.4 (Derivation of System Inputs): See Subsection 7.3.3.2 and Table 7.3-5.
- Section 6.5 (Capability of Test and Calibration): See Subsections 7.3.3.4 for MSIV and 7.3.5.2.3, 7.3.5.2.4, & 7.3.5.4 for non-MSIV.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the LD&IS are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the LD&IS (MSIV) are not applicable beyond that discussed in Subsection 7.1.6.6.1.23. See Subsections 7.3.5.2.3 & 7.3.5.2.4 for (non-MSIV).
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the LD&IS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the LD&IS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The LD&IS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The LD&IS design complies by providing automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(xiv)[II.E.4.2], TMI Action Plan Item IIE.4.2, Containment Isolation Systems:

- Conformance: The LD&IS design complies with this requirement.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions:

- Conformance: The LD&IS (non-MSIV) conforms to these requirements.

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The LD&IS (non-MSIV) conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The LD&IS conforms to these requirements.

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The LD&IS conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: The resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the LD&IS in the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 15, 16, 19, 20, 21, 22, 23, 24 29, and 30:

- Conformance: The LD&IS (non-MSIV) design complies with these GDCs.

GDC 1, 2, 4, 13, 15, 16, 19, 20, 21, 22, 23, 24, and 29:

- Conformance: The LD&IS (MSIV only) design complies with these GDCs.

7.3.3.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The LD&IS and ESF designs conform to item II.Q of SECY-93-087 (BTP HICB-19) by implementation of diverse I&C, described in Section 7.8.

7.3.3.3.4 Regulatory Guide

RG 1.22, (Safety Guide 22) Periodic Testing of Protection System Actuation Function:

- Conformance: The LD&IS design conforms to RG 1.22.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance is discussed in DCD Tier 2 Section 5.2.5.8 Regulatory Guide 1.45.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System:

- Conformance: The LD&IS design conforms to RG 1.47.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The LD&IS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379

will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The LD&IS design conforms to RG 1.62.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The LD&IS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The safety-related portions of the LD&IS design conform to RG 1.105. Reference 7.3-2 provides detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: NBS provides the measurement inputs to LD&IS (non-MSIV). The NBS instrument sensing lines conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.152.

RG 1.153, Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The LD&IS design conforms to 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.168 as implemented on the RTIF platform.
- The LD&IS (non-MSIV) design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.169 as implemented on the RTIF platform.
- The LD&IS (non-MSIV) design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.170 as implemented on the RTIF platform.
- The LD&IS (non-MSIV) design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.171 as implemented on the RTIF platform.
- The LD&IS (non-MSIV) design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.172 as implemented on the RTIF platform.
- The LD&IS (non-MSIV) design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The LD&IS (MSIV Only) design conforms to RG 1.173 as implemented on the RTIF platform.
- The LD&IS (non-MSIV) design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The LD&IS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The LD&IS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.3.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The LD&IS design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The LD&IS (MSIV only) design complies with BTP HICB-11. RTIF logic controllers for the LD&IS (non-MSIV) use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

  The LD&IS (non-MSIV) design complies with BTP HICB-11. SSLC/ESF logic controllers for the LD&IS (non-MSIV) use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The LD&IS design complies with BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The LD&IS design complies with BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The LD&IS design complies with BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The LD&IS design complies with BTP HICB-17.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The LD&IS design complies with BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The LD&IS design complies with BTP HICB-21.

7.3.3.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3], and 10 CFR 50.34(f)(2)(xiv)[II.E.4.2] apply to the LD&IS. The LD&IS complies with these requirements as indicated above. TMI action plan requirements are addressed in Appendix 1A.

7.3.3.4 Testing and Inspection Requirements

7.3.3.4.1 In-service & Surveillance Tests

In-service testing of the leak detection and monitoring channels is performed periodically to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include instrument channel checks, functional tests, verification of proper sensor and channel calibration, and response time tests.

The LD&IS instrument channels use conventional sensors for leak detection and monitoring, and require no special or unique testing methods.

The setpoint verifications, trip logic tests, and channel integrity tests for the safety-related functions of LD&IS are processed and tested by the RTIF and SSLC/ESF platforms.

7.3.3.4.2 Main Steam Isolation Valve Closure Tests

The LD&IS design provides manual capability and incorporates logic provisions to test closure of each of the MSIVs during normal reactor operation. To verify MSIV closure capability, each MSIV is tested periodically for partial closure while in service without causing a plant outage.

7.3.3.4.3 Testing and Maintenance in the Bypass Mode

Testing, calibration, and maintenance are performed on the equipment in accordance with established procedures when the channel is either out of service or deliberately has been bypassed.

7.3.3.5 Instrumentation and Controls Requirements

The LD&IS is designed to detect and monitor leakage from the RCPB, using a diversity of parameters and redundant instrument channels. The monitored leakage parameters are provided continuously to the RTIF and SSLC/ESF for processing and initiation of trips required for the isolation functions.

The LD&IS instrumentation requirements for each specific monitoring and isolation function are described in detail in Subsection 5.2.5. The plant parameters monitored for leakage detection, isolation, and alarms are summarized in Tables 5.2-6 and 5.2-7. The containment isolation functions accomplished by valves and control signals required for the isolation of process lines penetrating the containment are summarized in Tables 6.2-15 through 6.2-42.

7.3.4 Control Room Habitability System

The Control Room Habitability System (CRHS) is an SSLC/ESF system that provides a safe environment within the MCR, allowing the operator(s) to:

- Control the nuclear reactor and its auxiliary systems during normal conditions,
- Safely shut down the reactor, and
- Maintain the reactor in a safe condition during abnormal events and accidents.

The CRHS includes:

- CB shielding and area radiation monitoring,
- The Control Room Habitability Area HVAC Subsystem,
- Provision for emergency food and water storage,
- Emergency kitchen and sanitary facilities,
- Provision for protection from, and removal of, airborne radioactive contaminants, and
- Provision for removal of smoke.

The Control Room Habitability Area (CRHA) envelope, ventilation inlet/return isolation dampers, redundant Emergency Filtration Units (EFUs) in the emergency HVAC, and their associated controls are safety-related. Section 6.4 and Subsections 9.4.1 and 9.5.1.11 provide detailed information on the CRHS.

7.3.4.1 System Design Bases

The design bases of the CRHS are detailed in Subsections 6.4.1 and 9.4.1.1.

7.3.4.2 System Description

The CRHS safety-related instrumentation is designed to isolate the MCR envelope and re-align to the emergency filtration mode following:

- Detection of high radiation in the inlet air supply (automatic action)(safety-related function);
- Detection of loss of AC power / station black out (SBO) (automatic action) (safety-related function); and
- Detection of smoke in the inlet air supply, or in the CRHA general area (manual isolation)(nonsafety-related function).

Additional CRHS safety-related instrumentation is designed to only swap over the operating emergency filtration train following:

- Detection of high radiation downstream of the operating EFU filter train (automatic action) (nonsafety-related function).
- Detection of low flow at the outlet of the operating EFU filter train (automatic action) (safety-related function).

The PRMS in the CRHA consists of four safety-related divisional radiation channels to monitor the air intake to the CB. The monitoring systems warn of the presence of significant radioactive contamination in inlet air. Each radiation channel consists of a gamma sensitive detector and an area radiation monitor located in the MCR. The PRMS is safety-related as described in Subsection 11.5.3.1.4.

Each PRMS sensor provides an input signal to the associated SSLC/ESF VLU function, on detection of high radiation in the inlet ventilation air. The main air ventilation duct, the smoke purge intake duct, the smoke purge exhaust duct, and the restroom exhaust duct in the CRHA are each furnished with a pair of safety-related, normally closed, air operated isolation dampers connected in series. The air operated dampers are controlled by four independent solenoid valves powered from four separate divisions. This configuration ensures that the system returns automatically to its safe condition upon failure of a mechanical component, loss of air, loss of control, or loss of power. The air operated dampers installed in the smoke purge intake duct, the smoke purge exhaust duct, and in the restroom exhaust duct can be controlled manually.

Each EFU train is equipped with two parallel fans, 100% capacity each, and four electrically operated, normally closed discharge isolation dampers, mounted in a redundant (two in series) parallel configuration. Electrically operated dampers installed in series are powered from the same division as their respective fan. Failure of one division does not affect the operation of the other division.

EFU automatic operations are controlled by four redundant safety-related EFU discharge flow detectors installed in each EFU discharge duct. If the discharge flow drops to the low set point, the operating fan motor is de-energized, its electrically operated discharge dampers are closed, a stand-by (second in the unit) fan motor is energized and its electrically operated discharge dampers are opened. If the discharge flow is not sufficiently improved, the affected EFU train is automatically disengaged and a secondary EFU train is energized, following the protocol described above. The secondary EFU train also starts automatically to continue the emergency filtration mode if radiation is detected downstream, of the EFU filter train. The radiation setpoint for initiation of the EFU train swap combined with the radiation sensor location and air duct length is such that the swap over will occur prior to exceeding the 10 CFR 50, Appendix A, GDC 19 requirements.

During radioactive release events, the SSLC/ESF voting algorithm in each division uses two-out-of-four logic to produce an actuation signal to start the CRHA isolation mode which:

- Energizes the primary divisional fan of the primary EFU,
- Opens the primary EFU's redundant divisional electrically operated isolation dampers,
- Generates the signal to close the safety-related air operated isolation dampers installed in the main air supply duct,
- Stops the nonsafety-related fan in the main air supply air handling unit (signal forwarded to the N-DCIS via an isolation gate), and
- Closes the nonsafety-related damper in the air handling unit (signal forwarded to the N-DCIS via an isolated signal path and gateway).

Normally closed air operated safety-related isolation dampers, installed in series in the main air supply air handling unit discharge duct are controlled by four divisional solenoid valves. During normal operation the SSLC/ESF is used to manually open the redundant safety-related air operated isolation dampers by producing an actuation signal to energize the associated four solenoid valves. Simultaneously a permissive and start signal is given to the non safety-related air intake handling unit and its non safety-related air operated damper through an isolated signal path and gateway to allow the main air to be discharged into the MCR. During the isolation mode, the SSLC/ESF de-energizes the solenoid valves and closes the isolation dampers. Because the two air operated dampers are in series, any one of them can close the airflow path.

The functions of the SSLC/ESF are depicted in Figure 7.3-5 and detailed information is presented in Subsection 7.3.5. The four redundant divisions provide a fault-tolerant architecture allowing a single division of sensors bypass for on-line testing, maintenance, and repair without losing reliable trip capability. In such a bypass condition the system automatically defaults to 2-out-of-3 coincident voting. If one of the three remaining active divisions fails, the two remaining independent and redundant divisions are able to generate an actuation signal to close isolation damper(s). At least one of the redundant dampers always actuates in response to the detection of high inlet air radiation under all of the postulated design basis failures. This arrangement thus conforms to safety-related system requirements for single-failure proof capability, fault tolerance, independence, and separation, as required by IEEE Std. 603, Sections 5.1, 5.5, and 5.6.

The CRHA isolation dampers have the capability to be actuated manually from the MCR in accordance with IEEE Std. 603, Sections 5.8, 6.2, and 7.2.

If the nonsafety-related main air supply units are de-energized due to a loss of AC power / SBO, the SSLC/ESF automatically starts the emergency filtration mode which starts the primary EFU providing air to the CRHA. The signal processing and actuation logic are as described above for isolation following detection of high radiation at the CRHA main air supply inlet.

The nonsafety-related smoke detectors are provided as required by NFPA 90A to detect smoke in the system ductwork and in the CRHA general areas. Each smoke detection channel contains redundant smoke detectors. Each smoke detector signal provides alarm inputs to the MCR. Based on the smoke location, the operator manually starts an EFU (if smoke is not detected in the EFU's air intake zone), manually initiates CRHA isolation, or starts smoke removal from the CRHA. When the isolation dampers are closed and AC power is available, the Control Room Habitability Area Heating, Ventilation, and Air Conditioning Subsystem recirculation air handling unit continues to operate normally providing temperature control in the MCR. If the normal AC power is not available, the nonsafety-related redundant HVAC equipment installed in the CRHA is powered for two hours from nonsafety-related batteries. After that interval, if the nonsafety-related HVAC equipment stops running, safety-related temperature sensors with two-out-of-four logic automatically trip the power to predefined N-DCIS components and other nonsafety-related electrical loads in the MCR, removing the heat load generated by these sources. Smoke removal is described in Subsections 9.4.1.2 and 9.5.1.11.

If the redundant, nonsafety-related Control Room Habitability Area HVAC Subsystem (CRHAVS) cooling is lost, and the CRHA temperature increases, safety-related sensors provide a trip signal via SSLC/ESF to de-energize nonsafety-related predefined N-DCIS equipment located and other nonsafety-related electrical loads in the CRHA. Safety-related temperature sensors monitoring CRHA temperatures provide the logic to trip selected N-DCIS loads in the CRHA.

The redundant safety-related components, including the I&C (i.e., monitoring channels) in the CRHA, CRHA isolation dampers, and EFUs, satisfy the single-failure criterion. The isolation dampers in each pair are physically separated. They are physically separated from the EFUs as well. The nonsafety-related air handling units and the safety-related isolation dampers and EFUs are mechanically and electrically separated. There is no intervention by the nonsafety-related components on the safety-related components. CRHA air operated isolation dampers are closed following loss of power, loss of air, or control signal failures. This conforms to the fail-safe principle, in which components or systems are designed to return automatically to their safe condition upon failure.

The CRHS isolation and EFU operation cannot be shut down automatically. EFU disengagement and de-energization of safety-related isolation dampers can be accomplished manually.

The CRHS isolation and EFU actuation are part of the SSLC/ESF system logic is illustrated in Figure 7.3-5. The required instrumentation for CRHS is described in Subsection 9.4.1.5. Alarms for CRHA/Control Room Habitability Area Heating, Ventilation, and Air Conditioning Subsystem conditions are discussed in Subsection 6.4.8.

7.3.4.3 Safety Evaluation

A safety evaluation of the CRHS is provided in Subsections 6.4.5 and 9.4.1.3.

Table 7.1-1 identifies the CRHS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.4.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The CRHS design complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The CRHS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the CRHS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 6.4.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are discussed in Subsection 7.3.4.2.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to CRHS.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.

- Section 5.7 (Capability for Test and Calibration): Test and Calibrate features beyond that discussed in section 7.1.6.6.1.8 are not applicable.
- Section 6.2 and 7.2 (Manual Control): See Subsection 7.3.4.2.
- Section 6.4 (Derivation of System Inputs): The CRHS derives its sense and command features from direct measurements as described in section 7.3.4.2.
- Section 6.5 (Capability of Test and Calibration): Capability for Test and Calibrate features beyond that discussed in section 7.1.6.6.1.21 is not applicable.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the CRHS are discussed in subsection 7.3.4.2..
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the CRHS are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the CRHS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the CRHS are discussed in subsection 7.3.4.2.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The CRHS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The CRHS design complies by providing automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(xxviii)[III.D.3.4], Control Room Habitability Problems Under Accident Conditions:

- Conformance: The CRHS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The CHRS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The CRHS conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the CRHS in the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.4.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24 and 29:

- Conformance: The CRHS design complies with these GDCs.

7.3.4.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The CRHS and ESF designs conform to these criteria, as described in Subsection 7.8.2.2.

7.3.4.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Function:

- Conformance: The CRHS design conforms to RG 1.22.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System:

- Conformance: The CRHS design conforms to RG 1.47.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The CRHS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The CRHS design conforms to RG 1.62.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The CRHS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for safety-related Instrumentation:

- Conformance: The CRHS design conforms to RG 1.105. Reference 7.3-2 provides detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.152.

RG 1.153, Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The CRHS design conforms to 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The CRHS design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The CRHS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The CRHS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.4.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The CRHS design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The CRHS design complies with BTP HICB-11. SSLC/ESF logic controllers for the CRHS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The CRHS design complies with BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The CRHS design complies with BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The CRHS design complies with BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The CRHS design complies with BTP HICB-17.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The CRHS design complies with BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The CRHS design complies with BTP HICB-21.

7.3.4.3.6 Three Mile Island Action Plan Requirements

In accordance with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3] applies to the CRHS. The CRHS complies with the regulatory requirements indicated above. TMI action plan requirements are addressed in Appendix 1A.

7.3.4.4 Testing and Inspection Requirements

Testing and inspections requirements are identified in Subsections 6.4.7 and 9.4.1.4.

7.3.4.5 Instrumentation and Control Requirements

The required instrumentation for the CRHS is described in Subsection 9.4.1.5 and alarms for abnormal CRHA/Control Room Habitability Area Heating, Ventilation, and Air Conditioning Subsystem conditions are addressed in Subsection 6.4.8.

7.3.5 Safety System Logic and Control/Engineered Safety Features

7.3.5.1 System Design Bases

The SSLC/ESF system performs the control logic processing of the plant sensor data and manual control switch signals activating the functions of the LD&IS (non-MSIV), ECCS and CRHS. The SSLC/ESF also performs control logic processing for the decay heat removal, - safe, stable shutdown, and reactor pressure control functions of the ICS. SSLC/ESF also provides safety-related display information in support of safety-related system performance and accident monitoring. Logic for detecting and signaling a control rod separation is also included in the SSLC/ESF system.

The SSLC/ESF:

- Monitors safety-related signals providing automatic control of the plant safety protection systems;

- Performs processing of plant sensor and equipment interlock signals according to the required trip and interlock logic, including time delays, of each safety-related interfacing plant system or system important to safe plant operation;
- Meets the performance requirements of each safety-related interfacing plant system or system important to safe plant operation, including transient response, delay time, and overall time to trip system actuators, or initiates necessary system operation;
- Monitors safety-related manual control switches used for system or component test, protection system manual initiation, and individual control of equipment actuators;
- Furnishes trip output signals to actuators driving safety-related system equipment (e.g. solenoids and squib explosive-actuated valves);
- Furnishes trip or initiation outputs signals to the logic of interfacing functions;
- Provides diagnostic facilities for detecting imminent failure of safety-related system components and provides an operator interface facilitating quick repair;
- Provides safety-related accident monitoring display information, alarm and status outputs to operator displays, annunciators, and the PCF; and
- Satisfies regulatory requirements for implementation of:
  - The single failure criterion,
  - Defense-in-depth protection,
  - Testability,
  - Separation and independence, and
  - Bypass of certain functions and indication thereof.

7.3.5.2 System Description

SSLC/ESF is the decision-making control logic segment for the ESF systems. The SSLC/ESF processes automatic and manual demands for ESF system actuations, based upon sensed plant process parameters or at operator request. The SSLC/ESF includes the I&C implementing the following functions:

- The non-MSIV isolation functions of the LD&IS;
- The ADS functions of the NBS for SRV and DPV control;
- The ECCS, and decay heat removal – safe, stable shutdown and reactor pressure control functions of the ICS;
- The control room isolation function of the CRHS.
- Logic for the detection of a CRD system control rod separation event and transmits the rod separation signal to the RC&IS (described in Subsections 4.6.1 and 7.7.2.2.7).

The SSLC/ESF system also provides safety-related display information for system performance monitoring and accident monitoring (described in Subsection 7.5.1), and pool monitoring (described in Subsection 7.5.5) with the exception of SPTM, which is collected by RTIF.

7.3.5.2.1 General SSLC/ESF Arrangement

The SSLC/ESF resides in four independent and separated instrumentation divisions. The SSLC/ESF integrates the control logic of the safety-related systems in each division into firmware or microprocessor-based, software-controlled, processing modules located in divisional cabinets in the safety-related equipment rooms of the CB. The SSLC/ESF runs without interruption in all modes of plant operation to support required safety functions.

The SSLC/ESF consists of the non-MSIV isolation functions of the LD&IS, the ECCS functions, and the isolation function of the CRHS. The ESF/ECCS part includes the functions of SRV and DPV initiation, GDCS initiation, SLC initiation, and the core cooling and shutdown cooling logic functions of the ICS. There are separate multiplexing networks for RTIF and SSLC/ESF functions within each division. Figure 7.3-4 shows a functional block diagram of the SSLC/ESF portion of the system. The RPS function is discussed in Subsection 7.2.1, with the RPS functional block diagram shown in Figure 7.2-1. The ATWS/SLC mitigation function is discussed in Subsection 7.8.1.1.

Most SSLC/ESF input data are process variables multiplexed by the Q-DCIS in four physically and electrically isolated redundant instrumentation divisions (Subsection 7.1.3). Each of the four independent and separated Q-DCIS channels feeds separate and independent SSLC/ESF equipment in the same division.

Additional SSLC configuration and communication layout is provided in Figures 7.3-6 through 7.3-10

Figure 7.3-6 presents the design configuration of the SSLC/ESF comprising centralized and triply redundant sets of main processors with RMU (data acquisition) cabinets located in both the reactor and control building.

Figure 7.3-7 is a detailed view of the main processor and communication card depicting the I/O and communications extensions -

Figure 7.3-8 depicts the interdivisional communication used to support two-out-of-four logics. All communication paths are redundant. Since CIM devices are actively powered and the SSLC/ESF design is N-2, the two paths are arranged such that if any two divisions lose power or any single communication path fails (failure would require at least two "breaks"), there will still be communication available between the remaining two divisions to allow a two-out-of-four initiation vote.

Figure 7.3-9 depicts the intradivisional communication used to support the SSLC/ESF and RTIF-NMS communication to the divisional VDUs. All divisions are each connected to two VDUs in the main control room and divisions 1 and 2 are additionally connected to the remote shutdown panels. The same message authentication protocols are used as for interdivisional and nonsafety-related communication.

Figure 7.3-10 depicts the communication between the divisional SSLC/ESF and the N-DCIS where the various signals can be recorded, alarmed, sent to nonsafety-related controllers or monitored.

7.3.5.2.2 Signal Logic Processing

Signals that must meet time response constraints and signals from system logic that are proximal to the SSLC/ESF cabinets are directly connected to the divisional cabinets in the safety-related equipment rooms in the CB. These signals are derived from sensors that are redundant in the four divisions (for each sensed variable).

All input data are processed within the RMU function of the Q-DCIS. The sensor data are transmitted through the DCIS network to the SSLC/ESF Digital Trip Module (DTM) function for setpoint comparison. A trip (or non-trip) signal is generated from this function. Processed trip signals from a division and trip signals from the other three divisions are transmitted through the communication interface and are processed in the VLU function for two-out-of-four voting. The final trip signal (from two or more divisions) is then transmitted to the RMU function via the Q-DCIS network to initiate mechanical actuation devices.

The VLU functions are implemented in the SSLC/ESF triply redundant logic and processors and the results of the two-out-of-four vote is sent to the two or three separate load drivers/discrete outputs in the RMUs. Each load driver/discrete output is individually addressed and all two (solenoid) or three (squib initiator) load drivers/discrete outputs must close to operate the solenoid/squib initiator. The redundancy within a division is necessary to prevent single failures within a division from causing a squib initiator to fire; as a result two of three processors and all three load drivers/discrete outputs are required to produce an output. Self tests within the SSLC/ESF determine if there are component failures and these failures are alarmed in the MCR.

To prevent a single I&C failure from causing inadvertent actuations, the triply redundant SSLC/ESF logic requires that at least two-out-of-three processors (DTM and VLU function) provide a initiation signal to the load drivers/discrete outputs and also requires that two (solenoid) or three (squib initiator) load drivers/discrete outputs individually determine that two-out-of-three processors have sent a signal to initiate the squib initiator. Trip signals are hardwired from the RMU to the equipment actuator. The same logic process is performed for all four divisions. The resulting logic provides single-failure proof actuation and single-failure proof inadvertent actuation. The four-division, two-out-of-four coincident signal voting occurs simultaneously for the equivalent signals in the four divisions. This arrangement provides multiple, independent trip channels, to accommodate a random single failure. The four divisions are interconnected by fiber optic communication links via a safety-related fiber optic communication interface module (CIM). The CIMs provide electrical isolation for data transmission. Subsections 7.1.2, 7.1.3.2, and 7.1.3.3 provide discussions of electrical isolation between divisions.

In summary, at the division level, the four redundant divisions provide a fault-tolerant architecture allowing single division of sensors bypass for on-line maintenance, testing, and repair without losing reliable trip capability. In such a bypass condition, the system automatically defaults to two-out-of-three coincident voting. The fault-tolerant arrangement thus conforms to safety-related system requirements for single-failure tolerance, independence, and separation, as required by IEEE Std. 603, Sections 5.1 and 5.6.

The SSLC/ESF does not require operator intervention during normal operation and allows manual bypass under abnormal conditions or required maintenance conditions such as failure of sensors. Safety-related automatic operations are provided with manual switches in each division for equipment initiation. Key safety-related RPS and ESF trip logics are duplicated in the DPS, which addresses the common mode failure concern and provides diverse protection of digital computer systems performing safety-related functions. The DPS is described in Section 7.8.

Testing and maintenance activities are supported through use of manual control switches that can activate the trip logic signal of each safety-related system. In addition, on-line self-diagnostic tests checking the safety-related performance of the digital control instruments are performed continuously within SSLC/ESF. An illustration of SSLC/ESF and its relationship with the RPS and other interfacing systems is shown in Figure 7.3-5.

The RPS trip logic and MSIV isolation functions of RTIF use "de-energized-to-trip" and "fail-safe" logic. The SSLC/ESF trip logic uses "energized-to-trip" and "fail-as-is" logic. The isolated SSLC/ESF trip signal is transmitted via load drivers/discrete outputs to the actuators for protective action. The load drivers/discrete outputs are solid-state power switches, directing appropriate currents to devices such as the scram pilot valve solenoids, air-operated valves, and explosive-actuated squib valves. The logic is designed so once it is initiated automatically or manually, the intended sequence of protective actions continues until completion, satisfying the requirement of IEEE Std. 603, Section 5.2.

More detailed descriptions of the SSLC/ESF trip logics for ADS and GDCS initiation are included in Subsection 7.3.1.1.2 and Subsection 7.3.1.2.2.

7.3.5.2.3 Division-of-Sensors Bypass

Bypassing any single division-of-sensors is accomplished from each divisional SSLC/ESF cabinet by manual switch control. This bypass disables the DTM outputs of a division at the associated VLU inputs in the four divisions. Interlocks are provided by a four-position joystick-type switch so only one division of sensors at a time can be placed in bypass. When such a bypass is made, all four divisions of two-out-of-four logic become two-out-of-three logic while the bypass is maintained. Bypass permits calibration and repair of sensors or the DTM function. Although all sensors for all systems are bypassed in one division, the remaining three divisions furnish sufficient redundant sensor data for safe operation. The logic is such that all four divisions still can perform two-out-of-four (two-out-of-three) trip decisions - even if sensors are bypassed. Bypass status is indicated to the operator until the bypass condition is removed. An interlock rejects simultaneous attempts to bypass more than one SSLC/ESF division. Any loss of communication caused by a bypass switch is interpreted as a "no bypass" signal.

7.3.5.2.4 Division-Out-of-Service Bypass

There are no surveillance activities or maintenance activities that require taking the division out of service but bypasses can be used to prevent that division's sensors or logic from contributing to a two-out-of-four trip decision. Bypass status is indicated to the operator until the bypass condition is removed. Only one division can be bypassed at any one time. For the SSLC/ESF logic because the division-of-sensors bypass is implemented, and because the logic is implemented with triple redundancy; no additional division trip logic bypass is required. The triply redundant logic and processors in the SSLC/ESF sends individual initiation commands to the two (solenoid) or three (squib initiator) load drivers/discrete outputs in the RMUs. The load drivers/discrete outputs are wired in series and each must individually determine that two-out-of-three processors have issued an initiation command before the final output is initiated. It is undesirable to perform bypass or maintenance activities with the RMUs electrically connected to the solenoid/squib actuator. The disable/test switch that bypasses the load driver/discrete output actuation for the squib initiators provides the effective bypass function required at the actuator level. (Refer to Figures 7.3-1a and 7.3-1b.)

7.3.5.3 Safety Evaluation

The SSLC/ESF consists of a set of logic processing functions for the ESF systems and therefore is a safety-related system. The functions related to sensor signal processing and trip output are safety-related.

The four separated divisions of logic processing equipment provide the necessary degree of redundancy and independence to maintain safe operation despite the loss of portions of the processing capacity.

The SSLC/ESF system is designed so no single equipment failure causes inability to:

- Perform a reactor trip,
- Perform safety-related decay heat removal and reactor pressure control, or
- Initiate the ESF.

Physically separate divisions are established by their relationship with the RPV, which is spatially divided into four quadrants. The sensors, logic, and output actuators of the various systems are allocated to these divisions.

The digital devices in SSLC/ESF are, in general, microprocessor-based, software-controlled instruments.

Microprocessor-based logic in the SSLC/ESF activates the solenoid-controlled SRVs squib-actuated DPVs, GDCS injection and equalizing valves, ICS valves, and SLC squib valves.

A diverse I&C system is incorporated, featuring a totally independent set of selected reactor trip logic functions and ESF initiation logic functions addressing the requirements of the BTP HICB-19 position. This system is described in Section 7.8. The RPS logic is implemented using a diverse hardware/software platform. The SSLC/ESF system is designed to operate in a mild environment in clean areas within the CB and RB safety envelopes. Refer to Appendix 3H, Subsections 9.4.1 and 9.4.6 for specific environmental conditions.

Panel internal environments are maintained to ensure that reliability goals are achieved. Panel internal cooling is by natural convection. Fans are used to improve long-term reliability, but no credit is taken for forced-air cooling in the qualification of safety-related functions. Thermal design adequacy is considered during detail equipment design by analysis of heat loads (per circuit module, per bay, and per module).

Table 7.1-1 identifies the SSLC/ESF and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.5.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The SSLC/ESF design conforms to these standards.

10 CFR 50.55a(h), Protection and Safety Systems Compliance with IEEE Std. 603:

- Conformance: The SSLC/ESF design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the SSLC/ESF design conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.3.5.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): See Subsections 7.3.5.2.2, 7.3.5.2.3 and 7.3.5.2.4.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to SSLC/ESF.
  - Section 5.2 (Completion of Protective Actions): See Subsections 7.3.5.2.2.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 7.3.5.2.2 and 7.3.5.4.
  - Section 6.2 and 7.2 (Manual Control): See Subsection 7.3.5.1.
  - Section 6.4 (Derivation of System Inputs): The SSLC/ESF is a logic processing system only and its sensors are part of other systems.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 7.3.5.2.2 and 7.3.5.4.
  - Section 6.6 and 7.4 (Operating Bypasses): See Subsection 7.3.5.2.2, 7.3.5.2.3 and 7.3.5.2.4.
  - Section 6.7 and 7.5 (Maintenance Bypasses): See Subsection 7.3.5.2.2, 7.3.5.2.3 and 7.3.5.2.4.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the SSLC/ESF are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the SSLC/ESF are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34 (f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The SSLC/ESF complies by providing automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(viii)[II.B.3] Capability to Promptly Obtain and Analyze Samples from the Reactor Coolant System and Containment:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(x)[II.D.1], Relief and Safety Valve Test Requirements:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xi)[II.D.3], Direct Indication of Relief and Safety Valve Position in the Control Room:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34 (f)(2)(xiv)[II.E.4.2], Containment Isolation Systems:

- Conformance: The SSLC/ESF logic controlling containment isolation functions conforms to these criteria.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: NBS provides the reactor water level measurement (temperature compensated) inputs to SSLC/ESF. The reactor water level instrumentation errors due to non-condensable gases in instrument reference legs are addressed in Subsection 7.7.1.2.2.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xxi)[II.K.1.22], Auxiliary Heat Removal Systems:

- Conformance: The SSLC/ESF conforms to these requirements.

10 CFR 50.34 (f)(2)(xxiii) [II.K.2.10], Anticipatory Reactor Trip:

- Conformance: The SSLC/ESF initiates the ICS in response to a Loss of All Feedwater Flow Event. This is an anticipatory trip actuated on a power generation bus loss event.

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.34(f)(2)(xxviii)[III.D.3.4] Control Room Habitability Problems Under Accident Conditions:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.44(c)(4), Combustible Gas Control For Nuclear Power Reactors, Monitoring:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The SSLC/ESF design conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The SSLC/ESF design conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the SSLC/ESF within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.3.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 15, 16, 19, 20, 21, 22, 23, 24, 29, 30, 33, 34, 35, 37, 41, 43, 63 and 64:

- Conformance: The SSLC/ESF design complies with these GDCs.

7.3.5.3.3 Staff Requirements Memorandum

SRM on SECY-93-087, Item II.Q Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The Reactor Trip (Protection) System and ESF designs conform to Item II.Q of SRM on SECY-93-087 (BTP HICB-19) in conjunction with the implementation of the DPS, described in Section 7.8.

SRM on SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability:

- Conformance: The SSLC/ESF VDU design meets the requirements of SECY-93-087, Item II.T for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:

- Alarm points are sent via dual networks to redundant message processors using dual power supplies. The processors are dedicated to alarm processing.
- The alarms are displayed on multiple independent VDUs (dual power supplies on each).
- The alarms are driven by redundant data links to the AMS (dual power). There are redundant alarm processors.
- There is one horn and one voice speaker. Test buttons are available to test the horn(s) and all the lights.
- There are no alarms requiring manually controlled actions for systems to accomplish their safety-related functions.

7.3.5.3.4 Regulatory Guides

RG 1.22, Safety Guide 22 Periodic Testing of Protection System Actuation Functions:

- Conformance: The SSLC/ESF design complies with the guidance of RG 1.22.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance: The SSLC/ESF design complies with the guidance of RG 1.45.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The SSLC/ESF provides bypass capability and status that complies with RG 1.47.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The SSLC/ESF is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The SSLC/ESF design complies with the guidance of RG 1.62. Signals for manual initiation of protective actions are hardwired to the SSLC/ESF equipment.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The SSLC/ESF design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-related Systems:

- Conformance: The SSLC/ESF design complies with RG 1.105. Reference 7.3-2 provides detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118. Testing of the SSLC/ESF is performed in conjunction with the Q-DCIS.

RG 1.152, Criteria for Programmable Digital Computer System Software in safety-related Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to the guidelines of RG 1.152. Additional discussion is provided in Subsection 7.2.1.3 describing RPS system compliance.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The SSLC/ESF design, in conjunction with the Q-DCIS, conforms to 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used In Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SSLC/ESF design complies with RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The SSLC/ESF design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The SSLC/ESF design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.5.3.5 Branch Technical Positions

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Conformance: The SSLC/ESF design complies with BTP HICB-1.

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The SSLC/ESF is fully operational during reactor operation, and is tested in conjunction with the Q-DCIS. Therefore, the SSLC/ESF design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: SSLC/ESF logic controllers use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices. The Q-DCIS provides the communication functions for SSLC/ESF. See Subsection 7.1.2, 7.1.3.2 and 7.1.3.3 for descriptions of the Q-DCIS communication system design.

Portions of RPS and SSLC/ESF may use coil-to-contact isolation of relays or contactors. This is acceptable according to BTP HICB-11 when the application is analyzed or tested in accordance with the guidelines of RG 1.75 and RG 1.153.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The SSLC/ESF design conforms to BTP HICB-12. Setpoint implementation is in accordance with Reference 7.3-2.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-based Instrumentation and Control:

- Conformance: [*Development of software for the safety-related system functions within SSLC/ESF conforms to the guidance of BTP HICB-14 as discussed in the LTRs "ESBWR - Software Management Program Manual," NEDO-33226, NEDE-33226P and "ESBWR - Software Quality Assurance Program Manual," NEDO-33245, NEDE-33245P. (References 7.3-3 and 7.3-4.) Safety-related software to be embedded in the memory of the SSLC/ESF controllers is developed according to a structured plan outlined in References 7.3-3 and 7.3-4.*]*

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in the SSLC/ESF subsection conforms to BTP HICB-16.

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

- Conformance: The RPS and SSLC/ESF controller designs conform to BTP HICB-17. Discussions on self-test and surveillance tests of RPS and ESF are provided in Subsections 7.2.1.3.5 and 7.3.5.4, respectively.

BTP HICB-18, Guidance on Use of Digital Computer-based Instrumentation and Control Systems:

- Conformance: Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance of Branch Technical Position HICB-18. The Q-DCIS is built and qualified specifically for ESBWR applications as safety-related and not as commercial grade programmable logic controllers (PLCs). The embedded and operating system software meet the acceptance criteria contained in BTP HICB-14, for safety-related applications.

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

- Conformance: SSLC/ESF has a four-division, independent and separated equipment arrangement. Isolation of signal transmission between safety-related divisions and between safety-related and nonsafety-related equipment, is provided by non-conductive fiber optic cable. System functions are segmented among multiple controllers. Automatic functions are backed up by diverse automatic and manual functions. Control system functions are separate, independent, and diverse from the protection system functions. The RPS logic is implemented using a diverse hardware/software platform.

Additional diverse features are discussed in Section 7.8, which specifically addresses compliance with the guidance of BTP HICB-19.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The real-time performance of SSLC/ESF in meeting the requirements for safety-related system trip and initiation response conforms to BTP HICB-21. Each SSLC/ESF controller operates independently and asynchronously with respect to other controllers. The real-time performance of the safety-related control system is deterministic based on the Q-DCIS internal and external communication system design and the SSLC/ESF controller design. Timing signals are not exchanged – neither between divisions of independent equipment, nor between controllers within a division.

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7.3.5.4 Testing and Inspection Requirements

A periodic, automatic self-test feature is included to verify proper operation of each SSLC/ESF logic processor. The self-test is an on-line, continuously operating self-diagnostics function. The on-line self-test operates independently within each of the four SSLC/ESF divisions.

The major purpose of automatic self-testing is improving system availability by checking and confirming transmission path continuity for safety-related signals, verifying operation of each two-out-of-four coincidence trip logic function, and detecting, alarming, and recording the location of hardware or software faults. Tests verify the basic integrity of each card and the microprocessors. Discrete logic cards contain diagnostic circuitry monitoring critical points within the logic configuration and determine whether a discrepancy exists between an expected output and the existing present state. The self-test operations are part of normal data processing and do not affect system response to incoming trip or initiation signals. Automatic initiation signals from plant sensors override automatic test sequences and perform the required safety-related function. Process or logic signals are not changed as a result of self-test.

The self-testing includes continuous error checking of transmitted and received data on the serial data links of each SSLC/ESF controller; for example, error checking by parity check, checksum, or Cyclic Redundancy Checking (CRC) techniques. Self-test failures are alarmed to the operator at the MCR console and recorded in a log maintained by the PCF of the N-DCIS.

In-service testing of the SSLC/ESF is performed periodically to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include, as required, instrument channel checks, functional tests, verification of proper sensor and channel calibration, verification of applicable VLU logic functions, and response time tests.

All test features adhere to the single failure criterion so that:

- No single failure in the test circuitry incapacitates an SSLC/ESF safety function, and
- No single failure in the test circuitry causes an inadvertent scram, MSIV closure, other PCV isolation, or actuation of any ESF system.

7.3.5.5 Instrumentation and Controls Requirements

The SSLC/ESF equipment uses microprocessor-based programmable logic and control instruments, with standardized interchangeable modules. Discrete solid-state logic also is used when applicable.

Control programs for each microprocessor-controlled instrument are in the form of software residing in non-volatile memory. The storage medium is in general Programmable Read-Only Memory (PROM). Programs are under the control of a real-time operating system residing in non-volatile memory. The equipment is qualified with a verification and validation program conforming to applicable codes and standards.

The SSLC/ESF component design accommodates electrostatic discharge withstand capability. Administrative controls ensure that the associated channel is bypassed prior to opening any system cabinet. Alternatively, administrative actions consistent with standard electronics electrostatic discharge control practices are required prior to opening a cabinet. These practices implement manufacturer recommendations.

Logic and controls for SSLC/ESF are located on each divisional SSLC/ESF cabinet in the secure Q-DCIS equipment rooms in the CB, with controls and system operating status available on the operator interface section in the MCR. The SSLC/ESF controls are used infrequently. Such controls are available for operator action during plant operation or during accident or transient conditions, and are also used to support testing and maintenance. The SSLC/ESF cabinets are accessible for maintenance and testing. Access to the SSLC/ESF cabinets is administratively controlled. If required the affected division's sensors are bypassed such that they do not provide trip inputs to other divisions, and the division can be disconnected from its actuators so that its logic remains functional. After maintenance or other access the affected division's diagnostics, self-testing, and actuator/sensor monitoring confirm correct operation.

The minimum required SSLC/ESF displays provided in the MCR (per division) are:

- Division-of-sensors in bypass,
- SSLC/ESF controller inoperative (DTM or VLU), and
- Communication Interface Module (CIM) inoperative.

7.3.6 Containment System Wetwell-to-Drywell Vacuum Breaker Isolation Function

The Vacuum Breaker Isolation Function (VBIF) is an independent control platform that, upon detection of excessive vacuum breaker (VB) leakage, prevents the loss of long-term containment integrity. Figures 7.1-1, 7.1-2, and 7.3-5 indicate VBIF interfaces.

7.3.6.1 System Design Bases

The wetwell-to-drywell VB isolation function has the following safety-related requirements and 10 CFR 50.2 Design Bases.

- Automatically isolates an excessively leaking VB using a VB isolation valve.
- The VB and VB isolation valve are qualified for a harsh environment inside the drywell.
- Manual opening and closing of a VB isolation valve is provided for in the design.

- No single control logic and instrumentation failure opens/closes more than one VB isolation valve.
- VB and VB isolation valve positions are displayed in the MCR.
- The safety-related function is met with one VB/VB isolation valve path isolated together with any active identifiable single failure.
- Divisional instruments performing VB isolation valve logic are powered by the associated safety-related divisional power supplies.
- Containment system VB isolation function logic controllers are independent.

7.3.6.2 System Description

The wetwell-to-drywell VB isolation function comprises ICPs, three sets of VBs, and three sets of VB isolation valves. A more detailed description is given in Subsection 6.2.1.1.2.

- Automatic Operation
  - Closure of the VB isolation valve is performed automatically, without need for operator action, once excessive bypass leakage through a VB is detected.
  - Automatic actuation logic is performed by a control system with components similar to those used in the ATWS/SLC control system. These components are an independent Q-DCIS subsystem.
  - Each VB/VB isolation valve pair has dedicated sensors and logic. Each VB isolation valve operates independently of the other VB isolation valves according to input received from its sensors. Logic is processed for each individual isolation valve; failure of the logic for one isolation valve does not affect the logic for any other isolation valve.
- Manual Operation
  - Manual controls are available to the operator in the MCR to:
    - Open each VB isolation valve, and
    - Close each VB isolation valve.
  - Manual controls are independent for each VB isolation valve and are hard-wired to the same hardware as the VB isolation valve automatic control logic.
- Actuation Logic
  - The primary closure demand for the VB isolation valve is based upon a temperature differential between the drywell and wetwell and upon the bypass status of the associated division of logic. A separate LOCA temperature value also is provided to the logic.
  - A secondary closure demand signal is based upon a temperature differential between the drywell and wetwell and upon VB position. A separate LOCA temperature value also is provided to the logic.
  - Manual control over each VB isolation valve is available to the operator.

- Logic for each VB isolation valve is controlled by 16 thermocouples (four groups of four) and four proximity switches. Each of the four thermocouples in each group is assigned to a separate division. Each of the four groups provides temperature values for separate drywell and wetwell locations.
- Proximity switches on each VB body give positive indication of fully open or fully closed positions.
- The thermocouples are located in the:
  - Wetwell (on or adjacent to the VB debris screen);
  - Wetwell cavity (in the pipe cavity between the VB isolation valve and the end of the VB penetration on the wetwell side);
  - Drywell (1) (on or near the outlet of the VB); and
  - Drywell (2) (inside the drywell separate from the VB/VB isolation valve assembly).
- Each VB isolation function ATWS/SLC division can be placed into manual bypass status that is automatically indicated in the MCR.

7.3.6.3 Safety Evaluation

Section 6.2 evaluates the VB isolation function and shows that for the entire range of nuclear process system pipe break sizes, the opening of a single VB ensures containment structure functional integrity.

Table 7.1-1 identifies the VB isolation function and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.3.6.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The VB isolation function design complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The VB isolation function conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the VB isolation function conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-Related Function): See Subsection 7.3.6.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the VB isolation function.
  - Section 4.6 (Spatially Dependent Variables): See the Actuation Logic section of Subsection 7.3.6.2 & Subsection 6.2.1.1.5.5.1.
  - Section 5.2 (Completion of Protective Actions): Completion of protective actions is not applicable beyond that discussed in Subsection 7.1.6.6.1.3.

- Section 5.7 (Capability for Test and Calibration): See Subsection 7.6.3.4.
- Section 6.2 and 7.2 (Manual Control): See Subsections 7.3.6.1 & 7.3.6.2.
- Section 6.4 (Derivation of System Inputs): Derivation of system inputs for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.20.
- Section 6.5 (Capability of Test and Calibration): See Subsection 7.6.3.4.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance Bypasses for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the VB isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The VB isolation function design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The VB isolation function design complies by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The VB isolation function conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the design of the VB and VB isolation function within the DCD complies with this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety-related functions.

7.3.6.3.2 General Design Criteria

GDC 1, 2, 4, 13, 16, 19, 20, 21, 22, 23, 24 and 29:

- Conformance: The VB isolation function design complies with these GDCs.

7.3.6.3.3 Staff Requirements Memorandum

SRM on SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The VB isolation function design complies with these criteria through demonstration that no postulated common-mode failure of the control system could disable the VB isolation function. The discrete logic and solid state controls used in this design are not subject to the vulnerabilities described by SECY-93-087, Item II.Q.

7.3.6.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Function:

- Conformance: The VB isolation function design conforms to RG 1.22. System logic and components are tested periodically during refueling outages.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety:

- Conformance: The VB isolation function design conforms to RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The VB isolation function is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The VB isolation function design complies with RG 1.62. Each division has a manual actuation switch in the MCR. Initiation of the system requires actuation of two switches to ensure that manual initiation is a premeditated act.

RG 1.75, Physical Independence of Electric Systems:

- The VB isolation function design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints established to control the VB isolation valve conform to RG 1.105. Reference 7.3-2 provides a detailed description of the GEH methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.152.

RG 1.153, Criteria for Power, I&C Portions of Safety Systems:

- Conformance: The VB isolation function design complies with IEEE Std. 603.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.168 as implemented on the independent control platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The VB isolation function design conforms to RG 1.169 as implemented on the independent control platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.170 as implemented on the independent control platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.171 as implemented on the independent control platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.172 as implemented on the independent control platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.173 as implemented on the independent control platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The VB isolation function design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The VB isolation function design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.3.6.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the VB isolation function:

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The VB isolation function design conforms to BTP HICB 8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: Logic controllers for the VB isolation function use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The setpoints established to control the VB isolation valve conform to this guide. Reference 7.3-2 provides a detailed description of the GEH methodology.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The VB isolation function design conforms to BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR 52:

- Conformance: The level of detail in the VB isolation function description conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The VB isolation function design conforms to BTP HICB-17.

BTP HICB-18, Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and control Systems:

- Conformance: Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance of Branch Technical Position HICB-18. Q-DCIS is built and qualified specifically for ESBWR applications as safety-related and not as commercial grade PLCs. The embedded and operating system software meet the acceptance criteria contained in BTP HICB-14, for safety-related applications.

BTP HICB-19, Guidance on Evaluation of Defense-in-Depth and Diversity in digital Computer-based Instrumentation and Control Systems:

- Conformance: The VB isolation function design conforms to BTP HICB-19. The discrete logic and solid state controls used in this design are not subject to the vulnerabilities described by BTP HICB-19.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The VB isolation function design conforms to BTP HICB-21.

7.3.6.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3] and 10 CFR 50.34(f)(2)(xiv)[II.E.4.2] apply to the VB isolation function. The VB isolation function complies with the requirements as indicated above. TMI action plan requirements are addressed in Appendix 1A.

7.3.6.4 Testing and Inspection Requirements

The VB isolation function TLUs are self-tested continually at preset intervals and can be tested during plant operation. VB isolation function equipment is tested during reactor operation to support VB Isolation Valve stroke testing as specified in Table 3.9-8 and Subsection 6.2.1.1.5. Refer to Subsection 6.2.1.1.5 for a discussion of mechanical tests performed on the VB isolation functions.

7.3.6.5 Instrumentation and Control Requirements

The performance and effectiveness of the VB isolation function in a postulated accident is verified by observing the following MCR indications (additional discussion on the VB isolation function instrumentation is contained in Subsection 7.3.6.1 and in Subsection 6.2.1.1.5):

- Status indication of VB position;
- Status indication of VB isolation valve position;
- Drywell and wetwell pressure indication;
- Drywell and wetwell temperature indications;

- VB isolation valve bypass status; and
- Status indication of bypass leakage.

The VB isolation function instrumentation located in the drywell is designed to operate in the harsh drywell environment that results from a LOCA. Safety-related instruments, located outside the drywell, are qualified for the environment in which they must perform their safety-related function.

7.3.7 COL Information

None.

7.3.8 References

7.3-1 (Deleted)

7.3-2 GE-Hitachi Nuclear Energy, "GEH ABWR/ESBWR Setpoint Methodology," NEDE-33304P, Class III (Proprietary), Revision 1, November 2008, and NEDO-33304, Class I (Non-proprietary), Revision 1, November 2008.

7.3-3 [*GE Hitachi Nuclear Energy, "ESBWR - Software Management Program Manual (SMPM)," NEDE-33226P, Class III (Proprietary) Revision 4, May 2009, and NEDO-33226, Class I (Non-proprietary), Revision 4, May 2009.*]*

7.3-4 [*GE Hitachi Nuclear Energy, "ESBWR - Software Quality Assurance Program Manual (SQAPM)," NEDE-33245P, Class III (Proprietary), Revision 3, July 2008, and NEDO-33245, Class I (Non-proprietary), Revision 3, July 2008.*]*

7.3-5 (Deleted)

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

Table 7.3-1

Automatic Depressurization System Parameters

Parameter	Value
Number of ADS divisions	4
Processor/logic redundancy per division	3
Number of load drivers/discrete outputs within a division used to actuate the separate solenoid-operated gas pilots on each SRV	2
Number of load drivers/discrete outputs within a division used to actuate the separate igniter circuits on each squib-actuated DPV	3
Minimum number of ADS logic divisions to actuate any SRV pilot and open the SRV	2
Minimum number of ADS logic divisions to actuate (energize) one of the igniter circuits and open the DPV	2
(Deleted)	

Table 7.3-2

Safety Relief Valve Initiation Parameters

Parameter	Value*
Number of SRV groups	2
Number of SRVs in the first group (Group 1-initial ADS start signal)	5
Number of SRVs in the second group (Group 2 – second ADS start signal)	5
Time delay to a sustained RPV Level 1 signal	10 sec
Time delay to a sustained Drywell Pressure High signal	60 min
Time after a sustained RPV Level 1 signal or a sustained Drywell Pressure High signal before signaling Group 1 SRVs to open	0 sec
Time after a sustained RPV Level 1 signal or a sustained Drywell Pressure High Level signal before signaling Group 2 SRVs to open	10 sec

*The time delay values represent design or analytical limits.

Table 7.3-3

Automatic Depressurization Valve Parameters

Parameter	Value*
Number of DPVs groups	4
Number of DPVs in Group 1 (third ADS start signal)	3
Number of DPVs in Group 2 (fourth ADS start signal)	2
Number of DPVs in Group 3 (fifth ADS start signal)	2
Number of DPVs in Group 4 (sixth ADS start signal)	1
Initial ADS time delay, after a sustained RPV Level 1 signal or sustained Drywell Pressure High signal, before Group 1 DPVs are signaled to open	50 sec
Additional ADS time delay, after Group 1 initiation, before Group 2 DPVs are signaled to open	50 sec
Additional ADS time delay, after Group 2 initiation, before Group 3 DPVs are signaled to open	50 sec
Additional ADS time delay, after Group 3 initiation, before Group 4 DPVs are signaled to open	50 sec

*The time delay values represent design or analytical limits

Table 7.3-4

Gravity Driven Cooling System Parameters

Parameter	Value*
Deluge squib valves initiated by lower drywell high temperature	>538°C (1000°F)
GDCS Injection squib valve logic time delay after a sustained RPV Level 1 or a sustained Drywell Pressure High signal	150 sec
GDCS Equalization line squib valve initiation logic time delay after a sustained RPV Level 1 signal	30 min
Manual GDCS equalization squib valve initiation logic time delay after a sustained RPV Water Level 1 signal	30 min
Manual GDCS injection squib valve initiation logic time delay after low RPV pressure permissive signal	30 min

*These values represent design or analytical limits.

Table 7.3-5

LD&IS Interfacing Sensor Parameters

Temperatures:

- Main Steam Line (MSL) Tunnel Area
- Drywell
- MSL Turbine Area
- RWCU/SDC rooms

Pressures:

- MSL Turbine Inlet
- Main Condenser
- RPV Head Flange Seal Leakage
- Drywell
- Feedwater Line Differential

Radiation Levels:

- RCCWS Intersystem Leakage
- Drywell Fission Product
- RB HVAC Air Exhaust
- Refueling Handling Area Vent Exhaust
- Isolation Condensers Pool Vent Discharge

Flow Rates:

- MSL Steam
- RWCU/SDC Differential Mass (Temperature Compensated)
- Drywell Air Cooler Condensate Discharge
- Isolation Condenser Steam
- Isolation Condenser Condensate Return

Levels:

Table 7.3-5

LD&IS Interfacing Sensor Parameters

- RPV Water Level 0.5, Level 1, Level 2, Level 8, and Level 9.
- Drywell drain Sump
- Containment Sump
- Drywell Water

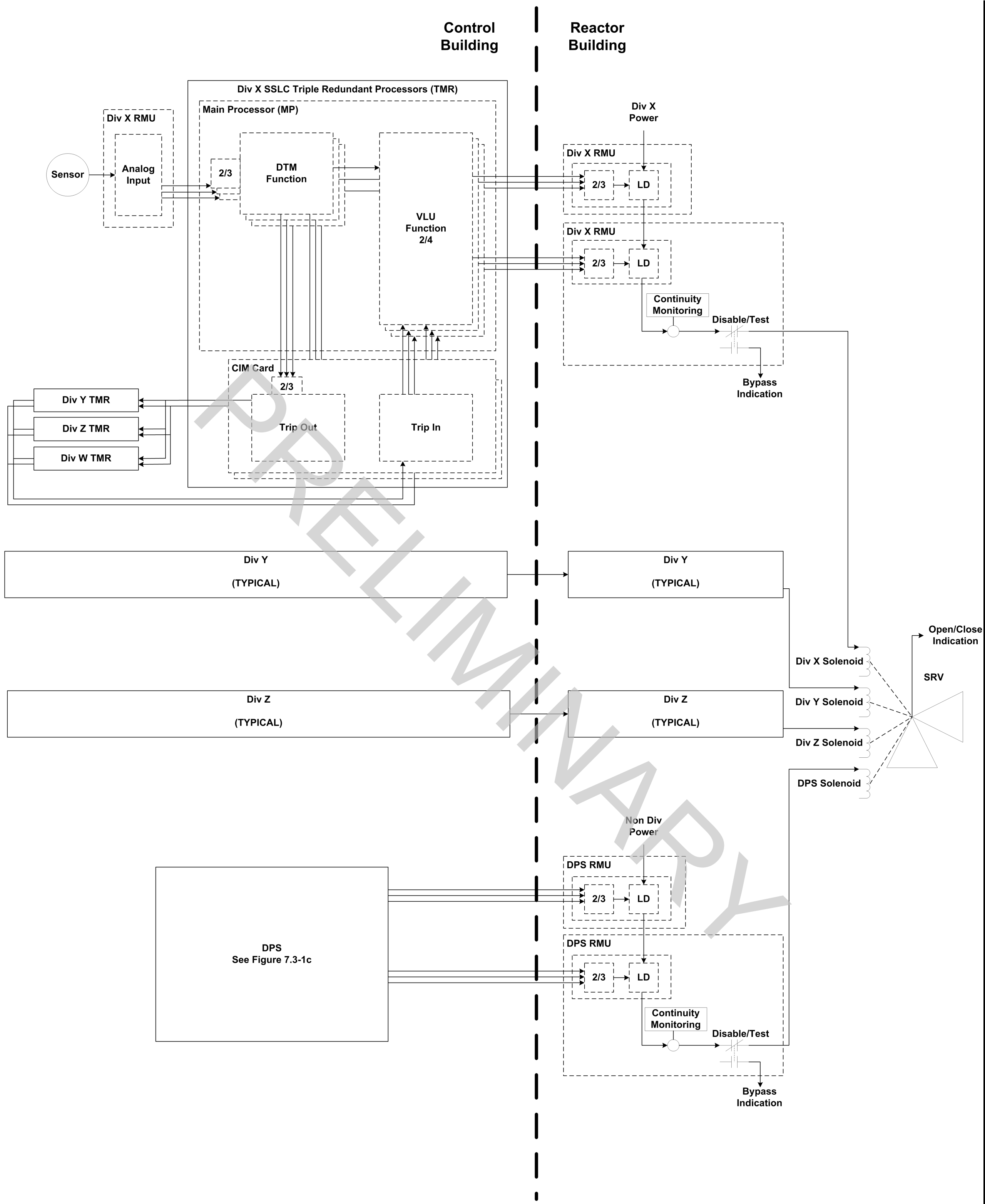


Figure 7.3-1a. SRV Initiation Logics

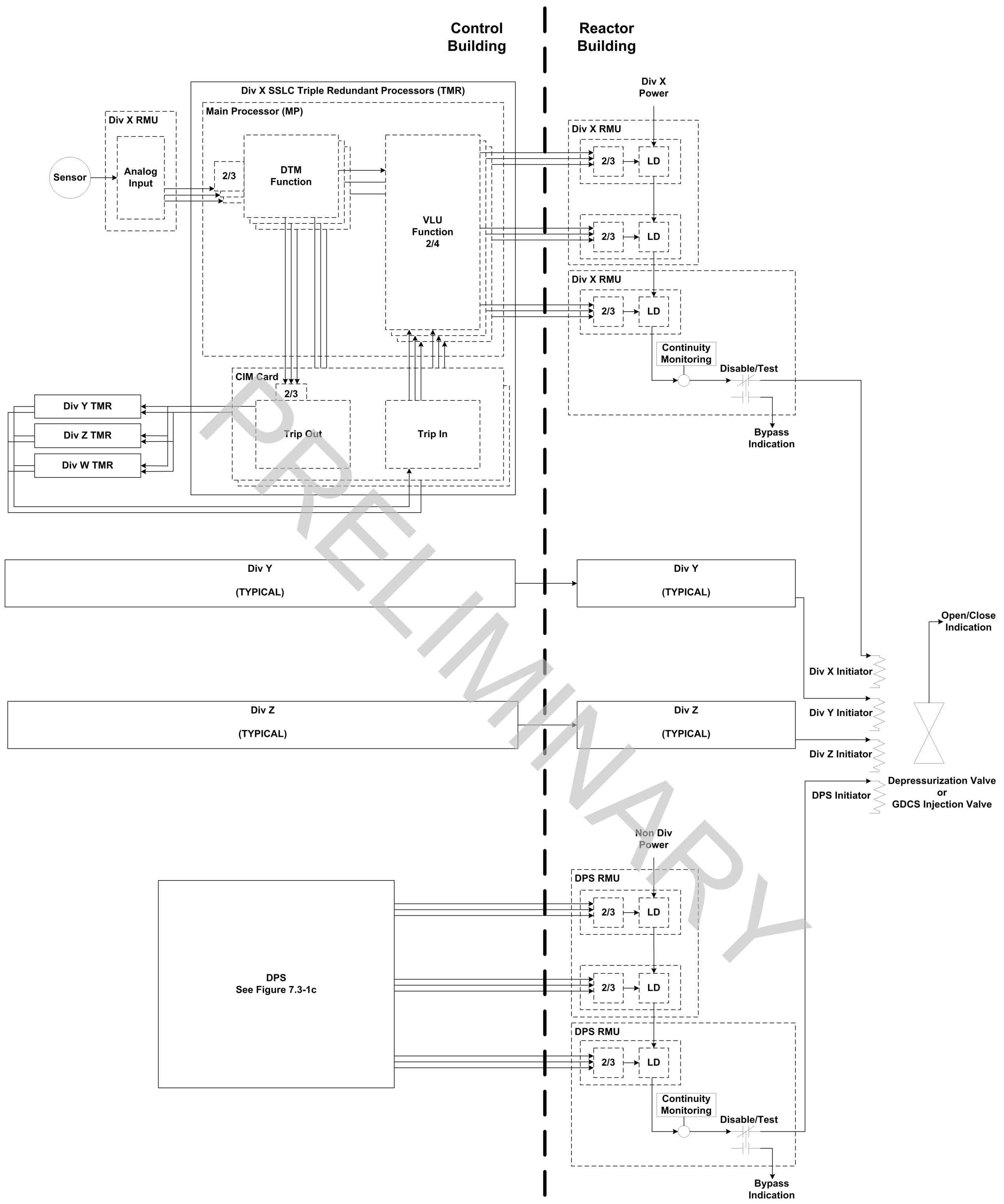


Figure 7.3-1b. GDCS and DPV Initiation Logics

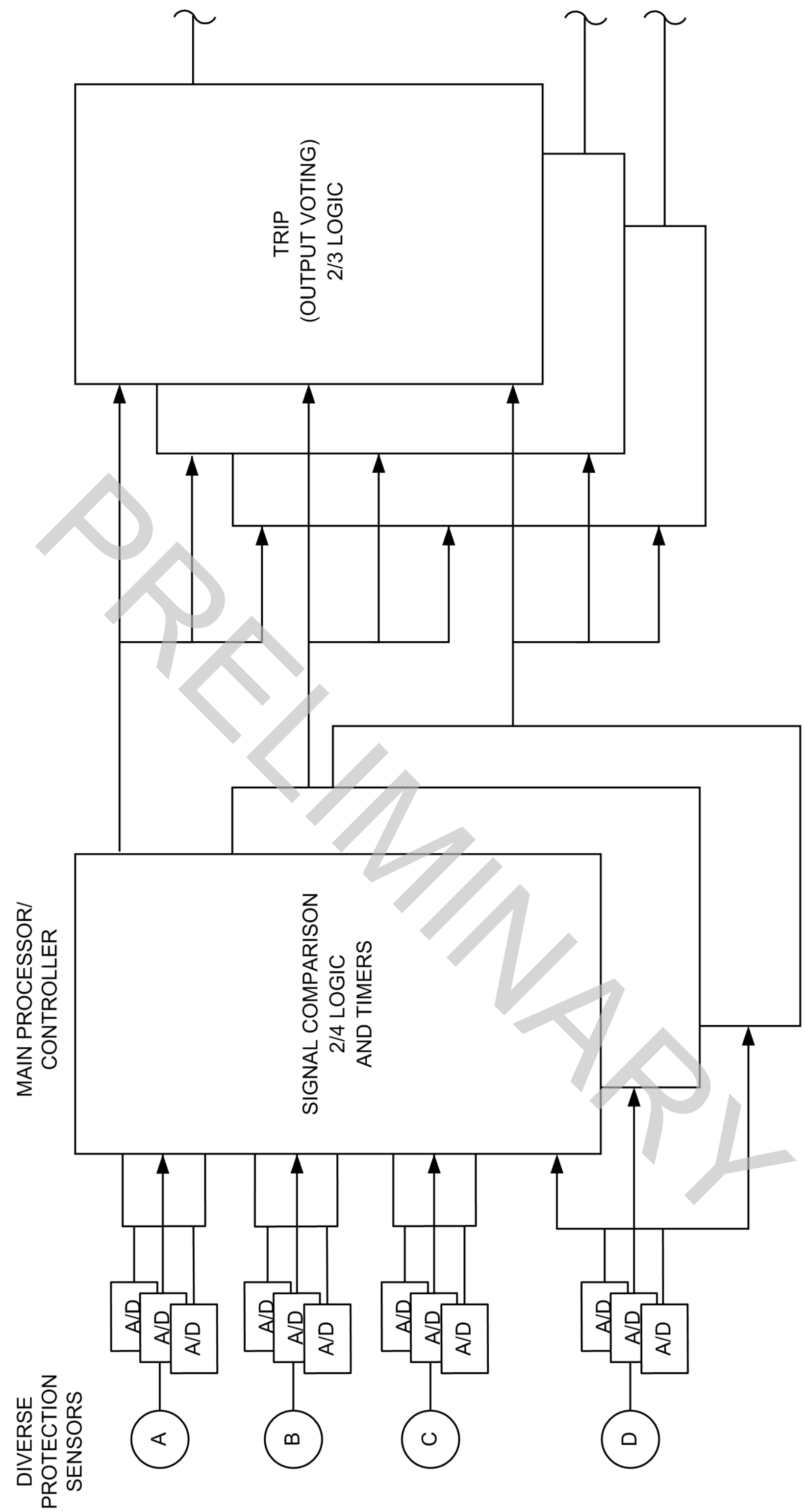


Figure 7.3-1c. DPS Initiation Logic

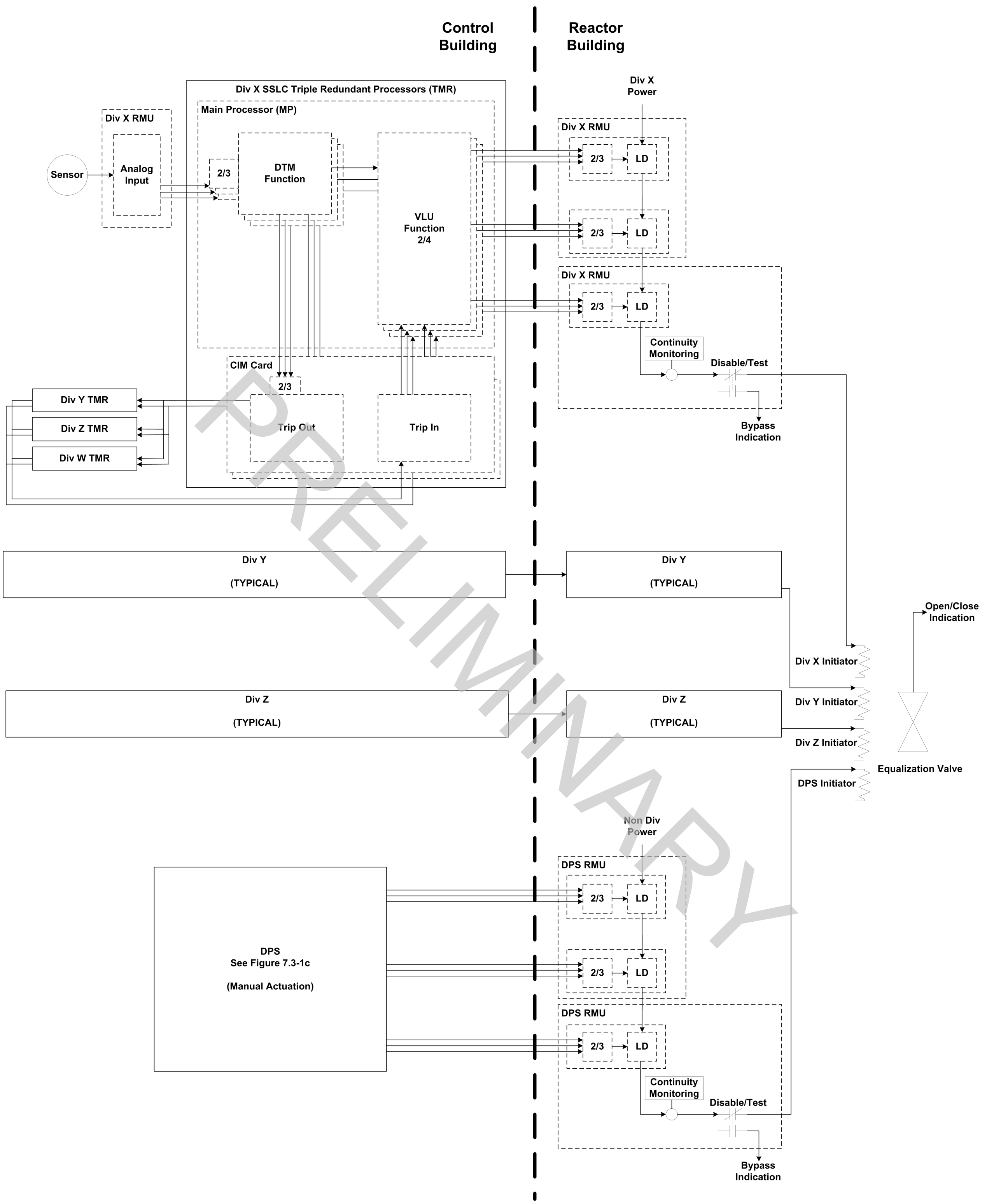


Figure 7.3-2. GDCS Equalizing Valve Initiation Logics

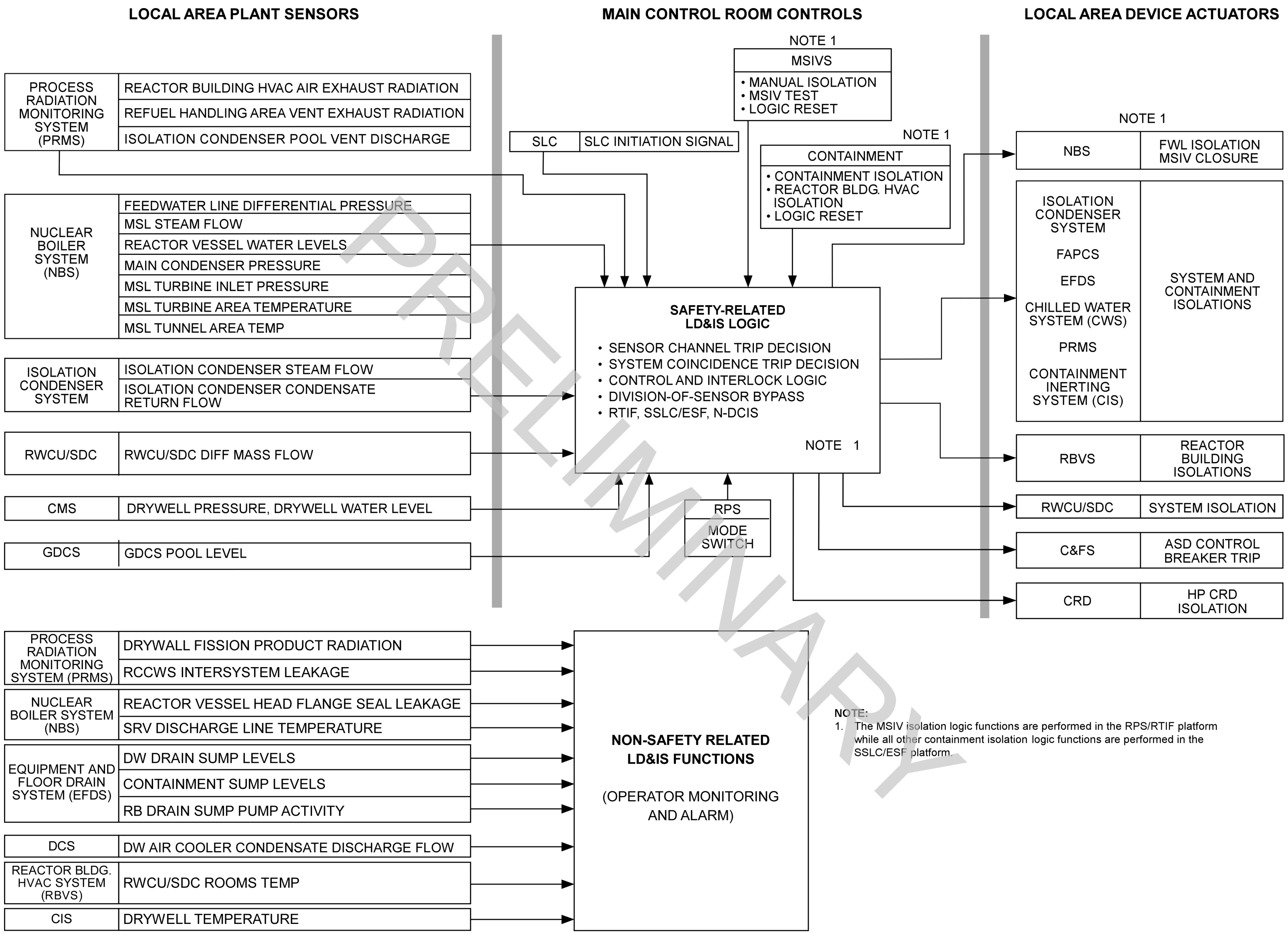
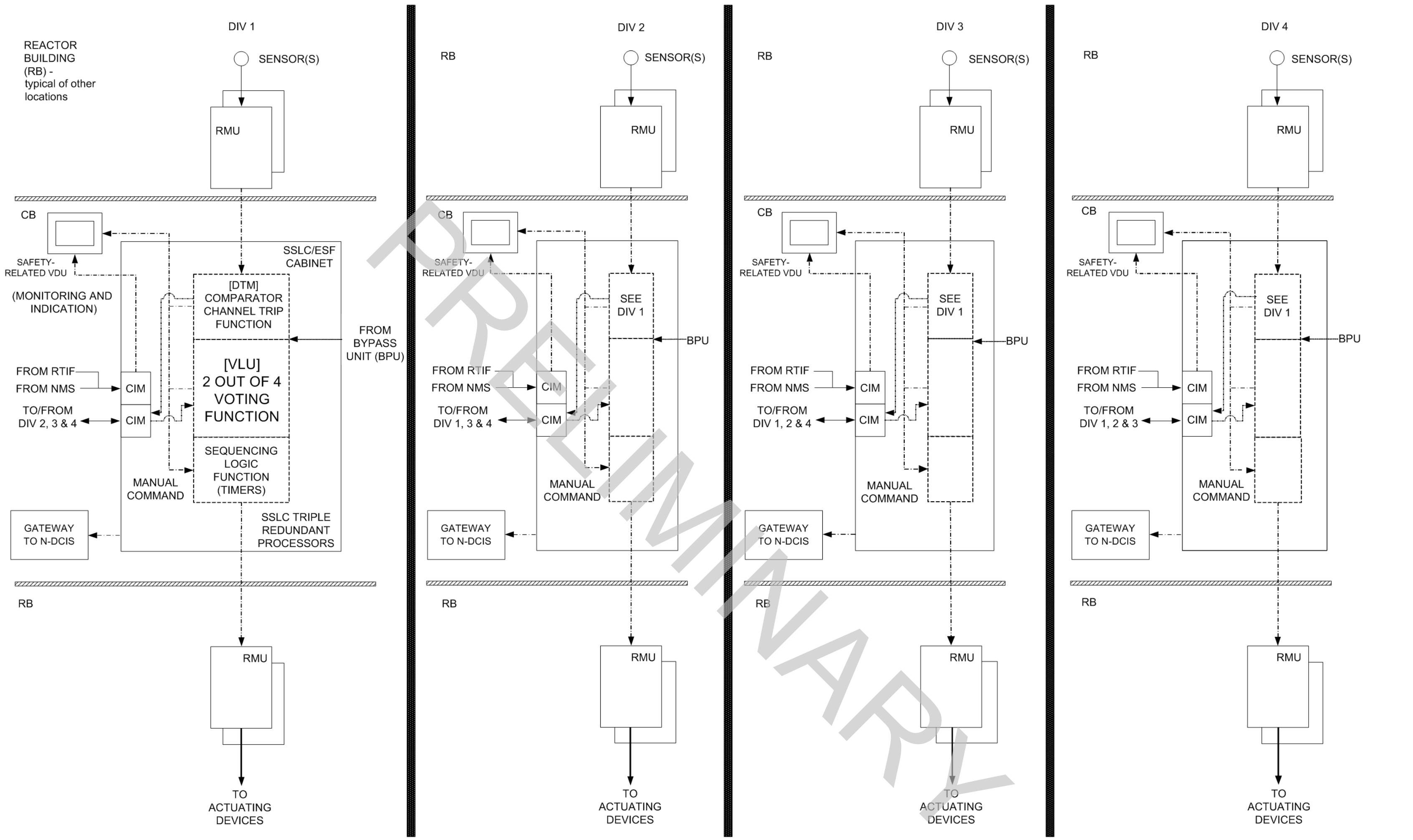


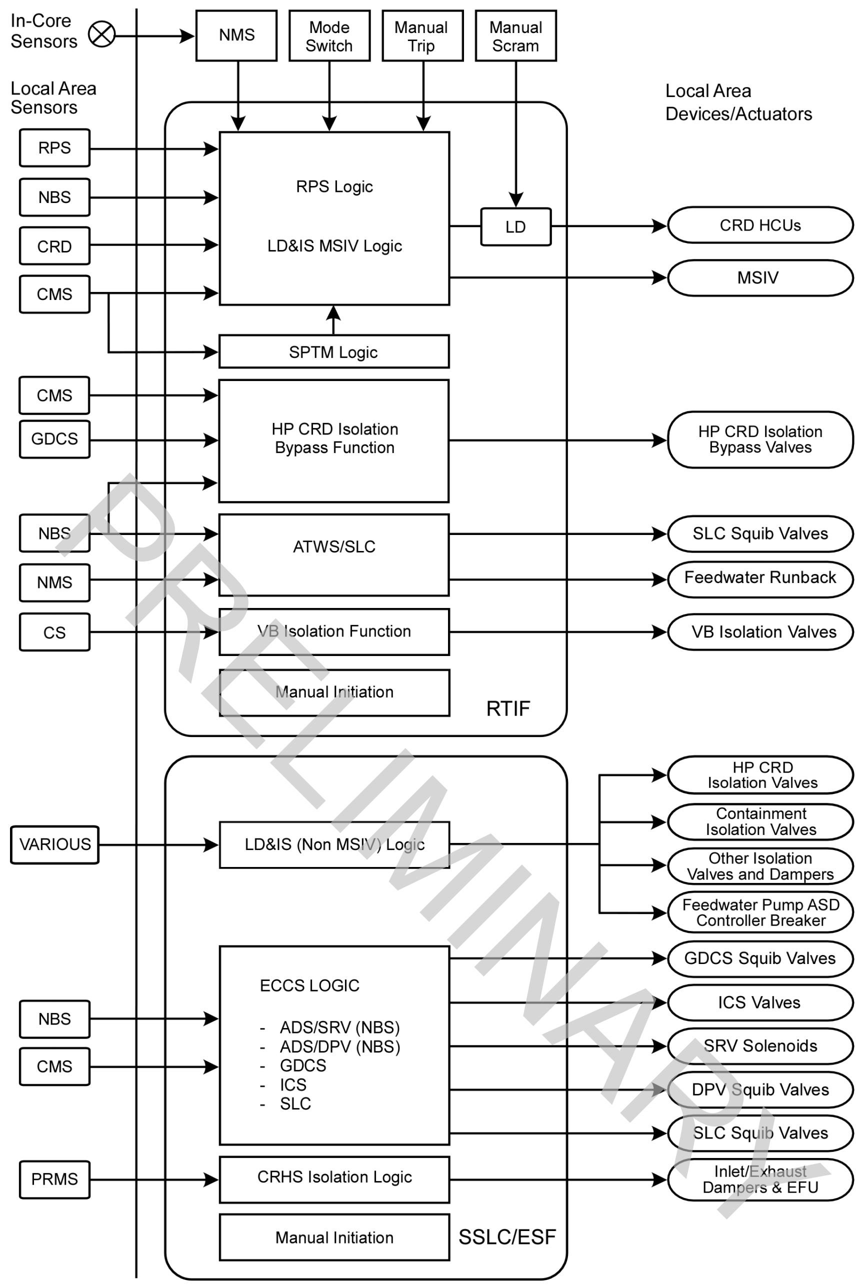
Figure 7.3-3. LD&IS System Design Configuration



NOTES:
Redundant DIV 1 and 2 VDUs are located at the Remote Shutdown Panels
CIM=COMMUNICATION INTERFACE MODULE-ISOLATOR

(Note: the VLU contains dual redundant 2/4 logics with two independent trip outputs.)

Figure 7.3-4. SSLC/ESF Functional Block Diagram



Notes:
1) Local area sensors include:

RPS:	Turbine stop valve position, turbine CV oil pressure, turbine bypass valve position, main condenser pressure and loss of power generation bus
PRMS:	Process radiation - control room inlet ventilation
NBS:	MSIV position (for RTIF only), RPV pressure, water level
CRD:	Scram accumulator charging water header pressure
CMS:	Drywell pressure, drywell level, suppression pool temperature
HP CRD	High Pressure Control Rod Drive System
CS:	(Containment System) wetwell and drywell temperature, Vacuum Breaker (VB) and VB isolation valve position

2) Manual scram interrupts power to the LD circuit
3) LD&IS MSIV isolation logic shares RTIF sensors. LD&IS non-MSIV isolation logic shares SSLC/ESF sensors.
4) The various LD&IS sensors and functions are depicted on Figure 7.3-3.

Figure 7.3-5. SSLC/ESF System Interface Diagram

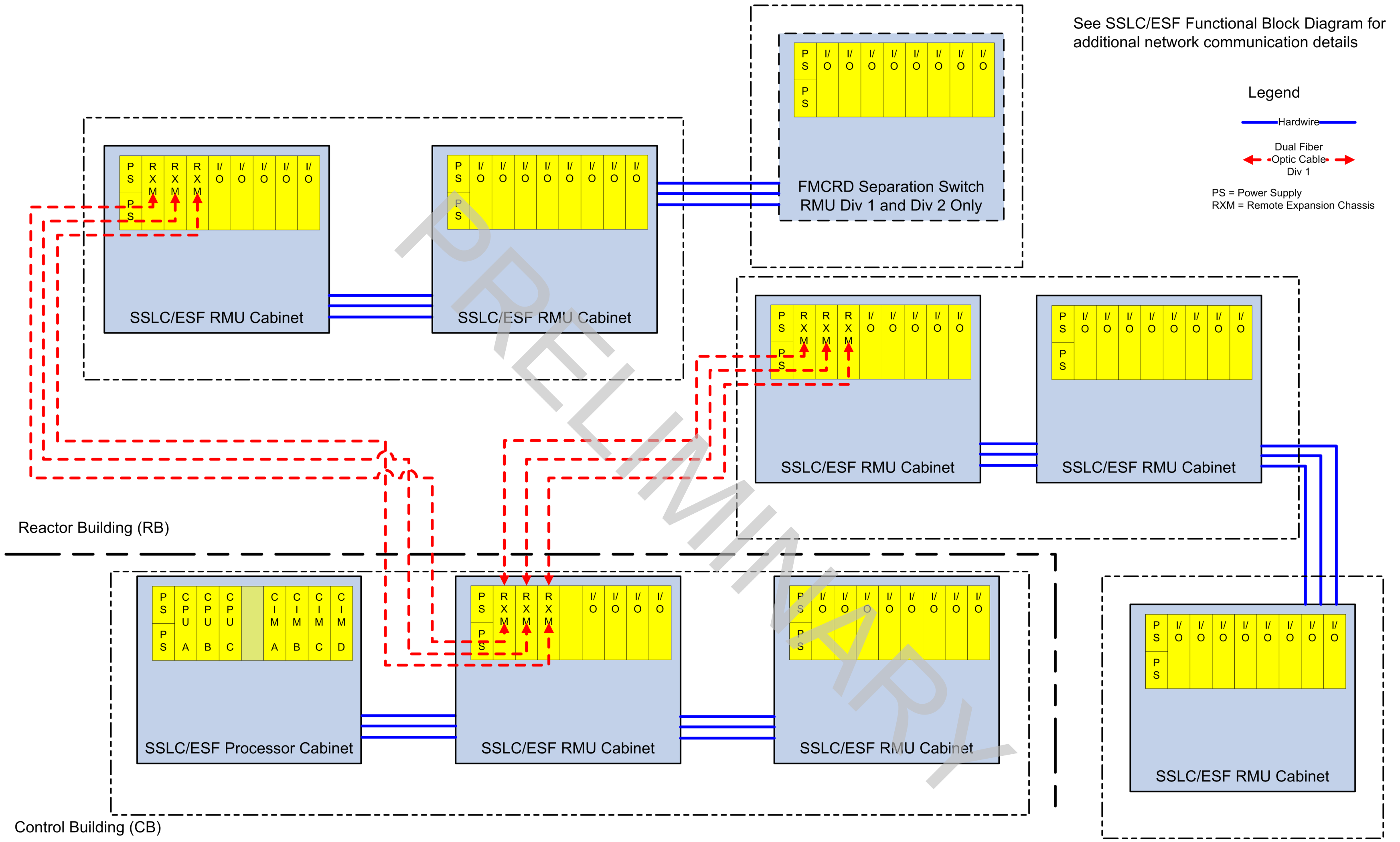


Figure 7.3-6. SSLC/ESF Division 1 Layout

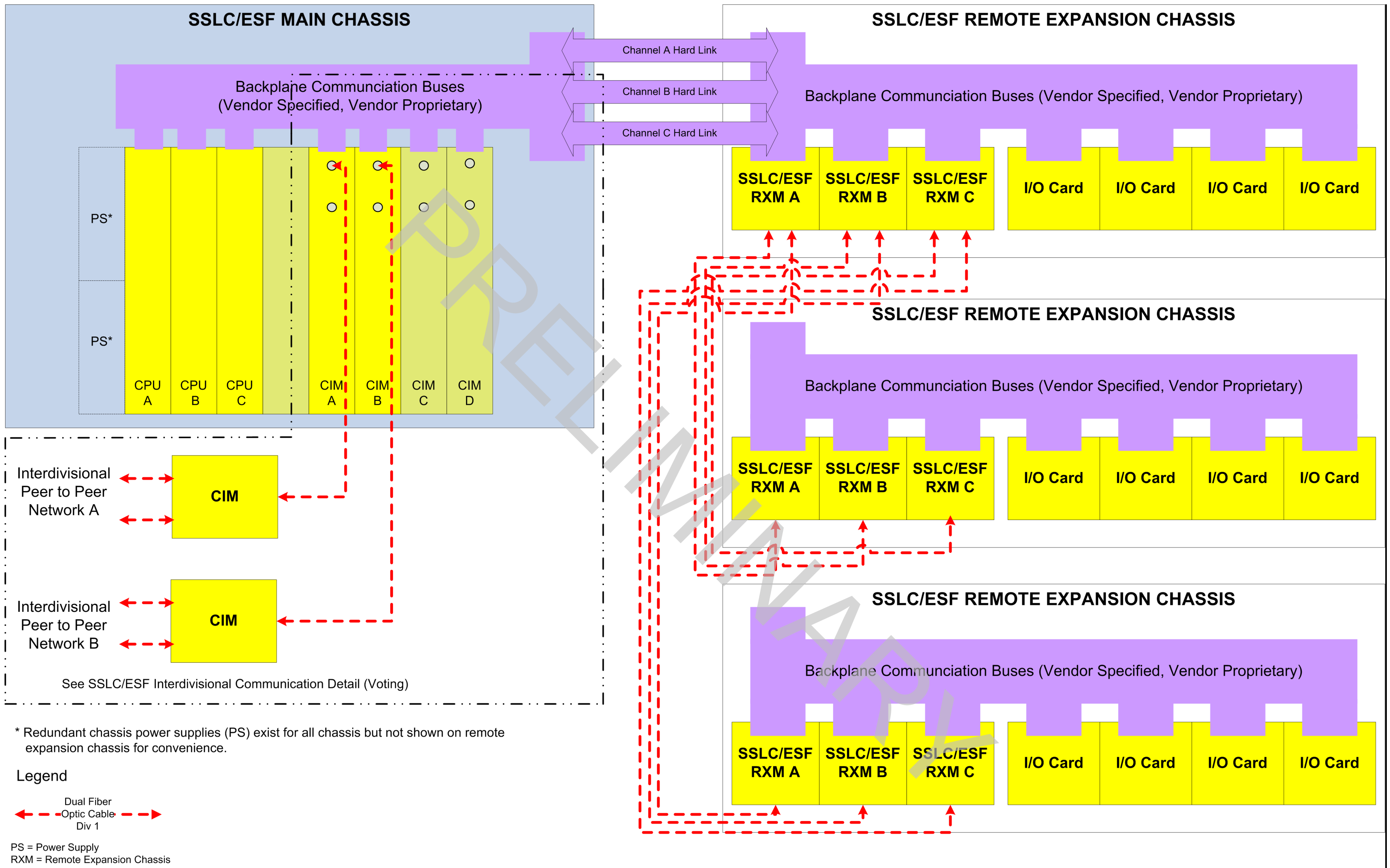


Figure 7.3-7. SSLC/ESF Functional Block Diagram

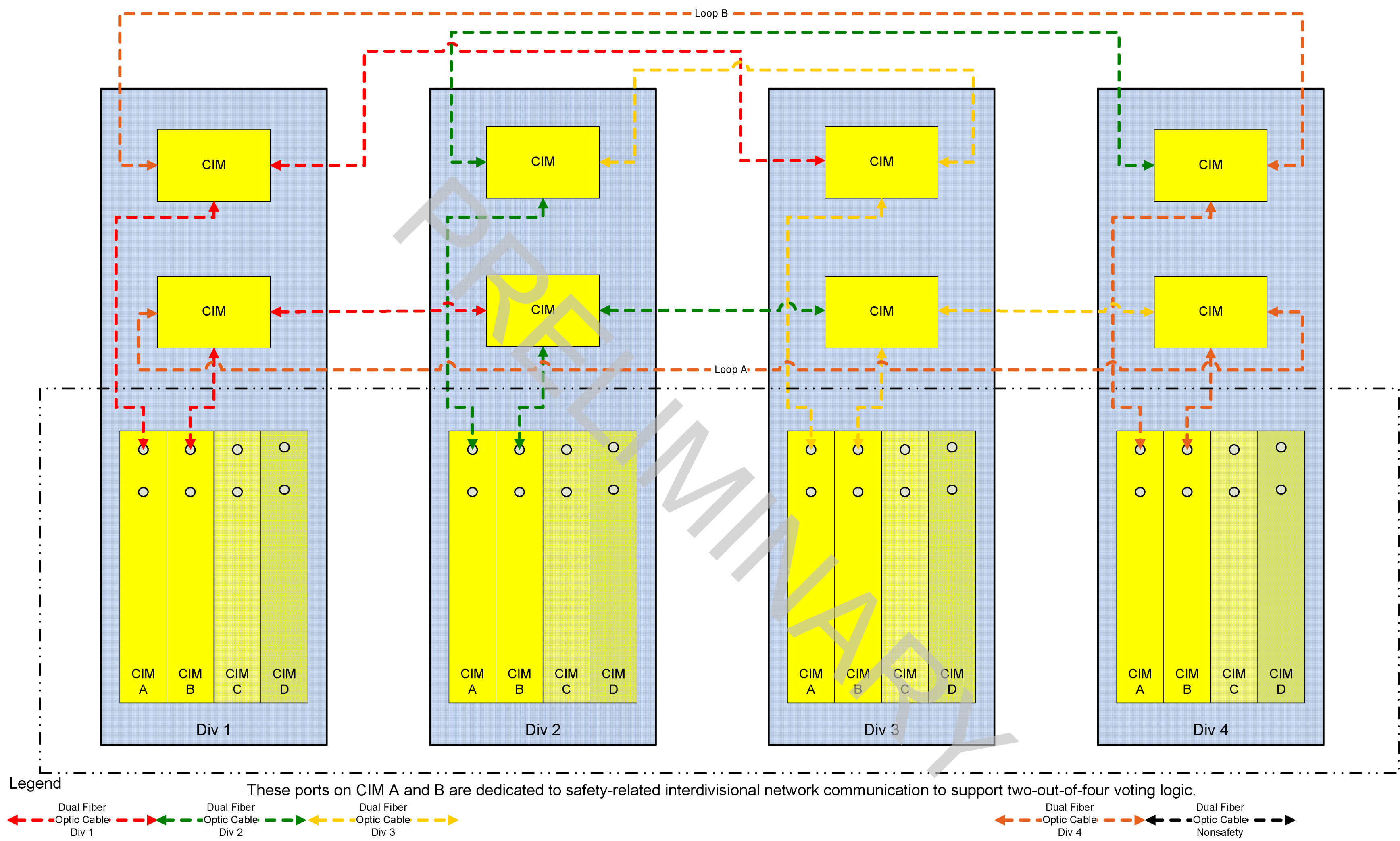


Figure 7.3-8. SSLC/ESF Interdivisional Communication Detail

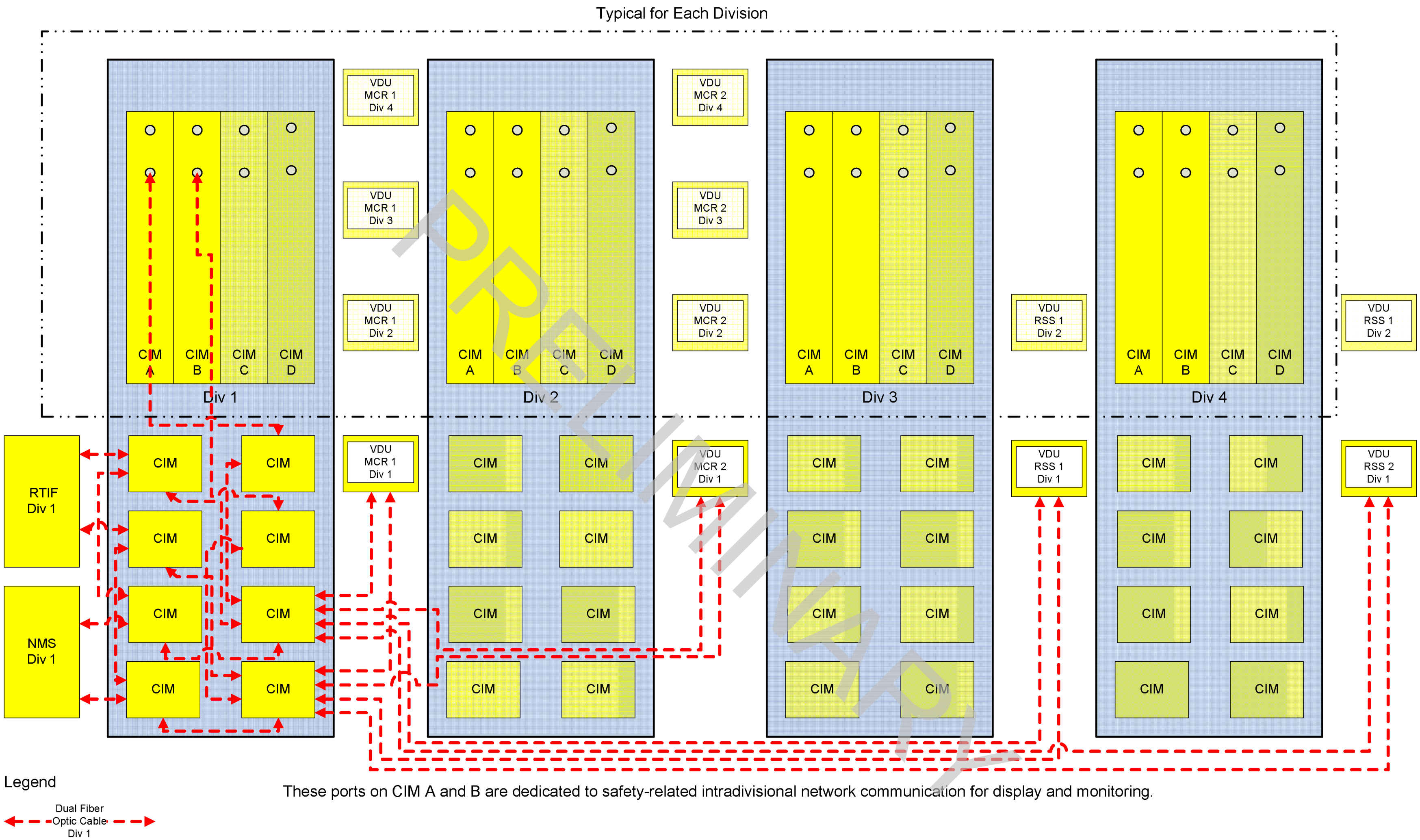


Figure 7.3-9. SSLC/ESF Safety-Related VDU Communication Detail

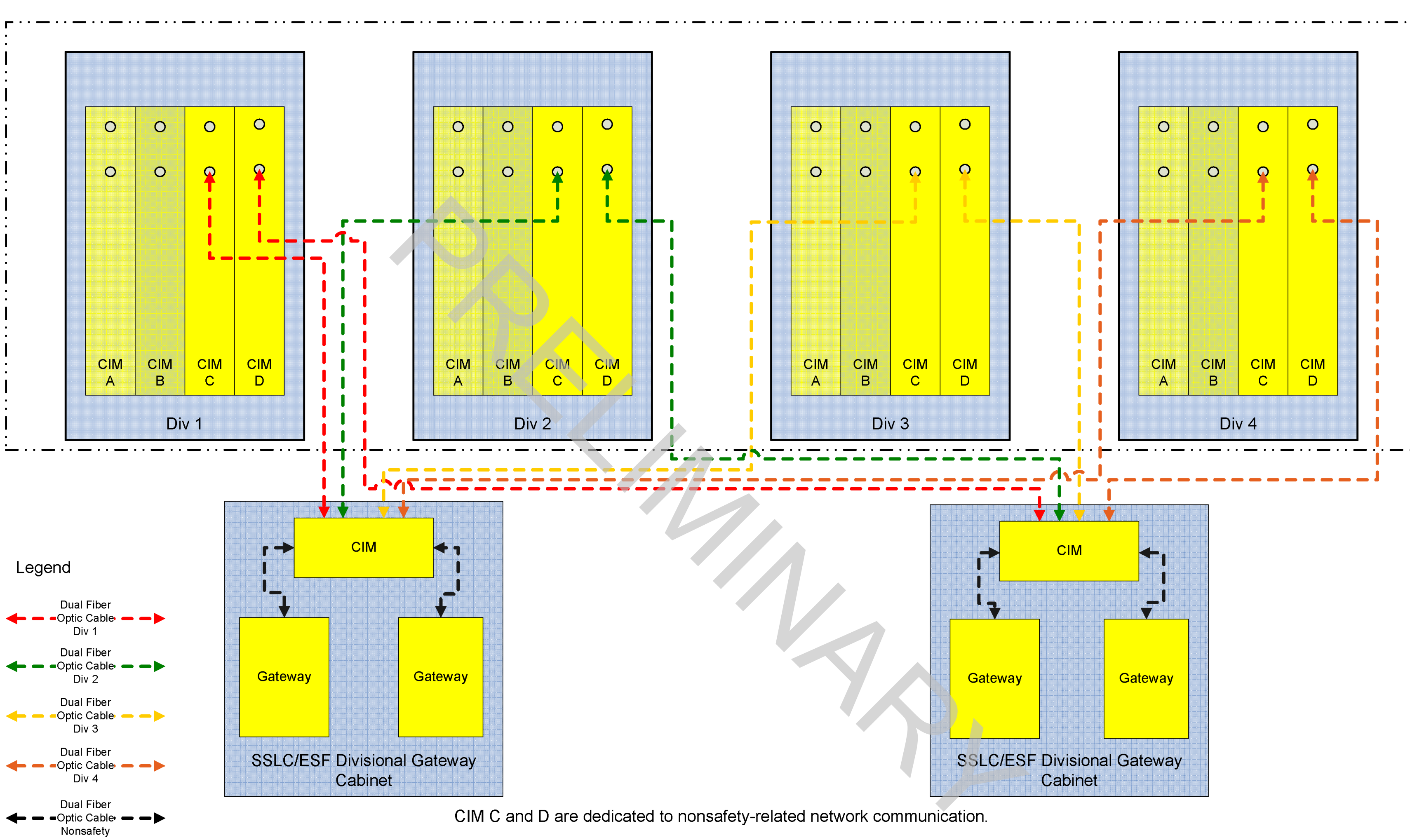


Figure 7.3-10. SSLC/ESF Nonsafety-Related Communication Detail

7.4 SAFETY-RELATED SAFE SHUTDOWN AND NONSAFETY-RELATED COLD SHUTDOWN SYSTEMS

In accordance with the Standard Review Plan, this section describes "...those instrumentation and control (I&C) systems used to achieve and maintain a safe shutdown condition of the plant." Some I&C systems perform cold shutdown functions and are not safety-related. This is justified by the existence of safety-related systems (Isolation Condenser System [ICS], Gravity-Driven Cooling System [GDCS], Standby Liquid Control [SLC] system, and Passive Containment Cooling System [PCCS]) that use natural circulation in the performance of their shutdown functions. Additionally, some safety-related criteria, such as provision of redundant trains and protection against single failures, are implemented in the design of the nonsafety-related systems. Consequently, safety-related and nonsafety-related systems performing safe shutdown or cold shutdown functions, respectively, are addressed in this section.

7.4.1 Standby Liquid Control System

7.4.1.1 System Design Bases

The SLC system design bases are presented within Subsection 9.3.5.

The I&C for the SLC support the passive system capability requirements to perform the following.

- Provide a diverse, backup means to shut down the reactor from full power to a subcritical condition, using soluble boron injection, and maintain the reactor subcritical while it is brought to a cold shutdown condition. SLC system logic provides manual initiation capability in the Main Control Room (MCR), to satisfy the diverse shutdown requirements, and is independent of normal reactivity control provisions.
- Provide system actuation upon receipt of manual and automatic initiation signals in response to either Anticipated Transients Without Scram (ATWS) events, or design basis events (DBE) requiring Emergency Core Cooling System (ECCS) operation.

Four divisions of safety-related sense and command logic implemented in the four Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) divisions (refer to Subsection 7.3.5) are used to support the ECCS function. The safety-related ATWS mitigation (ATWS/SLC) logic is utilized to perform the diverse emergency shutdown function and for automatic SLC initiation and for automatic SLC accumulator isolation. Redundant SLC accumulator level and pressure instrumentation is provided to monitor system performance and to ensure reliable logic processing. Valve position indication and continuity monitoring of the SLC squib injection valves are provided to ensure availability.

Safety-related SLC system components are designed for the environmental conditions applicable to their location. Safety-related SLC system components are also designed to preclude adverse interaction from nonsafety-related portions of the system.

The SLC design bases are discussed further within Subsection 9.3.5, and Figure 9.3-1 shows the basic configuration. Table 15.1-5, NSOA System Event Matrix, shows the events crediting the SLC system for mitigation.

The SLC system initiation functions are part of a group of systems collectively called the Safety-Related Distributed Control and Information System (Q-DCIS). A simplified network functional diagram of the DCIS is included as Figure 7.1-1. This diagram indicates the relationships of the SSLC/ESF and ATWS/SLC system with its safety-related peers, and with nonsafety-related plant data systems collectively called the Nonsafety-Related distributed Control and Information System (N-DCIS). Section 7.1 contains a description of these relationships.

7.4.1.2 System Description

A detailed system description is given in Subsection 9.3.5.2. The I&C of the SLC system are described below. The safety-related SLC system provides diverse backup capability for reactor shutdown, which is independent of the Reactor Protection System (RPS). For the reactor shutdown function, the SLC system is manually initiated from the MCR by using any two of four switches that will require at least two manual operator actions. Parameters such as neutron flux, reactor vessel pressure and level, and control rod position are available to the operator in the MCR to assess the need for manual SLC initiation. Additionally, accumulator pressure and solution level, as well as squib injection valve and shut-off valve status indication, are provided in the MCR to monitor the operating and performance status of the SLC system.

The SLC system is initiated automatically as part of the ECCS, to mitigate Loss-of-Coolant-Accident (LOCA) events. The SLC system receives an actuation command 50 seconds after a sustained RPV Level 1 signal for 10 seconds (as described in the Automatic Depressurization System [ADS] logic discussion in Subsection 7.3.1). The SLC system also receives a diverse ECCS initiation signal from the Diverse Protection System (DPS).

The SLC system also starts automatically on an ATWS mitigation signal persisting for 180 seconds. The ATWS mitigation (ATWS/SLC) logic performs the diverse emergency shutdown function (in compliance with the requirements of 10 CFR 50.62). ATWS/SLC logic is described in Section 7.8.1, Diverse I&C Systems, and is depicted on Figure 7.8-3, ATWS Mitigation Logic (SLC System Initiation, Feedwater Runback).

The ATWS/SLC logic uses hardware, and software platforms diverse from the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF), RPS, and DPS hardware/software platforms. ATWS/SLC sensors are not shared with the SSLC/ESF hardware/software platform and are diverse from the DPS hardware/software platform sensors.

To avoid reducing boron concentration during SLC operation, the SLC system logic transmits an isolation signal to the Reactor Water Clean-Up/Shutdown Cooling System (RWCU/SDC) via the Leak Detection and Isolation System (LD&IS).

To avoid the injection of nitrogen into the Reactor Pressure Vessel (RPV) System, four divisional, safety-related level sensors per SLC accumulator are used to provide automatic isolation of series injection shut-off valves on (a voted two-out-of-four) low accumulator level. The SLC system processors of the ATWS/SLC independent control platform perform the shut-off valve isolation logic.

Accumulator temperature, solution level, and accumulator pressure are indicated locally inside the accumulator room.

Boron injection and shut-off valve position status are provided in the MCR.

7.4.1.2.1 Power Sources

Power for the safety functions of the SLC system is derived from safety-related 120 VAC Uninterruptible Power Supplies (UPS) (see Subsection 8.3.1.1.3). Divisional assignments are made to ensure the availability of each SLC system loop, assuming one safety-related division of power is not in service in addition to a single active failure. Additionally, a squib initiator in each loop is activated by the DPS as part of the diversity and defense-in-depth strategy (described in Subsection 7.8.1.2). To avoid adverse interaction, electrical isolation is maintained between the safety-related divisions, and between the safety-related divisions and the DPS.

7.4.1.2.2 Control Functions

There are four control functions for the SLC system.

- The firing signals to the squib initiators originate from SSLC/ESF for the ECCS injection function, from ATWS/SLC for the ATWS mitigation function, and from DPS. The system can also be initiated by manual control switches in the MCR. Successful firing of either or both squib valves in each SLC system loop assures completion of the SLC system operation.
- An open signal is provided to the normally open injection shut-off valves to support the injection function. Control logic also is provided for automatic closure of the shut-off valves. Shut-off valve isolation occurs automatically on a two-out-of-four low-level logic, using the safety-related accumulator level instrumentation. Closure signals to the redundant, fail-as-is shut-off valves ensure that at least one valve closes, to prevent nitrogen entry into the RPV. To prevent interference with the safety-related SLC injection function, neither DPS nor SSLC/ESF can operate the injection shut-off valves, only ATWS/SLC controllers can terminate injection after its two-out-of-four low accumulator level signal is received.
- Control logic also is provided for manual venting of the accumulators. This function is not safety-related. Serial solenoid valves in each vent line may be actuated by respective manual switches in the MCR.
- Automatic nitrogen makeup to the accumulators is provided to accommodate slow long-term leakage from the system. This makeup function only is required to maintain accumulator pressure. It is not required to assure full solution injection and therefore, is not safety-related.

7.4.1.3 Safety Evaluation

The safety evaluation for the mechanical aspects of the SLC system is presented in Subsection 9.3.5.3). The SLC I&C are capable of performing their intended safety-related functions based on the following design features. The safety-related SLC I&C are designed to operate under the environmental conditions anticipated at their equipment locations. Inter-division communication (and communication with nonsafety-related interfaces) occurs through qualified isolation devices. Isolated ECCS initiation signals, as well as isolated ATWS mitigation signals from the DPS, are transmitted to the SLC squib injection valves to provide defense against a common mode software failure of the SSLC/ESF logic platform (discussed in Section 7.8).

Only the automatic actuation logic originating from within the SLC system logic processors transmits the low accumulator-level isolation signals for the injection shut-off valves, and the RWCU/SDC isolation signal via the LD&IS on SLC system injection. The SLC logic processors are separate components of the diverse ATWS/SLC independent control platform.

Redundant divisions of voting logic enable the SLC system to perform its safety-related function with one division removed from service coincident with a single failure. Division of sensors bypass capability allows a safety-related SLC sensor to be removed from service, while maintaining a high level of reliability. Alarmed indication of the bypass condition provides off-normal condition status monitoring. With an SLC accumulator-level sensor removed from service, the shut-off valve voting logic changes from two-out-of-four to two-out-of-three. Triplicate SSLC/ESF and ATWS/SLC signals are used to confirm the demand for squib injection valve operation. Three load drivers in series are provided to avoid spurious operation of the squib valves. Alarmed, disable/test switches are provided to allow removal of a squib valve initiator and associated control circuit from service, and to protect against spurious operation while performing maintenance. Continuity monitoring of the squib injection valve circuitry is provided to confirm availability automatically. Position indication for the SLC system valves also is provided to determine system configuration.

Manual SLC system initiation requires operation of two of four control switches, with each switch requiring two distinct operator actions.

In addition to squib injection valve continuity monitoring, status indication of squib injection and injection shut-off valves, accumulator level and pressure indication, and alarms are provided to allow monitoring of SLC accumulator standby status.

The SLC system also conforms to the applicable general requirements for safety-related systems presented in Chapter 3.

Table 7.1-1 identifies the SLC system and associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.4.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The SLC system design conforms to these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The SLC system design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the SLC system design conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsections 7.4.1.1 and 9.3.5.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are discussed in Subsection 9.3.5.2.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to SLC system design.

- Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in Subsection 7.1.6.6.1.3.
- Section 5.7 (Capability for Test and Calibration): Test and Calibrate features are discussed in Subsections 7.4.1.4 and 9.3.5.4.
- Section 6.2 and 7.2 (Manual Control): See Subsections 7.4.1.2.2, 7.4.1.3, 9.3.5.2 and 9.3.5.5.
- Section 6.4 (Derivation of System Inputs): The SLC system derives its sense and command features from direct measurements as described in Subsections 7.4.1.2, 7.4.1.5 and 9.3.5.5.
- Section 6.5 (Capability of Test and Calibration): Capability for Test and Calibrate features are discussed in Subsections 7.4.1.4 and 9.3.5.4.
- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the SLC system design beyond that discussed in Subsections 7.1.6.6.1.22 are not applicable.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the SLC system design beyond that discussed in Subsection 7.1.6.6.1.23 are not applicable.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the SLC system design are discussed in Subsections 7.4.1.2.1 and 9.3.5.2.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the SLC system design are discussed in Subsection 7.4.1.3.

* 10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:
* Conformance: The SLC design conforms to these requirements.
* 10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:
* Conformance: The SLC system design conforms to this requirement.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

* Conformance: The SLC conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

* Conformance: The SLC system design complies with this criterion. Reference Section 1.11 for resolution of unresolved and generic safety issues.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

* Conformance: ITAAC are provided for I&C Equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

* Conformance: There are no interface requirements for the SLC system.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the SLC system within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Function:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.4.1.3.2 General Design Criteria.

In accordance with Table 7.1-1, the following General Design Criteria (GDC) are addressed for the SLC system:

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, 35, and 37:

- Conformance: The SLC system design conforms to these GDC.

7.4.1.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The SLC system design conforms to these criteria by providing diverse I&C, as described in Section 7.8.

7.4.1.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: The SLC system design conforms to RG 1.22.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The SLC system design conforms to RG 1.47.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The SLC is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

  The SLC system design is a redundant backup to the reactor control and scram systems, and performs an ECCS function. The SLC system design has two redundant and parallel squib-type valves in each loop. Only one valve in each loop is required for the safety-related function of the SLC system. The SLC system instrumentation assuring operability of the system also is redundant.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The SLC system design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The SLC system design conforms to RG 1.105, as described in Reference 7.4-2.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: The SLC system design conforms to RG 1.151.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The SLC system design conforms to 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.168 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.168 as implemented on the independent control platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The SLC system design conforms to RG 1.169 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.169 as implemented on the independent control platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.170 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.170 as implemented on the independent control platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.171 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.171 as implemented on the independent control platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.172 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.172 as implemented on the independent control platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.173 as implemented on the SSLC/ESF platform. The SLC system design conforms to RG 1.173 as implemented on the independent control platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The SLC system design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The SLC system design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.4.1.3.5 Branch Technical Positions

BTP HICB-8, Guidance on Application of Regulatory Guide 1.22:

- Conformance: The SLC system design conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The SLC system design conforms to BTP HICB-11. SSLC/ESF logic controllers for the SLC use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Setpoints:

- Conformance: The SLC system design conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The SLC system design conforms to BTP HICB-14.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the SLC system conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The SLC system design conforms to BTP HICB-17.

BTP HICB-19, Guidance on Evaluation of Defense-in-Depth and Diversity in digital Computer-based Instrumentation and Control Systems:

- Conformance: The SLC system design conforms to BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The SLC system design conforms to BTP HICB-21.

7.4.1.4 Testing and Inspection Requirements

Testing and inspection requirements are described further in Subsection 9.3.5.4. An initial SLC system performance verification test is conducted as part of the startup test program. This test is intended to demonstrate that the SLC system performance is in accordance with design requirements.

A full test of this system is not possible during plant operation. Other than the two squib valves in each loop, there are no active components in this system, that are required to actuate for injection to occur. Only one squib valve actuation in each loop is required for injection to occur. If one of the valves in each loop actuates with the system in its normal operating configuration, and critical system parameters (accumulator level and pressure) are within their normal ranges, then injection would occur. Testing of the squib injection and injection shut-off valve logic is performed periodically to verify operability.

Routine testing, monitoring of critical system parameters, and surveillances ensure operability with low probability of demand failure.

7.4.1.5 Instrumentation and Control Requirements

Status indications of full-open or full-closed valve positions are provided for the key valves in the SLC system, such as the squib injection valves and the injection shut-off valves. An open indication for these valves is required to ensure SLC system operation.

Pressure-level and solution-level alarms and indications for each accumulator are provided in the MCR to:

- Ensure operability of the system;
- Warn the operator of an out-of-tolerance level or pressure condition; and
- Provide verification of proper system operation after initiation.

The measurements are redundant to minimize vulnerability to instrument or indicator failure. The level instrumentation for each accumulator is quadruple redundant to support the two-out-of-four initiation logic for closure of the shut-off valve. The pressure indications and alarms are dual redundant and the signals from both channels are needed before adding nitrogen to an accumulator. These instruments also provide local level and pressure indication.

Local indication and MCR alarms are provided for the nitrogen gas and neutron poison solution makeup. The low-level alarms are set to provide adequate time for recharging the manually operated nitrogen and sodium pentaborate solution supply systems.

7.4.2 Remote Shutdown System

7.4.2.1 System Design Bases

The safety-related Remote Shutdown System (RSS) is used to provide operators with the means to safely shut down the reactor from a place outside the MCR. The RSS provides remote control of the systems needed to bring and maintain the reactor to a hot shutdown after a scram. The RSS also provides the subsequent capability to achieve and maintain stable shutdown conditions as well as cold shutdown conditions.

7.4.2.2 System Description

7.4.2.2.1 General

The RSS consists of two redundant and independent panels located in the Division 1 and Division 2 quadrants of the Reactor Building. Division 1 and Division 2 and nonsafety-related parameters displayed and controlled on the MCR VDUs can also be displayed and controlled from either of the two RSS panels. Each panel contains:

- Division 1 Manual Scram Switch,
- Division 2 Manual Scram Switch,
- Division 1 Manual Main Steam Isolation Valve (MSIV) Isolation Switch,
- Division 2 Manual MSIV Isolation Switch,
- Division 1 Safety-related Video Display Unit (VDU),
- Division 2 Safety-related VDU,

- PIP A Nonsafety-related VDU,
- PIP B Nonsafety-related VDU, and
- Nonsafety-related Communications Equipment.

Data from the Q-DCIS and N-DCIS networks are available for display on the RSS panels. Because the VDUs on the RSS panels are connected to Q-DCIS or N-DCIS through the same networks serving corresponding VDUs at the MCR, Division 1 and 2 safety-related and nonsafety-related display/control functions at the Q-DCIS and N-DCIS MCR VDUs also are available at the RSS panels. A simplified RSS panel schematic is provided in Figure 7.4-1. A simplified network functional diagram of the Q-DCIS and N-DCIS is included as Figure 7.1-1. This diagram indicates the relationships of safety-related and nonsafety-related systems with their peers, and with plant data acquisition systems. Section 7.1 contains a description of these relationships. The software for the RSS safety-related VDUs is developed as part of the SSLC/ESF platform hardware/software development process. The software for the RSS nonsafety-related VDUs is developed as part of the nonsafety-related network segment hardware/software development processes.

The two RSS panels are located in different rooms inside the Reactor Building (RB). Each RSS Panel room has a sliding fire door with a minimum fire rating of three hours. The RSS panel room environment typically is similar to the MCR environment. Access to and use of the RSS panels is administratively controlled. This satisfies the control access requirement of IEEE Std. 603, Section 5.9.

The RSS provides sufficient redundancy in its control and monitoring capability, to accommodate a single failure in the interfacing systems, a single failure in the RSS controls and the event that caused the MCR evacuation. The RSS is designed such that any failure within it does not degrade the capability of interfacing safety-related systems. The RSS satisfies the single-failure criterion and independence requirements of IEEE Std. 603, Sections 5.1, 5.6, and 6.3.

7.4.2.2.2 Operating Conditions

The following conditions are assumed coincident with the event necessitating evacuation of the MCR and transfer of operation to the RSS panel.

- The plant is operating under normal conditions and at less than or equal to rated power. No Anticipated Operational Occurrence (AOO), seismic event, or other abnormal plant condition except for loss of off-site power is assumed.
- The RSS panel is powered from buses supplied by uninterruptible safety-related and nonsafety-related 120 VAC systems.
- The reactor operator can either manually scram the reactor before leaving the MCR, or use the manual scram switches on the RSS panel.
- Plant personnel have evacuated the MCR.
- The reactor operator can isolate the main steam lines by closing the manual Main Steam Isolation Valve (MSIV) isolation switches from the RSS.

- The reactor feedwater system, which is normally available, is conservatively assumed to be inoperable.
- The initiating event is assumed not to cause failure of the Alternating Current (AC) control power supplies to the RSS panel, or failure of the power feeds to equipment functionally controlled from the RSS panel. This assumption is justified because the power feeds to the RSS do not pass through the MCR.

7.4.2.2.3 System Operation

When evacuation of the MCR is necessary, the reactor is manually scrammed. If there has been no loss of off-site power, the turbine bypass valves automatically control reactor pressure, and the reactor feedwater system automatically maintains RPV water level. These functions will remain operable because the safety-related and nonsafety-related controllers are not located in the same fire area as the MCR nor are they affected by adverse impacts on the MCR VDUs and switches after an MCR evacuation; as a result, reactor cooldown is achieved through the normal heat sinks. This cooldown process can be supplemented from the RSS panel using the RWCU/SDC system. The RWCU/SDC system provides the capability to bring the reactor from a high-pressure condition to cold shutdown. Control of both RWCU/SDC trains is provided on the RSS panel. The Reactor Component Cooling Water System (RCCWS) is aligned to provide cooling water to the RWCU/SDC non-regenerative heat exchangers, and the Plant Service Water System (PSWS) is aligned to cool the RCCW heat exchangers. Control of two RCCW trains and two PSWS trains is provided on the RSS panel.

However, if the reactor feedwater system is not available due to loss of off-site power, as postulated in the first bullet of Subsection 7.4.2.2.2 Operating Conditions, control of the Control Rod Drive (CRD) system from the RSS may be utilized. Control of the high-pressure makeup injection capability of the CRD system ensures that the RPV water level remains above the ADS trip setpoint and above the elevation of the RWCU/SDC mid-vessel suction line nozzle. If main steam line isolation automatically occurs, or is manually initiated from the RSS, the ICS automatically controls reactor pressure. Because the logic processing equipment for the ICS (or any other safety or nonsafety-related system) is outside the MCR, ICS operation is not affected by an event necessitating MCR evacuation, and continued operation of the isolation condensers is assured. If the event necessitating MCR evacuation results in a loss of the reactor pressure regulator, but does not cause main steam line isolation, the ICS initiates on high pressure. With the ICS in operation, the isolation condensers provide initial decay heat removal, and further reactor cooldown is achieved from the RSS panels using the RWCU/SDC.

7.4.2.3 Safety Evaluation

The RSS is classified as a safety-related system that can control safety-related systems or equipment.

The RSS provides instrumentation and controls (I&C) outside the MCR to allow prompt hot shutdown of the reactor after a scram and to maintain safe conditions during hot shutdown. It also provides capability for achieving stable shutdown conditions as well as subsequently achieving cold shutdown of the reactor through the use of suitable operating procedures.

Table 7.1-1 identifies the RSS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.4.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The RSS design conforms to these requirements.

10 CFR 50.55a(h), Protection and Safety Systems Compliance with IEEE Std. 603:

- Conformance: The RSS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the RSS design conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-Related Function): See Subsections 7.4.2.1 and 7.4.2.2.2.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the RSS design.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to RSS design.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions is not applicable beyond that discussed in section 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 7.4.2.4.
  - Section 6.2 and 7.2 (Manual Control): See Subsections 7.2.1.5.5 & 7.4.2.2.3.
  - Section 6.4 (Derivation of System Inputs): Derivation of System Inputs is not applicable for the RSS.
  - Section 6.5 (Capability of Test and Calibration): Testing sense and command sensors is not applicable to RSS.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the RSS are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the RSS are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the RSS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the RSS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The RSS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The RSS design conforms to these requirements by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The RSS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC for the RSS are identified in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for RSS.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the RSS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.4.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, and 29:

- Conformance: The RSS design conforms to these GDC.

7.4.2.3.3 Staff Requirements Memorandum

SRM on SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability:

- Conformance: The AMS meets the requirements of SECY-93-087, Item II.T for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:
  - Alarm points are sent via dual networks to redundant message processors using dual power supplies. The processors are dedicated to alarm processing.
  - The alarms are displayed on multiple independent Video Display Units (VDUs) (dual power supplies on each).
  - The alarms are driven by redundant datalinks to the AMS (dual power). There are redundant alarm processors.
  - There is one horn and one voice speaker. Test buttons are available to test the horn and all the lights.
  - There are no alarms requiring manually controlled actions for safety systems to accomplish their safety-related functions.

7.4.2.3.4 Regulatory Guides

RG 1.22, (Safety Guide 22) Periodic Testing of Protection System Actuation Function:

- Conformance: The RSS design conforms to RG 1.22.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The RSS system design conforms to RG 1.47.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The RSS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

In addition, separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603, Sections 5.6 and 6.3, and RG 1.75.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The RSS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The RSS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The RSS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.153, Power Instrumentation & Control Portions of Safety Systems:

- Conformance: The RSS design conforms to 10 CFR 50.55a(h).

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems:

- Conformance: The RSS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The RSS design conforms to RG 1.204.

RG 1.209, Guidelines For Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The RSS Safety-Related system design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.4.2.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The RSS design complies with BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The RSS design conforms to BTP HICB-11. Logic controllers for the RSS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The RSS design conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The RSS design conforms to BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR, Part 52:

- Conformance: The level of detail provided for RSS conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The RSS design conforms to BTP HICB-17.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The RSS design conforms to BTP HICB-21.

7.4.2.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.4 and with Table 7.1-1, there are no Three Mile Island (TMI) action plan requirements applicable for the RSS. TMI action plan requirements are generically addressed in Table 1A-1 of Appendix 1A.

From the foregoing analyses, it is concluded that the RSS meets its design bases.

7.4.2.4 Testing and Inspection Requirements

The capability to safely shut down the reactor from outside the MCR is confirmed during the Initial Plant Test Program (Refer to Section 14.2). Testing to confirm the functionality of each RSS control circuit is performed during each refueling outage.

Minimum Requirements to Place and Maintain Plant in MODE 3 from Location Outside MCR

On the basis of Sections 15.5.6.2 and 15.5.6.3 which provide the assumptions and results of safe shutdown fire analysis, only a manual scram of the plant from the MCR is required to reach and maintain Mode 3 (hot shutdown). If the operator is not able to initiate manual scram from the MCR due to spread of the fire, manual scram can be initiated from either of the RSS panels. Therefore, the operability of Division 1& 2 Manual Scram Switches at either of the two RSS panels is the minimum requirement to achieve and maintain Mode 3 from a location outside MCR.

7.4.2.5 Instrumentation and Control Requirements

The Division 1 and Division 2 parameters and nonsafety-related parameters displayed and controlled on the MCR VDUs can also be displayed and controlled from either of the RSS panels.

7.4.3 Reactor Water Cleanup/Shutdown Cooling System

7.4.3.1 System Design Bases

The RWCU/SDC system design bases are described further in Subsections 5.4.8.1 and 5.4.8.2. Figure 5.1-4 shows the basic configuration of the RWCU/SDC system.

The RWCU/SDC system is one of the dual redundant Plant Investment Protection (PIP) systems whose instrumentation belongs to the N-DCIS. The RWCU/SDC system functions are not safety-related. Accordingly, the RWCU/SDC system has no safety-related design bases beyond a containment isolation function and providing instrumentation for detection of system breaks outside the containment. The containment is isolated by signals from the LD&IS (as described in Subsection 7.3.3).

7.4.3.1.1 (Deleted)

7.4.3.1.2 (Deleted)

7.4.3.1.3 (Deleted)

7.4.3.2 System Description

7.4.3.2.1 Summary Description

The overall functional description of the RWCU/SDC system is provided in Subsection 5.4.8.

The I&C maintains the RWCU/SDC system process conditions within the limits necessary to control the system and satisfy its design bases. Protective features include isolating the RWCU/SDC system from the RPV in response to an LD&IS signal. The above isolation features protect the reactor core by minimizing the potential loss of RPV coolant inventory and avoid removal of boron from the reactor coolant if the SLC system is actuated.

7.4.3.2.2 Detailed System Description

The RWCU/SDC system measurements of flow, pressure, temperature, and conductivity are recorded, indicated, and alarmed in the MCR. Valves behind shielding are furnished with on-off air operators that are individually controlled from local panels or from extension stems penetrating the shielding.

Indicating and control instruments and components are mounted on panels or local racks and are visible and accessible for repair, calibration, and testing.

The main process pumps are started automatically or from the MCR by VDU control with status indication. The pumps are driven by solid-state adjustable speed drives. Temperature elements located in the Nuclear Boiler System (NBS) and a reactor cooldown controller with temperature feedback control each pump to limit the rate of reactor water cooldown. A low pump suction flow interlock either prevents the pumps from starting or runs back or stops the pumps automatically. A reactor low water level (Level 3) pump speed runback interlock is provided to protect the pumps from cavitation during shutdown.

The pumps typically are supplied from separate and preferred power sources. The power supplies are automatically switched to dual on-site standby diesel-generators following the loss of preferred power (LOPP).

Motor-operated valves are operable automatically or manually by a VDU switch from the MCR. Each valve motor is stopped by limit switches or torque switches. The positions of air/nitrogen-operated containment isolation valves are indicated in the MCR to permit the plant operators to assess their status. An automatic signal overrides a manual signal to these valves. Containment isolation valve closing speeds are selected to protect the reactor core and limit radioactivity release in case of a RWCU/SDC system pipe break outside the containment.

The signals that either prevent all containment isolation valves from opening (if closed) or close the valves (if open) are:

- SLC system actuation is sent to the RWCU/SDC system via the LD&IS, and
- LD&IS actuation occurs.

The isolation signal from the LD&IS to the reactor bottom suction sampling line containment isolation valves can be overridden by a manual opening signal when a reactor bottom fluid sample is required for post-accident sampling purposes.

The plant LD&IS, including the portion related to the RWCU/SDC system, is further described in Subsection 7.3.3.

A flow control valve from the upper RPV nozzle controlling flow from the upper RPV region is located on the RWCU/SDC system suction line. The flow is set manually using a flow controller located in the MCR. Using thermocouples on the RPV bottom head drain line and the system suction line, the control valve from the RPV upper region can be throttled during reactor startup and shutdown modes to maintain the required temperature difference across the vessel. The valve actuator is air-operated.

The RWCU/SDC system also has a dump, or "overboarding," control valve to maintain RPV water level during reactor startup. This excess water typically is overboarded to the main condenser (Subsection 5.4.8). The valve is operated using instrument air and controlled both manually and automatically from the MCR using a controller and flow indicator. Pressure switches or transmitters located downstream of the overboarding control valve protect low-pressure components by alarming in the MCR on high pressure and by closing the control valve with a high-high pressure signal. When the overboarding valve is used during reactor high-pressure conditions, a downstream orifice is used to assist in reducing system pressure; otherwise the orifice is bypassed using a motor-operated valve. The overboarding control valve fails closed upon loss of power or air pressure.

The demineralizer bypass piping has an air-operated modulating flow control valve that bypasses the excess flow above the demineralizer capacity. The demineralizer is protected from over-temperature by automatic controls that first open the demineralizer bypass valve and then close the demineralizer inlet valve.

Conductivity cells are located in the influent and effluent process sample streams of the demineralizers. These detectors are located in sample systems, which cool the sample stream to a constant temperature, eliminating the need for temperature compensation. Influent and effluent conductivity are continuously measured and transmitted to MCR recorders. Measured values in excess of water quality requirements are alarmed in the MCR.

The reactor coolant is sampled manually during cooldown, flood-up, or early periods of fuel off-loading when spiking of soluble and insoluble radioisotopic concentrations of corrosion products may occur.

Temperature elements are provided in the RPV bottom drain, the regenerative heat exchanger supply inlet and outlet, the non-regenerative heat exchanger outlet, the demineralizer influent (located at the pump suction), and the inlet and outlet of the regenerative heat exchanger return.

Temperature elements located in the NBS and a reactor cooldown controller with temperature feedback are used to provide the necessary signals to control pump speed during cooldown to maintain the required cooldown rate.

Density compensated system mass flow is measured in the process lines (by mid-vessel nozzles with venturi-type flow elements in each line) from the reactor bottom, located inside the containment. Flow elements also are provided in the Seismic Category I RWCU/SDC return lines to the feedwater lines and in the overboarding lines. The flow transmitters for all of these flow elements are arranged in a two-out-of-four logic configuration used to detect high RWCU/SDC differential mass flow due to a break outside the containment and to close the inboard and outboard containment isolation valves of the affected RWCU/SDC train. The containment isolation function on detection of RWCU/SDC high differential mass flow (due to a break outside the containment) is part of the LD&IS described in Subsection 7.3.3. See Figures 7.4-2a through 7.4-2e for the logic for detection of a RWCU/SDC pipe break outside containment.

Flow orifices are used for flow monitoring of demineralizer inlet flow and to open the demineralizer bypass control valve if the flow exceeds the demineralizer capacity.

7.4.3.3 Safety Evaluation

The RWCU/SDC system functions are nonsafety-related, with the exception of containment isolation functions and providing instruments to detect high differential mass flow following a RWCU/SDC break outside the containment. Refer to Subsection 6.2.4 for the containment isolation functions, and Subsection 7.3.3 for the containment isolation and leak detection functions performed by the LD&IS.

Table 7.1-1 identifies the RWCU/SDC system and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.4.3.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The RWCU/SDC system design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The RWCU/SDC design conforms to these requirements.

10 CFR 50.55a(h), Protection and Safety System Compliance with IEEE 603:

- Conformance: The safety-related requirements are addressed in Subsection 7.3.3, LD&IS.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The RWCU/SDC conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The RWCU/SDC conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues for I&C is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for the RWCU/SDC system.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the RWCU/SDC within the DCD documents conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The RWCU/SDC design does not use innovative means for accomplishing safety functions.

7.4.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, 33, and 38:

- Conformance: The RWCU/SDC system is nonsafety-related, but is designed to conform to these GDC.

7.4.3.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.97, which endorses IEEE 497.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: RG 1.151 is applicable to safety-related sensing lines. However, sections of endorsed standard ANSI/ISA-S67.02.01 on design practices for tubing, vents, and drains also apply to nonsafety-related instrumentation.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The RWCU/SDC system design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The safety-related requirements are addressed in Subsection 7.3.3, LD&IS.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The RWCU/SDC design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems:

- Conformance: The RWCU/SDC system design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The RWCU/SDC system design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.4.3.3.4 Branch Technical Positions

BTP HICB-1, Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System:

- Conformance: The RWCU/SDC design conforms to BTP HICB-1.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the RWCU/SDC system design conforms to BTP HICB-16.

7.4.3.4 Testing and Inspection Requirements

The RWCU/SDC system instruments are calibrated and tested during the preoperational testing program to confirm the instrumentation is correctly installed and functions as designed. In addition, calibration and surveillance testing of the containment isolation devices is performed at regular intervals. To the maximum extent possible, instrumentation requiring regular calibration, testing, and maintenance is mounted on accessible panels or racks located outside high radiation areas.

7.4.3.5 Instrumentation and Control Requirements

Operation of the RWCU/SDC system is from the MCR. The main I&C available to the MCR operator includes:

- Manual and automatic flow controllers for system, demineralizer, and overboarding flow;
- Flow indications for system, demineralizer, and overboarding flow;
- Position indications for containment isolation valves, flow control valves, and motor-operated valves;
- Temperature indication for demineralizer influent water;
- Conductivity recorders for demineralizer influent and effluent;
- Temperature of the system supply water (from the RPV bottom head);
- Temperature of the system return (to feedwater line) water;
- Temperatures of the non-regenerative and regenerative heat exchanger water (reactor coolant sides);
- Process alarms (for example, high water temperatures, high overboarding line pressure, low system flow, high system flow, high conductivity, etc.); and
- Pressure indication for the overboarding line.

7.4.4 Isolation Condenser System

7.4.4.1 System Design Bases

Refer to Subsection 5.4.6.1 for the design bases of the ICS. Figure 5.1-3 shows the basic configuration of the ICS.

The ICS is one of the ESF systems whose I&C implemented in SSLC/ESF, belong to a group of systems collectively called the Q-DCIS. A simplified network functional diagram of the DCIS is included as Figure 7.1-1. This diagram indicates the relationships of the SSLC/ESF with its safety-related peers, and with nonsafety-related plant data systems collectively called the N-DCIS. Section 7.1 contains a description of these relationships.

7.4.4.2 System Description

Refer to Subsection 5.4.6.2 for the ICS system description.

7.4.4.3 Safety Evaluation

Conformance of ICS equipment to the requirements of IEEE Std. 603 (other than I&C) is addressed in Subsections 5.4.6.2 and 5.4.6.3. The paragraph on "Isolation Condenser Operation" in subsection 5.4.6.2 addresses the requirements of IEEE Std. 603, Section 4.10. Subsection 5.4.6.3 addresses the requirements of IEEE Std. 603, Section 4.8. Conformance of ICS I&C equipment to the requirements of IEEE Std. 603, Sections 5.1 and 8.1, is addressed in this subsection. The ICS is designed to operate from safety-related power sources. The system instrumentation is powered by four divisionally separated sources of safety-related power. The ICS uses two-out-of-four logic from SSLC/ESF (refer to Subsection 7.3.5) for automatic operation or isolation of each of the four separate isolation condenser trains as shown in Figure 7.4-3. The actuating logic and actuator power for the inner isolation valves for the four ICS trains are on two safety-related 120 VAC divisional UPS (Refer to Subsection 8.3.1.1.3) different from the two divisional power sources for the outer isolation valves.

Interdivisional fiber optic isolators are used to separate the four sensor inputs to the single divisional actuation logic circuits. An ICS train requires power from at least one of three safety-related divisional power sources to automatically start. Each of the four ICS trains has three of the four safety-related power sources. Consequently, the loss of two of the four safety-related power supplies does not result in the loss of any one ICS train. However, second and third sources of safety-related power are provided to operate the ICS automatic venting system during long-term ICS operation; otherwise the manually controlled backup venting system, which uses one of the divisional power sources starting the ICS, can be used for long-term operation.

If the three safety-related power supplies used to start an individual ICS train fail, then the ICS would automatically start, because of the "fail open" actuation of the condensate return bypass valves upon loss of electrical power to the solenoids controlling its nitrogen-actuated valves.

The ICS is initiated automatically as part of the ECCS to provide additional liquid inventory to mitigate LOCA events. The signals that initiate ICS operation are:

- High reactor pressure,
- Low reactor water level (Level 2) with time delay,
- Low reactor water level (Level 1),
- Loss of power generation buses (loss of feedwater flow) in reactor run mode,
- MSIV position indication (indicating closure) whenever the Reactor Mode Switch is in the Run position, and
- Operator manual initiation.

The operator is able to stop any individual ICS train whenever the RPV pressure is below a reset value overriding the ICS automatic actuation signal following MSIV closure.

The IC/PCCS pool has four safety-related level sensors in each IC/PCCS inner expansion pool. These level sensors are part of the Fuel and Auxiliary Pool Cooling System (FAPCS). Each IC/PCCS pool is connected to the equipment storage pool by two cross-connect valves in parallel where one valve is a pneumatic operated valve with an accumulator (actuation similar to Figure 7.4-3) and the other is a squib valve (actuation similar to Figure 7.3-2). These valves open when a low water level condition is detected in either of the IC/PCCS inner expansion pools to provide makeup water for the first 72 hours of design basis events. The residual heat removal function of the safety-related ICS is further backed up by the safety-related ESF combination of ADS, PCCS, and GDCS; by the nonsafety-related RWCU/SDC loops; or by the make-up function of the CRD system operating in conjunction with safety relief valves and the suppression pool cooling systems.

The DPS discussed in Section 7.8 provides diverse nonsafety-related signals for ICS initiation and opening of pool cross-connect valves between the equipment storage pool and the IC/PCCS expansion pools.

Table 7.1-1 identifies the ICS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.4.4.3.1 Code of Federal Regulations

10 CFR 50.55a(h), Protection and Safety Systems Compliance with IEEE Std. 603:

- Conformance: The ICS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the ICS conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 5.4.6.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are discussed in Subsections 5.4.6.2.3 and 7.4.4.3.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to ICS.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in Subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): Test and Calibrate features are discussed in Subsection 5.4.6.4.
  - Section 6.2 and 7.2 (Manual Control): See Subsections 5.4.6.2.2 and 5.4.6.2.3.
  - Section 6.4 (Derivation of System Inputs): The ICS derives its sense and command features from direct measurements as described in Subsections 5.4.6.5, 7.4.4.3 and 7.8.
  - Section 6.5 (Capability of Test and Calibration): Capability for Test and Calibrate features beyond that discussed in are discussed in Subsection 5.4.6.4.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the ICS beyond that discussed in Subsections 7.1.6.6.1.22 are not applicable.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the ICS beyond that discussed in Subsection 7.1.6.6.1.23 are not applicable.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the ICS beyond that discussed in Subsection 7.1.6.6.1.26 are not applicable.

- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the ICS beyond that discussed in Subsection 7.1.6.6.1.27 are not applicable.

10 CFR 50.34(f)(1)(v)[II.K.3.13], HPCI and RCIC Initiation Levels,

- Conformance: The ICS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design,

- Conformance: The ICS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The ICS design conforms to this requirement because it is an ECCS.

10 CFR 50.34(f)(2)(xxi)[II.K.1.22], Auxiliary Heat Removal Systems:

- Conformance: The ICS conforms to these requirements.

10 CFR 50.34(f)(2)(xxiii)[II.K.2.10], Anticipatory Reactor Trip:

- Conformance: The ICS will initiate in response to a Loss of All Feedwater Flow Event. This is an anticipatory trip actuated on a power generation buss loss event.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The ICS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:

- Conformance: The ICS conforms to these requirements.

10 CFR 50.63, Loss of All Alternating Current Power:

- Conformance: The ICS conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for ICS.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the ICS within the DCD conforms to this BTP.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.4.4.3.2 General Design Criteria

In accordance with the SRP for Section 7.4 and Table 7.1-1, the following GDC are addressed for the ICS:

GDC 1, 2, 4, 13, 19 , 20, 21, 22, 23, 24, 29, 33, 34, 35, 37, and 44:

- Conformance: The ICS design conforms to these GDC.

7.4.4.3.3 Staff Requirements Memorandum

SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The ICS design conforms to these criteria by providing diverse I&C, as described in Section 7.8.

7.4.4.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: The ICS system design conforms to RG 1.22.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The ICS design conforms to RG 1.47.

RG 1.53, Application of the Single-Failure to Nuclear Power Protection Systems:

- Conformance: The ICS is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The ICS design conforms to RG 1.62.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The ICS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints used to initiate ICS automatic operation or isolation are established consistent with this guide. Reference 7.4-2 provides a detailed description of the GEH methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.151 - Instrument Sensing Lines:

- Conformance: The ICS design conforms with RG 1.151.

RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.152 as implemented on the SSLC/ESF platform.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The ICS design conforms to 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems:

- Conformance: The ICS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The ICS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.4.4.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The ICS design conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The ICS design conforms to BTP HICB-11. SSLC/ESF logic controllers for ICS use safety-related fiber optic communication interface modules and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The ICS logic resides within the SSLC/ESF so that the design conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based I&C Systems:

- Conformance: The ICS design conforms to BTP HICB-14 as implemented on the SSLC/ESF platform.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided in the ICS description conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The ICS design conforms to BTP HICB-17.

BTP HICB-19, Guidance on Evaluation of Defense-in-Depth and Diversity in digital Computer-based Instrumentation and Control Systems:

- Conformance: The ICS design conforms to BTP HICB 19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The ICS design conforms to BTP HICB-21.

7.4.4.4 Testing and Inspection Requirements

Refer to Subsection 5.4.6.4.

7.4.4.5 Instrumentation and Control Requirements

Refer to Subsection 5.4.6.5.

The ICS indications reported in the MCR are:

- Radiation level in each IC pool compartment airspace,
- Mass flow rate in condensate return line,
- Mass flow rate in steam supply line,
- Temperatures of steam and condensate return lines,
- Temperatures of IC top and bottom vent lines, and
- Valve positions.

The following manual controls are provided by the ICS to:

- Open/close condensate return valves,
- Close condensate return isolation valves,
- Close steam supply isolation valves,
- Open/close all bottom vent valves,
- Open/close all top vent valves, and
- Open/close purge line valve.

7.4.5 High Pressure Control Rod Drive (HP CRD) Isolation Bypass Function

The Control Rod Drive Hydraulic Subsystem supplies high pressure makeup water to the reactor vessel in response to a low RPV water level (Level 2) condition, or in the event GDCS fails to inject following a LOCA. The CRD system is discussed in Subsection 4.6.1. The Control Rod Drive Hydraulic Subsystem is discussed in Subsection 4.6.1.2.4 and depicted on Figure 4.6-8. This subsection discusses the HP CRD isolation bypass function that mitigates the beyond design basis failure of the GDCS to inject following a LOCA. The Control Rod Drive Hydraulic Subsystem is normally isolated following a LOCA. LD&IS logic for the HP CRD isolation under LOCA conditions is discussed in Subsection 7.3.3.

Upon detection of a LOCA and detection of a subsequent failure of the GDCS to inject, the HP CRD isolation bypass logic opens redundant motor-operated isolation bypass valves installed in parallel with the air operated HP CRD isolation valves to provide additional coolant inventory. Safety-related logic for the HP CRD Isolation Bypass Function is implemented in the Independent Control Platform (ICP). Manual initiation capability of the HP CRD Isolation Bypass valves is provided in case of loss of instrument air events.

7.4.5.1 System Design Bases

HP CRD Isolation Bypass Function has the following requirements and 10 CFR 50.2 Design Bases.

- Using safety-related logic inputs, the normally closed HP CRD isolation bypass valves are opened automatically on failure of GDCS to successfully inject water into the reactor.
- Nonsafety-related manual control of the HP CRD isolation bypass valve is provided and isolation bypass valve positions are displayed in the MCR.
- Divisional instrumentation performing the HP CRD isolation bypass function logic are powered by the associated safety-related divisional power supplies.
- Bypass of a division of sensors is annunciated in the MCR.
- The HP CRD isolation bypass function logic executed in the ICP and is diverse from SSLC/ESF.

7.4.5.2 System Description

The HP CRD isolation bypass function automatically bypasses the HP CRD injection isolation valve to compensate for a failure of the GDCS to inject. The RTIF cabinets house the ICP logic controllers that perform the HP CRD isolation bypass function. The ICP is diverse from the RTIF-NMS platform and SSLC/ESF platforms. The RPV level, drywell pressure and GDCS pool level sensors are used to determine the failure of the GDCS to inject.

- Automatic Operation
  - Normally closed HP CRD isolation bypass valves are open automatically when failure of GDCS system is detected following a LOCA.
- Manual Operation
  - Manual initiation capability is provided for the HP CRD isolation bypass logic.

  - Manual controls for the operation of each HP CRD isolation bypass valve are available in the MCR.

- Actuation Logic
  - ICP logic controls the actuation of the HP CRD isolation bypass valves ICP.
  - Opening of the two HP CRD isolation bypass valves is performed automatically when failure of the GDCS system is detected following a LOCA. Failure of the GDCS is based on pool level in two-out-of-three GDCS pools remaining above setpoint for 11 minutes following a LOCA signal. Level in each of the three GDCS pools are monitored by four redundant ICP sensors.

The following signals are replicated as part of the HP CRD isolation bypass logic:

- Two-out-of-four sensors detect a sustained low RPV water level condition (Level 1) for 10 seconds; or
- Two-out-of-four sensors detect a sustained high drywell pressure condition for 60 minutes.

7.4.5.3 Safety Evaluation

Although the normally closed HP CRD motor-operated isolation bypass valves are nonsafety-related, the automatic HP CRD isolation bypass logic, which mitigates the beyond design basis failure of multiple GDCS pools to provide coolant make-up, is implemented as a safety-related function. For defense-in-depth, the logic is implemented on the ICP, a safety-related, energized-to actuate, fail-as-is, platform which is diverse from the SSLC/ESF platform and RTIF-NMS platform that contains the HP CRD isolation ESF logic. To provide electrical independence, the safety-related HP CRD isolation bypass logic actuation signal is sent to the Control Rod Drive Hydraulic Subsystem via qualified electrical isolators. The safety-related HP CRD isolation bypass logic provides redundant output contacts for each HP CRD isolation bypass valve motor. Since the nonsafety-related HP CRD isolation bypass valves require power to operate, these redundant safety-related contacts prevent an inadvertent opening of the HP CRD isolation valve flow path in the event of a single failure. Opening of the HP CRD isolation bypass valve can occur only with the HP CRD isolation bypass logic activated either automatically or manually.

The HP CRD isolation bypass function instrumentation located in the drywell is designed to operate in the harsh drywell environment that results from a LOCA. Instrumentation, located outside the drywell, is qualified for the environment in which they must perform their function.

Table 7.1-1 identifies the HP CRD isolation bypass function and the associated codes and standards applied, in accordance with the SRP. This subsection addresses the I&C systems conformance to regulatory requirements, guidelines and industry standards.

7.4.5.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The HP CRD isolation bypass function design complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The HP CRD isolation function conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the HP CRD isolation function conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-Related Function): See Subsection 7.4.5.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the HP CRD isolation function.
  - Section 4.6 (Spatially Dependent Variables): See the Actuation Logic section of Subsection 7.4.5.2
  - Section 5.2 (Completion of Protective Actions): Completion of protective actions is not applicable beyond that discussed in Subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsection 7.4.5.3.
  - Section 6.2 and 7.2 (Manual Control): See Subsections 7.4.5.1 & 7.4.5.2.
  - Section 6.4 (Derivation of System Inputs): Derivation of system inputs for the HP CRD isolation functions are not applicable beyond that discussed in Subsection 7.1.6.6.1.20.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 7.4.5.3.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the HP CRD isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance Bypasses for the HP CRD isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the HP CRD isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the HP CRD isolation function are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The HP CRD isolation bypass function design conforms to these requirements.

10 CFR 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication:

- Conformance: The HP CRD isolation bypass function design complies by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The HP CRD isolation bypass function conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the design of the HP CRD isolation bypass function within the DCD complies with this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety-related functions.

7.4.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24 and 29:

- Conformance: The HP CRD isolation bypass function design complies with these GDC.

7.4.5.3.3 Staff Requirements Memorandum

SRM on SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

- Conformance: The HP CRD isolation bypass function design complies with these criteria. The HP CRD isolation bypass function mitigates a beyond design basis failure of multiple GDCS pools to inject. Although not credited for mitigating the effects of an SSLC/ESF common cause software failure, the logic is implemented on the ICP.

7.4.5.3.4 Regulatory Guides

RG 1.22, Periodic Testing of Protection System Function:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.22. System logic and components are tested periodically during refueling outages.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The HP CRD isolation bypass function is organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and

IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The HP CRD isolation bypass function design complies with RG 1.62. Each division has a manual actuation switch in the MCR. Initiation of the system requires actuation of two switches to ensure that manual initiation is a premeditated act.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

- RG 1.105, Instrument Setpoints for Safety-Related Systems:

- Conformance: The setpoints established to control the HP CRD isolation bypass function conform to RG 1.105. Reference 7.3-2 provides a detailed description of the GEH methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: The HP CRD isolation bypass function conforms to RG 1.151. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.152, Criteria for Digital computers in Safety Systems of Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.152 as implemented on the independent control platform.

RG 1.153, Criteria for Power, I&C Portions of Safety Systems:

- Conformance: The HP CRD isolation bypass function design complies with IEEE Std. 603.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.168 as implemented on the independent control platform.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.169 as implemented on the independent control platform.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.170 as implemented on the independent control platform.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.171 as implemented on the independent control platform.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.172 as implemented on the independent control platform.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.173 as implemented on the independent control platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related I&C Systems:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The HP CRD isolation bypass function design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.4.5.3.5 Branch Technical Positions

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the HP CRD isolation bypass function:

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The HP CRD isolation bypass function design conforms to BTP HICB 8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The ESBWR I&C conform to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

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

- Conformance: Logic controllers for the HP CRD isolation bypass function use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12 - Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The setpoints established to control the HP CRD isolation bypass function conform to this guide. Reference 7.3-2 provides a detailed description of the GEH methodology.

BTP HICB-14 – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The HP CRD isolation bypass function design conforms to BTP HICB-14 as implemented on the independent control platform.

BTP HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR 52:

- Conformance: The level of detail in the HP CRD isolation bypass function description conforms to BTP HICB-16

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The HP CRD isolation bypass function design conforms to BTP HICB-17.

BTP HICB-18 - Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and control Systems:

- Conformance: Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance of Branch Technical Position HICB-18. Q-DCIS is built and qualified specifically for ESBWR applications as safety-related and not as commercial grade PLCs. The embedded and operating system software meet the acceptance criteria contained in BTP HICB-14, for safety-related applications.

BTP HICB-19 - Guidance on Evaluation of Defense-in-Depth and Diversity in digital computer based Instrumentation and Control Systems:

- Conformance: The HP CRD isolation bypass function design conforms to BTP HICB-19. The discrete logic and solid-state controls used in this design are not subject to the vulnerabilities described by BTP HICB-19.

BTP HICB-21 – Guidance on Digital Computer Real-Time Performance:

- Conformance: The HP CRD isolation bypass function design conforms to BTP HICB-21.

7.4.5.3.6 Three Mile Island Action Plan Requirements

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3] and 10 CFR 50.34(f)(2)(xiv)[II.E.4.2] apply to the HP CRD isolation bypass function. The HP CRD isolation bypass function complies with the requirements as indicated above. TMI action plan requirements are addressed in Appendix 1A.

7.4.5.4 Testing and Inspection Requirements

The HP CRD isolation bypass function ICP are self-tested continually at preset intervals and can be tested during plant operation. The HP CRD isolation bypass valves are tested as part of the High Pressure Makeup Line test. Refer to Subsection 4.6.1.2.5 for more information on system arrangement.

7.4.5.5 Instrumentation and Control Requirements

The performance and effectiveness of the HP CRD isolation bypass valve function in a postulated accident is verified by observing the following MCR indications:

- Status indication of HP CRD isolation bypass valve position;
- GDCS pool level indication;
- RPV water level indication; and
- Drywell and RPV pressure indication.

The HP CRD isolation bypass function instrumentation located in the drywell is designed to operate in the harsh drywell environment that results from a LOCA. Instrumentation, located outside the drywell, is qualified for the environment in which they must perform their function.

7.4.6 COL Information

None.

7.4.7 References

7.4-1 (Deleted)

7.4-2 GE-Hitachi Nuclear Energy, “GEH ABWR/ESBWR Setpoint Methodology,” NEDE-33304P, Class III (Proprietary), Revision 1, November 2008, and NEDO-33304, Class I (Non-proprietary), Revision 1, November 2008.

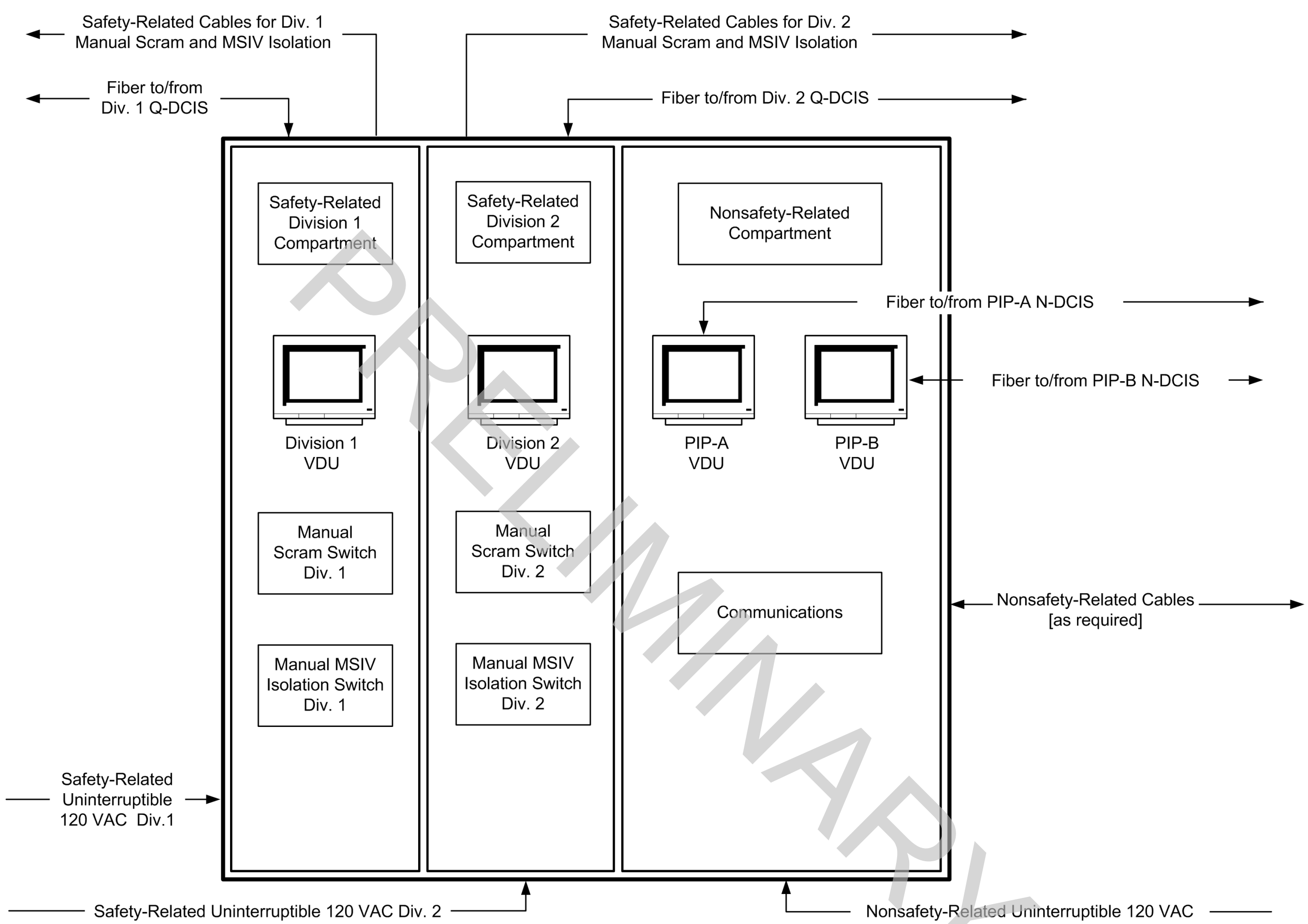


Figure 7.4-1. Remote Shutdown System Panel Schematic

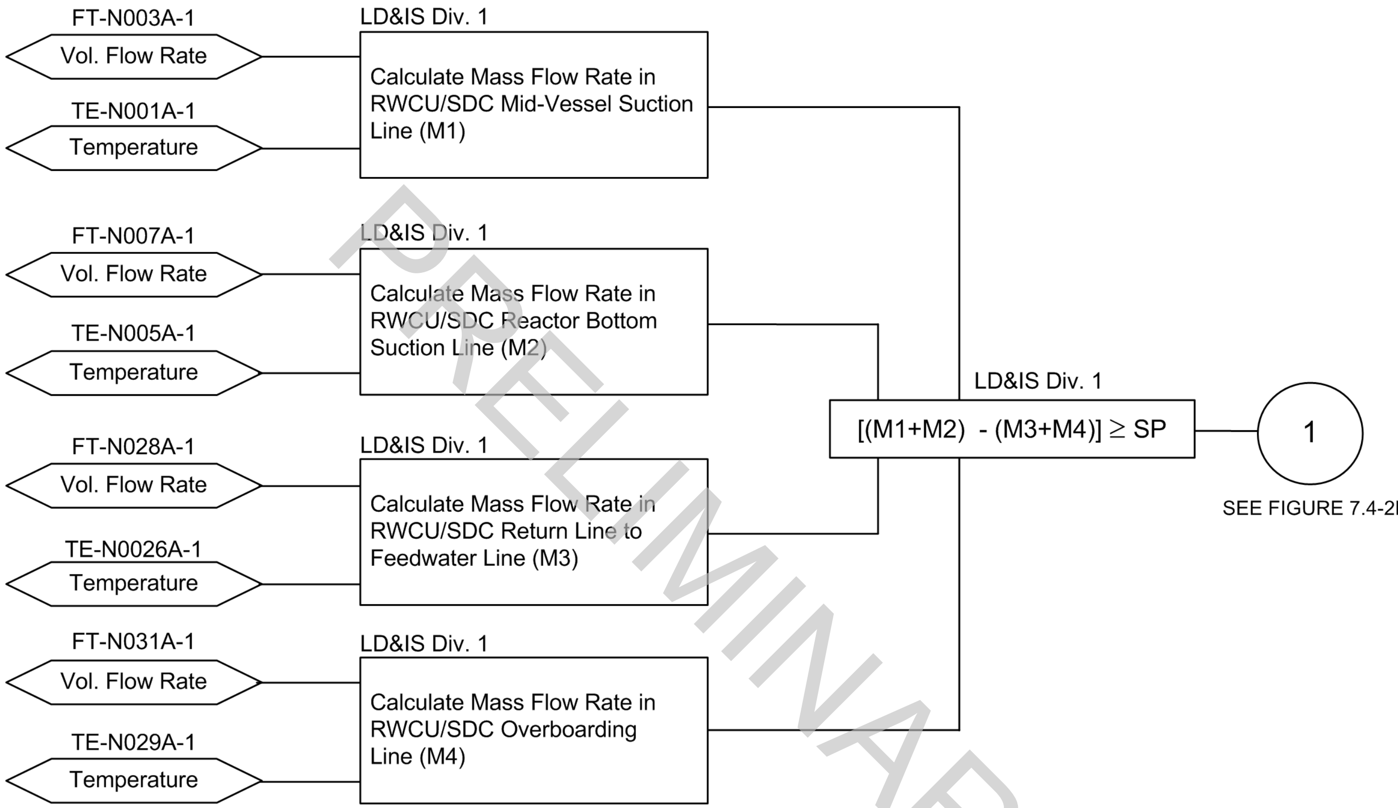


Figure 7.4-2a. RWCU/SDC System Train A Differential Mass Flow Logic- Division 1 (Typical For Train B)

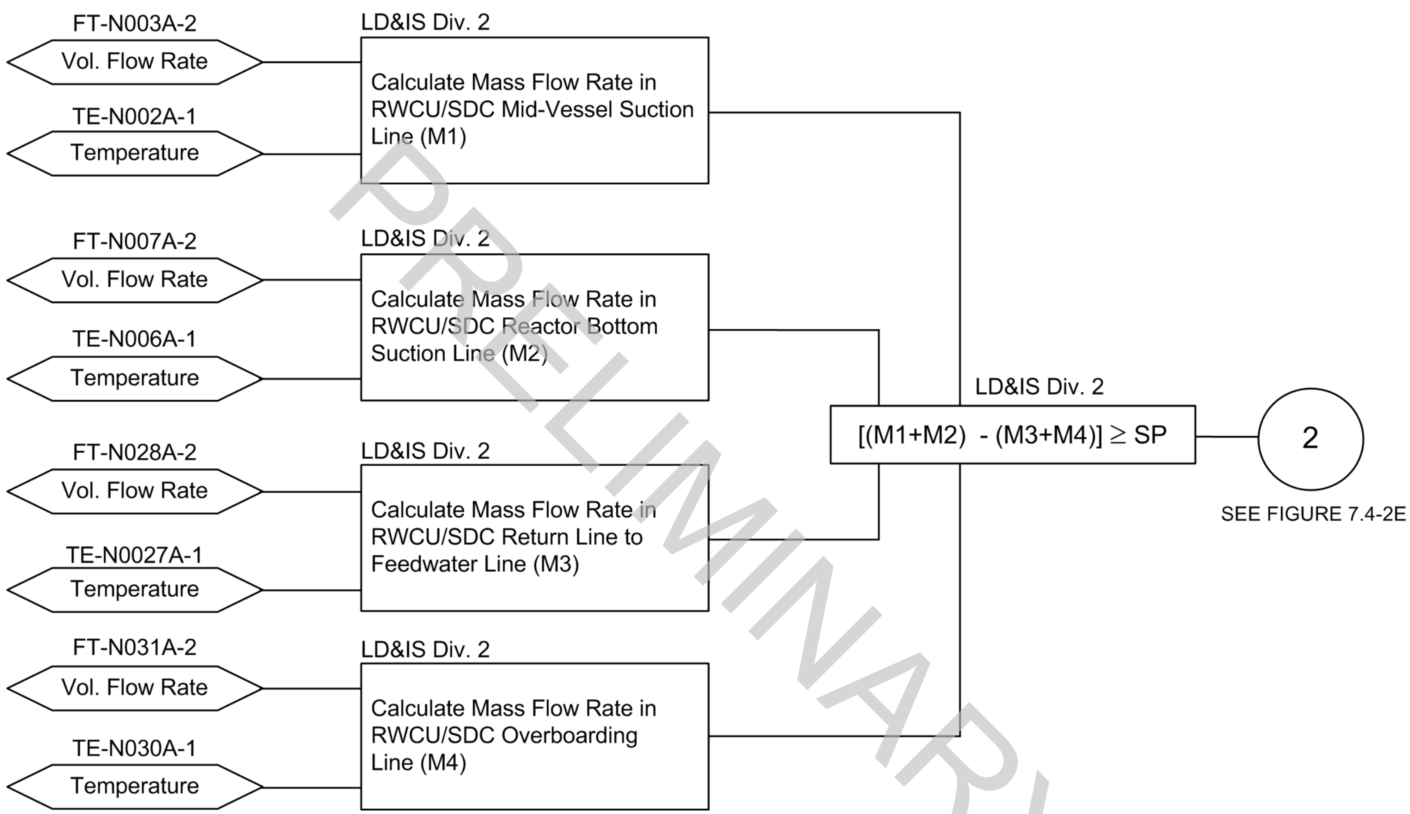


Figure 7.4-2b. RWCU/SDC System Train A Differential Mass Flow Logic- Division 2 (Typical For Train B)

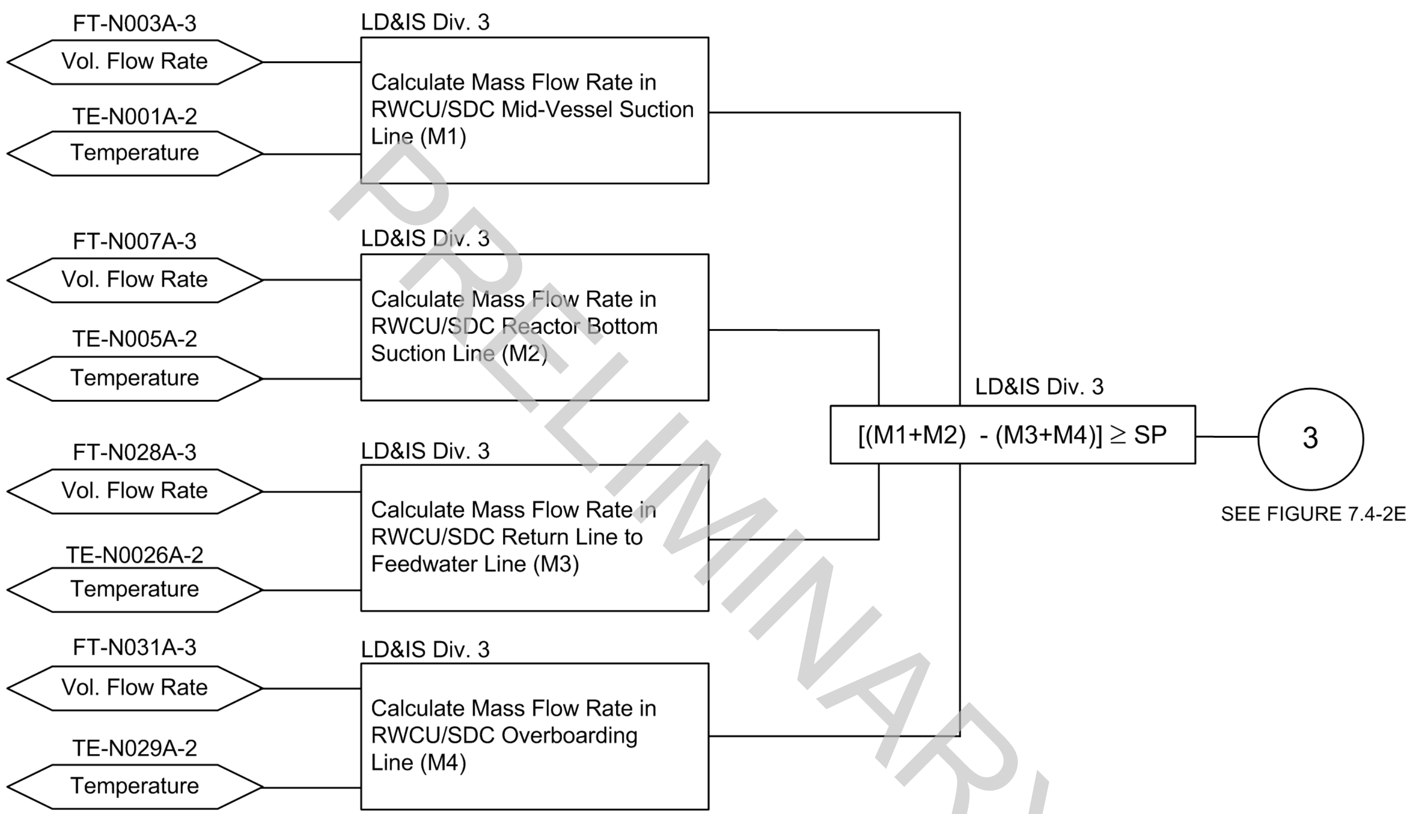


Figure 7.4-2c. RWCU/SDC System Train A Differential Mass Flow Logic- Division 3 (Typical For Train B)

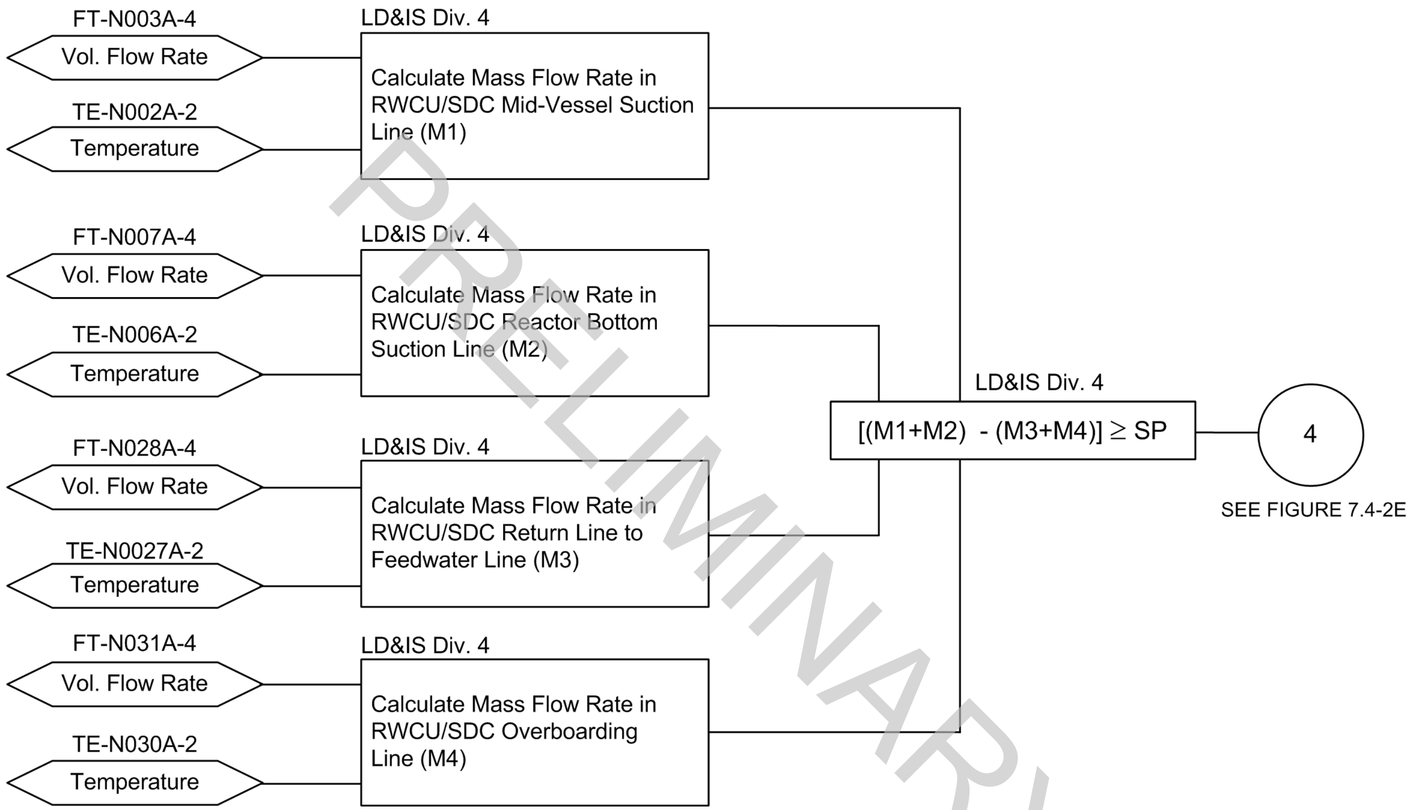


Figure 7.4-2d. RWCU/SDC System Train A Differential Mass Flow Logic- Division 4 (Typical For Train B)

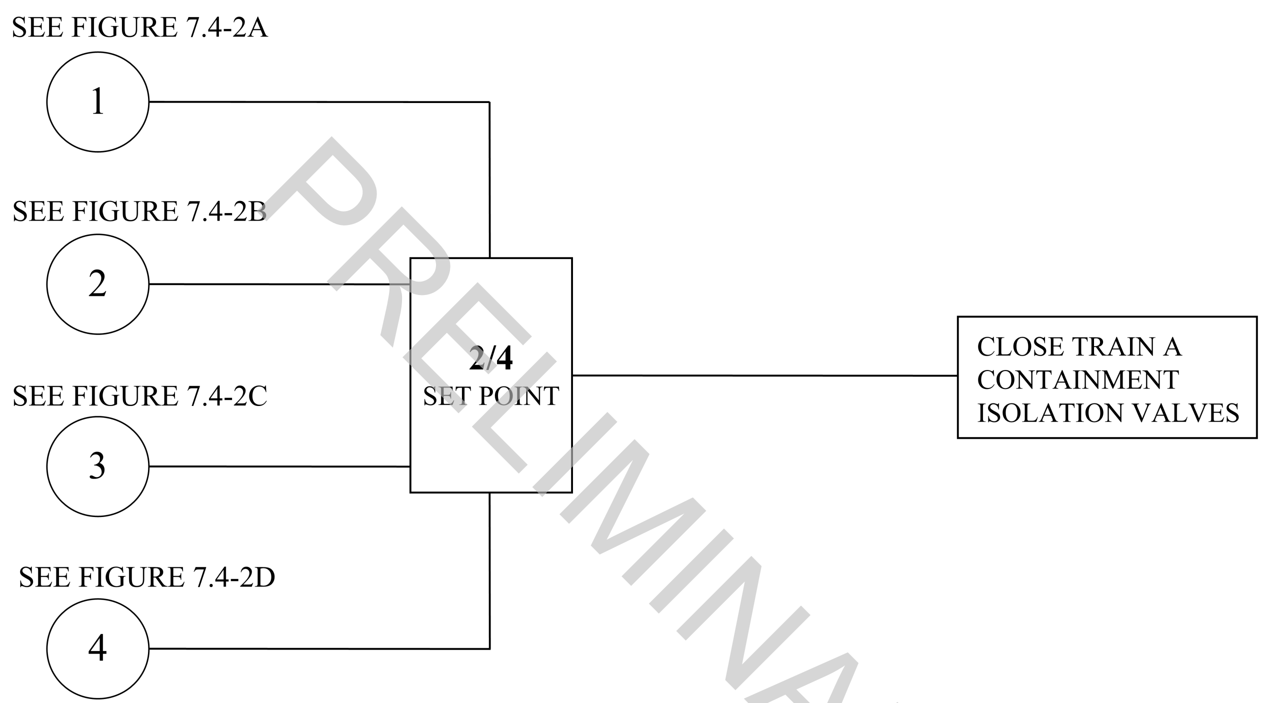


Figure 7.4-2e. RWCU/SDC Line Break Outside Containment Train A Isolation Logic (Typical For Train B)

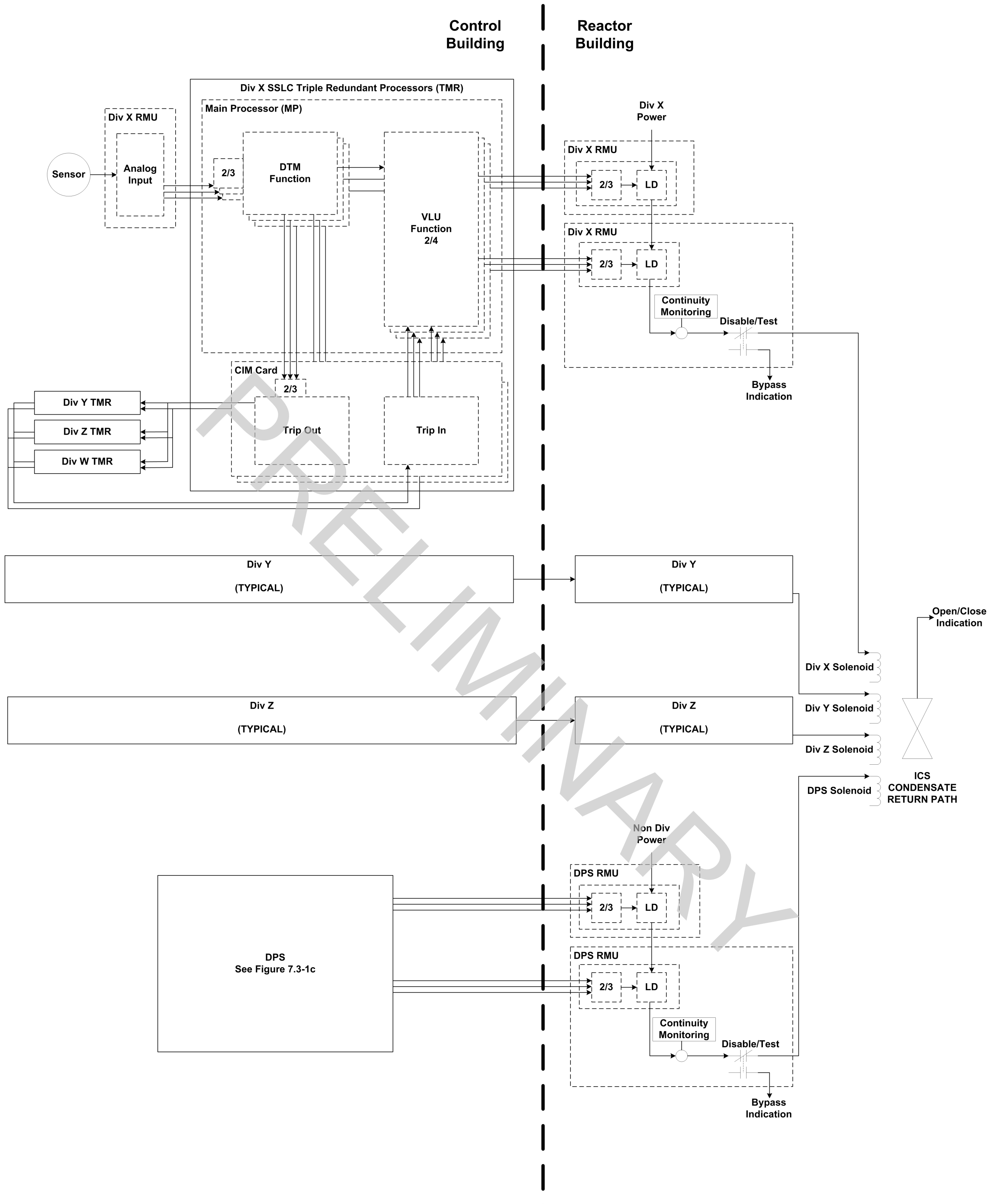


Figure 7.4-3. Isolation Condenser System Initiation and Actuation

7.5 SAFETY-RELATED AND NONSAFETY-RELATED INFORMATION SYSTEMS

This section discusses instrumentation associated with:

- Post Accident Monitoring (PAM),
- Containment Monitoring System (CMS),
- Process Radiation Monitoring System (PRMS),
- Area Radiation Monitoring System (ARMS), and
- Pool Monitoring Instrumentation.

The safety-related portions of the PAM Instrumentation, CMS, PRMS, and Pool Monitoring Instrumentation are part of a group of instruments/equipment collectively called the Safety-Related Distributed Control and Information System (Q-DCIS). A simplified network functional diagram of the DCIS is included as Figure 7.1-1 (not all systems are shown on this figure.)

This diagram schematically indicates the relationships of a safety-related system with its safety-related peers and with nonsafety-related plant data systems called the Nonsafety-Related Distributed Control and Information System (N-DCIS). Section 7.1 contains a description of these relationships.

The nonsafety-related portions of the PAM instrumentation, CMS, PRMS, and the ARMS are part of the N-DCIS.

7.5.1 Post Accident Monitoring Instrumentation

7.5.1.1 System Design Bases

The PAM instrumentation safety-related design bases are to:

- Provide instrumentation to monitor variables and systems over their anticipated ranges for accident conditions as appropriate to ensure adequate safety.
- Provide the appropriate Main Control Room (MCR) instrumentation and displays to provide the information from which actions can be taken to maintain a safe plant condition under accident conditions, including Loss-of-Coolant Accidents (LOCAs).
- Provide equipment (including the necessary instrumentation) at appropriate locations outside the MCR with the capability for prompt hot shutdown of the reactor, and
- Provide the means for monitoring the reactor containment atmosphere spaces containing components that recirculate LOCA fluids, effluent discharge paths, and the plant environs for radioactivity that may be released as a result of accidents.

7.5.1.2 System Descriptions

The safety-related portions of the PAM systems are those systems that provide information for the safe operation of the plant during normal operation, Anticipated Operational Occurrences (AOOs) and accidents, to help ensure performance of manual safety-related functions. The safety-related information systems:

- Include those systems that provide information for manual initiation and control of safety-related systems,
- Indicate that safety-related plant functions are being accomplished, and
- Provide information, from which appropriate actions can be taken to mitigate the consequences of accidents.

The nonsafety-related portions of the PAM systems include the Safety Parameter Display System (SPDS), information systems associated with the emergency response facilities and the Emergency Response Data System (ERDS), none of which perform safety-related functions.

7.5.1.3 Safety Evaluation

PAM instrumentation conforms to regulatory requirements, guidelines, and industry standards.

7.5.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards Important to Safety:

- Conformance: The PAM instrumentation design complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The PAM instrumentation design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the PAM conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.5.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the PAM instrumentation design.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to PAM instrumentation design.
  - Section 5.2 (Completion of Protective Actions): The Post Accident Monitoring system does not provide any trip or isolation functions.
  - Section 5.7 (Capability for Test and Calibration): Test and Calibration requirements are not applicable beyond that discussed in Subsection 7.1.6.6.1.8.
  - Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable beyond that discussed in Subsection 7.1.6.6.1.18.
  - Section 6.4 (Derivation of System Inputs): Derivation of System Inputs for PAM instrumentation is not applicable beyond that discussed in Subsection 7.1.6.6.1.20.
  - Section 6.5 (Capability of Test and Calibration): Test and Calibration requirements for PAM instrumentation design is not applicable beyond that discussed in Subsection7.1.6.6.1.21.

- Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the PAM instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for PAM instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for PAM instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for PAM instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The PAM design conforms to these requirements.

10 CFR 50.34a(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The PAM instrumentation design conforms to the Bypass and Inoperable Status Indication (BISI) requirements of 10 CFR 50.34(f)(2)(v)(I.D.3). General conformance is discussed in Subsection 7.1.6.1, and specific conformance is discussed in the system specific sections.

10 CFR 50.34(f)(2)(xvii) [II.F.1], Accident Monitoring Instrumentation:

- Conformance: The PAM instrumentation design conforms to this requirement.

10 CFR 50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: The PAM instrumentation design conforms to this requirement. The direct water-level instrument system provides for the detection of conditions indicative of inadequate core cooling (Refer to Table 1A-1 of Appendix 1A, Three Mile Island [TMI] Action Plan Items).

10 CFR 50.34(f)(2)(xix) [II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The PAM instrumentation design conforms to this requirement. The PAM instrumentation design conforms to RG 1.97.

10 CFR 50.34(f)(2)(xxiv) [II.K.3.23], Recording of Reactor Vessel Water Level:

- Conformance: The PAM instrumentation design conforms to this requirement. (Refer to Table 1.A-1 of Appendix 1A TMI Action Plan Items).

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The PAM design conforms to this requirement.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The PAM design conforms to this requirement.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) in Design Certification Applications:

- Conformance: ITAAC are provided for the Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the PAM instrumentation within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, 63, and 64:

- Conformance: The PAM instrumentation design conforms to these GDC.

7.5.1.3.3 Staff Requirements Memorandum

Item II.T of SECY 93-087, Control Room Annunciator (Alarm) Reliability:

- Conformance: The alarm management system (AMS) design conforms to the Control Room Annunciator (Alarm) Reliability requirements of SECY 93-087, Item II.T. The systems to which this requirement applies are defined in Table 7.1-1. General conformance is discussed in Subsection 7.1.6.3, and specific conformance is discussed in the system specific sections.

7.5.1.3.4 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The PAM instrumentation design conforms to RG 1.97, which endorses (with certain exceptions specified in Section C of the RG) IEEE Std. 497 that establishes flexible, performance-based criteria for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables. IEEE Std. 497 identifies five types of variables for accident monitoring and the criteria for the selection of each type of variable.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The PAM design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The PAM instrumentation design conforms to IEEE Std. 603.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The PAM design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAM design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The PAM instrumentation design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

Variable Types and Selection Criteria

The five variable types (A, B, C, D, E) and their selection criteria are defined in Section 4 and Table 1 of IEEE Std. 497. Table 1 summarizes the selection criteria for each variable type and the source documents such as plant accident analysis licensing basis, Emergency Procedure Guidelines (EPGs) or plant specific Emergency Operation Procedures (EOPs) and Abnormal Operating Procedures (AOPs) related to the variable type.

The Functional Requirements Analysis (FRA), Allocation of Functions (AOF), (Section 18.4) and Task Analysis (TA) (Section 18.5) address Critical Safety Functions, and provide an independent list of the required RG 1.97 parameters via their respective Results Summary Reports (RSR). The FRA, AOF and TA are iteratively integrated into the design process to provide a final design that effectively balances human factors and system design.

The list of parameters, generated by the Human Factors Engineering (HFE) process, is compared with the information generated from the design process and the differences are entered into the Human Factors Engineering Issue Tracking System (HFEITS) for resolution. During the detailed (second iteration) TA, the RG 1.97 parameters are categorized into the five variable types.

When the EPG/ Severe Accident Guidelines (SAG)/AOP guidelines are released, they are compared with the list of RG 1.97 parameters and the differences are entered into the HFEITS for resolution.

Performance Criteria

Performance criteria defined in IEEE Std. 497, Section 5 include:

- Range,
- Accuracy,
- Response time,
- Required instrumentation duration,
- Reliability, and
- Performance assessment documentation.

RG 1.97 endorses IEEE Std. 497 Section 5, "Performance Criteria" with modification (the RG provides guidance on the application of these requirements).

Performance criteria (identified in IEEE Std. 497, Section 5) are developed during the design process using inputs from the HFE process together with other design and accident analysis inputs. The performance criteria (range, accuracy, response time, required instrument duration, and reliability) for each required variable are documented in the PAM Variable List.

Performance is verified to meet the as-designed performance criteria of Section 18.11, Human Factors Verification and Validation (HF V&V). Performance deviations are entered into the HFEITS for resolution. The results of this assessment are documented in the HF V&V RSR.

Design Criteria

The design criteria defined in IEEE Std. 497, Section 6, include:

- Single failure,
- Common cause failure,
- Independence and separation,
- Isolation,
- Information ambiguity,
- Power supply,
- Calibration,
- Testability,
- Direct measurement,
- Control of access,
- Maintenance and repair,
- Minimizing measurements,
- Auxiliary supporting features,
- Portable instruments, and
- Documentation of design criteria.

RG 1.97 endorses IEEE Std. 497 Section 6, "Design Criteria" with modification.

The design conforms to the specific criteria identified in IEEE Std. 497, Section 6. Each specific criterion is addressed and documented during the detailed design process using appropriate inputs from the licensing basis, the design process and the HFE process, as identified in Chapter 18.

Qualification Criteria

The design conforms to the requirements to qualify the instrumentation associated with the identified variables within each type (A, B, C, D, E) in accordance with the qualification criteria of IEEE Std. 497 Criteria, Section 7, "Qualification Criteria." Specific qualification requirements are developed during the design process for:

- Type A variables,
- Type B variables,
- Type C variables,
- Type D variables,
- Type E variables,
- Portable instruments,
- Post event operating time, and
- Documentation of qualification criteria.

Display Criteria

The display criteria defined in IEEE Std. 497 Section 8 include:

- Information characteristics,
- Human factors,
- Anomalous indications,
- Continuous vs. on –demand display,
- Trend or rate information,
- Display identification,
- Type of monitoring channel display,
- Display location,
- Information ambiguity,
- Recording,
- Digital display signal validation, and
- Display criteria documentation.

The design conforms to the specific display criteria identified in IEEE Std. 497, Section 8. Each specific criterion is addressed and documented during the detailed design process using appropriate inputs from the licensing basis, the design process and the HFE process, as identified in Chapter 18.

Display characteristics consistent with inputs from design, safety analysis, and HFE include:

- Range,
- Accuracy,
- Precision,
- Display format,
- Units, and
- Response time.

The Distributed Control and Information System (DCIS) provides the required signal paths to process the information. The DCIS is subdivided into the Q-DCIS and the N-DCIS. These DCIS systems are described in Section 7.1.

For PAM instrumentation associated with Critical Safety Functions and powered from the safety-related sources, the Q-DCIS provides the required signal path to process data. This information then is shown on Q-DCIS divisional safety-related displays.

The safety-related information is also available to the N-DCIS, through the qualified safety-related isolation devices, for input to nonsafety-related displays, Plant Computer Functions (PCF) and the AMS. Type A, Type B, and Type C variables are powered from safety-related sources. For Type D and Type E variables that are powered from nonsafety-related sources the N-DCIS provides the required signal paths to process information.

The Q-DCIS has four separate divisions, each powered by a different safety-related (AC) uninterruptible power supply (UPS). The safety-related power is discussed in Subsection 8.3.1.1.3. The design complies with required instrument duration requirements of IEEE Std. 497, Section 5.4, as modified by RG 1.97.

The nonsafety-related AMS, SPDS, and BISI are discussed in Subsections 7.1.4 and 7.1.5. Subsection 7.1.5.3.3 discusses additional acceptance criteria applicable to Annunciator Systems (SECY-93-087, Item II.T). The PCF provides nonsafety-related navigational or top-level displays for safety parameter displays, Alarms and Annunciators, and bypass and inoperable status indicator (BISI). The N-DCIS also provides data support functions (for example, Technical Support Center [TSC] and Emergency Operations Facility [EOF], and Emergency Response Data Systems [ERDS]).

Quality Assurance

All equipment is provided in accordance with the GEH 10 CFR 50 Appendix B Quality Assurance Program (Reference 7.5-1). The NRC accepted GEH Quality Assurance Program, along with its implementing procedures constitute the Quality Assurance system that is applied to the safety-related I&C system design. It satisfies all applicable requirements of:

- 10 CFR 50 Appendix B,
- American National Standards Institute (ANSI) / American Society of Mechanical Engineers (ASME) NQA-1, and
- ISO 9001.

Post Accident Monitoring Variable List Documentation

The PAM variable list is prepared as a separate document, using inputs from the design process, licensing design basis, and HFE process, including the development of the EPGs and/or EOPs and AOPs.

The PAM variable list document provides summary information for each PAM variable as applicable. Typical information provided includes:

- PAM variable name,
- Type,
- Range,
- Extended range (Type C),
- Instrument channel accuracy,
- Required instrument duration,
- Power source,
- Required number of channels,
- Qualification criteria, and

- Type of monitoring channel display.

7.5.1.3.5 Branch Technical Positions

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The PAM instrumentation design conforms to RG 1.97 Revision 4, IEEE Standard 497-2002 (with clarifications and exceptions stated in RG 1.97 Revision 4), and RG 1.100.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the PAM instrumentation design conforms to BTP HICB-16.

7.5.1.4 Testing and Inspection Requirements

Testing and inspection requirements for RG 1.97 instrumentation are defined in IEEE Std. 497, Criterion 6.8, "Testability" and Criterion 6.11, "Maintenance and Repair." Compliance with these requirements is addressed during the detailed design phase.

7.5.1.5 Instrumentation and Controls Requirements

Instrumentation requirements for RG 1.97 instrumentation are defined in IEEE Std. 497. Identification of specific instrument requirements and conformance to these requirements is addressed during the detailed design phase.

7.5.2 Containment Monitoring System

The CMS provides the instrumentation to monitor the:

- Atmosphere in the containment for high gross gamma radiation levels,
- Pressure of the drywell and wetwell,
- Drywell/wetwell differential pressure,
- Lower and upper drywell water level (post-LOCA),
- Temperature of the suppression pool water,
- Suppression pool water level,
- Drywell/wetwell hydrogen/oxygen concentration levels, and
- Containment area radiation.

These parameters are monitored during both normal reactor operations and post-accident conditions to evaluate the integrity and safe conditions of the containment. Abnormal measurements and indications initiate alarms in the MCR.

7.5.2.1 System Design Bases

The CMS design conforms to the following system design criteria.

- The CMS is classified as safety-related and Seismic Category 1 except as noted, and conforms to the relevant codes and standards specified in Table 7.1-1 for this system. IEEE Std. 603, Sections 4.5 and 5.8, apply to the safety-related portions of the CMS.
- The safety-related Hydrogen/Oxygen (H_2/O_2) analyzers are active during normal operation. Additional sampling capacity is automatically initiated by a LOCA signal for post-accident monitoring of oxygen and hydrogen content in the containment.
- Each CMS gas sampling subsystem monitors the atmospheric oxygen and hydrogen contents in the drywell and the wetwell, and provides measurements in the MCR in percent by volume for each of the sampled gases. Table 7.5-5 provides the instrument ranges for these parameters. Sampling of the drywell or the wetwell is initiated either manually (remotely or locally) or automatically.
- Dual redundant divisions of gas sampling and radiation monitoring are provided.
- Nonsafety-related radiation monitoring consists of two channels per division. Each radiation monitoring channel portion consists of a gamma sensitive Radiation Detection Assembly and a digital Signal Conditioning Unit. The Radiation Detection Assemblies are installed at widely separated locations to provide comprehensive coverage of the containment volume. The channels measure gross gamma radiation in the drywell and wetwell. The gross gamma radiation signals are provided to the MCR where they are continuously displayed. The channels are equipped with upscale alarms to indicate high radiation and an alarm to indicate channel malfunction.
- MCR alarms are provided for indications of high radiation dose rates, inoperative radiation monitors, high oxygen concentration levels, high hydrogen concentration levels, and abnormal samples for each subsystem.
- Each gas sampling rack is provided with its own gas calibration sources of known concentration levels to calibrate periodically the oxygen and hydrogen analyzers and the sensors.
- The lower drywell water level is monitored to indicate any increases in water level that may occur in the lower drywell following a LOCA condition.
- The upper drywell water level is also monitored and compared with the RPV nozzle elevations.
- The drywell and wetwell pressure instrumentation taps are located throughout the containment and the sensors located outside containment provide safety-related and nonsafety-related functions for both normal and post-accident monitoring, including drywell pressure inputs for reactor scram protection monitoring. In addition, pressure signals are provided to the Diverse Protection System (DPS) for diverse scram protection monitoring.

MCR alarms and indication are provided for suppression pool temperature monitoring as discussed in Subsection 7.2.3.

7.5.2.2 System Description

The CMS is a divisionalized and segregated (safety/nonsafety-related) monitoring system, and is configured as shown in Figure 7.5-1. The specific system features are as follows:

- Radiation monitoring and gas H_2/O_2 sampling are provided for the drywell and for the airspace above the suppression pool.
- Each radiation monitoring channel uses one gamma-sensitive ion chamber and one digital log radiation monitor. Four channels are provided, two for the drywell and two for the suppression pool (wetwell) airspace.
- During normal plant operation, both the radiation monitoring and gas sampling subsystems are operating. For post-accident monitoring, the gas sampling subsystem is automatically activated by the LOCA signal to alternate its sampling between the drywell and the wetwell. The area of sampling can be selected manually or sequentially controlled.
- Heat tracing is provided on the gas sampling lines for control of moisture and condensation.
- Two isolation valves are provided on each sample and return line that penetrates the containment. Each line has one valve inside containment and one valve outside containment.
- Each gas sampling analyzer has dual redundant pumps. One is used during normal operation; the other is used for added capacity or backup.
- Separate oxygen and hydrogen gas sources are provided in each CMS sampling rack with known compositions for monitor calibration.
- CMS piping connections are provided. Piping connections are required in order to connect the sampling instrumentation.
- The drywell pressure instrumentation taps are located throughout the containment and the sensors are located outside the containment.
- Four drywell pressure transmitters are provided for safety-related signals for use by the Reactor Protection System (RPS) for reactor scram. Four additional safety-related drywell pressure signals are transmitted to the Leak Detection and Isolation System (LD&IS), where they are used to initiate isolation of containment valves, transfer pump suction, and initiate suppression pool cooling. The containment isolation function is discussed in Subsection 6.2.4.
- Four drywell water level transmitters are provided as safety-related signals for use by the LD&IS for feedwater line isolation and FW ASD controller breaker trip.
- Two wide-range safety-related pressure transmitters are used for providing safety-related drywell pressure information meeting the requirements of post-accident monitoring.
- Four nonsafety-related drywell pressure transmitters are used by the DPS for diverse scram protection monitoring and by the Containment Inerting System (CIS) for controlling the position of the nitrogen makeup pressure control valve.

- The suppression pool water level is monitored during all plant operating conditions and post-accident conditions. Suppression pool water level monitoring consists of ten channels of water level detection sensors distributed into four safety-related narrow-range and four nonsafety-related wide-range instruments. The narrow range suppression pool water level signals are used to detect the uncovering of the first set of suppression pool temperature sensors below the pool surface. When the suppression pool water level drops below the elevation of a particular set of temperature sensors, those sensor signals are not used in computing the average pool temperature.
- The wide range water level signals are available for displaying suppression pool water level on the Remote Shutdown System (RSS) Panels.
- Suppression pool temperatures are monitored (see Subsection 7.2.3).

7.5.2.3 Safety Evaluation

The CMS design, including the sensors and the instrumentation channels, is designed into both safety-related and nonsafety-related subsystems. Safety-related systems are environmentally and seismically qualified for continuous monitoring during normal reactor operation, as well as during and after DBEs. The system design conforms to the System Design Bases.

Table 7.1-1 identifies the CMS and the associated regulatory requirements, guidelines, and codes and standards applied, in accordance with NUREG 0800. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.5.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The CMS design complies with these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The CMS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the CMS design conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.5.2.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the CMS system.
  - Section 4.6 (Spatially Dependent Variables): See Subsection 7.5.2.2.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 7.5.2.1.
  - Section 6.2 and 7.2 (Manual Control): See Subsection 7.5.2.1 and 7.5.2.2.
  - Section 6.4 (Derivation of System Inputs): The CMS derives its sense and command features from direct measurements, See Subsections 7.5.2.2.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 7.5.2.4.

– Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the CMS are not applicable.

– Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the CMS are not applicable.

– Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the CMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.

– Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the CMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The CMS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The CMS design complies by being able to provide automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(viii)[II.B.3], Compatibility to Promptly Obtain and Analyze Containment Atmosphere Samples:

- Conformance: The CMS design complies with this requirement.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The CMS design complies with this requirement.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The CMS design complies with these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The CMS design complies with this requirement.

10 CFR 50.44(c)(4), Combustible Gas Control For Nuclear Power Reactors, Monitoring:

- Conformance: The CMS design complies with this requirement.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The CMS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the CMS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.2.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, 41, 43, and 64:

- Conformance: The CMS design complies with these GDC.

7.5.2.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The CMS design conforms to item II.Q of SECY-93-087 (BTP HICB-19) by implementation of diverse I&C, described in Section 7.8.

7.5.2.3.4 Regulatory Guides

RG 1.22, (Safety Guide 22) Periodic Testing of Protection System Actuation Function:

- Conformance: The CMS design conforms to RG 1.22.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- The CMS design conforms to RG 1.45.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The CMS design conforms to RG 1.47.

RG 1.53, Application of the Single Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The CMS is organized into four physically and electrically-isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.

RG 1.75, Physical Independence of Electrical Systems:

- Conformance: The CMS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The CMS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The CMS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The safety-related portions of the CMS design conform to RG 1.105. Reference 7.5-2 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.151, Instrument Sensing Lines

- Conformance: The CMS design conforms to RG 1.151.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The CMS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The CMS design conforms to 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.168 as implemented on the SSLC/ESF platform.

RG 1.169, Configuration Management Plans For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.169 as implemented on the SSLC/ESF platform.

RG 1.170, Software Test Documentation For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.170 as implemented on the SSLC/ESF platform.

RG 1.171, Software Unit Testing For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.171 as implemented on the SSLC/ESF platform.

RG 1.172, Software Requirements Specifications For Digital Computer Software Used In Safety Systems:

- Conformance: The CMS design conforms to RG 1.172 as implemented on the SSLC/ESF platform.

RG 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems:.

- Conformance: The CMS design conforms to RG 1.173 as implemented on the SSLC/ESF platform.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The CMS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The CMS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control System in Nuclear Power Plants.

- Conformance: The CMS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.5.2.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The CMS design conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The CMS design conforms to BTP HICB-11. SSLC/ESF logic controllers for the CMS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The CMS design conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The CMS design conforms to BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the CMS design conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The CMS design conforms to BTP HICB-17.

BTP HICB-19, Guidance on Evaluation of Defense-in-Depth and Diversity in digital Computer-based Instrumentation and Control Systems:

- Conformance: The CMS design conforms to BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The CMS design conforms to BTP HICB-21.

Subsection 7.3.5.3.5 provides a discussion of BTP HICB-14, BTP HICB-17, and BTP HICB-21 in conjunction with the SSLC/ESF system.

7.5.2.3.6 Three Mile Island Action Plan Requirements

In accordance with SRP 7.5, and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) [I.D.3], 10 CFR 50.34(f)(2)(xvii)[II.F.1], 10 CFR 50.34(f)(2)(viii)[II.B.3], and 10 CFR 50.34 (f)(2)(xix)[II.F.3] apply to the CMS. In addition, 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], also applies. The CMS complies with these requirements, as indicated above. TMI action plan requirements are addressed generically in Appendix 1A.

7.5.2.4 Testing and Inspection Requirements

In-service and Surveillance Testing: In-service testing is performed periodically on each CMS subsystem to verify operability and to ensure its readiness status for post accident monitoring. Surveillance testing includes instrument channel checks of the radiation and gas monitors, functional tests to verify equipment operability, sensor calibration and response tests, and leakage tests of the gas sampling lines.

Validation Test of the Calibrated Gas Sources: Tests are conducted on the gas calibration sources to verify equipment operability and to certify that the required gas concentration levels are within acceptable limits.

Specific Channel Calibration Checks: Each radiation monitoring channel is checked and calibrated using a known gamma radiation source. Channel response is checked for proper measurement and display and for alarm initiation.

Each oxygen and hydrogen gas-sampling channel is checked for proper calibration and response using at least two input gas levels (Refer to Table 7.5-4).

Sample Gas Leakage Tests: The design leakage from the sampling lines and associated gas analyzer panel is specified in Table 7.5-4.

7.5.2.5 Instrumentation and Control Requirements

Radiation Level Monitoring: Each compartment in containment is monitored by two-divisional channels for gross gamma radiation levels. Each channel consists of an ion chamber detector and a digital log radiation monitor, with trip circuits set for high radiation and low/INOP indications.

Oxygen/Hydrogen Concentration Monitoring: Two divisional racks for analysis and measurement sample the oxygen/hydrogen concentration levels in each compartment of the containment. The range of measurement of hydrogen and oxygen contents is displayed in percent (by volume) for the inerted containment. Separate gas indicators for measurement of oxygen and hydrogen content are provided in the MCR for each CMS subsystem. Trip circuits for alarm initiation are set for high oxygen and hydrogen concentration levels and for abnormal sampling flow indication.

7.5.3 Process Radiation Monitoring System

The PRMS provides the instrumentation for radiological monitoring, sampling and analysis of the:

- Turbine Building,
- TSC,
- Radwaste Building,
- Control Building,
- Reactor Building,
- Fuel Building,
- Reactor Building/Fuel Building Stack,
- Turbine Building Stack, and
- Radwaste Building Stack.

The PRMS alerts operators when radiation levels exceed preset limits and initiates automatically the required protection action to isolate, contain or redirect radioactivity releases from the environs. See Subsection 11.5.1.1.2 for process and effluent paths and/or areas with the potential for excessive radiation levels.

The system is configured as shown in Figure 11.5-1 and Table 11.5-3.

7.5.3.1 Design Bases

The design bases are provided in Section 11.5.

7.5.3.2 System Description

The system description is provided in Section 11.5.

7.5.3.3 Safety Evaluation

The safety-related PRMS, including the sensors and the instrumentation channels, is environmentally and seismically qualified for continuous monitoring during reactor operation as well as abnormal and accident plant conditions.

Table 7.1-1 identifies the PRMS and the associated regulatory requirements, guidelines and codes and standards applied, in accordance with NUREG-0800. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.5.3.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The PRMS design conforms to this standard.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The PRMS design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the SLC conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 11.5.1.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the PRMS system.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to PRMS.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions are not applicable beyond that discussed in subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): See Subsections 11.5.6.1, 11.5.6.2, and 11.5.6.3.
  - Section 6.2 and 7.2 (Manual Control): See Subsection 7.5.3.3.3.
  - Section 6.4 (Derivation of System Inputs): The PRMS derives its sense and command features from direct measurements.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 11.5.6.1, 11.5.6.2, and 11.5.6.3.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the PRMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.
  - Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the PRMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
  - Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the PRMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
  - Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the PRMS are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design,

- Conformance: The PRMS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The PRMS design conforms by being able to provide automatic indication of bypassed and inoperable status.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The PRMS design conforms to this requirement.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The PRMS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The PRMS design conforms to this requirement.

10 CFR 50.34(f)(2)(xxviii)[III.D.3.4] Control Room Habitability Problems Under Accident Conditions:

- Conformance: The PRMS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The PRMS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the PRMS within the DCD documents conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, and 64:

- Conformance: The PRMS design complies with these GDC.

7.5.3.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The PRMS design conforms to item II.Q of SECY-93-087 (BTP HICB-19).

7.5.3.3.4 Regulatory Guides

RG 1.22, (Safety Guide 22) Periodic Testing of Protection System Actuation Function:

- Conformance: The PRMS design conforms to RG 1.22.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance: The PRMS design conforms to RG 1.45.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The PRMS design conforms to RG 1.47.

RG 1.53, Application of the Single Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The PRMS is organized into four physically and electrically-isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.

RG 1.75, Physical Independence of Electrical Systems:

- Conformance: The PRMS design conforms to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The PRMS design conforms to RG 1.89. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The PRMS design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The safety-related portions of the PRMS design conform to RG 1.105. Reference 7.5-2 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: Periodic testing of the protection systems is performed in accordance with IEEE Std. 338, as modified by RG 1.118.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The PRMS design conforms to RG 1.152.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The PRMS design conforms to 10 CFR 50.55a(h).

RG 1.168, Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.168 as implemented on the SSLC/ESF platform..

RG 1.169, Configuration Management Plans For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.169 as implemented on the SSLC/ESF platform..

RG 1.170, Software Test Documentation For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.170 as implemented on the SSLC/ESF platform..

RG 1.171, Software Unit Testing For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.171 as implemented on the SSLC/ESF platform..

RG 1.172, Software Requirements Specifications For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.172 as implemented on the SSLC/ESF platform..

RG 1.173, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems:

- Conformance: The PRMS design conforms to RG 1.173 as implemented on the SSLC/ESF platform..

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The PRMS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The PRMS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The PRMS design conforms to RG 1.209. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.5.3.3.5 Branch Technical Positions

BTP HICB-8, Guidance for Application of RG 1.22:

- Conformance: The PRMS design conforms to BTP HICB-8.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The PRMS design conforms to BTP HICB-11. SSLC/ESF logic controllers for the PRMS use safety-related fiber optic CIMs and fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The PRMS design conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The PRMS design conforms to BTP HICB-14.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the PRMS design conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The PRMS design conforms to BTP HICB-17.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The PRMS design complies with BTP HICB-19.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The PRMS design conforms to BTP HICB-21.

BTP HICB-14, BTP HICB-17, BTP HICB-18, and BTP HICB-21 are addressed in conjunction with the SSLC/ESF in Subsection 7.3.5.3.5.

7.5.3.3.6 Three Mile Island Action Plan Requirements

In accordance with SRP 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v)[I.D.3], 10 CFR 50.34(f)(2)(xvii) [II.F.1], 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], and 10 CFR 50.34(f)(2)(xix)[II.F.3] apply to the PRMS. The PRMS conforms to these requirements, as indicated above. TMI action plan requirements are generically addressed in Appendix 1A.

7.5.3.4 Testing and Inspection Requirements

The capability for testing and calibration is discussed in Subsections 11.5.6.1, 11.5.6.2, and 11.5.6.3 and conforms to the requirements of IEEE Std. 603, Sections 5.7 and 6.5.

7.5.3.5 Instrumentation and Control Requirements

I&C requirements are provided in Subsections 11.5.2.2, 11.5.3.1 and 11.5.3.2.

7.5.4 Area Radiation Monitoring System

The primary function of the nonsafety-related ARMS is to continuously monitor the gamma radiation levels throughout the plant and to provide an early warning that predetermined radiation levels are exceeded. The ARMS consists of area radiation detectors located at accessible areas of the plant and utilizes local and MCR alarms for immediate warning. The gross gamma radiation levels are monitored on a continuous basis, because changes are caused by operational transients or maintenance activities. Any high and very high radiation levels are indicated by audible area alarms and MCR alarms.

A functional block diagram of the ARMS is shown in Figure 7.5-3.

7.5.4.1 Design Bases

The ARMS continuously measures, indicates, and records area radiation levels.

7.5.4.2 System Description

A design description of this system, together with detector locations, channel ranges, and alarm requirements, is covered in Subsection 12.3.4.

7.5.4.3 Safety Evaluation

The ARMS design, including the sensors and the instrumentation channels, is a nonsafety-related system designed for continuous monitoring during normal operation, as well as AOOs and plant accidents. The system design conforms to the System Design Bases.

Table 7.1-1 identifies the ARMS and the associated regulatory requirements, guidelines and codes and standards applied, in accordance with NUREG-0800. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.5.4.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The ARMS design conforms to these standards.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design,

- Conformance: The ARMS design conforms to these requirements.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The ARMS design conforms to this requirement.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: ARMS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of In-plant Airborne Radioactivity:

- Conformance: The ARMS design conforms to this requirement.

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The ARMS design conforms to this requirement.

10 CFR 50.34(f)(2)(xxiv)[II.K.3.23] Capability to Record Reactor Vessel Water Level in One Location on Recorders that Meet Normal Post-Accident Recording Requirements:

- Conformance: The ARMS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvi)[III.D.1.1], Leakage Control and Detection in Design Systems Outside Containment:

- Conformance: The ARMS conforms to these requirements.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the ARMS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The ARMS design does not use innovative means for accomplishing safety functions.

7.5.4.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, 63, and 64:

- Conformance: The ARMS design conforms to these GDC.

7.5.4.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The ARMS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The ARMS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The ARMS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The ARMS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.5.4.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the ARMS conforms to BTP HICB-16.

7.5.4.3.5 Three Mile Island Action Plan Requirements

In accordance with SRP 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(xvii)[II.F.1], 10 CFR 50.34(f)(2)(xix)[II.F.3], and 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3] apply to the ARMS. The ARMS design conforms to these requirements, as indicated above. TMI action plan requirements are addressed generically in Appendix 1A.

7.5.4.4 Testing and Inspection Requirements

ARMS channels are tested and calibrated using the plant operating and maintenance procedures. Each Signal Conditioning Unit (SCU) is equipped with an internal self-diagnostic feature to detect and locate instrument failures. The SCU is also equipped with internal software to facilitate electronic calibration. Each SCU is provided with a means for adjustment of electronic calibration and trip setting. These adjustments do not require equipment removal from its associated panel. The SCU is also provided with a means for generating internal signals that can be used both to check the calibration of the electronic circuits that process the Radiation Detector Assembly's signal and to verify trip setpoints.

The SCU is provided with a means for administrative control of all adjustments and setpoints.

7.5.4.5 Instrumentation and Control Requirements

Every ARM channel consists of a gamma sensitive detector and a digital area radiation processor. All channels are provided with local visual and audible alarms and local readouts. Where appropriate, additional readouts and alarms are provided by local auxiliary units.

7.5.5 Pool Monitoring Instrumentation

General Functional Requirements Conformance

Suppression Pool

The safety-related requirement of the Suppression Pool Temperature Monitoring (SPTM) function is to protect the suppression pool temperature from exceeding established limits. The SPTM, which is a Containment Monitoring (CMS) function, continuously monitors pool temperatures and provides visual indications and alarms to the MCR panels for automatic suppression pool cooling during reactor operation and accident conditions as discussed and evaluated in Subsection 7.2.3.

The CMS provides temperature and level instruments for monitoring suppression pool water temperature and water level, respectively. The CMS instruments provide functions necessary to maintain suppression water temperature and level required for safety-related Emergency Core Cooling System (ECCS) functions described in Subsection 7.3.1.2. For this reason, they are classified as safety-related. The CMS also includes nonsafety-related temperature sensors for the DPS diverse scram function described in Subsection 7.8.1.2.1.

The suppression pool-cooling mode of the Fuel and Auxiliary Pools Cooling System (FAPCS) is automatically initiated by a high pool-temperature signal provided that either FAPCS Train A or Train B is in standby mode. The water level instrument generates a low water level signal when the suppression pool level decreases to a low level setpoint. This signal trips the FAPCS pump when it operates with suction from the suppression pool.

Gravity-Driven Cooling System Pools

The Gravity-Driven Cooling System (GDCS) provides the GDCS pools with safety-related instruments that monitor water level. Each instrument generates high or low water level signals when the water level reading increases above or decreases below its setpoint. Each high and low-level signal initiates an alarm in the MCR. Additionally, a low-level trips the FAPCS system pump operating in the GDCS pool-cooling mode. The high-level setpoint is established to avoid overflow of GDCS pool water. The low water level setpoint is established to prevent inadvertent draining of the pool water below the minimum safe level.

The instruments provide necessary information to the operator for maintaining GDCS water level required for the safety-related ECCS function as discussed and evaluated in Subsection 7.3.1.2. The GDCS also provides nonsafety-related instrumentation for the DPS diverse emergency core cooling function described in Subsection 7.8.1.2.2.

An additional set of GDCS level instrumentation is provided to the ICP for the HP CRD that is discussed in Subsection 7.4.5.

IC/PCCS Expansion Pools

The FAPCS provides the Isolation Condenser / Passive Containment Cooling System (IC/PCCS) expansion pools component with safety-related instruments that monitor water level. Each instrument generates high or low water-level signals when the water level reading increases above or decreases below its setpoint. Each high or low level signal initiates an alarm in the MCR. Additionally, a low level signal trips the IC/PCCS pool cooling and cleanup system. The high water-level setpoint is established to avoid overflow of IC/PCCS expansion pool water. The low water-level setpoint is established to prevent inadvertent draining of the IC/PCCS expansion pool water below the minimum safe level.

The instruments provide necessary information to the operator for refilling the IC/PCCS pools following an accident. Safety-related water level sensors are included to allow ICS to automatically open the pool cross-connect valves between the equipment storage pool and the IC/PCCS expansion pools when a low water level is detected in either of the IC/PCCS inner expansion pools to provide makeup water to support design basis events, as discussed and evaluated in Subsection 7.4.4. The FAPCS also includes nonsafety-related IC/PCCS expansion pool level sensors for use by DPS as described in Subsection 7.8.1.2.5.

Spent Fuel Pool

The FAPCS provides the Spent Fuel pool with safety-related instruments that monitor water level. Each instrument generates a high and low water level signal when the water level reading increases above or decreases below its setpoint. Anti-siphoning holes are provided in all submerged portions of FAPCS discharge lines at the elevation of normal water level to prevent significant draining of the pool in the event of a pipe break. These level instruments are safety-related to ensure proper level is maintained.

The skimmer surge tanks are used for receiving overflow water from the spent fuel pool, and as a pump suction source during the spent fuel pool-cooling mode of operation. These tanks are provided with instruments that monitor their water level. The instruments generate high-high, high, low, or low-low water level signals when the water level reading increases above or decreases below its setpoint. The high and low level signals are used for the opening and closing of the Condensate Storage and Transfer System valve for make up water to skimmer surge tanks. The high-high and low-low signals initiate high and low water level alarms in the MCR. Additionally, the low level signal is used for tripping the FAPCS pump operating in the spent fuel pool-cooling mode. The high level setpoint is established to avoid overflow of skimmer surge tank water. The low water level setpoint is established to prevent inadvertent draining of the tank water below the minimum safe level.

The level instruments for the spent fuel pool are classified as safety-related components because they provide necessary information to the operator for performing the safety-related function of refilling the spent fuel pool following an accident.

Buffer Pool

The FAPCS provides the buffer pool with safety-related instruments that monitor water level. Each instrument generates low water level signals when the water level reading decreases below its setpoint. Each low-level signal initiates an alarm in the MCR.

The level instruments for the buffer pool are classified as safety-related components because they provide necessary information to the operator for refilling the buffer pool following an accident.

7.5.5.1 System Design Bases

See Subsection 9.1.3.1.

7.5.5.2 System Description

See Subsection 9.1.3.2.

7.5.5.3 Safety Evaluation

This subsection addresses Pool Monitoring Instrumentations conformance to regulatory requirements, guidelines, and industry standards.

7.5.5.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards Important to Safety:

- Conformance: The safety-related Pool Monitoring instrumentation design conforms to these standards.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603:

- Conformance: The safety-related Pool Monitoring instrumentation design conforms to IEEE Std. 603. Conformance information is found in Subsection 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the Pool Monitoring conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): Safety-related functions of the Pool Monitoring instrumentation are described in Subsection 7.5.5. The design bases for the instrumentation is included with the system that uses the signal from the sensor as shown below.
    - GDCS pools (Subsection 7.3.1.2.1),
    - IC/PCCS Expansion Pools (Subsection 5.4.6.1),
    - Spent Fuel Pool (Subsection 7.5.1.1), and
    - Buffer Pool (Subsection 7.5.1.1).
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are not applicable for the Pool Monitoring instrumentation design.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to Pool Monitoring instrumentation design.
  - Section 5.2 (Completion of Protective Actions): The Pool Monitoring instrumentation does not provide any trip or isolation functions.
  - Section 5.7 (Capability for Test and Calibration): See Subsection 9.1.3.4.
  - Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable beyond that discussed in Subsection 7.1.6.6.1.18.
  - Section 6.4 (Derivation of System Inputs): Derivation of System Inputs for Pool Monitoring instrumentation is not applicable beyond that discussed in Subsection 7.1.6.6.1.20.
  - Section 6.5 (Capability of Test and Calibration): See Subsection 9.1.3.4.
  - Section 6.6 and 7.4 (Operating Bypasses): Operating bypasses for the Pool Monitoring instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.22.

- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for Pool Monitoring instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for Pool Monitoring instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for Pool Monitoring instrumentation design are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The Pool Monitoring instrumentation design conforms to these standards.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident Monitoring Instrumentation:

- Conformance: The Pool Monitoring instrumentation design conforms to these requirements.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: The Pool Monitoring instrumentation design conforms to this requirement. The direct water-level instrument system provides for the detection of conditions indicative of inadequate core cooling (Refer to Table 1A-1 of Appendix 1A, Three Mile Island [TMI] Action Plan Items).

10 CFR 50.34(f)(2)(xix)[II.F.3], Instrumentation for Monitoring Plant Conditions Following Core Damage:

- Conformance: The Pool Monitoring instrumentation design conforms to this requirement. The Pool Monitoring instrumentation design conforms to RG 1.97.

10 CFR 50.34(f)(2)(xxiv)[II.K.3.23], Recording of Reactor Vessel Water Level:

- Conformance: The Pool Monitoring instrumentation design conforms to this requirement. (Refer to Table 1.A-1 of Appendix 1A TMI Action Plan Items).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) in Design Certification Applications:

- Conformance: ITAAC are provided for the Instrumentation and Control (I&C) systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the Pool Monitoring instrumentation within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.5.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, 34, 35, 38, and 63:

- Conformance: The Pool Monitoring instrumentation design conforms to these GDC.

7.5.5.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The Pool Monitoring instrumentation design conforms to RG 1.97, which endorses (with certain exceptions specified in Section C of the RG) IEEE Std. 497 that establishes flexible, performance-based criteria for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables. IEEE Std. 497 identifies five types of variables for accident monitoring and the criteria for the selection of each type of variable.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The Pool Monitoring instrumentation design conforms to RG 1.100. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The Pool Monitoring instrumentation design, in conjunction with the Q-DCIS, conforms to IEEE Std. 603.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The Pool Monitoring instrumentation design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.5.5.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of RG 1.97:

- Conformance: The Pool Monitoring instrumentation design conforms to RG 1.97 Revision 4, IEEE Standard 497-2002 (with clarifications and exceptions stated in RG 1.97 Revision 4), and RG 1.100.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the Pool Monitoring instrumentation design conforms to BTP HICB-16.

7.5.5.4 Testing and Inspection Requirements

See Subsection 9.1.3.4.

7.5.5.5 Instrumentation and Control Requirements

See Subsection 9.1.3.5.

7.5.6 (Deleted)

7.5.7 COL Information

None.

7.5.8 References

7.5-1 GE Nuclear Energy, “GE Nuclear Energy Quality Assurance Program Description”, NEDO 11209-04A, Class I (Non-proprietary), Revision 8, March 1989.

7.5-2 GE-Hitachi Nuclear Energy, “GEH ABWR/ESBWR Setpoint Methodology,” NEDE-33304P, Class III (Proprietary), Revision 1, November 2008, and NEDO-33304, Class I (Non-proprietary), Revision 1, November 2008.

Table 7.5-1

(Deleted)

Table 7.5-2

(Deleted)

Table 7.5-3

(Deleted)

Table 7.5-4

CMS Testing and Inspection Requirements

Specified Channel Calibration - Each oxygen and hydrogen gas sampling channel	0% gas concentration and nominal level from 0% to approximately 5%
Sample Gas Leakage Test - Sample lines and associated gas analyzer panel	Design leakage is less than 0.01cc/sec at peak sample pressure

Table 7.5-5

Instrument Ranges for Hydrogen/Oxygen Analyzers

Variable	Range
Drywell/Wetwell Hydrogen Concentration	0 to 30 Vol%
Drywell/Wetwell Oxygen Concentration	0 to 10 Vol%

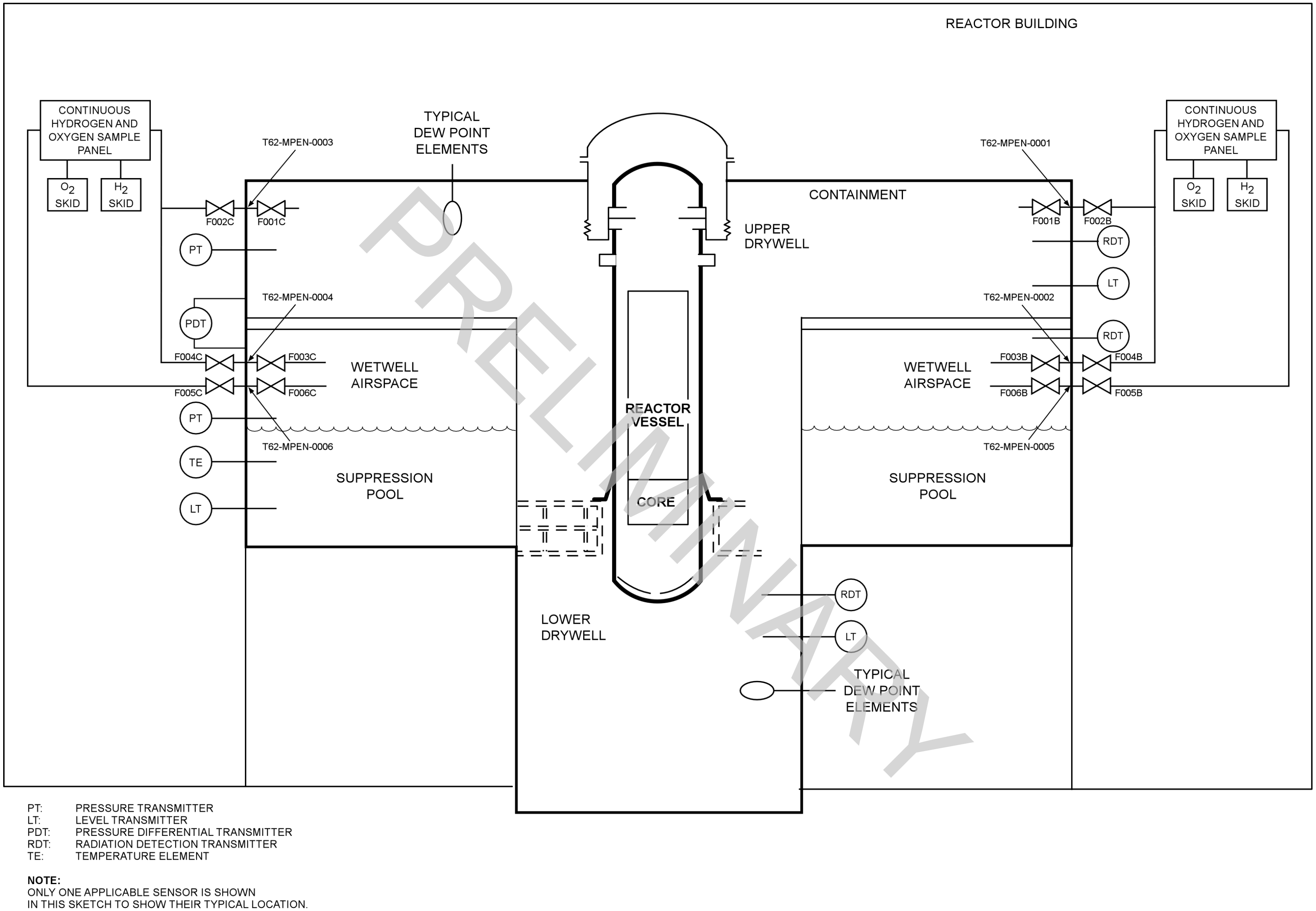


Figure 7.5-1. Containment Monitoring System Design

Figure 7.5-2. (Deleted)

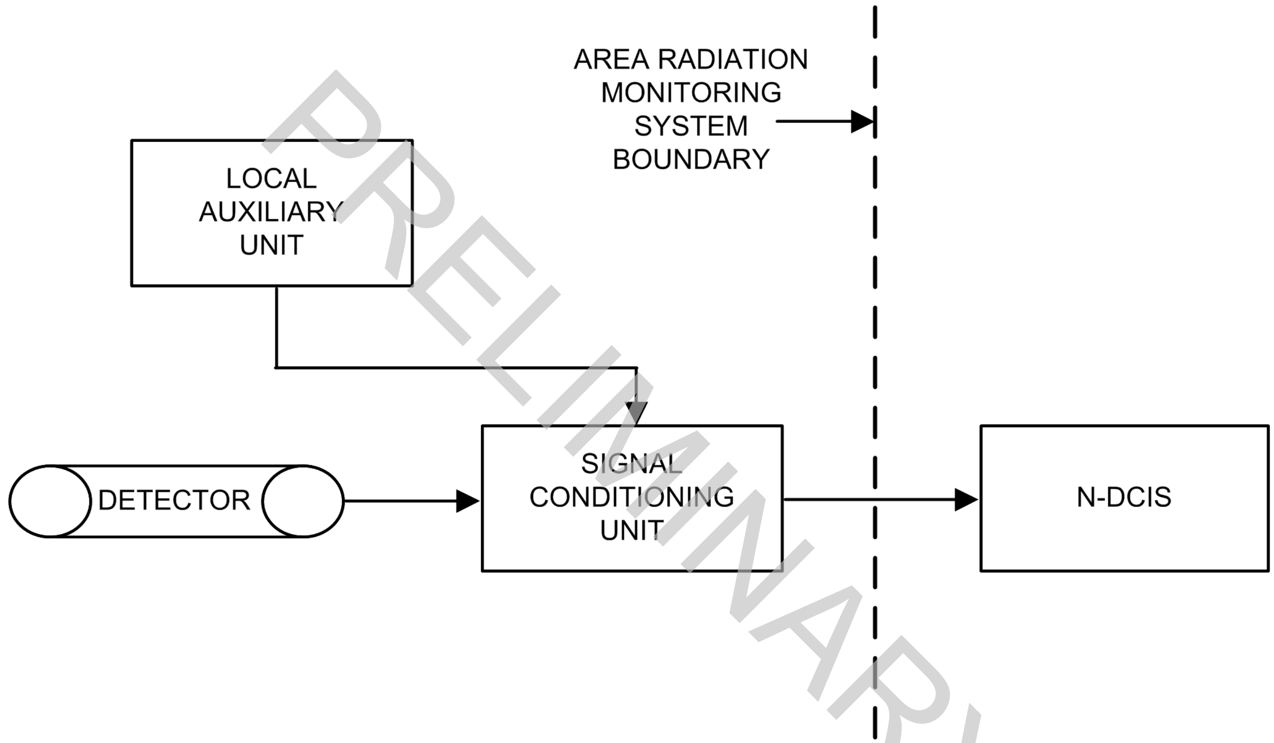


Figure 7.5-3. Area Radiation Monitoring System Functional Block Diagram

7.6 INTERLOCK LOGIC

In accordance with the Standard Review Plan (NUREG-0800), the High Pressure/Low Pressure interlock logic addressed in this section are "those interlock logics important to safety which operate to reduce the probability of occurrence of specific events or to maintain safety systems in a state to assure their availability in an accident" and are not addressed in other sections. While there are no ESBWR systems that meet this scope, this section includes discussion of the Low Pressure Coolant Injection (LPCI) High Pressure/Low Pressure (HP/LP) interlock logic that prevents over-pressurization of this low-pressure system which is connected to high pressure systems.

7.6.1 High Pressure/Low Pressure Interlock Logic

7.6.1.1 System Design Bases

The FAPCS HP/LP interlock logic prevents the operation of the LPCI mode of the FAPCS whenever there is a high pressure signal from the RPV pressure transmitters of the NBS by preventing the isolation valves from opening or closing them if opened. The high pressure signal also prevents testing of the air-operated testable check valves and closes them if they are open for testing. During reactor power operation, the high pressure in the RWCU/SDC system piping exceeds the design pressure of the low pressure FAPCS piping. The following subsections describe the nonsafety-related interlock logic provided to prevent over-pressurization of the FAPCS piping. The FAPCS design is discussed in Subsection 9.1.3. The reactor pressure instruments of the Nuclear Boiler System (NBS) are discussed in Subsection 7.7.1.

The Fuel and Auxiliary Pools Cooling System (FAPCS) is a low pressure piping system. It has the following interfaces with the high pressure Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) system.

- Its Low Pressure Coolant Injection (LPCI) line is connected to the RWCU/SDC system Loop B discharge line, which is connected to the Reactor Pressure Vessel (RPV) via the Feedwater Loop A discharge line.
- Crosstie connections are provided from the FAPCS suppression pool suction to the RPV RWCU line to the regenerative heat exchanger (RHX) (RWCU suction) and from the RWCU return line (discharge line to RPV) to the FAPCS discharge line to the suppression pool, Gravity-Driven Cooling System (GDCS) pools and containment spray line.

The only other HP/LP interface exists in the GDCS. Because the GDCS piping downstream of squib valves connected to the RPV has a design pressure equivalent to the reactor operating pressure, and the low pressure GDCS piping upstream of squib valves is open to the GDCS pools, there is no need for overpressure protection of the low pressure portion. A high pressure interlock logic is provided to prevent inadvertent manual initiation of the GDCS. The GDCS design basis is discussed in Subsection 7.3.1.2.

7.6.1.2 System Description

7.6.1.2.1 Function Identification

The LPCI line isolation valves consist of parallel pairs of air-operated, testable safety-related check valves and nonsafety-related motor-operated valves to protect the FAPCS low pressure piping from over-pressurization during reactor power operation. These valves are normally closed. Parallel valves are provided for redundancy and fire zone separation. Both sets of parallel valves have identical interlock logic for operation except that the power supplies for operation of these valves are provided from different sources, the Plant Investment Protection (PIP) systems PIP A and PIP B buses, for redundancy and fire zone separation. The logic for operation of the valves is implemented in the PIP A Nonsafety-related Distributed Control and Information System (N-DCIS) and PIP B N-DCIS. The FAPCS modes are described in Subsection 9.1.3.2. A safety relief valve is provided upstream of the LPCI line check valves to protect against over-pressurization of the pipe by leakage through the check valves. The relief valve discharge line is monitored to detect any leakage through the check valves.

The crosstie from the FAPCS to the RWCU/SDC system is used only following a Loss of coolant Accident (LOCA). No interlock logic exists between the low pressure FAPCS crosstie and the high pressure RWCU/SDC system. Refer to Subsection 5.4.8 for additional information.

7.6.1.2.2 Power Sources

The power supplies for nonsafety-related pressure instruments, logic, and solenoids (for operation of testable check valves) are provided by the PIP A N-DCIS and PIP B N-DCIS. The power supplies for operation of the LPCI line nonsafety-related motor operated parallel valves are provided from different sources, the PIP A and PIP B buses, for redundancy and fire zone separation. These nonsafety-related power supplies are backed up by nonsafety-related batteries and diesel generators. Refer to Subsection 8.3.2 for a description of the DC power supplies and Subsection 8.3.1 for a description of the AC power supplies.

7.6.1.2.3 (Deleted)

7.6.1.2.4 Logic Description

The high reactor pressure signals from the NBS processed in the N-DCIS are used to determine whether a high pressure condition exists in the RWCU/SDC discharge line to the RPV feedwater inlet line. If a high pressure condition exists the interlock system logic sends a signal to close the motor operated valves. This signal also prevents testing of the check valves and prevents the LPCI mode of operation of the FAPCS. The N-DCIS is described in Subsection 7.1.5.

7.6.1.2.5 (Deleted)

7.6.1.2.6 Bypasses and Interlocks

The HP/LP interlock logic design has no bypass.

7.6.1.2.7 Redundancy and Diversity

The LPCI line uses pairs of redundant isolation valves (a parallel pair of motor operated valves, a parallel pair of testable check valves). Each set of valves is installed in series and provides overpressure protection. Parallel valves provide redundancy and fire zone separation. Diversity is provided by a testable check valve, equipped with a pneumatic-assist actuator having a fail-closed feature and a motor-operated fail as-is, normally closed block valve.

7.6.1.2.8 Actuated Devices

The LPCI line motor operated, parallel isolation valves and air-operated, parallel, testable check valves are the actuation devices affected by the HP/LP interlock logic. Separate solenoids are used for controlling air to each of the testable check valve actuators. The solenoids for the parallel testable check valves are powered by the PIP A N-DCIS for the solenoid for one valve and the PIP B N-DCIS for the solenoid for the other parallel valve. The PIP A bus powers one of the parallel motor operated valves and the PIP B bus powers the other motor operated valve. The motor operated valves are fail as-is.

7.6.1.2.9 Separation

Electrical separation is provided by different power sources (PIP A and PIP B buses) with the logic separation provided by having implementation of valve operation in the PIP A N-DCIS and PIP B N-DCIS.

7.6.1.2.10 Testability

Testing of the reactor pressure instruments is discussed in Subsection 7.7.1.

Due to the high pressure interlock, the LPCI line isolation valves and check valves are stroke-tested only during low reactor pressure conditions. These valves are not subjected to the 10 CFR 50 Appendix J leak rate test, because they are neither containment isolation valves nor part of the Reactor Coolant Pressure boundary (RCPB). However, they are leak rate tested per American Society of Mechanical Engineers (ASME) Code Section XI.

7.6.1.2.11 Environmental Considerations

The instrumentation and controls (I&C) for the HP/LP interlock logic are classified as nonsafety-related equipment and qualified to the environmental conditions existing at the locations of the devices.

7.6.1.2.12 Operational Consideration

The HP/LP interlock logic prevents manual initiation of the LPCI mode of FAPCS until the RPV has been depressurized below the reactor pressure instrument setpoint for the HP/LP interlock logic.

7.6.1.2.13 Reactor Operator Information

The status of each valve providing the HP/LP boundary is indicated in the Main Control Room (MCR). The status of the pressure instruments also is indicated in the MCR.

7.6.1.2.14 Setpoints

The HP/LP interlock logic setpoint is based on the design pressure of the low pressure FAPCS piping.

7.6.1.3 Safety Evaluation

There is no HP/LP interface involving safety-related systems. There is a nonsafety-related HP/LP interface involving the low pressure FAPCS LPCI line, which interfaces with a high pressure condition in the RWCU/SDC system piping. The RWCU/SDC system piping interfaces with the feedwater line, which maintains the RCPB.

The parallel testable safety-related check valves provide protection to the low pressure FAPCS from the high pressure RWCU system. The motor-operated, normally closed, fail-as-is gate valves provide defense-in-depth protection against any leakage passing through the check valves. A safety relief valve is provided upstream of the testable check valves to protect against over-pressurization of the pipe by leakage through the check valves. The relief valve discharge line is monitored to detect any leakage through the check valves.

The interlock logic prohibits the LPCI line isolation valves from being opened whenever the reactor pressure is greater than the reactor pressure permissive setpoint for the interlock logic, thereby precluding over-pressurization of the low pressure FAPCS piping during reactor power operation. The interlock logic permits LPCI mode initiation when the reactor pressure is below its reactor pressure permissive setpoint allowing the operator to manually open either isolation valve. The interlock logic operates automatically, and its status is provided to the reactor operator in the MCR.

This subsection addresses conformance of the nonsafety-related HP/LP interlock logic to regulatory requirements, guidelines, and industry standards.

7.6.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The HP/LP interlock logic is nonsafety-related.

10 CFR 50.55a(h), Protection and Safety Systems compliance with IEEE Std. 603

- Conformance: The HP/LP interlock logic is nonsafety-related. 10 CFR 50.55a(h) and IEEE Std. 603 are not applicable.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The HP/LP interlock logic does not have a bypass feature.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), Inspections, Tests, Analyses and Acceptance Criteria (ITAAC) in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the interlock logic conforms to this criterion.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.6.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24 and 25:

- Conformance: Because the HP/LP interlock logic does not involve reactivity control, GDC 25 is not applicable. The interlock logic design complies with the remaining GDC listed above.

7.6.1.3.3 Regulatory Guides

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The HP/LP interlock logic does not have a bypass feature.

RG 1.53, Application of the Single Failure Criterion to Nuclear Power Protection Systems:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.53 is not applicable.

RG 1.75, Physical Independence of Electrical Systems:

- Conformance: The HP/LP interlock logic is nonsafety-related. The physical and electrical separations maintained between safety-related and nonsafety-related systems conform to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.105, Setpoints for safety-related Instrumentation:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.105 does not apply to the HP/LP interlock logic.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: The parallel safety-related testable check valves and parallel nonsafety-related motor-operated gate valves are stroke-tested only during low reactor pressure conditions due to the interlock logic.

RG 1.151, Instrument Sensing Lines:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.151 is not applicable.

RG 1.152, Criteria for use of computers in Safety systems of nuclear power plants.

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.152 is not applicable.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.153 is not applicable.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital computer software used in Safety systems of nuclear power plants:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.168 is not applicable.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.169 is not applicable.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.170 is not applicable.

RG 1.171, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.171 is not applicable.

RG 1.172, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.172 is not applicable.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.173 is not applicable.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The HP/LP interlock logic is nonsafety-related. RG 1.180 is not applicable.

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The HP/LP interlock logic is not a separate system RG 1.204 is not applicable.

7.6.1.3.4 Branch Technical Positions

BTP HICB-1, Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System:

- Conformance: Because the motor operated valves are normally closed and are interlocked as described above, and the check valves are tested only when the reactor pressure is below the permissive setpoint for the interlock, the nonsafety-related HP/LP interlock logic design conforms to BTP HICB-1.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices:

- Conformance: The HP/LP interlock logic is not an isolation device. BTP HICB-11 is not applicable.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints:

- Conformance: The HP/LP interlock logic is nonsafety-related. BTP HICB-12 does not apply to the HP/LP interlock logic.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The HP/LP interlock logic is nonsafety-related so BTP HICB-14 does not apply.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the HP/LP interlock logic conforms to BTP HICB-16.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions:

- Conformance: The HP/LP interlock logic is nonsafety-related. The motor operated valves and testable check valves are stroke-tested only during low reactor pressure because of the interlock. No surveillance tests are conducted.

BTP HICB-18, Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems.

- Conformance: The HP/LP interlock logic is nonsafety-related. BTP HICB-18 is not applicable.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The HP/LP interlock logic is nonsafety-related. BTP HICB-21 does not apply to the HP/LP interlock logic.

7.6.1.3.5 Three Mile Island Action Plan Requirements

In accordance with NUREG-0800 Section 7.6 and Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3) applies to the HP/LP interlock system and is addressed above. Three Mile Island (TMI) action plan requirements are generically addressed in Appendix 1A.

7.6.1.4 Testing and Inspection Requirements

HP/LP interlock logic functions are calibrated and tested during the preoperational testing program to confirm that the HP/LP interlock logic functions as designed

Testing and inspection of the NBS system pressure instruments are described in Subsection 7.7.1.4.

The parallel safety-related testable check valves and parallel nonsafety-related motor-operated gate valves are stroke-tested only during low reactor pressure conditions due to the interlock logic.

7.6.1.5 Instrumentation and Control Requirements

The following information is available to the reactor operator for the instrumentation and interlock logic described in this subsection.

- The reactor pressure is indicated in the MCR and at four local racks in the Reactor Building outside the containment.
- HP/LP interlock logic status is indicated in the MCR and is alarmed when any LPCI valve is open and the interlock logic is active.
- The open and closed positions of the isolation valves and check valves are indicated in the MCR.

7.6.2 (Deleted)

7.6.2.1 (Deleted)

7.6.3 COL Information

None.

7.6.4 References

7.6-1 (Deleted)

7.7 CONTROL SYSTEMS

This section describes the Instrumentation and Control (I&C) systems for normal plant operation that do not perform plant safety-related functions. However, these systems do control plant processes that have a significant effect on plant safety. These systems can affect the performance of safety-related functions either through normal operation or through inadvertent operation. The systems described in this section include:

- The Nuclear Boiler System (NBS) – nonsafety-related subsystems,
- Rod Control and Information System (RC&IS),
- Feedwater Control System (FWCS),
- Plant Automation System (PAS),
- Steam Bypass and Pressure Control (SB&PC) System,
- Neutron Monitoring System (NMS) - nonsafety-related subsystems, and
- Containment Inerting System (CIS).

The nonsafety-related monitoring and control for the RC&IS, FWCS, PAS, SB&PC System, NMS and NBS is part of a group of systems that is collectively referred to as the Nonsafety-Related Distributed Control and Information System (N-DCIS). A simplified network functional diagram of the DCIS is included as Figure 7.1-1. This diagram indicates the relationships of RC&IS, FWCS, PAS, SB&PC System, NMS and NBS with their nonsafety-related peers and with safety-related plant data systems that are collectively referred to as the Q-DCIS. Section 7.1 contains a description of these relationships.

7.7.1 Nuclear Boiler System

The NBS instrumentation provides monitoring and control input for operational variables during normal plant operating modes and during the plant response to accidents. The NBS sensors used for safety-related system actuation and control functions are addressed in other subsections within this chapter. This subsection describes only those NBS instruments used for actuation and control of nonsafety-related systems.

7.7.1.1 System Design Bases

7.7.1.1.1 Safety Design Bases

Section 7.7 addresses only the nonsafety-related portion of the NBS instruments.

7.7.1.1.2 Power Generation (Non-safety) Design Bases

The nonsafety-related portions of the NBS instrumentation meet power generation requirements by providing indication of parameters in support of normal plant operations. These parameters are:

- Reactor coolant and RPV temperatures;
- RPV water level:

- Shutdown range,
- Narrow range,
- Wide range, and
- Fuel zone range.

- RPV pressure;
- Safety relief valve discharge line temperature; and
- Main steam flow rate.

The NBS design provides for periodic calibration and testing of its instrumentation during plant operation.

7.7.1.2 System Description

7.7.1.2.1 Summary Description

The NBS instruments are used to provide the operator with information during normal, transient, accident, and post-accident conditions. The NBS instruments measure the reactor coolant temperature, RPV temperature, RPV water level, RPV pressure, main steam flow rate, and detect SRV leakage.

Nonsafety-related instruments are powered from the nonsafety-related instrument power supply buses.

For instruments that are located below the process tap, including the RPV water level measurements, the sensing line slopes downward from the process tap to the instrument to preclude air traps. Where it is impractical to locate the instruments below the process connection, the sensing lines descend below the process connection before sloping upward to a high point vent located at an accessible location with a fill connection. This permits filling and venting of noncondensible gases from the sensing line during calibration procedures.

Level and pressure sensing lines, up to the outboard excess flow check valve, are connected to the Reactor Coolant Pressure Boundary (RCPB) and are classified as Quality Group A, ASME Section III, safety-related, and Seismic Category 1. The typical arrangement for these sensing lines is a restricting orifice located inside the containment and a manual isolation valve located outside the containment, which is followed by an excess flow check valve.

7.7.1.2.2 Detailed System Description

Reactor Coolant and Reactor Pressure Vessel Temperature Monitoring System

The reactor coolant temperature is measured at the mid-vessel inlet to the Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) system and at the bottom head drain. Coolant temperature can also be determined in the steam-filled parts of the RPV and steam-water mixture by measuring the reactor pressure. In the saturated system, reactor pressure connotes saturation temperature. Coolant temperatures (core inlet temperature) can normally be measured by the redundant core inlet temperature sensors located in each Local Power Range Monitor (LPRM) assembly below the core plate elevation.

The RPV outside surface temperature is measured at the head flange and at the bottom head locations. Temperatures needed for operation and for compliance with the Technical Specification operating limits are obtained from these measurements.

Reactor Pressure Vessel Water Level

Figure 7.7-1 shows the water level range and the vessel penetrations for each water level range. The instruments are differential pressure devices calibrated for the specific vessel pressure and liquid temperature conditions. The reactor water level measurement is temperature compensated through the thermocouples installed on the sensing line. As described in Subsection 4.6.1.2.4, the Control Rod Drive Hydraulic Subsystem provides a purge flow that keeps the RPV water level reference leg instrument lines full. These lines are filled to address the effects of noncondensible gases in the instrument lines and to prevent erroneous reference information after a rapid RPV depressurization event. The reactor water level instrumentation is referenced to level zero, which is at the Top of Active Fuel (TAF).

Reactor water level instrumentation that initiates safety-related system functions and engineered safety features (ESF) system functions is discussed in Subsections 7.2.1 and 7.3.1. Reactor water level instrumentation that is used as part of the FWCS is discussed in Subsection 7.7.3. Reactor water level instrumentation used for Diverse Protection System (DPS) functions is discussed in Subsection 7.8.1.

The Shutdown Range Water Level is used to monitor the RPV water level during shutdown conditions when the RPV head is removed, including when the reactor system is flooded for refueling or maintenance. The water level measurement design method is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. The vessel temperature and pressure conditions that are used for the calibration are given in Section 5.1. The two vessel instrument nozzles used for this water level measurement are located at the top of the RPV head and just below the bottom of the dryer skirt.

The Narrow Range Water Level uses the RPV taps near the top of the steam outlet nozzle and the taps near the bottom of the dryer skirt. The instruments are calibrated to be accurate during normal reactor operating conditions. The method of water level measurement is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. The FWCS uses this range for its water level control and indication inputs. Refer to Subsection 7.7.3 for more information on the FWCS.

The Wide Range Water Level uses the RPV taps below the bottom of the active fuel. The upper taps are also used for the Narrow Range Water Level. The instruments are calibrated to be accurate at normal power operating conditions. The water level measurement method is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. Information from the RPV Wide Range Water Level instrumentation is used for safety-related and nonsafety-related applications, for DPS, and is provided for the range of normal, transient, and accident conditions. Separate sensors and indicators are provided for Wide Range Water Level indication.

The Fuel Zone Range Water Level uses the RPV taps near the top of the steam outlet nozzle and the taps below the bottom of the active fuel. The instruments are calibrated to be accurate at zero Pa gauge (0 psig) and saturated conditions. The water level measurement method is the condensing chamber reference type and uses differential pressure devices as its primary elements. The RPV Fuel Zone Water Level instrumentation is provided for post-accident monitoring situations in which the water level is substantially below the normal range. Separate sensors and indicators are provided for Fuel Zone Range Water Level indication.

Reactor Pressure Vessel Pressure

Pressure transmitters detect RPV pressure from the instrument lines used for measuring RPV water level and provide indications in the Main Control Room (MCR).

Safety Relief Valve Leak Detection

Thermocouples are located in the discharge pipes of ten Safety Relief Valves (SRVs) (Reference Subsection 5.2.5). The temperature signals are recorded, and temperatures indicative of a leaking SRV are alarmed in the MCR.

Main Steam Flow Rate

Differential pressure transmitters are used to infer main steam flow rate. Pressure taps from the throat of the RPV steam outlet nozzles, in conjunction with the RPV dome pressure taps, measure differential pressure. The square root of differential pressure is proportional to the main steam flow rate. Outputs from nonsafety-related transmitters are used for feedwater (FW) control.

7.7.1.3 Safety Evaluation

Section 7.7 addresses only the nonsafety-related portion of the NBS instruments.

The nonsafety-related instruments discussed in this subsection are designed to operate under normal and peak operating conditions of system pressure and at ambient pressures and temperatures. Any mechanical interface between nonsafety-related instruments and safety-related instrument piping or the RCPB is classified as safety-related to avoid compromise of the safety-related sensing capability and/or the RCPB. If a line break occurs in a nonsafety-related portion of a sensing line, the excess flow check valve closes to stop the flow of reactor coolant. If there is a single failure of the excess flow check valve, a restriction orifice limits the flow of coolant to within acceptable bounds.

7.7.1.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards Important to Safety:

- Conformance: The NBS conforms to these criteria, as shown by the following commitments to applicable Regulatory Guides (RG) and standards.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The NBS design conforms to these requirements.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate Core Cooling Instrumentation:

- Conformance: Reactor water level instrumentation errors due to non-condensable gases in instrument reference legs are addressed in Subsection 7.7.1.2.2.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the NBS within the DCD conforms to this regulation.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The I&C design does not use innovative means for accomplishing safety functions.

7.7.1.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24:

- Conformance: The NBS design complies with these GDC.

7.7.1.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RGs 1.151, Instrument Sensing Lines:

- Conformance: The instrument sensing lines for the NBS instrumentation conform to the guidelines of RG 1.151 and ISA-67.02.01. Flow restrictors are provided inside containment on instrument lines connected to the RCPB. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISA-67.02.01 and RG 1.151 are met as applicable for each installation.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.

- Conformance: The NBS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The NBS design conforms to RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.1.3.4 Branch Technical Positions

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for this system complies with BTP HICB-16.

BTP HICB-14, 17, 18, 19, and 21 are discussed in association with the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) in Subsection 7.3.5.3.

7.7.1.4 Testing and Inspection Requirements

Calibration and testing of the various instruments are performed during preoperational testing to confirm that the instrumentation is installed correctly and performs as intended.

Pressure, differential pressure, water level, and flow instruments are located outside the drywell so that calibration and test signals can be applied during reactor operation. Temperature elements located inside the drywell can be tested and calibrated from junction boxes located outside the drywell .

7.7.1.5 Instrumentation and Control Requirements

The information available to the reactor operator from the NBS instrumentation is discussed in Section 7.1.

7.7.2 Rod Control and Information System

The main objective of the RC&IS is to control the Fine Motion Control Rod Drive (FMCRD) motors of the Control Rod Drive (CRD) (explained in Subsections 4.6.1 and 4.6.2) to permit changes in core reactivity so that reactor power level and power distribution can be controlled. The RC&IS acquires status and control rod position information from the CRD FMCRD instrumentation. The RC&IS sends purge water valve control signals to and acquires status signals from the Hydraulic Control Units (HCUs) of the CRD. The RC&IS also sends and receives status and control signals to and from other plant systems and RC&IS modules.

7.7.2.1 System Design Bases

7.7.2.1.1 Safety Design Bases

The RC&IS has no functional safety-related design basis and is designed so that it does not adversely affect functional capabilities of safety-related systems.

7.7.2.1.2 Power Generation (Non-safety) Design Bases

The RC&IS performs the following functions.

- Controls changes to core reactivity, and thereby reactor power, by moving neutron absorbing control rods within the reactor core as initiated by the following.
  - The plant operator, when the RC&IS is in a manual or semiautomatic mode of operation.
  - The automatic rod movement mode of the PAS, when the RC&IS is in an automatic mode of operation.
- Displays summary information to the plant operator about positions of the control rods in the core and the status of the FMCRDs and RC&IS. This summary information is provided by a RC&IS dedicated operator interface in the MCR. There are dual redundant measurements of the absolute rod position during normal FMCRD conditions. If one position detector fails for an individual FMCRD, the failed position detector can be bypassed, and the reactor can continue to operate without power restrictions.
- Provides RC&IS and FMCRD status data and control rod position data to other plant systems that require this data, such as the N-DCIS.
- Provides automatic, electric motor Run-in of all operable control rods, following detection of activation of the hydraulic insertion of the control rods, by a reactor scram. This is called the scram-follow function.
- Automatically enforces rod movement blocks to prevent potentially undesirable rod movements. These blocks do not affect a hydraulic scram insertion function, the scram-follow function, the alternate rod insertion (ARI) function, or the Selected Control Rod Run-in (SCRRI) function.
- Manually and automatically inserts all control rods by an alternate and diverse method called the FMCRD motor Run-in function. The associated ARI activation signals, which are activated if the automatic or manual ARI function is activated by the N-DCIS logic, are provided to the RC&IS from the N-DCIS. The RC&IS logic is designed so that a single failure in the single-channel FMCRD control logic and equipment associated with one FMCRD, cannot result in insertion failure of that rod when the ARI function is activated.
- Inserts selected control rods upon Select Control Rod Run-in (SCRRI) / Select Rod Insertion (SRI) command signals from the DPS. Manual initiation capability is also provided in the MCR. The RC&IS also sends a confirmatory SCRRI signal to the DPS to initiate an SRI.

- Ensures that the pattern of control rods in the reactor is consistent with specific control rod pattern restrictions. This function is performed by the Rod Worth Minimizer (RWM) subsystem of the RC&IS and is only effective when reactor power is below the Low Power Setpoint (LPSP).
- Enforces fuel operating thermal limits Minimum Critical Power Ratio (MCPR) and Maximum Linear Heat Generation Rate (MLHGR) when reactor power is above the ATLM enable setpoint. This function is performed by the Automated Thermal Limit Monitor (ATLM) subsystem of the RC&IS.
- Provides for FMCRD-related surveillance tests, including periodic individual HCU scram performance testing.
- Enforces adherence to a predetermined rod pull/insert sequence, the Reference Rod Pull Sequence (RRPS), during automatic and semi-automatic rod movements, through the capabilities of the gang rod selection and verification logic of the Rod Action and Position Information (RAPI) subsystem.

7.7.2.2 System Description

A simplified, typical RC&IS block diagram is shown in Figure 7.7-2 that depicts the major components of the RC&IS and their interconnections and interfaces with other plant systems.

7.7.2.2.1 System Configuration

The RC&IS uses a dual redundant architecture of two independent channels for normal monitoring of control rod positions and executing normal control rod movement commands. Under normal conditions, each channel receives separate input signals, and both channels perform the same functions. The outputs of the two channels are continuously compared. For normal functions of enforcing and monitoring control rod positions and emergency rod insertion, the outputs of the two channels must agree. Any sustained disagreement between the two channels results in a rod block. However, when the conditions for generating a rod block signal in a single channel are satisfied, that channel alone (independent of the other channel) issues a rod block signal.

For the FMCRD emergency insertion functions, 3-out-of-3 logic is used in the induction motor controller logic. To assure high reliability for the emergency insertion function, a single RC&IS bypass is automatically enabled with the ARI signal.

Failure or malfunction of the RC&IS has no effect on the hydraulic scram function of the CRD. The circuitry for normal insertion and withdrawal of control rods in the RC&IS is completely independent of the Reactor Protection System (RPS) circuitry controlling the scram valves. This separation of the RPS scram and the RC&IS normal rod control functions prevents any failure in the RC&IS circuitry from affecting the scram circuitry.

The RC&IS consists of multiple types of cabinets, or panels, that contain special electronic/electrical equipment modules for performing the RC&IS logic in the RB and Control Building (CB). It also includes a dedicated operator interface on the main control panel in the MCR. The RC&IS dedicated operator interface provides summary information to the plant operator with respect to control rod positions, FMCRD, RC&IS status, and HCU status. The RC&IS also provides controls for performing normal rod movement functions, bypassing major RC&IS subsystems, performing CRD surveillance tests (except the FMCRD holding brake testing performed during a refueling outage), resetting RC&IS trips and most abnormal status conditions. A few abnormal status conditions require reset actions at local control panel equipment. There are nine types of electronic/electrical cabinets/panels that perform the logic functions of the RC&IS:

Rod Action Control Subsystem Cabinets

There are two types of cabinets in the back-panel area referred to as the Rod Action Control System (RACS). The RACS consists of RAPI panels and an ATLM/RWM panel, which provides for a dual redundant architecture. The RAPI panels are RAPI-A and -B. The channel A logic is in the RAPI-A panel, and the channel B logic is in the RAPI-B panel. In addition, the RAPI-A panel includes the RAPI dedicated operator interface that displays the same information that is available on the RC&IS dedicated operator interface in the MCR. The RAPI dedicated operator interface also serves as a backup for the RC&IS dedicated operator interface control capabilities, should the RC&IS dedicated operator interface become unavailable. A hard-wired switch located in the RAPI-A panel changes the selection of dedicated operator interface control operation capability between the RC&IS dedicated operator interface and the RAPI dedicated operator interface. In other words, only one of these dedicated operator interfaces can be selected for control capability at any given time. Normally, the RC&IS dedicated operator interface rather than the RAPI dedicated operator interface is selected for control functions.

The two ATLM/RWM panels each contain channel logic for the ATLM, the RWM and the RAPI Signal Interface Unit (SIU).

Remote Communication Cabinets

The remote communication cabinets are located in sets with each set containing a dual channel File Control Module (FCM). The FCMs interface with the Rod Server Modules (RSMs) that are contained in the same set of cabinets, and interface with the RAPI subsystems in the MCR, through the RC&IS multiplexing network. Each RSM comprises logic for two Rod Server Processing Channels (RSPCs A and B) so that there is a dual redundant logic design for each RSM. There are also associated Resolver-to-Digital Converters (RDCs A and B) that convert the Resolver A and Resolver B analog signals of the CRD system into two independent digital representations of the absolute position of the corresponding FMCRD.

Both RSPCs receive the digital representations from both RDCs for use in the RSPC control and monitoring logic. The logic for each channel of the RSPC can either be located in the associated FCM channel equipment or located in a separate, replaceable RSPC module located in the remote communication cabinet. Figure 7.7-2 shows a typical representation with the logic of each RSPC channel implemented in a separate RSPC module. However, regardless of the final detailed remote communication cabinet hardware configuration for RSPC logic implementation, channel A RSPC logic is implemented in equipment separate from the equipment in which the channel B RSPC logic is implemented, to maintain tolerance for single channel failures.

Induction Motor Controller Cabinets

The Induction Motor Controller Cabinets (IMCCs) consist of motor control equipment required for turning on and off the Alternating Current (AC) power required to energize the FMCRD 3-Phase motor and its directly associated Motor Built-in Brake (MBB) to perform FMCRD movements. The control capability includes AC phase swapping, of the 3-phase AC power supplied to each motor, so that both insertion and withdrawal movements of each FMCRD can be accomplished. The MBB accurately positions each FMCRD. The de-energization of this brake, promptly after AC power is turned off by the motor control, prevents excessive movement after the desired stopping position has been reached. Each motor controller includes logic to process rod movement commands received from the logic of the associated RSPCs in a remote communication cabinet. Each motor control also provides status signals to the associated RSPCs. All motor controls also receive a separate discrete input signal from an Emergency Rod Insertion Control Panel (ERICP) used in the logic for providing the emergency rod insertion movement functions (that is scram-follow, ARI, or SCRRI).

Rod Brake Controller Cabinets

The Rod Brake Controller Cabinets (RBCCs) contain electrical and/or electronic logic and other associated electrical equipment for the proper operation of the FMCRD holding brakes. The Rod Brake Controllers (RBCs) receive signals for brake disengagement or engagement from the logic of the associated RSPCs. RBC logic provides two separate brake status signals (channel A and channel B) to the logic of the associated RSPCs.

Emergency Rod Insertion Control Panel

The ERICP is located in the back-panel area of the MCR. It serves as an additional logic panel that contains relay (or solid-state equivalent) hardware needed to transmit discrete output signals to the ERIP in the RB. The discrete output signals are activated by input signals received from the RPS (that indicate a scram-follow function is active) or based upon input signals received from the N-DCIS (that indicate a ARI function or automatic SCRRI function is active) or by input signals from the two manual SCRRI pushbuttons on the Main Control Room Panel (MCRP).

Emergency Rod Insertion Panels

The emergency rod insertion panels (ERIP) are located in the RB and provide discrete output signals to the induction motor controllers in the IMCCs. The discrete output signals are activated by input signals received from the ERICP that indicate the scram-follow function, the ARI function or the SCRRI function is active.

Scram Time Recording Panels

The Scram Time Recording Panels , located in the RB, monitor the FMCRD position reed switch status using Reed Switch Sensor Modules (RSSMs). They communicate this information to the RAPI through the RC&IS multiplexing network. Also, the Scram Time Recording Panels automatically record and time tag FMCRD scram timing position reed switch status changes. This is done either after initiation of an individual HCU scram test at the RPS Scram Time Test Panel or after a full-core reactor scram has been initiated. The recorded scram timing data can be transmitted to the scram time recording and analysis panel (STRAP) in the MCR back-panel area.

Scram Time Recording and Analysis Panel

The STRAP receives scram timing position information from the Scram Time Recording Panels and performs scram timing performance analysis. The recorded performance information can also be transmitted to the N-DCIS equipment for further data analysis and archiving.

RAPI Auxiliary Panels

RAPI Auxiliary Panels, located in the RB, provide output signals to open a purge water valve whenever either FMCRD associated with the corresponding HCU receives an insertion command from the RAPI subsystem. These panels also monitor scram valve position status as well as whether the scram accumulator water pressure and level status are normal or abnormal. Communication of this information to and from the RAPI subsystem is achieved through the N-DCIS equipment. Two or more of the nonsafety-related remote multiplexing unit (RMU) cabinets of the N-DCIS equipment are used as the RAPI auxiliary panels that are physically not part of the RC&IS equipment, even though they provide the RC&IS related functions described above.

7.7.2.2.2 Multiplexing Network

The RC&IS multiplexing network consists of two separate channels that use fiber optic communication links. The first channel handles communication between the RACS and the RSPCs in the remote communication cabinets (through the FCMs), and communication between the Scram Time Recording Panels and the RACS. The second channel handles communication between the Scram Time Recording Panels and the STRAP. Communication between the RAPI auxiliary panels, for HCU purge water valve control and HCU status monitoring, and the RAPI channels is achieved by the N-DCIS equipment, not the RC&IS multiplexing network.

The plant Q-DCIS communication equipment interfaces with FMCRD dual redundant separation switches (A and B). It provides the appropriate status signals to the RACS cabinets used in the RC&IS logic for initiating rod block signals of the appropriate FMCRD if a separation occurs. The Q-DCIS communication equipment provides these signals to the RAPI SIUs of the RC&IS via communication with the N-DCIS through proper isolation. Refer to Subsection 7.1.3.3. The Q-DCIS and N-DCIS communication equipment is not part of the RC&IS equipment. Each RAPI SIU transmits status signals to the associated RAPI channel for use in the RAPI rod block logic.

7.7.2.2.3 Classification

The RC&IS is not classified as a safety-related system because it has a control design basis only and is not required for the safe and orderly shutdown of the plant. A failure of the RC&IS cannot result in gross fuel damage. The rod block function of the RC&IS, however, is important in limiting the potential consequences of a rod withdrawal error during normal plant operation, because it prevents an abnormal operating transient that might result in local fuel damage.

7.7.2.2.4 Power Sources

The Low Voltage Distribution System normally provides the required incoming 3-phase AC power for the induction motor controllers equipment. This 3-phase AC power source is required by the IMCCs to energize the associated FMCRD induction motors and MBBs. The Low Voltage Distribution System also provides the required AC power for the RBC power supplies in the RBCCs, the ERIPs and the associated ERICP. The Medium Voltage Distribution System power bus and equipment design assures that the associated Low Voltage Distribution System equipment that provides required AC power to the IMCCs, RBCCs, and ERIPs is automatically powered from the standby AC diesel generators if the normal power source is lost. Excitation power required for logic in the ERICP is provided directly from the ERIPs.

The power distribution design provides four distinct electrical groups of power. The distribution of these four groups of electrical power to FMCRDs is such that approximately one fourth of the FMCRDs belong to each group. The FMCRDs in each electrical group are distributed throughout the reactor core so complete insertion of the FMCRDs (in any three of the four electrical groups to the full-in position) assures that the reactor reaches shutdown conditions. This approach provides increased reliability for the capability of the FMCRD motor Run-in function, if activated, to ensure that the reactor achieves shutdown conditions.

The power for all RC&IS equipment, except as noted above, is derived from two separate, non-divisional AC power sources (See Chapter 8) with at least one of the redundant AC power sources being a UPS. Redundant power supplies are also provided for this equipment so that failure of a single power source or of a single power supply does not result in the complete loss of capability of the RC&IS to perform rod movements. For certain types of power sources or supply failures, the operator has to perform appropriate bypass of the affected RC&IS equipment in order to restore rod movement capability.

On the loss of the normal power source, the nonsafety-related standby diesel generators provide an alternate power source for the IMCCs, RBCCs, and ERIPs.

7.7.2.2.5 Scope

The equipment in the RC&IS scope includes:

- The electrical/electronic equipment contained in the RACS cabinet, the remote communication cabinets, the IMCCs, the RBCCs, the Scram Time Recording Panels, the STRAP, the ERIPs, and the ERICP. (Note: RAPI auxiliary panels are designated as part of the N-DCIS);
- The RC&IS multiplexing network equipment;
- The cross-channel communication links between equipment located in the RACS cabinets; and
- The dedicated RC&IS dedicated operator interface and the communication links from the RACS cabinets to this interface.

7.7.2.2.6 Cabinet Subsystems

The RACS cabinets each have four identical dual-channel subsystems: the RAPI, the RWM, the ATLM, and the RAPI SIU. This subsection describes the key functions performed by the RAPI and RWM subsystems.

The RAPI is the primary RC&IS equipment that performs the following functions.

- Accepts and responds appropriately to manual, semi-automatic, and automatic rod movement commands.
- Enforces rod blocks based upon signals, internal and external, to RC&IS. Internal RC&IS signals include those initiated from either of the two channels of rod blocks initiated by signals from the ATLM, RWM, RAPI SIU equipment, and those caused by any RAPI two-channel disagreement. External input signals to each RAPI channel that are used for the rod block logic originate from:

- The safety-related four divisions of the RPS (required isolation provided by RPS related equipment);
- The safety-related four divisional Startup Range Neutron Monitor (SRNM) and Average Power Range Monitor (APRM) subsystems of the NMS (required isolation provided by the NMS);
- The safety-related FMCRD dual redundant separation switches (A & B) of each control rod through Divisions 1 and 2 of the Q-DCIS communication (required isolation is provided by fiber optic cable and one way communication links to the N-DCIS equipment);
- The nonsafety-related dual-channel Multi-Channel Rod Block Monitor (MRBM) of the NMS; and
- Refueling equipment.

- Enforces adherence to a predetermined rod pull sequence that is stored in RRPS memory. The RRPS memory defines the order in which gangs of control rods are selected and moved when either semi-automatic or automatic rod movements are performed (that is the equivalent to the pull sheet used by plant operators when performing manual rod movements for conventional Boiling Water Reactor (BWR) plants. Violation of the RRPS causes RAPI logic to issue:
  - A switch to manual mode when the RC&IS is in the automatic rod movement mode or the semi-automatic rod movement mode.
  - An alarm signal when the RC&IS is in the manual rod movement mode. (Gangs of rods can still be moved while in manual mode, but are limited to the RRPS gangs and only one gang at a time can be moved.)
- Provides control rod position and FMCRD status information to the N-DCIS, the NMS, the RWM, and the ATLM. The RAPI transmits signals required by the NMS, ATLM, and RWM to the associated RAPI SIU. The RAPI SIU then transmits required status signals to both channels of the ATLM, RWM, and the MRBM channels of the NMS.
- Provides the scram-follow function that automatically activates motor run-in of the ballnuts of all operable FMCRDs to the normal full-in position after a reactor scram has occurred. If the rapid hydraulic insertion function for any FMCRD does not work properly, this function provides an electric motor driven backup means to achieve full insertion of all operable FMCRDs.
- Provides the SCRRI function that results in automatic insertion of predefined control rods to specified target insertion positions so that required reactor power reduction is achieved when this function is activated. The RC&IS also sends a SCRRI signal to the DPS to initiate the SRI function.
- Provides for FMRCD motor Run-in of all control rods based on the receipt of the ARI initiation signals from the N-DCIS.
- Sends/receives rod movement commands, rod position, FMCRD status information and RC&IS related status information from the logic of all of the RSPC (A & B) of each

RSM in the remote communication cabinets, by means of FCMs and the RC&IS multiplexing network. The RAPI also receives FMCRD position reed switch status information from the Scram Time Recording Panels by means of the RC&IS multiplexing network.

- Sends and receives information and control signals to and from the other RAPI channel.
- Sends HCU purge water valve control signals to, and receives HCU status signals from, the N-DCIS equipment.
- Provides for different CRD surveillance tests, including:
  - Scram Time Test,
  - Coupling Check Test, and
  - Double-Notch Test.
- Enforces the applicable RWM rod block by sending appropriate rod block signals to the logic of the RSPCs in the remote communication cabinets. Either channel of RWM can cause a rod block independently.

The RWM issues a rod withdrawal block signal and a rod insertion block signal that are used in the RAPI rod block logic. This rod block signal ensures the following.

- Absolute rod pattern restrictions, called the Ganged Withdrawal Sequence Restrictions (GWSR) when reactor power is below the LPSP, are not violated. This is only applicable when the RPS Reactor Mode Switch is in either the Startup or Run position. The GWSR assure that control rod worths are maintained to within reasonable values by only allowing rod patterns that result in relatively low rod worths when control rods are withdrawn.
- Only the two control rods associated with the same HCU can be withdrawn for the 2-CRD scram time test when the RPS Reactor Mode Switch is in the Refuel position and the scram test mode has been activated. This function provides for performing individual HCU scram testing during planned refueling outages.

The RWM also includes logic for performing shutdown margin testing when the RPS Reactor Mode Switch is in the Startup position. This mode allows only a limited set of pre-specified control rods to be withdrawn to perform this special testing.

The ATLM issues internal rod withdrawal block signals within RC&IS. These signals, when the RC&IS is in the Automatic rod movement mode, cause the RC&IS to transfer to the manual rod movement mode. The ATLM-based rod block prevents violation of normal operating limit restrictions on fuel thermal limit values, (MCPR and MLHGR operating limits) if operations stay in the automatic mode. The ATLM algorithm is based upon input signals from the LPRMs and APRMs of the NMS and control rod positions and status data and other plant data from the RAPI signals transmitted from RAPI channels via the RAPI SIUs. The ATLM operating limit setpoints can be updated based upon calculated inputs from the core monitoring function of the N-DCIS. Updates of the ATLM setpoints can occur automatically or they can occur manually when the operator uses the N-DCIS VDU capabilities to request a manual ATLM update. Either channel of the ATLM can independently cause transfer to the Manual mode from the Automatic mode and rod withdrawal block initiation.

7.7.2.2.7 Operation Description

7.7.2.2.7.1 Single Rod Movements

Though this mode of rod movement is not normally used, the capability exists for the plant operator to perform manual movements of individual control rods. To perform this type of rod movement, the operator must select the manual, single rod movement mode by controls provided at the RC&IS dedicated operator interface, and designate the individual rod to be moved. After confirming that the correct rod has been designated, the operator then selects the desired rod movement mode, either step movement, notch movement, or continuous mode.

Step movement means movements of 36.5 mm (1.44") nominal distance for each step movement activated except for the last withdrawal or for the first step movement from normal full-out position, which have a nominal step distance of 37.5 mm (1.48"). Notch movement means movement to the next rod position that is an integer multiple of 2 steps movement from being fully inserted. In the continuous mode, rod movement continues as long as the operator activates a movement command, and after the operator deactivates the movement command, the rod settles to the effective target position.

To accomplish the desired movement in the selected movement mode, the operator activates the "insert" or "withdraw" movement command. This is done by activating associated hard pushbutton switches located adjacent to the RC&IS dedicated operator interface on the main control panel in the MCR. The desired rod movement occurs if no abnormal conditions, such as a rod block, are activated. If any of the higher priority automatic rod movement actions are activated (for example SCRRI, scram-follow, or ARI), these movements override the operator desired normal movement and are completed as required. This is true no matter what mode of normal rod movement is activated.

The RAPI of the RC&IS enforces rod blocks based upon signals internal or external to the system. These rod blocks can prevent desired rod movements or stop rod movements, if activated while normal rod movements are underway. This applies to both single rod movement and ganged rod movement modes.

The internal signals include those signals from ATLM and RWM. If there is any disagreement between the two-channel logic of the subsystems of the RC&IS, rod block signals are transmitted to the RSM unless one of the channels of logic has been manually bypassed.

Examples of external input signals which could cause rod withdrawal blocks include those from the SRNM and APRM subsystems and the MRBM subsystems of the NMS or from FMCRD separation status signals received from the Q-DCIS through data transmission to the RC&IS. A rod withdrawal block condition is activated from the corresponding FMCRD if the status of either separation switch A or B indicates that FMCRD separation has occurred, if the RPS Reactor Mode Switch is in either the Startup or Run position, and if that rod is currently selected for normal movement. A more complete list of rod block conditions is provided in Subsection 7.7.2.2.7.4.

When normal rod movements are performed (no abnormal conditions exist), the RAPI of the RC&IS transmits the appropriate rod movement command signals to a dual channel FCM located in a remote communication cabinet. These rod movement command signals are received at the dual channel FCM and routed to logic for the associated rod server processing channel RSPC A and RSPC B of the RSMs of the selected rod. They are then transmitted as channel A and channel B inputs for the corresponding induction motor controllers. Channel A and channel B brake energization signals are transmitted to the associated RBC. The induction motor controllers perform two-out-two voting on the command signals received from the logic of both RSPCs. It then activates the proper power control signals to accomplish the FMCRD motor movement that provides the required 3-phase AC power output to the FMCRD motor and power to the associated MBB to perform the desired movement.

The RBC similarly performs two-out-of-two voting and energizes (mechanically releases) the FMCRD holding brake just prior to the start of FMCRD motor movement. It then de-energizes (mechanically engages) the FMCRD holding brake just after the desired normal rod movement is completed.

The RDCs of the RSM interface with instrumentation of the FMCRD, a subsystem of the CRD. They collect absolute rod position for the corresponding FMCRD by converting the resolver A and resolver B analog signals into digital data representing the FMCRD rod position. The data are used in the associated RSPCs' logic and transmission (via the RC&IS multiplexing system) to the RAPI logic and for the RAPI to transmit rod position data to other systems and subsystems and to the RC&IS dedicated operator interface.

7.7.2.2.7.2 Ganged Rod Movements

There are three means of controlling ganged rod motion. The RC&IS provides for automatic mode, semi-automatic mode, and manual mode. When in the automatic mode of operation, commands for insertion or withdrawal are received from the PAS.

The RC&IS dedicated operator interface provides controls for activating the automatic, semi-automatic, or manual rod movement mode of operation. When the system is in the semi-automatic mode, all rod movements are controlled by the operator. However, the RC&IS, by using a database called the RRPS and keeping track of the current control rods' positions, provides for automatic selection of the next gang, as required, to perform the sequence of rod movements in accordance with the RRPS definition. With this approach, the operator only needs to decide when to either insert or withdraw control rods and does not have to decide which gang of control rods to select next. This ensures that the RRPS sequence is followed.

When the RC&IS is in manual mode, the ganged rod movement mode has been chosen, and the operator selects a specific rod in a gang, the logic automatically selects all associated rods in that gang. The operator does not have to follow the RRPS sequence when performing manual rod movements; however, in order to re-establish either semi-automatic or automatic rod movement modes, the operator has to establish an initial rod pattern that is consistent with the RRPS allowed rod patterns.

When the automatic mode is active, the RC&IS responds to signals for a rod movement request from the PAS. In this mode, the PAS simply requests either desired control rod insertion or withdrawal movements. The RC&IS responds to this request by using the RRPS and the current rods' positions and automatically selects the appropriate gang and executes the next in sequence withdrawal/insert commands as required.

In order for the automatic rod movement feature of the RC&IS to be active, the soft switch on the RC&IS dedicated operator interface for automatic rod movement mode must be activated with none of the abnormal conditions that could prevent the RC&IS automatic operation mode from being active. The operator has the option of discontinuing the automatic operation by changing the RC&IS mode switches to the manual or the semi-automatic position.

7.7.2.2.7.3 Establishment of RRPS

The RRPS is normally established before plant startup and stored in the memory of the N-DCIS equipment and the RC&IS. The N-DCIS and RC&IS allow modifications to be made to the RRPS through operator actions. The N-DCIS provides compliance verification of the proposed changes to the RRPS with the ganged withdrawal sequence requirements.

The RC&IS provides the capability for an operator to request a download of the RRPS from the N-DCIS. The new RRPS data are loaded into the RAPI. Download of the new RRPS data can only be completed when the RC&IS is in manual rod movement mode and when a permissive switch located at the RAPI-A panel is activated. The RC&IS provides feedback signals to the N-DCIS to confirm a successful download of the RRPS data.

Rod withdrawal block signals are generated whenever selected single or ganged rod movements differ from those allowed by the RRPS. The RC&IS can either be in the automatic or semi-automatic rod movement mode. The RC&IS provides for activation of an alarm at the operator's panel for an RRPS violation.

7.7.2.2.7.4 Rod Block Function

The rod block logic of the RC&IS, upon receipt of input signals from other systems and internal RC&IS subsystems, inhibits movement of control rods. In most cases, only a rod withdrawal block is activated. However, the RWM can also activate a rod insertion block for enforcement of the GWSR.

Rod block signals to the RC&IS from safety-related systems are appropriately isolated. This provides required isolation between safety-related and nonsafety-related systems while preventing electrical failures from propagating into the safety-related systems.

The presence of any rod block signal, in either channel or both channels of the RC&IS logic, causes automatic changeover from automatic mode to manual mode. The automatic rod movement mode can be restored by taking the appropriate action to clear the rod block and by using the RC&IS mode switch to restore the automatic rod movement mode.

If either channel or both channels of the RC&IS logic receives a signal from any of the following type of conditions, a rod block is initiated. These conditions are:

- Rod separation detection (rod withdrawal block only for those selected rod(s) for which the separation condition is detected and for which the rods are not in the Inoperable Bypass condition, applicable when the RPS Reactor Mode Switch is in the Startup or Run position);
- Reactor Mode Switch in Shutdown position (rod withdrawal block for all control rods, applicable when the RPS Reactor Mode Switch is in the Shutdown position);
- SRNM withdrawal block (rod withdrawal block for all control rods, not applicable when the RPS Reactor Mode Switch is in the Run position);

- APRM withdrawal block (rod withdrawal block for all control rods);
- Scram accumulator charging water header pressure - low (rod withdrawal block for all control rods);
- Scram accumulator charging water header pressure - low-low trip bypass (rod withdrawal block for all control rods);
- RWM withdrawal block (rod withdrawal block for all control rods, applicable below the Low Power Setpoint);
- RWM insert block (rod insertion block for all control rods, applicable below the low power setpoint);
- ATLM withdrawal block (rod withdrawal block for all control rods, not applicable below the ATLM enable setpoint);
- MRBM withdrawal block (rod withdrawal block for all control rods, not applicable below the ATLM enable setpoint);
- Gang large deviation (for example, gang misalignment) withdrawal block (rod withdrawal block for all operable control rods of the selected gang, applicable when RC&IS Gang mode selection is active);
- Refuel mode withdrawal block (rod withdrawal block for all control rods, applicable when the RPS Reactor Mode Switch is in the Refuel position if a fuel bundle is being handled by the refueling platform while positioned over the RPV);
- Startup mode withdrawal block (rod withdrawal block for all control rods, applicable when the RPS Reactor Mode Switch is in the Startup position if the refueling platform is positioned over the reactor pressure vessel);
- RAPI trouble (rod withdrawal block and rod insertion block for all control rods);
- RAPI SIU trouble (rod withdrawal block for all control rods); and
- Electrical group power abnormal (rod withdrawal block and rod insertion block for all control rods).

The RC&IS enforces all rod blocks until the rod block condition is cleared. The bypass capabilities of the RC&IS permit clearing certain rod block conditions that are caused by failures or problems that exist in only one channel of the logic.

7.7.2.2.7.5 RC&IS Reliability

The RC&IS has a high reliability and availability due to its dual channel configuration design. The design allows its continued operation, when practicable, in the presence of component hardware failures. This is achieved because the operator is able to reconfigure the operation of the RC&IS through bypass capabilities while the failures are being repaired.

The expected system availability during its 60-year life exceeds 0.99. The expected reliability is based upon the expected frequency of an inadvertent movement of more than one control rod, due to failure. The expected frequency is less than or equal to one inadvertent movement in 100 reactor operating years.

The RC&IS design ensures that no credible single failure or single operator error can cause or require a scram or require a plant shutdown. The RC&IS design preferentially fails in a manner that results in no further normal rod movement.

7.7.2.2.7.6 RC&IS Bypass Capabilities

The RC&IS provides the capability to bypass resolver A, or resolver B if either fails, and select resolver B, or resolver A, to provide rod position data to both channels of the RC&IS. The RC&IS logic prevents the simultaneous bypassing of both resolver signals for an individual FMCRD.

The RC&IS allows the operator to completely bypass up to eight control rods by declaring them "inoperable" and placing them in this bypass condition. More control rods can be bypassed when the RPS Reactor Mode Switch is in the Refuel position, as described below. Through operator action, an update to the status of the control rods placed into the "inoperable" bypass condition can be performed at the RC&IS dedicated operator interface.

Activating a new RC&IS "inoperable bypass status" to the RAPI is only allowed when the RC&IS is in a manual rod movement mode and when a bypass permissive switch located near the RC&IS dedicated operator interface on the main control panel in the MCR is activated.

The operator can substitute a position for the rod that has been placed in this bypass state in both channels of the RC&IS, if the substitute position feature is used. The substituted rod position value entered by the operator is used as the effective measured rod position that is stored in both RAPI channels and sent to other subsystems of the RC&IS and to other plant systems (such as the N-DCIS). The position substitution status of each FMCRD can also be displayed at the RC&IS dedicated operator interface and the RAPI dedicated operator interface.

To conduct periodic inspections on FMCRD components, the RC&IS only allows up to 54 control rods to be placed in an "inoperable" bypass condition, when the RPS Reactor Mode Switch is in the Refuel position.

The RC&IS enforces effective rod movement blocks when the control rod has been placed in an inoperative bypass status. When the "inoperable" bypass status is active, the RC&IS logic does not send any rod movement or brake energization power to the associated FMCRD.

In response to activation of either normal rod movement or special insertion functions, such as ARI, control rods in this bypass condition do not respond to movement commands.

The RC&IS Single/Dual Rod Sequence Restriction Override (S/DRSRO) bypass feature allows the operator to perform special dual or single rod scram time surveillance testing at any power level of the reactor. In order to perform this test, it is often necessary to perform single or HCU pair rod movements that are not allowed normally by the sequence restrictions of the RC&IS. When a control rod or pair of control rods associated with an individual HCU is placed in a S/DRSRO bypass condition, the control rod(s) are no longer used to determine compliance with the RC&IS sequence restrictions (for example, the ganged withdrawal sequence and RRPS).

The operator can only perform manual rod movements of control rods in the S/DRSRO bypass condition. The logic of the RC&IS allows this manual single/dual rod withdrawal for special scram time surveillance testing. The operator can place up to two control rods associated with the same HCU in the S/DRSRO bypass condition. The dedicated RC&IS dedicated operator interface display information contains status indication of control rods in the S/DRSRO bypass condition.

The RC&IS ensures that S/DRSRO bypass logic conditions have no effect on special insertion functions for an ARI, SCRRI, or scram following condition. There is also no effect on other rod block functions, such as MRBM, APRM, or SRNM rod blocks.

The drive insertion following a single/dual rod scram test occurs automatically. The operator makes the necessary adjustment of control rods in the system prior to the start of the test for insertions, and restores the control rods to the desired positions after test completion.

In addition to the RC&IS bypass functions that affect both channels (the bypass capabilities are described above), there are additional RC&IS bypass functions provided for the operator to establish conditions that affect only one channel of the RC&IS. The interlock logic prevents the operator from placing both channels in bypass for these types of bypass conditions. Logic enforces bypass conditions to ensure that the capability to perform any special function (such as an ARI, scram following, and SCRRI) is not prevented by the bypass conditions.

The RC&IS logic ensures enforcement of associated special restrictions placed on plant operation during invoked bypass conditions that affect a single channel. The status and extent of the bypass functions can be determined at the RC&IS dedicated operator interface.

Bypass conditions allow continuation of normal rod movement capability by bypassing failed equipment in one RC&IS channel. After repair or replacement of the failed equipment is completed, the operator can restore the system or subsystem to a full two-channel operability. The operator has the capability to establish single-channel bypass conditions within the following systems / subsystems:

- RSPC channel A or B,
- FCM channel A or B,
- ATLM channel A or B,
- RWM channel A or B, or
- RAPI channel A or B.

7.7.2.2.7.7 Automated Thermal Limit Monitor Algorithm Description

The ATLM is a microprocessor-based subsystem of the RC&IS that executes two different algorithms for enforcing fuel operating thermal limits when reactor power is above the ATLM enable setpoint. One algorithm enforces Operating Limit Minimum Critical Power Ratio (OLMCPR), and the other enforces the Operating Limit Maximum Linear Heat Generation Rate (OLMLHGR). For the OLMCPR algorithm, the core is divided into multiple regions, each consisting of 16 fuel bundles. For the OLMLHGR algorithm, each region is further vertically divided into four segments. During a calculation cycle, ATLM Rod Block Setpoints (RBS) are calculated for OLMCPR monitoring and for OLMLHGR monitoring. The calculated setpoints are compared with the real time averaged LPRM readings for each region/segment. The ATLM issues a trip signal if any regionally averaged LPRM reading exceeds the calculated RBS. This trip signal causes a rod block within the RC&IS. The ATLM provides a FW temperature control valve one-way block and a rod withdrawal block if the reactor thermal power versus FW temperature combination is outside of the area allowed by the reactor power versus FW temperature map, or if the FW temperature decrease causes thermal limit violations. The ATLM calculates a reference FW temperature for the purpose of detecting a loss of feedwater heating event. During each pass through the algorithm, the reference temperature is set to the maximum of: the current FW temperature, the existing reference temperature, or the minimum allowed FW temperature for the current reactor power. The reference temperature is only allowed to decrease for a slow FW temperature decrease for which reactor power is at or below 100% and MCPR limits are met. The ATLM provides a FW temperature control valve one-way block, rod withdrawal block, and SCRRI/SRI initiation, if the FW temperature decreases by more than 16.7°C (30°F) from the reference FW temperature.

The ATLM algorithm is also based upon control rod positions and status data and other plant data from the RAPI. The ATLM operating limit setpoints can be updated based upon calculated inputs from the core monitoring function of the N-DCIS. Updates of the ATLM setpoints can occur either automatically or by operator request.

7.7.2.2.7.8 Operational Considerations

RC&IS dedicated operator interface in the MCR, along with associated control switches located close to the RC&IS dedicated operator interface such as withdrawal and insertion pushbuttons, are the main interfaces for the operator to perform manual or semi-automatic control rod movements, activate and deactivate the RC&IS automatic rod movement mode, and activate and deactivate RC&IS bypass conditions. In addition, the operator can determine the details of the RC&IS status and related FMCRD status information at this interface. Dedicated control switches are also provided on the MCR panel for manual initiation of an ARI function and for manual initiation of an SCRRI/SRI function. The DPS sends associated FMCRD motor Run-in and SCRRI initiation signals to the RC&IS. The DPS directly activates the ARI valves of the CRD system for accomplishing the hydraulic ARI function.

7.7.2.2.7.9 Reactor Operator Information

The RC&IS dedicated operator interface provides the primary interface for the operator to access detailed RC&IS information, including details of the RC&IS status and related FMCRD status. RC&IS detection of abnormal conditions activates alarms so that the operator is notified of the change in RC&IS and/or FMCRD status. In addition, the RC&IS provides FMCRD position information and summary RC&IS and FMCRD status information to the N-DCIS equipment that provides for additional operator information to be displayed on other nonsafety-related VDUs in the MCR.

7.7.2.2.7.10 Setpoints

The RC&IS has no safety setpoints. The ATLM RBSs are continuously calculated when the reactor power is above the ATLM enable setpoint. These setpoints also depend upon the last operating thermal limit information received from the N-DCIS during an ATLM thermal limit update process. All other setpoints are established prior to plant startup operations and only adjusted, if needed, as a result of plant startup testing results. It is anticipated that none or very few of the RC&IS setpoints (besides the continual ATLM rod block setpoint updates) require adjustment as a result of startup testing results.

7.7.2.2.7.11 Environmental Considerations

The RC&IS is not required for safety-related purposes, nor is it required to operate after a design basis accident. This system is required to operate in the normal plant environmental conditions at the locations of the RC&IS equipment, in the back-panel area of the MCR and in applicable areas of the RB.

7.7.2.3 Safety Evaluation

The circuitry described for the RC&IS is completely independent of the circuitry controlling the scram valves. This separation of the scram and normal rod control functions prevents failures in the RC&IS circuitry from affecting the scram circuitry. The scram circuitry is discussed in Subsection 7.2.1. Because the RC&IS directly controls movement of each control rod as an individual unit, a failure that results in inadvertent movement of a control rod affects only one control rod. The malfunctioning of any single control rod does not impair the effectiveness of a reactor scram. Therefore, no single failure in the RC&IS prevents a reactor scram. Repair, adjustment, or maintenance of the RC&IS components does not affect the scram circuitry.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed in Subsections 15.2.3.1, 15.2.3.2, 15.3.1, 15.3.7, 15.3.8, and 15.3.9 envelope the failure modes associated with RC&IS digital controls.

Table 7.1-1 identifies the RC&IS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.2.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The RC&IS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The RC&IS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The RC&IS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for reduction of risk from Anticipated Transients Without Scram (ATWS) events for light-water-cooled nuclear power plants:

- Conformance: The ATWS mitigation functions are designed in accordance with the requirements of 10 CFR 50.62.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues for I&C is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the RC&IS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The RC&IS design does not use innovative means for accomplishing safety functions.

7.7.2.3.2 General Design Criteria

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28 and 29:

- Conformance: The RC&IS complies with these GDC.

7.7.2.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The portions of RC&IS that provide interface support for DPS conform to item II.Q of SECY-93-087.

7.7.2.3.4 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The RC&IS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The RC&IS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The RC&IS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The RC&IS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.2.3.5 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the RC&IS design conforms to BTP HICB-16.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems:

- Conformance: The portions of RC&IS that provide interface support for DPS conform to BTP HICB-19.

7.7.2.4 Testing and Inspection Requirements

The RC&IS equipment is designed with consideration for online testing capabilities. The system can be maintained on line while repairs or replacement of hardware take place without causing any abnormal upset condition. The single-channel bypass capabilities support having continued RC&IS operation while repair or maintenance work is being performed on the dual-channel portion of the RC&IS equipment.

7.7.2.5 Instrumentation and Control Requirements

The CRD system is the RC&IS main direct interface to gather control rod position information and FMCRD status information and execute control rod movement commands. The FMCRD-related instrumentation that provides direct input to the RC&IS is addressed as part of the CRD system in Subsection 4.6.1. The primary output of the RC&IS to accomplish the RC&IS related rod movement functions is the 3-phase AC power to the FMCRD motors, associated AC power to the MBBs, and the holding brakes of the CRD system.

The RC&IS modules that interface with FMCRD instrumentation include the appropriate signal conditioning and conversion components (for example, RDC, discrete contact closure or reed switch input circuitry, and excitation power sources/supplies) for acquisition of:

- Resolver A and B position feedback signals (continuous signals);
- Coupling check (overtravel-out) position reed switch (discrete signal);
- Latched full-in and full-in position reed switches (discrete signal; these two reed switches are wired in parallel);
- Buffer contact reed switch (discrete signal); and
- Scram timing position reed switches (discrete signals) at the following positions:
  - 0% insertion,
  - 10% insertion,
  - 40% insertion,
  - 60% insertion, and
  - 100% insertion.

The induction motor controllers provide the proper 3-phase power to the FMCRD motor, the directly associated MBB, and the holding brakes of the CRD system to accomplish the RC&IS rod movement functions.

The RC&IS does not directly interface with any other basic plant instrumentation. The other inputs to the RC&IS are by hardwired signal interfaces, data communication links with other systems, or from the RC&IS dedicated operator interface.

7.7.3 Feedwater Control System

The FWCS accomplishes both RPV water level control and FW temperature control. RPV water level control is accomplished by manipulating the speed of the FW pumps. FW temperature control is accomplished by manipulating the heating steam flow to the seventh stage FW heaters or directing a portion of the FW flow around the high-pressure FW heaters. The two functions are performed by two sets of triple redundant fault tolerant digital controllers (FTDCs) located in separate cabinets. Each set of FTDCs is dedicated to perform one function. The ESBWR HP FW Heater Temperature Control Diagram is provided in Figure 7.7-7.

7.7.3.1 System Design Bases

7.7.3.1.1 Safety-Related Design Bases

The FWCS is not a safety-related system and is not required for safe shutdown of the plant. Therefore, the FWCS has no safety-related design basis. In the power operation mode, only one of the triple redundant controllers can be removed from service. Refer to Subsection 7.3.3 (the LD&IS) for FW line isolation protections.

7.7.3.1.2 Power Generation (Nonsafety) Design Bases

The FWCS is designed so that the functional capabilities of safety-related systems are not inhibited. The FWCS regulates the flow of FW into the RPV to maintain predetermined water level limits during transients and normal plant operating modes; additionally the FWCS controls FW temperature to allow reactor power control without moving control rods. The desired range of water level during normal power operation is based on steam separator performance. The requirements include limiting carryover, which can affect turbine performance, and limiting carryunder, which can affect overall plant efficiency. FW temperature control allows independent control of temperature either above or below the temperature normally provided by the FW heaters with turbine extraction steam. An increase in FW temperature decreases reactor power and a decrease in FW temperature increases reactor power. FW temperature is normally set manually by the operator. The setpoint can also be adjusted by the Plant Automation System (PAS). There is a maximum allowable FW temperature setpoint change that cannot be exceeded. FW temperature cannot be decreased when the reactor thermal power exceeds 100%. The system does not accept a temperature setpoint outside of the area allowed by the reactor power versus FW temperature map which is described in Subsection 4.4.4.3.

If the RPV water rises to Level 8, equipment protective action trips the main turbine and reduces FW demand to zero. The DPS trips the FW pumps if the water continues to rise to Level 9. If the water falls to Level 3, the RPS, a fully independent safety-related system (Subsection 7.2.1), shuts down the reactor. If the water level continues to drop and reaches Level 2, the high-pressure make-up function of the CRD system is initiated (Reference Figure 7.7-1, Water Level Range Definition). The CRD system is fully independent of other plant delivery or injection systems. If the reactor thermal power versus FW temperature combination is outside of the area allowed by the reactor power versus FW temperature map, the RC&IS/ATLM initiates a control rod withdrawal block and a FW temperature control valve one-way block. If the reactor thermal power versus FW temperature combination further departs from the area allowed by the reactor thermal power versus FW temperature map (high reactor thermal power, high feedwater temperature or low feedwater temperature), the RPS initiates a reactor shutdown.

7.7.3.2 System Description

7.7.3.2.1 General Description

The FWCS is a power generation (control) system that maintains proper RPV water level in the operating range from high (Level 8) to low (Level 3). During normal operation, FW flow is delivered to the RPV through three Reactor Feed Pumps (RFPs), which operate in parallel. Each RFP is driven by an adjustable-speed induction motor that is controlled by an adjustable speed drive (ASD). In normal operation, the fourth RFP is in standby mode and starts automatically if any operating FW pump trips while at power. In abnormal operation, the fourth RFP can be set in manual mode or can be removed from service for maintenance. The reactor FW pumps receive suction from the FW booster pump discharge header. The FW booster pumps draw suction from the fourth open FW heater tank and increase FW pressure to the required suction pressure of the reactor FW pumps. There are four FW booster pumps with three in service during normal operation and the fourth in standby. In normal operation, FW temperature is controlled by FW heaters one through six using turbine extraction steam. If increased FW temperature is demanded, modulating valves admit steam from the main steam header to the seventh FW heater. If decreased FW temperature is demanded, modulating valves direct a part of the FW flow around the fifth, sixth, and seventh FW heaters.

Each function of the FWCS is implemented on its own dedicated set of triple redundant, FTDCs including power supplies and input/output signals. The controller is designed for a Mean Time to Failure (MTTF) of no less than 1000 years. Each set of FTDCs consists of three parallel processing controllers, each containing the hardware and software for execution of the control algorithms. Each FTDC executes the control software for the control modes. At the operator's discretion, the system operation mode can be selected from the main control console. The FWCS functional diagram is provided in Figure 7.7-3.

During normal operation the FWCS sends three speed-demand signals, each of which reflects a voted FWCS output, to each feed pump ASD. The ASD performs a mid value vote and uses it to control the speed/frequency of the feed pump motor. The mid value vote is also returned to the FWCS as an analog input and compared with the speed demands sent by the FWCS. If an FTDC detects a discrepancy between the field voter output and the FTDC output, a “lock-up” signal is sent to a “lock-up” voter which causes the feed pump ASD to maintain the current pump speed and activates an alarm in the MCR.

During FW temperature control, the FWCS sends a voted (median selected) position demand to either the modulating valves admitting steam to the seventh FW heater or the modulating valves directing a part of the FW flow around the fifth, sixth, and seventh FW heaters. The actual received position demand and actual valve position are returned to the FWCS as analog inputs and compared with the position demands sent by the FWCS. If an FTDC channel detects a discrepancy between the field voter output and the FTDC channel output, a lock-up signal is sent to a lock-up voter that maintains the valve position and activates an alarm in the MCR. For drawings of the FW system, FW heater, pump and valve configuration, see Section 10.4.

7.7.3.2.2 Operation Modes (Level Control)

The following modes of RPV water level control are provided.

- **Single Element Control** - At less than 25% of rated reactor power the FWCS uses single-element control based on RPV water level. In this mode the conditioned level error from the master level (proportional + integral, or PI) controller is used to determine the demand to either the Low Flow Control Valve (LFCV) or to an individual feed pump ASD. The ASDs control feed pump motor speed and thus FW flow rate. In addition, the FWCS can regulate the RWCU/SDC system Overboard Control Valve (OBCV) demand to counter the effects of density changes and purge flows into the reactor during heatup when the steam flow rate is low.

- **Three-Element Control** - During normal power range operation, the three-element control mode uses water level, total FW flow rate, total steam flow rate, and individual feed pump suction flow rate and pressure signals to determine the feed pump speed demand. The total FW flow rate is subtracted from the total steam flow rate signal to yield the RPV flow rate mismatch. The flow rate mismatch signal is summed with the conditioned level error signal from the master level controller to provide the input signal for the master flow controller. The master flow controller provides the demand signal to the individual RFP loop trim controllers that use the suction flow rate signals to balance RFP flow rate demand. The master flow controller output plus trim controller output are used to generate the speed demand signal to the ASDs that control feed pump motor speed and thus FW flow rate.
- **Manual Feed Pump Control** - Each RFP can be controlled manually from the main control console through the FTDC by selecting the manual mode for that pump. In manual mode, the RFP speed demand signal that is sent directly to the ASD of the selected feed pump has the capability of being increased or decreased. Each feed pump is controlled manually at the manual/automatic transfer station.

The FWCS also provides interlocks and control functions to other systems. If the reactor water reaches Level 8, the FWCS simultaneously activates a MCR alarm, and sends a zero-speed demand signal to the feed pump ASDs, and trips the turbine. On identification of an ATWS condition, the FWCS sends a zero flow demand signal to the feedpump ASDs. In addition, the FWCS initiates the signal to open the steam line condensate drain valves when steam flow rate falls below the 40% of nominal flow rate.

The worst case of a FW Pump ASD controller failure in the FW system would cause a run-out of one FW pump to its maximum flow rate. In the event of a one pump run-out (detected by FW flow high), the FWCS would respond by reducing the demand to the other pumps, automatically compensating for the excessive flow rate from the failed pump.

7.7.3.2.3 Operation Modes (Temperature Control)

The modes of FW temperature control are as follows.

- Manual – the FW temperature setpoint is controlled by the operator.
- Automatic – the FW temperature setpoint is controlled by the PAS.

Both modes of FW temperature control use eight FW temperature measurements, four per FW line. These redundantly measured temperatures are compared with the temperature setpoint and the error signal is used by a Proportional, Integral, Derivative controller. The Proportional, Integral, Derivative controller output range is between -100% to +100% depending on whether heating or cooling of the FW is required. The output signals are used to generate the position demands for both the FW heater bypass valves and the seventh FW heater steam heating valves.

Both the manual and automatic modes of FW temperature control include the following features.

- Neither the operator nor the automation system can input a setpoint outside the area allowed by the reactor power versus FW temperature operating map (Power-FW temperature Map) which is adjustable per fuel cycle and described in DCD Subsection 4.4.4.3.

- Neither the operator nor the automation system can change the setpoint faster than an allowable rate (nominally 55.6°C (100°F) per hour).
- No FW temperature control mode can be entered unless the controller has passed all its self-diagnostic tests and unless the operator has actively selected the control mode.
- The FW temperature controller is unable to decrease FW temperature if the reactor thermal power is greater than 100%. The validated reactor thermal power signal is provided by the NMS.
- Individual temperature control valves are "locked up" if they are not at their demanded position within a prespecified time or one-way "locked up" if there is an ATLM one-way block (to prevent FW temperature from additional decrease [increase], the steam heating valves are blocked from further closing [opening] the bypass valves are blocked from further opening [closing]).
- The heating valves to the seventh FW heater and the high pressure FW heater bypass valves are not open simultaneously.

7.7.3.3 Safety Evaluation

The FWCS is a power generation system that maintains proper RPV water level and FW temperature. Its level control range is from high water level (Level 8) to low water level (Level 3) and its nominal FW temperature control range at 100% rated power is from 188°C (370°F) to 215.6°C (420°F). FW temperature can be increased up to 252.2°C (486°F) which reduces the rated reactor power by approximately 15%. The RPV water level rising to Level 8 or falling to Level 3 results in the shutdown of the reactor by the RPS. If the RPV water level rises too high (Level 8), the main turbine trips, the ASD feed pump flow demand is reduced to zero, and the safety-related FW isolation valves are closed by LD&IS. Continued rising water level to Level 9 results in a trip of all ASD feed pumps by the DPS and the ASD controller power supply being interrupted by LD&IS . If the reactor thermal power versus FW temperature combination is outside of the area allowed by the reactor power versus FW temperature map, the RC&IS initiates a control rod withdrawal block and FW temperature control valve one-way block. If the reactor thermal power versus FW temperature combination further departs from the area allowed by the reactor power versus FW temperature map (high reactor thermal power, high feedwater temperature or low feedwater temperature), the RPS initiates reactor shutdown. The RPS uses eight safety-related measurements of FW temperature (two per division) and implements a reactor scram using two-out-of-four logic based on a validated reactor thermal power. Refer to Subsection 7.2.1 for the RPS description.

The FWCS initiates a runback of FW pump FW demand to zero and closes the LFCV and RWCU/SDC OBCV when it receives an ATWS trip signal from the ATWS/SLC Logic. Refer to Subsection 7.8.1.1.

A combined FW temperature change and FW flow/reactor water level change caused by controller failure is precluded by implementing the two control schemes in physically different cabinets and logic processors.

A loss of FW heating that results in a significant decrease in FW temperature is independently detected by the ATLMs and by the DPS, either of which will mitigate the event by initiating SCRRI and SRI functions. These interlocks mitigate the effects of a reactor power increase due to reduced FW temperature. Although no credit is taken for the function in a safety analysis, the FW temperature control system also mitigates inadvertent FW temperature changes in either direction by manipulating its control valves to maintain the setpoint temperature. The temperature difference between FW lines A and B is monitored and alarmed if it exceeds the allowable value.

A total failure of the triple redundant FW temperature control system such that the outputs all fail downscale (or upscale), and the heating steam valves close (or open), or the bypass valves close (or open) is highly unlikely. No single failure or operator error of the FW temperature control system results in more than a 55.6°C (100°F) decrease in the final FW temperature. The design meets the requirements for the condensate and FW system specification in Subsection 10.4.7.1.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed in Subsections 15.2.4.2, 15.3.1, and 15.3.2 envelope the failure modes associated with the FWCS digital controls.

Table 7.1-1 identifies the FWCS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.3.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The FWCS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The FWCS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The FWCS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants:

- Conformance: The ATWS mitigation functions are designed in accordance with the requirements of 10 CFR 50.62.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Unresolved and generic safety issues are discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the FWCS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The FWCS design does not use innovative means for accomplishing safety functions.

7.7.3.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, and 24:

- Conformance: The FWCS design complies with these GDC.

7.7.3.3.3 Staff Requirements Memorandum

SRM on SECY 93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrument and Control Systems:

- Conformance: The portions of FWCS that provide interface support for DPS conform to item II.Q of SECY-93-087.

7.7.3.3.4 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: The FWCS receives signals from sensors on vessel instrument lines in the NBS. Refer to Subsection 7.7.1.3 for a discussion of the guidance of RG 1.151 in relation to the NBS.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The FWCS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The FWCS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The FWCS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The FWCS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.3.3.5 Branch Technical Positions

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in this subsection conforms to BTP HICB-16.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I& Control Systems:

- Conformance: The portions of FWCS that provide interface support for DPS conform to BTP HICB-19.

7.7.3.4 Testing and Inspection Requirements

The FTDC self-test and on-line diagnostic test features are capable of identifying and isolating failures of process sensors, Input/Output (I/O) cards, power buses, power supplies, processors and inter-processor communication paths. These features identify the presence of a fault and determine the location of the failure down to the module level.

The FWCS components and critical components of interfacing systems are tested to ensure that specified performance requirements are satisfied. Preoperational testing of the FWCS is performed before fuel loading and startup testing to ensure that the system functions as designed and that stated system performance is within specified criteria.

7.7.3.5 Instrumentation and Control Requirements

7.7.3.5.1 Power Sources

Redundant UPS power the FWCS digital controllers and process measurement equipment. No single power source or single power supply failure results in the loss of FWCS functions.

7.7.3.5.2 Equipment

The FWCS consists of:

- The FTDC that contains the software and processors for execution of the control algorithms;
- FW flow rate signals that provide for the measurement of the total flow rate of FW into the RPV;
- Steam flow rate signals that provide for the measurement of the total flow rate of steam leaving the RPV;
- Feed water pump discharge flow rate signals that provide for the measurement of the discharge flow rate of each feed pump;
- The LFCV differential pressure transmitters that provide for the measurement of the pressure drop across the LFCV, for LFCV gain control;
- The LFCV flow transmitters that provide for the measurement of the flow rate through the LFCV, for both LFCV control and low thermal power calculations; and
- FW temperature signals that provide for the measurement of the FW temperature at the point prior to the FW penetration to the reactor building.

7.7.3.5.3 Reactor Vessel Water Level Measurement

Reactor vessel narrow-range water level is measured by at least three identical, independent sensing systems. For each level measurement channel, a differential pressure transmitter senses the difference between the pressure caused by a constant reference column of water and the pressure caused by the variable height of water in the RPV. The differential pressure transmitters are part of the NBS. (Refer to Subsection 7.7.1.2 for a description of the RPV instrumentation). The FWCS FTDC determines one validated narrow-range level signal using the multiple level measurements as inputs to a signal validation algorithm. The validated narrow-range water level is indicated on the main control console in the MCR.

7.7.3.5.4 Steam Flow Rate Measurement

The steam flow rate in each of four main steam lines is sensed at each RPV nozzle venturi, part of the NBS. (Refer to Subsection 7.7.1.2 for a description of the RPV instrumentation.) Two flow transmitters per steam line, which are part of the FWCS, sense the venturi differential pressure and send these signals to the FTDC through the multiplexing function of the N-DCIS. The FWCS multiplexing function signal-conditioning algorithms take the square root of the venturi differential pressures and provide eight steam flow rate signals, two for each steam line, to the FTDC for validation. These validated steam line flow rate measurements are summed in the FTDC to give the total steam flow rate out of the RPV. The total steam flow rate is indicated on the main control console in the MCR.

7.7.3.5.5 Feedwater Flow Rate Measurement

FW flow rate is sensed at a single flow element in each of the two FW lines, which are part of the Condensate and Feedwater System (C&FS). Three transmitters per FW line, which are part of the FWCS, sense the differential pressure and send these signals to the FTDC through the N-DCIS multiplexing function. The FWCS multiplexing function signal conditioning algorithms take the square root of the differential pressure and provide six FW flow rate signals, three for each FW line, to the FTDC for validation. These validated FW line flow rate measurements are summed in the FTDC to give the total FW flow rate into the RPV. The total FW flow rate is indicated on the main control console in the MCR.

Feed pump flow rate is sensed at a single flow element, which is part of the C&FS, upstream of each feed pump. The suction line flow element differential pressure is sensed by three transmitters, which are part of the FWCS, and sent to the FTDC through the N-DCIS multiplexing function. The FWCS multiplexing function signal conditioning algorithms take the square root of the differential pressure and provide the suction flow rate measurements to the FTDC. The feed pump suction flow rate is compared with the demand flow rate for that pump and the resulting error is used to adjust the speed demand to the ASD to reduce that error and balance RFP flow rate between operating pumps.

7.7.4 Plant Automation System

7.7.4.1 System Design Bases

7.7.4.1.1 Safety Design Bases

The PAS has no safety-related design basis, but is designed so that the functional capabilities of safety-related systems are not hindered. Abnormal events requiring control rod scrams are sensed and controlled by the safety-related RPS, which is fully independent of the PAS. Discussions of the RPS are provided in Subsection 7.2.1.

The PAS provides the capability for supervisory control of the entire plant. It does this by supplying setpoint commands to independent nonsafety-related automatic control systems as changing load demands and plant conditions dictate.

7.7.4.1.2 Power Generation (Non-Safety) Design Bases

The power generation basis of this system is to provide supervisory control that regulates reactivity during criticality control, provides heatup and pressurization control, regulates reactor power, controls turbine/generator output, controls secondary nonsafety-related systems, and provides reactor startup / shutdown controls.

7.7.4.2 System Description

The primary purposes of the PAS are reactivity control, heatup and pressurization control, reactor power control, generator power control (MWe control), and plant shutdown control. The PAS consists of triple redundant process controllers. The functions of the PAS are accomplished by suitable algorithms for different phases of reactor operation which include approach to criticality, heatup, reactor power increase, automatic load following, reactor power decrease, and shutdown. The N-DCIS accepts one-way communication from the Q-DCIS so that the safety-related information can be monitored, archived, and alarmed seamlessly with the N-DCIS data.

Through the N-DCIS, the PAS receives input from the following major safety-related systems: NMS (Subsection 7.2.2) and the RPS (Subsection 7.2.1). Through the N-DCIS, the PAS receives input from the following major nonsafety-related systems: the RC&IS (Subsection 7.7.2), SB&PC System (Subsection 7.7.5), FWCS (Subsection 7.7.3), RWCU/SDC (Subsection 7.4.3), and the Turbine Generator Control System (TGCS) (Subsection 10.2.2). The output demand request signals from the PAS are sent to the RC&IS to position the control rods, to the SB&CS for pressure setpoints, and to the TGCS for load following operation. A simplified functional block diagram of the PAS is provided in Figure 7.7-4.

The PAS interfaces with the operator's control console to perform its designed functions. From the operator's control console for automatic plant startup, power operation, and shutdown functions, the operator uses the PAS to issue supervisory control commands to nonsafety-related systems. The operator also uses the PAS to adjust setpoints of lower level controllers to support automation of the normal plant startup, shutdown, and power range operations. In the automatic mode, the PAS also issues command signals to the turbine master controller, which contains appropriate algorithms for automated sequences of turbine and related auxiliary systems. The PAS presents the operator with a series of break point controls on the main control console nonsafety-related VDUs for a prescribed plant operation sequence.

When all the prerequisites are satisfied for a prescribed breakpoint in a control sequence, a permissive is requested and upon operator acceptance, the prescribed control sequence is initiated or continued. The PAS then initiates demand signals to various system controllers to carry out the predefined control functions. For non-automated operations that are required during normal startup or shutdown (such as a change of Reactor Mode Switch status), automatic prompts are provided. Automated operations continue after the prompted actions are completed manually. The functions associated with reactor power control are performed by the PAS.

For reactor power control, the PAS contains algorithms that can change reactor power by control rod motions. A prescribed control rod sequence is followed when manipulating control rods for reactor criticality, heatup, power changes, and automatic load following. For reactor power control by FW temperature change, the PAS can provide the FW temperature control setpoint to allow reactor power maneuvering without moving control rods. Each of these functions has its own algorithm to achieve its design objective. In combination, the two reactor power control methods are utilized to form a sequential step-by-step power maneuvering strategy for the control rod pattern/movement and FW temperature change. During automatic load following operation, the PAS interfaces with the TGCS to coordinate main turbine and reactor power changes for stable operation and performance.

The normal mode of operation of the PAS is automatic. If any system or component conditions are abnormal during execution of the prescribed sequences, the PAS automatically switches into the manual mode. With the PAS in the manual mode, any in-progress operation stops and alarms are activated in the MCR. Also with the PAS in manual mode, the operator can manipulate control rods through the normal controls. A failure of the PAS does not prevent manual control of reactor power, and does not prevent safe shutdown of the reactor.

The triple redundant FTDC and redundant system controllers perform the PAS control functional logic.

7.7.4.3 Safety Evaluation

The PAS does not perform or ensure any safety-related function. This system is designed so that functionalities of safety-related systems in the plant are not affected by it.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed in subsections 15.2.3.1, 15.2.3.2, 15.3.8, and 15.3.9 envelope the failure modes associated with the PAS digital controls and the RC&IS digital controls. The expected and abnormal transients and accident events analyzed in Subsections 15.2.5.1, 15.3.3, 15.3.4, 15.3.5 and 15.3.6 envelope the failure modes associated with the PAS digital controls and the SB&PC digital controls. The expected and abnormal transients and accident events analyzed in Subsections 15.2.4.2, 15.3.1, and 15.3.2 envelope the failure modes associated with the PAS digital controls and the FWCS digital controls.

Table 7.1-1 identifies the PAS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.4.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The PAS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The PAS design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The PAS conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues for I&C is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the PAS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The PAS design does not use innovative means for accomplishing safety functions.

7.7.4.3.2 General Design Criteria

GDC 1, 2, 4,13, 19, and 24:

- Conformance: The PAS design complies with these GDC.

7.7.4.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The PAS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The PAS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The PAS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The PAS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.4.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided for the PAS conforms to BTP HICB-16.

7.7.4.4 Testing and Inspection Requirements

The FTDC input and output communication interfaces function continuously during normal power operation. Abnormal functioning of these components can be detected during operation. In addition, the FTDC is equipped with self-test and on-line diagnostic capabilities for identifying and isolating failures of input/output signals, buses, power supplies, processors, and inter-processor communications. These on-line tests and diagnostics can be performed without interrupting the normal control operation of the PAS.

7.7.4.5 Instrumentation and Control Requirements

The instrumentation required for the system can be categorized as (1) MCR instrumentation, needed for the man-machine interface, (2) hardware and software instrumentation for input/output interfaces and controller functions, and (3) direct non multiplexed sensor inputs needed by the system. The PAS hardware comprises triple redundant master controllers and duplicate system controllers. PAS software is required for controller functions and input/output interfaces.

7.7.5 Steam Bypass and Pressure Control System

7.7.5.1 System Design Bases

7.7.5.1.1 Safety Design Bases

The SB&PC System does not perform or ensure any safety-related function, is classified as a nonsafety-related system, and has no safety-related design basis. In the Power Operation Mode, only one of the three triple redundant FTDCs can be removed from service.

7.7.5.1.2 Power Generation (Non-safety) Design Bases

The SB&PC System is designed so that the functional capabilities of safety-related systems are not inhibited. The SB&PC System is required for the power generation cycle because it controls reactor pressure during plant startup, power generation, and shutdown modes of operation.

The design objective is to enable a fast and stable response to system pressure disturbances, and to pressure setpoint changes over the operating range. This is done using Turbine Control Valves (TCVs) through the TGCS and Turbine Bypass Valves (TBVs) for controlling reactor pressure. In addition, the design objective of the SB&PC System is to discharge reactor steam directly to the main condenser in order to regulate reactor pressure whenever the turbine cannot use all of the steam generated by the reactor.

7.7.5.2 System Description

7.7.5.2.1 General Description

The purpose of the SB&PC System is to control reactor pressure during plant startup, power generation, and shutdown modes of operation. The SB&PC System is implemented on triple redundant FTDCs. Power supplies and input/output signals are redundant. The controller is designed for a MTTF of no less than 1000 years. Control of reactor pressure is accomplished through control of the TCVs through the TGCS and TBVs, so that susceptibility to reactor trip, turbine-generator trip, main steam isolation, and safety relief valve opening is minimized. Triple redundant FTDCs using feedback signals from RPV dome pressure sensors generate command signals for the TBVs and pressure regulation demand signals used by the TGCS to generate demand signals for the TCVs. For normal operation, the TCVs regulate reactor pressure. However, whenever the total steam flow demand from the SB&PC System exceeds the effective TCV steam flow demand, the SB&PC System sends the excess steam flow directly to the main condenser through the TBVs.

The ability of the plant to load follow the grid system demands is accomplished by the aid of control rod actions. In response to the resulting steam production demand changes, the SB&PC System adjusts the demand signals sent to the TGCS so that the TGCS adjusts the TCVs to accept the control steam output change, thereby controlling pressure.

Controls and valves are designed so that steam flow is shut off when control system electrical power or hydraulic system pressure is lost.

Refer to Figure 7.7-5, SB&PC System Simplified Functional Block Diagram, and Figure 7.7-6, SB&PC System FTDC Block Diagram for an overview of SB&PC System functions and interfaces. Additional information is provided in Table 7.7-1, "Major Plant Automation System Interfaces".

7.7.5.2.2 Normal Plant Operation

At steady-state plant operation, the SB&PC System maintains RPV pressure at a set value, to ensure optimum plant performance. During normal operational plant maneuvers (pressure setpoint changes, level setpoint changes), the SB&PC System provides responsive, stable performance to minimize RPV water level and neutron flux transients. During plant startup and heatup, the SB&PC System provides for automatic control of the reactor pressure. Independent control of reactor pressure and power is permitted during RPV heatup by varying the turbine bypass flow as the main turbine is brought up to speed and synchronized. The SB&PC System also controls RPV pressure during normal (MSIVs open) reactor shutdown to control the reactor cooling rate.

7.7.5.2.3 Abnormal Plant Operation

Events that lead to reactor trip present significant transients while the SB&PC System maintains reactor pressure. These transients are characterized by large variations in steam flow and core thermal power output that affect RPV water level. The SB&PC System stabilizes system pressure and thus aids the FW/level control systems in maintaining RPV water level.

The SB&PC System is also designed to operate with other reactor control systems to avoid reactor trip after significant plant disturbances. Examples of such disturbances are loss of one FW pump, inadvertent opening of safety relief valves (SRVs)or TBVs, main turbine stop/control valve surveillance testing, and MSIV testing. To protect the condenser the SB&PC System inhibits opening of the TBVs when it detects high condenser pressure.

7.7.5.2.4 Operational Considerations

Manual operations permit opening of the main steam lines (up to the steam bypass valves and turbine stop valves [TSVs]) before normal condenser vacuum is obtained and permit cold shutdown testing of the isolation valves. The SB&PC System allows remote manual bypass operation in the normal opening sequence during plant start up and shut down. This facilitates purge of the RPV and main steam lines of accumulated noncondensible gases early on in the start-up process, and controls the rate of cooling during reactor shutdown to atmospheric pressures. When pressure transients increase during such manual operation, the controls provide automatic override of the manual demand signal by the normal bypass demand. The system automatically returns to the manual demand signal when the pressure transient causing the increased bypass demand is relieved.

Triple redundant FTDCs perform the SB&PC System functional logic and process control functions. Because of the triple redundancy, it is possible to lose one complete processing channel without affecting the system function. This also facilitates taking one channel out of service for maintenance, repair, or module replacement while the system is on-line.

During operation of the SB&PC System, the operator may observe the performance of the plant through nonsafety-related VDUs on the main control console or on the wide display panel

(WDP) in the MCR. As described in Subsection 7.7.5.5 below, the on-line diagnostic provision assures that all detections of transducer/controller failures are indicated to the operator and maintenance personnel. The triple redundant logic facilitates on line repair of the controller circuit boards. During abnormal conditions that result in high condenser pressure, the steam bypass valves and MSIVs close to prevent positive pressure conditions that would open the main condenser rupture disks. Manually operated provisions permit opening of the MSIVs (that is, inhibit the closure function) during startup operation. This vacuum protection function bypass permits heatup of the main steam lines, up to the steam bypass valves and TSVs, before normal main condenser vacuum is obtained. The bypass also permits cold shutdown testing of the isolation valves. Any plant or component condition that inhibits bypass valve opening is alarmed in the MCR and must be resolved before the TBV inhibit memory can be manually reset by the operator.

The SB&PC System has no safety setpoints because it is not a safety-related system. Actual operational setpoints are determined during startup testing.

The SB&PC System and bypass valves are powered by redundant uninterruptible nonsafety-related power supplies and sources. No single power failure results in the loss of any SB&PC System function. Upon detection of a failure of two or more channels in the controller, a turbine trip is initiated.

The pressure control function forces the TCVs to remain under pressure control supervision to provide automatic load following. This enables fast bypass opening for transient events that require fast reduction in turbine steam flow.

The steam bypass function controls reactor pressure by responding to the bypass flow demand signal. It modulates the regulating bypass valves, which are automatically operated. This control mode is assumed under the following conditions:

- During RPV heatup to rated pressure,
- While the turbine is brought up to speed and synchronized,
- During power operation when the reactor steam generation rate exceeds the turbine steam flow rate requirements,
- During plant load rejection and turbine/generator trips, and
- During cooldown of the nuclear reactor.

7.7.5.3 Safety Evaluation

The SB&PC System is classified as a primary power generation system. It is not safety-related, and is not required to operate during or after any DBAs. The system is required to operate in the normal plant environment and is required for the power production cycle. The SB&PC System equipment is located in both the MCR area of the CB and the turbine building (TB); and each SB&PC System component is subject to the environment of the applicable area. The SB&PC System FTDC panel and its components are designed to retain structural integrity during and after DBEs so that safety-related equipment in its area are able to perform their safety functions.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed in Subsections 15.2.5.1, 15.3.3, and 15.3.4, 15.3.5, and 15.3.6 envelope the failure modes associated with the SB&PC digital controls.

Table 7.1-1 identifies the nonsafety-related SB&PC System and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.5.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The SB&PC design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The SB&PC design conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: The SB&PC System is nonsafety-related and conforms in that there are no unresolved issues for the SB&PC System. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: Inspection, test, analyses, and acceptance criteria of the SB&PC System FTDC are identified in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the SB&PC within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The SB&PC design does not use innovative means for accomplishing safety functions.

7.7.5.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, and 24:

- Conformance: The SB&PC System design conforms to these GDC.

7.7.5.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: RG 1.151 is not applicable to the SB&PC System. The SB&PC System receives RPV dome pressure signals from sensors in the NBS (refer to Subsection 7.7.1.3). The SB&PC System also receives condenser absolute pressure signals from sensors in the Main Condenser and Auxiliaries System.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The SB&PC design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The SB&PC design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The SB&PC design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interface in Safety-related Instrumentation and Control Systems:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.5.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided in this subsection conforms to BTP HICB-16.

7.7.5.4 Testing and Inspection Requirements

The FTDC input and output communication interfaces function continuously during normal power operation. Abnormal operation of these components is detected during operation. The FTDC is equipped with on-line diagnostic capabilities to identify and isolate failure of I/O signals, buses, power supplies, processors, and inter-processor communications. On-line diagnostics are performed without interrupting the normal control operation of the SB&PC System.

The SB&PC System components and critical components of interfacing systems are tested to ensure the specified performance requirements are satisfied. Preoperational testing of the SB&PC System is performed before fuel loading and startup testing to ensure the system functions as designed and stated system performance is within specified criteria.

7.7.5.5 Instrumentation and Control Requirements

7.7.5.5.1 Power Sources

7.7.5.5.1.1 Uninterruptible Nonsafety–Related AC Power Supply

The nonsafety-related inverters of the UPS are powered by rectifiers that are supplied with AC power. However, if the AC power fails, the inverters receive power from a Direct Current (DC) source (batteries). The SB&PC System has three redundant nonsafety-related AC UPS of 120 ±10% VAC, 60 Hz. The SB&PC System panel is designed so that loss of one UPS or incoming power source does not affect SB&PC System functional operation and thus plant operation.

7.7.5.6 Major Instrument Interfaces with SB&PC System

7.7.5.6.1 Nuclear Boiler System

The NBS provides narrow range dome pressure, wide range dome pressure, inboard MSIV position, and outboard MSIV position signals to the SB&PC System.

7.7.5.6.2 Plant Automation System - Automatic Power Regulator

The SB&PC System supplies signals to the PAS-Automatic Power Regulator (APR). These signals are:

- SB&PC System Auto/OK status,
- Operating pressure setpoint,
- Total (average) TBV position,
- Pressure regulator output,
- Limited speed regulator output,
- Load reference, and
- First TBV position.

The PAS-APR transmits signals to the SB&PC System. These signals are:

- Automatic frequency control (AFC) status,
- Raise pressure setpoint,
- Lower pressure setpoint,
- PAS-APR fatal fault, and
- Reactor thermal power.

7.7.5.6.3 N-DCIS - Plant Computer Functions

The performance monitoring and control (PMC) function of the Plant Computer Functions (PCF) within the N-DCIS receives signals from the SB&PC System for performance monitoring.

7.7.5.6.4 Nonsafety-Related Distributed Control and Information System - Multiplexing

The multiplexing function of the N-DCIS provides the distributed control and instrumentation data communications network that supports the monitoring and control of interfacing plant systems. RMUs that support the SB&PC System and its interfaces with other systems are located throughout the plant.

7.7.5.6.5 Main Control Room Panels

The MCRP operator interface within the N-DCIS contains controls needed for SB&PC operation and displays variables and alarms from the SB&PC System.

7.7.5.6.6 Main Control Room Back Panels

The SB&PC System's triple redundant FTDC panel is mounted in a MCR Back Panel (MCRBP).

7.7.5.6.7 Turbine Bypass System

The Turbine Bypass System (TBS) provides temperature signals to the SB&PC System from thermocouples installed in each TBV discharge pipe, located between the TBV and condenser, for bypass steam leakage detection.

7.7.5.6.8 Turbine Generator Control System

The TGCS is a redundant process control system. Only the operator can switch the turbine generator controller to Automatic (remote), but either the operator or the APR can switch the turbine generator controller to Manual (local). The TGCS controls the turbine speed, load, and steam flow for startup and normal operations. The TGCS operates the TSVs, TCVs, and the intermediate stop and intercept valves. The TGCS also provides automation functions such as sequencing the appropriate turbine support systems and controlling turbine roll, synchronization of the main generator, and initial loading. The SB&PC System sends a steam flow demand to the Turbine Generator (TG) controller.

The SB&PC System sends signals to the TGCS. These signals are:

- Pressure regulation demand, and
- Turbine trip.

The TGCS provides signals to the SB&PC System. These signals are:

- Turbine speed regulator output,
- Load reference,
- Turbine steam flow demand,
- Turbine first stage pressure,
- Power-Load Unbalance (PLU) event,
- TGCS Central Processing Unit (CPU) failure, and
- Turbine trip.

7.7.5.6.9 Main Condenser and Auxiliaries

The main condenser receives steam from the TBVs and provides condenser narrow and wide range pressure signals, from all shells of the condenser, to the SB&PC System.

7.7.5.6.10 Auxiliary Boiler

The SB&PC System has the capability to start the auxiliary boiler and to command the auxiliary boiler to adjust steam production rate upon a MSIV closure condition as required.

7.7.6 Neutron Monitoring System - Nonsafety-Related Subsystems

7.7.6.1 System Design Bases

7.7.6.1.1 Safety-Related Design Bases

The NMS has two nonsafety-related subsystems, the Automatic Fixed In Core Probe (AFIP) subsystem and the MRBM subsystem. Neither the AFIP subsystem nor the MRBM subsystem performs or ensures any safety-related function; therefore the AFIP and MBRM subsystems have no safety-related design basis.

7.7.6.1.2 Power Generation (Non-Safety) Design Bases

The AFIP power generation design bases are:

- To provide a signal proportional to the axial neutron flux distribution at the radial core locations of the LPRM detectors. This signal allows calibration of the LPRM;
- To provide sufficient axial neutron flux monitoring with corresponding axial position and indication to allow point-wise measurement of the axial neutron flux distribution to support the determination of three-dimension core power distribution; and
- To receive LPRM information by direct interface with the N-DCIS PCF.

The MRBM power generation design bases are:

- To provide a signal to the RC&IS to block rod movement and prevent fuel damage if the MRBM signal exceeds a preset RBS to prevent fuel damage;
- To provide MRBM values to the N-DCIS;
- To provide bypass capability of one-out-of-two MRBM channels;
- To provide bypass of individual LPRM channels in its calculations;
- To provide online test and diagnostic capability to validate proper operation of its microprocessor-based system; and
- To provide rod block status to the MCR alarm system.

7.7.6.2 System Description

7.7.6.2.1 Automated Fixed In-Core Probe

7.7.6.2.1.1 General Description

The AFIP subsystem comprises AFIP sensors and their associated cables, as well as the signal processing electronic unit. The AFIP sensors are installed permanently within the LPRM assemblies. In each LPRM assembly in the core, there are seven AFIP sensors evenly distributed axially along the LPRM assembly. Consequently, there are AFIP sensors at and between all LPRM locations. The AFIP sensor cables are routed within the LPRM assembly and then out of the RPV through the LPRM assembly penetration of the vessel. The AFIP subsystem generates signals proportional to the axial power distribution at the radial core locations of the LPRM detector assemblies. The AFIP signal range is sufficiently wide to accommodate the corresponding local power range of approximately 5% to 125% of reactor rated power.

During core power and LPRM calibration, the AFIP signals are automatically collected and sent to the AFIP data processing and control unit. The data are properly amplified and compensated by applying correct sensor calibration adjustment factors. The data are sent to the PCF of the N-DCIS for core local power and thermal limits calculations. The calculated local power data are then used for LPRM calibration. The AFIP data collection and processing sequences are fully automated, with manual control available.

The AFIP sensor has near constant, very stable detector sensitivity due to its operating principle. Its sensitivity does not depend upon fissile material depletion or radiation exposure. The AFIP sensor, however, can be calibrated manually or automatically by using a built-in calibration device inside the LPRM assembly. The calibrated new sensitivity data of the AFIP sensors are stored in the AFIP control unit and are readily applied to the newly collected AFIP data to provide accurate local power information.

The AFIP sensors in an LPRM assembly are replaced together with the LPRM detectors when the whole LPRM assembly is replaced. The AFIP detectors within the LPRM assembly are installed so that physical separation is maintained between the LPRM detectors and the AFIP detectors. The AFIP cables are also routed within the LPRM assembly separately from the LPRM detector cables, with separate external connectors.

7.7.6.2.1.2 Classification

The AFIP subsystem is nonsafety-related. It is an operational subsystem with no safety-related function.

7.7.6.2.1.3 Power Supply

The power for the AFIP is supplied from the nonsafety-related instrument 120VAC Instrumentation and Control Power Supply power source. The power for the AFIP logic is supplied from redundant nonsafety-related instrument 120VAC UPS.

7.7.6.2.1.4 Environmental Considerations

The AFIP sensor meets ESBWR environmental requirements. The connectors and cabling located in the drywell are designed for continuous duty (see Appendix 3D). The AFIP instruments are designed to operate as intended under the expected environmental conditions at their locations.

7.7.6.2.1.5 Operational Considerations

The AFIP is operated to provide local power information for three-dimensional power calculations and for calibration of the LPRM channels. The AFIP operation is fully automated including AFIP data collection, AFIP sensor calibration, AFIP data amplification, and data transfer to the PCF. Manual operation capability is available.

7.7.6.2.2 Multi-Channel Rod Block Monitor

7.7.6.2.2.1 General Description

The MRBM subsystem logic issues a rod block signal used in the RC&IS logic to enforce rod blocks. Because it monitors more than one region, it is called the multi-channel rod block monitor. The rod blocks prevent fuel damage by ensuring that the MCPR does not violate fuel thermal limits or exceed MLHGR limitations. Once a rod block is initiated, manual action is required by the operator to reset the system.

The MRBM microcomputer-based logic receives input signals from the LPRMs and the APRMs of the NMS. It also receives control rod status data from the RAPI subsystem of the RC&IS to determine when rod withdrawal blocks are required. The MRBM uses the LPRM signals to detect local power change during the rod withdrawal. If the MRBM signal, which is based on averaged LPRM signal, exceeds a preset RBS, a control rod block demand is issued. The MRBM monitors the core in 4-by-4 fuel bundle regions where control rods are being withdrawn. The MRBM algorithm covers the monitoring of multiple regions simultaneously depending upon the size of the gang of rods being withdrawn. The MRBM is a dual channel system, but it is not a safety-related system.

7.7.6.2.2.2 Classification

The MRBM is nonsafety-related. Its activating interface is through the RC&IS, which is also a nonsafety-related system.

7.7.6.2.2.3 Power Supply

The power supply for the MRBM is from the non-divisional, nonsafety-related 120 VAC UPS buses in two different load groups.

7.7.6.2.2.4 Environmental Considerations

The MRBM is located in the MCR. It is physically and electrically isolated from the safety-related NMS subsystems. All interfaces with the safety-related NMS subsystems are through fiber optic isolators.

7.7.6.3 Safety Evaluation

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.6.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The AFIP and MRBM subsystem designs conform to these requirements.

10 CFR 50.34(f)(2)(iii)[I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The AFIP and MRBM designs conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Unresolved and generic safety issues are discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the AFIP and MRBM within the DCD conforms to this BTP.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The AFIP and MRBM designs do not use innovative means for accomplishing safety functions.

7.7.6.3.2 General Design Criteria

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28 and 29:

- Conformance: The AFIP and MRBM subsystem designs comply with these GDC.

7.7.6.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The AFIP and MRBM subsystem designs conform to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The AFIP and MRBM designs conform to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The AFIP and MRBM subsystem designs conform to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.6.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail provided in this subsection conforms to BTP HICB-16.

7.7.6.4 Testing and Inspection Requirements

7.7.6.4.1 Automated Fixed In-Core Probe

The AFIP instruments (not including sensors) are designed such that they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram, and with easy access for the service personnel.

The AFIP sensor is testable and can be calibrated for its sensitivity. The AFIP instrument unit includes an algorithm that automatically detects and rejects failed AFIP sensor signals. It also includes logic that verifies proper communication with the N-DCIS PCF.

The duration for AFIP testing and calibration is based on the applicable NMS AFIP design document. Additional information is provided in, "Gamma Thermometer System for LPRM Calibration and Power Shape Monitoring", NEDE-33197P (Reference 7.7-1).

7.7.6.4.2 Multi-Channel Rod Block Monitor

The MRBM subsystem is designed so that it can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or reactor scram. It provides easy access for the service personnel. The MRBM subsystem includes logic that verifies proper communication with the N-DCIS. The duration for MRBM testing and calibration is based on the applicable NMS MRBM design document and the instruction manual for the MRBM subsystem.

7.7.6.5 Instrumentation and Control Requirements

7.7.6.5.1 Automated Fixed In-Core Probe

The AFIP instrument is based on digital measurement and control design practices that include microprocessor-based programmable memory units. It follows a modular design concept so that each unit or its subunit is replaceable during repair service. The instrument has a flexible interface design that accommodates either metal wire or fiber optic communication links. The AFIP instrument is provided with necessary operator interface functions meeting NMS man-machine interface requirements.

The AFIP includes basic logic such as periodic demand for sensor calibration and data collection, as well as logic that is part of the communication protocol with the PCF. The AFIP instrument cabinets are located in areas of the CB having acceptable environmental conditions and physical and electrical separation from the safety-related NMS instruments.

7.7.6.5.2 Multi-Channel Rod Block Monitor

The MRBM subsystem is based on digital measurement and control design practices that include microprocessor-based programmable and memory units. The MRBM follows a modular design concept so that each unit or its subunit is replaceable during repair service. The MRBM has a flexible interface design to accommodate either metal wire or fiber optic communication links. The MRBM instrument is provided with necessary operator interface functions meeting NMS man-machine interface requirements.

The MRBM includes basic logic such as continuous LPRM data collection, MRBM rod block algorithm calculation, MRBM setpoint comparison, and communication protocol with the N-DCIS. The MRBM subsystem is located within the nonsafety-related equipment rooms of the CB having acceptable environmental conditions and physical and electrical separation from the safety-related NMS instruments..

7.7.7 Containment Inerting System

7.7.7.1 System Design Bases

The CIS design bases are discussed in Subsection 6.2.5.2.1.

7.7.7.2 System Description

The CIS system description is discussed in Subsection 6.2.5.2.

7.7.7.3 Safety Evaluation

The CIS safety evaluation is discussed in Subsection 6.2.5.2.3.

Table 7.1-1 identifies the CIS and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.7.7.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The CIS design conforms to these requirements.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The CIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Purge System Isolation Under Accident Conditions:

- Conformance: The CIS conforms to these requirements.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: The CIS conforms to these standards. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the CIS within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The CIS design does not use innovative means for accomplishing safety functions.

7.7.7.3.2 General Design Criteria

GDC 1, 2, 4, 13, 19, 24, 41, 42, and 43:

- Conformance: The CIS design conforms to these GDC. I&C are provided to operate the system and monitor process variables during startup, normal, and abnormal reactor operation. The CIS is operable from the MCR.

7.7.7.3.3 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.151, Instrument Sensing Lines:

- Conformance: The CIS instrument lines penetrating containment comply with the guidance of RG 1.151. Sensing lines are Seismic Category I Quality Group B and are provided with redundant isolation valves that can be isolated locally or remote manually from the MCR.

RG 1.152, Computer Software Used in Safety-related Systems:

- Conformance: The CIS design conforms to RG 1.152.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear power Plants:

- Conformance: The CIS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The CIS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems:

- Conformance: The CIS system design conforms to RG 1.180.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.7.7.3.4 Branch Technical Positions

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52, is applicable to the nonsafety-related CIS. The level of detail provided in this subsection conforms to BTP HICB-16.

7.7.7.4 Testing and Inspection Requirements

The CIS testing and inspection requirements are discussed in Subsection 9.4.9.

7.7.7.5 Instrumentation and Control Requirements

7.7.7.5.1 Logic and Interlocks

The CIS operation is manually or automatically activated from the MCR by aligning corresponding valves through remote manual control switches. During the inerting mode, a temperature controller accomplishes automatic control of the steam supply once the steam-heated nitrogen vaporizer has been activated. A temperature sensor at the outlet of the steam-heated vaporizer provides input to the temperature controller that then regulates the amount of steam. Low nitrogen temperature in the steam vaporizer outlet causes an alarm and a low-low temperature condition shuts off the main inerting line. The auxiliary steam supply is manually terminated. When the required inert containment pressure is reached, the CIS drywell pressure switch provides a signal to isolate the nitrogen supply shutoff valve.

Upon completion of the initial inerting, the CIS is manually or automatically aligned to its make-up mode. Make-up nitrogen is obtained by the automatic modulation of a pressure control valve on the nitrogen supply. The opening and closing of the pressure control valve is driven by the pressure controller in response to change of containment pressure. Make-up nitrogen supply is vaporized and heated up to an appropriate temperature by an electric heater that is manually loaded to its power source. Once activated, it continues to operate in automatic on-off mode until manually disconnected. Temperature sensors provide switching signals to start/stop the heater. When the required temperature is reached, the heater automatically cuts off electrical power to the heater elements.

The de-inerting process is manually or automatically activated, by aligning the CIS with the RB Heating, Ventilation and Air Conditioning (HVAC) to replace gases in the containment with breathable air.

During containment isolation events, the CIS containment isolation valves automatically close upon receipt of the isolation signal from LD&IS. Details of the isolation logic are discussed in Subsection 7.3.3.

The CIS can provide continued nitrogen makeup during isolation events. This is accomplished by overriding, with controlled bypass switches, the isolation signal to the makeup isolation valves.

A simplified system diagram is shown in Figure 6.2-29.

7.7.7.5.2 Instrumentation and Control

Drywell pressure sensors, part of the Containment Monitoring System (CMS), monitor containment pressure. These instruments provide input to the pressure controller that controls nitrogen makeup flow and provides alarm signals on a high drywell pressure condition.

Permanently installed temperature and humidity sensors are provided in several locations and elevations inside the containment. Outputs from these sensors are transmitted to the PCF for averaging and continuous monitoring of the containment. Drywell temperatures are provided directly to the LD&IS.

Oxygen analyzers monitor oxygen levels in the containment during startup, normal, and abnormal plant operating conditions. Two sample points (one in a high and one in a low location) are provided on opposite sides of each compartment (that is, the upper drywell area, lower drywell area, and wetwell air space). Each air lock is sampled. Oxygen levels in the CIS exhaust line are monitored. A high oxygen level indication is alarmed in the MCR.

A flow-metering device is installed in the makeup line to monitor the amount of nitrogen make up injected into the containment. Total nitrogen make-up flow (make-up flow to containment and make-up flow to the High Pressure Nitrogen Supply System (HPNSS) is also monitored. Total nitrogen flow indicates total containment atmosphere leakage during normal plant operation. An indication of excessive leakage is alarmed in the MCR.

Separate flow metering devices are also provided to both drywell and wetwell inerting and de-inerting flows.

The CIS is described in detail in Section 6.2.5.2.

7.7.7.5.3 Alarms and Indications

The alarms and indications provided in the MCR are:

- High drywell pressure,
- High nitrogen makeup flow,
- Excessive or gross containment leakage,
- High and low make-up flow temperature,
- High and low electric heater temperature,

- Low main vaporizer outlet temperature,
- Low nitrogen storage tank level,
- Disable switch in override position,
- High oxygen level,
- Wetwell pressure indication,
- Valve position switch status indication,
- Pilot solenoid status indication,
- Drywell temperature, and
- Wetwell temperature.

7.7.8 COL Information

None.

7.7.9 References

7.7-1 GE Hitachi Nuclear Energy, "Gamma Thermometer System for LPRM Calibration and Power Shape Monitoring," NEDE-33197P, Class III (Proprietary), Revision 2, August 2008, and NEDO-33197, Class I (Non-proprietary), Revision 2, August 2008.

7.7-2 (Deleted)

7.7-3 (Deleted)

7.7-4

Table 7.7-1

Major Plant Automation System Interfaces

APR Functions	Input Signals	Output Signals
Criticality Control	1. SRNM output (NMS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Criticality / subcriticality validation check (PCF)
Heatup & Pressurization	1. SRNM output (NMS) 2. Reactor water temperature (PGCS) 3. Reactor heatup schedule (PCF) 4. Reactor mode (PGCS) 5. Dome Pressure (SB&PC System)	1. CR control demand (RC&IS) 2. SB&PC System pressure setpoint
Reactor Power Control	1. Target generator power (PGCS) 2. Pressure controller output (equivalent load) (SB&PC System) 3. Load demand change (SB&PC System) 4. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Load demand (TGCS)
Generator Power Control	1. Generator power feedback signal (PGCS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Load demand (TGCS)
Reactor Shutdown Control	1. CR full insert signal (RC&IS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. SB&PC System pressure setpoint

Notes: Various status signal interfaces are not shown in this table for brevity.

CR – Control Rod

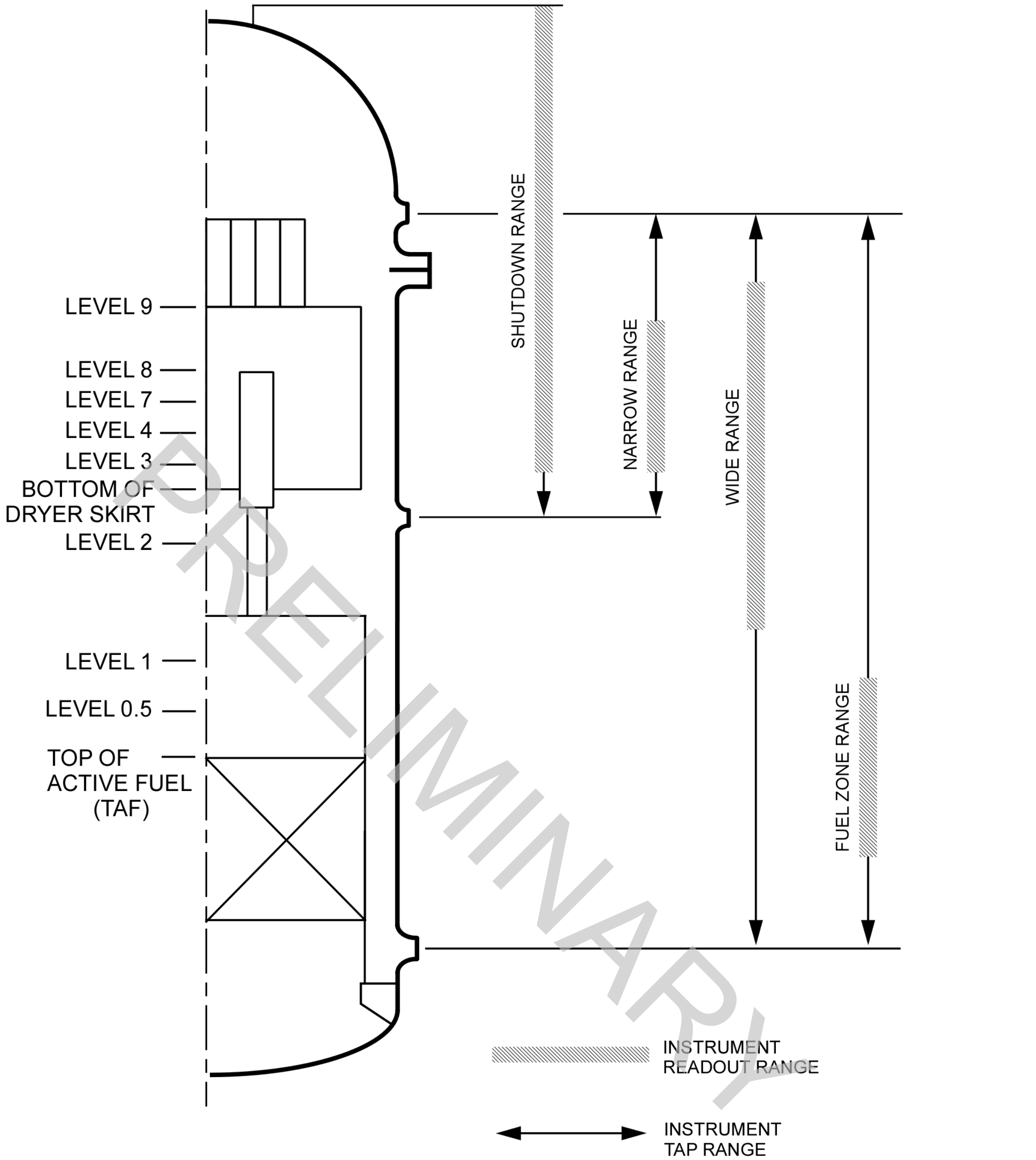


Figure 7.7-1. Water Level Range Definition

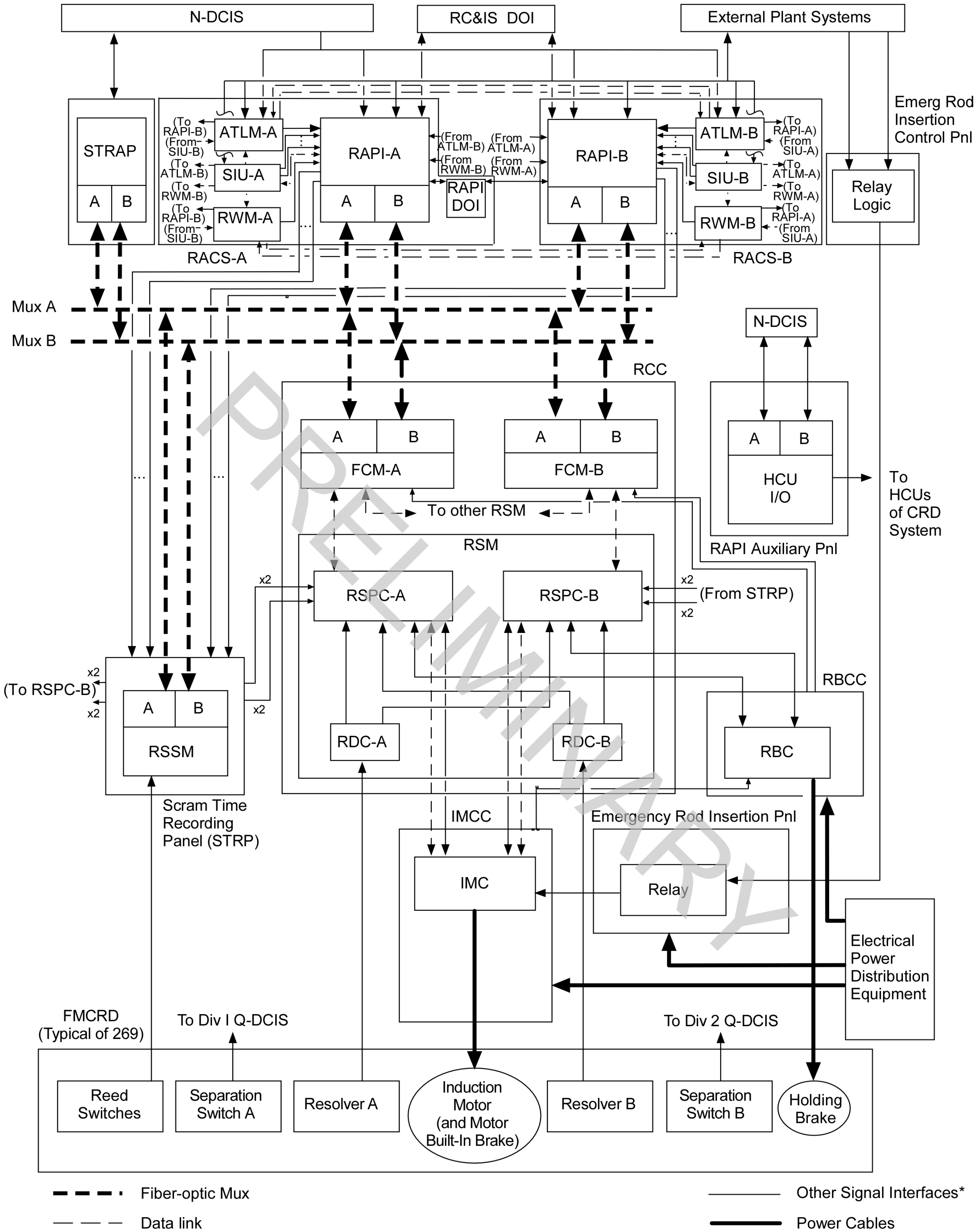


Figure 7.7-2. RC&IS Block Diagram

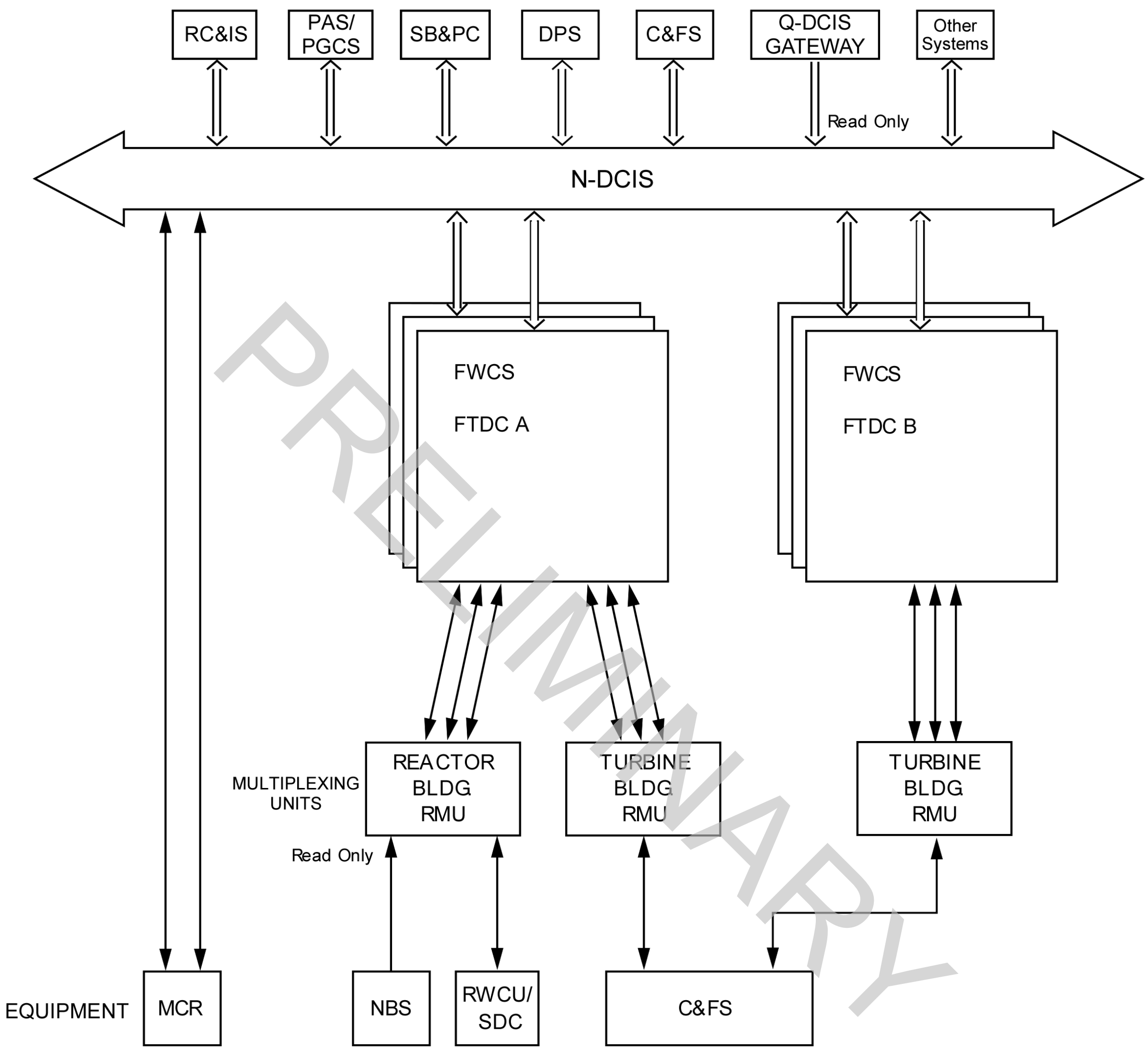


Figure 7.7-3. Feedwater Control System Functional Diagram

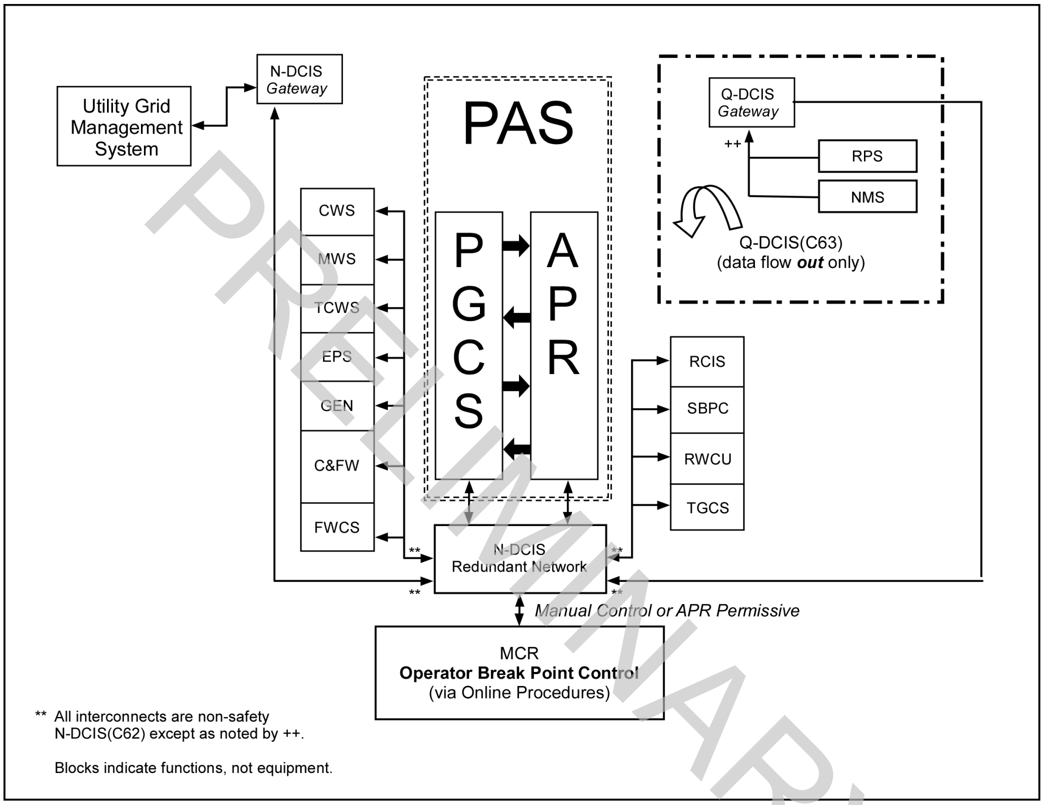


Figure 7.7-4. Plant Automation System Simplified Functional Diagram
(Only major systems are shown)

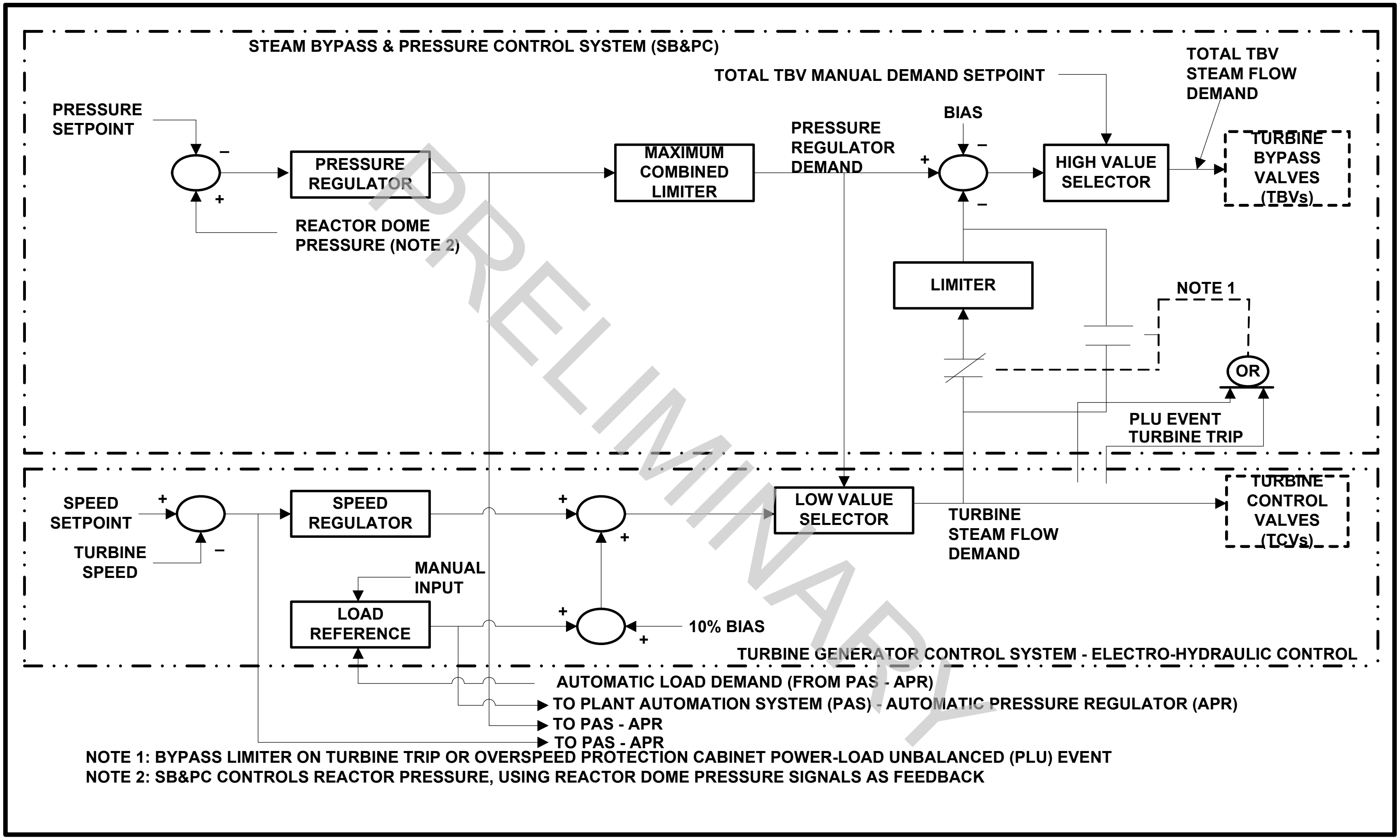


Figure 7.7-5. SB&PC System Simplified Functional Block Diagram

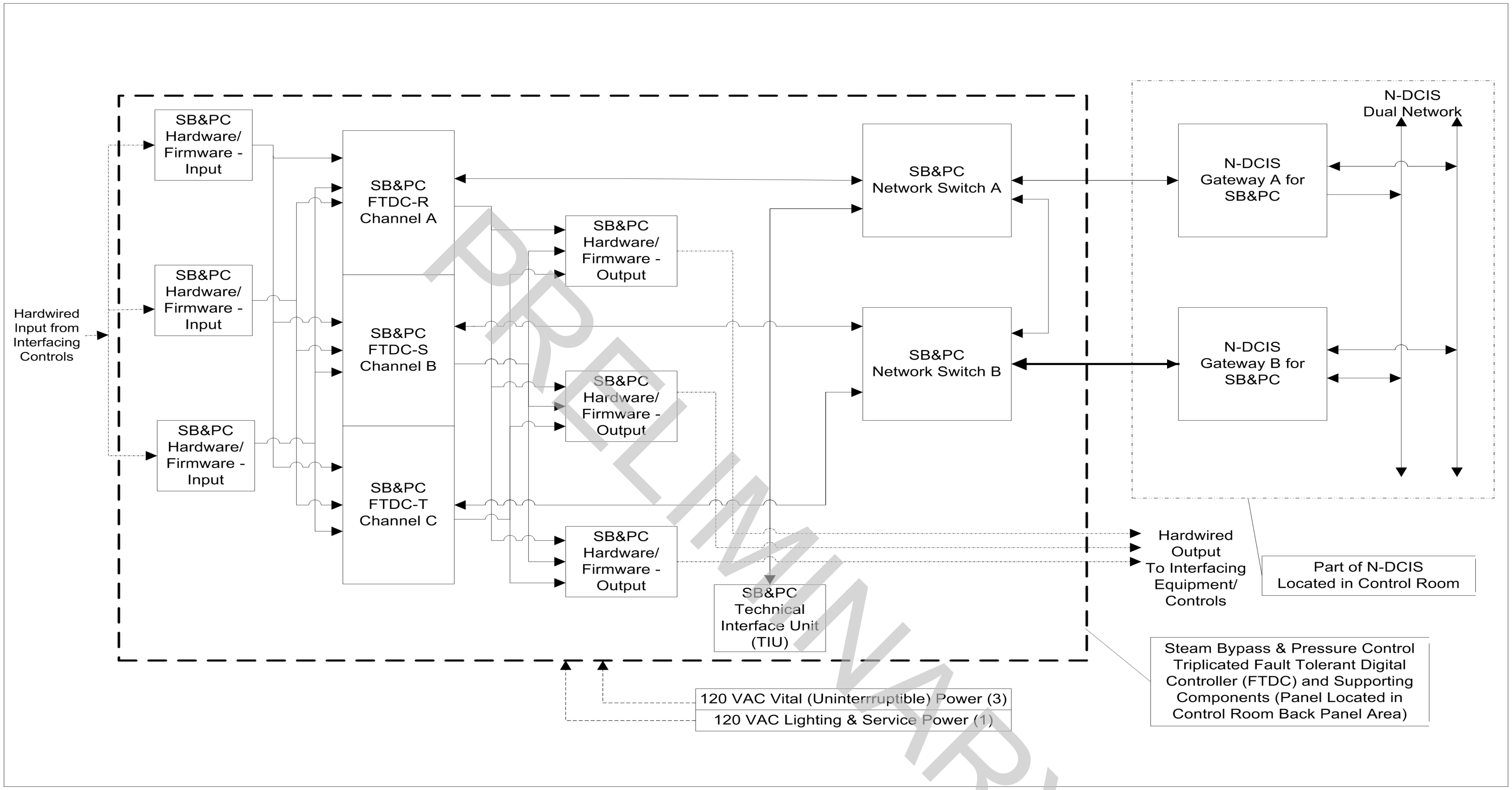


Figure 7.7-6. SB&PC System FTDC Block Diagram

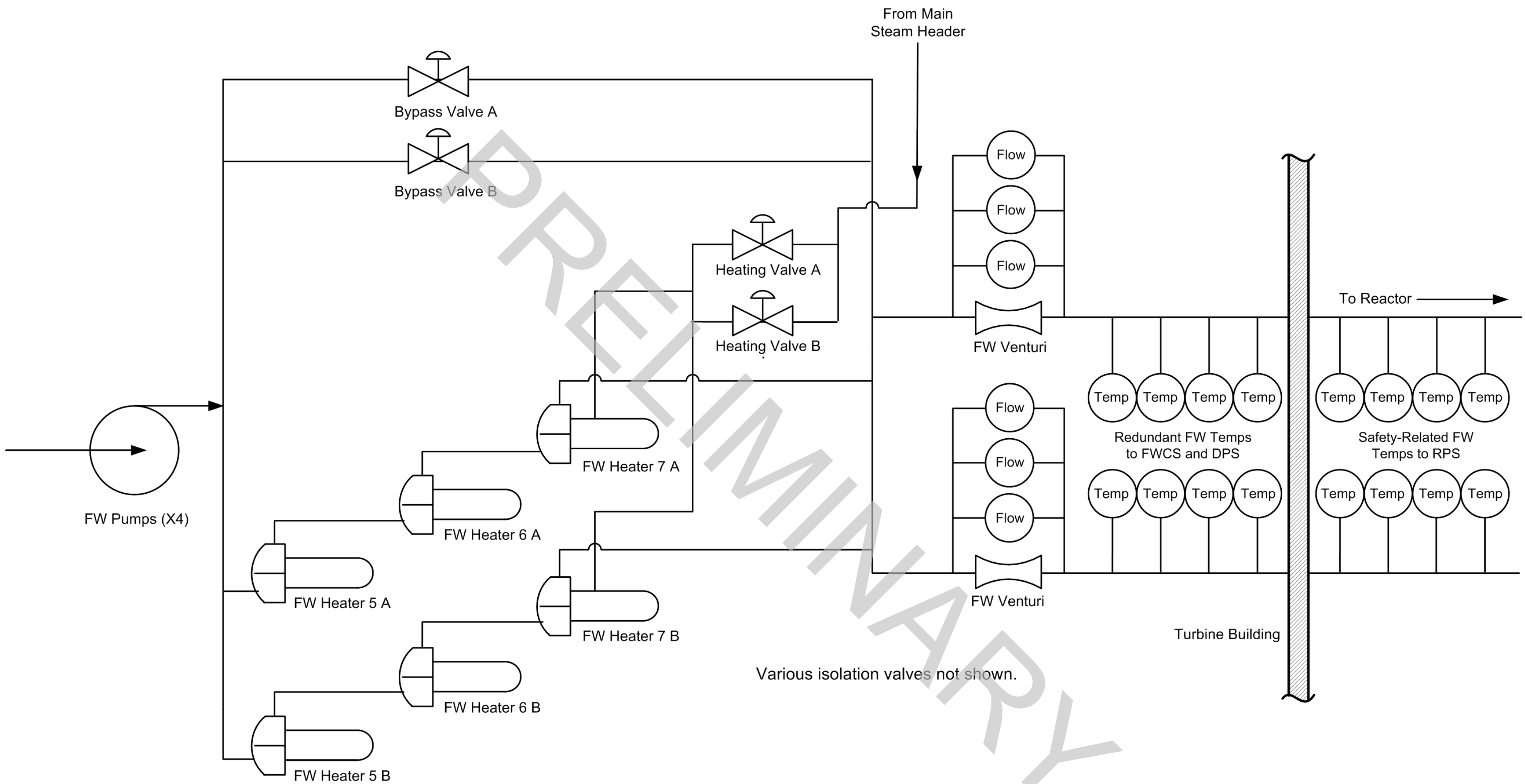


Figure 7.7-7. HP Feedwater Heater Temperature Control Diagram

7.8 DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS

7.8.1 System Description

The Anticipated Transient Without Scram and Standby Liquid Control (ATWS/SLC) system and the Diverse Protection System (DPS) comprise the diverse I&C systems that are part of the diversity and defense-in-depth strategy. They provide diverse backup to the Reactor Protection System (RPS) and the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF). The ATWS mitigating logic is designed to meet the diverse shutdown requirements of 10 CFR 50.62, "Requirements For Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants." The ATWS mitigating logic system is implemented with the Safety-Related Distributed Control and Information System (Q-DCIS) and the Nonsafety-Related Distributed Control and Information System (N-DCIS).

The nonsafety-related DPS (which is part of the N-DCIS) processes the nonsafety-related portions of the ATWS mitigation logic. It is designed to mitigate the possibility of digital protection system common mode failures discussed in Item II.Q of Commission Paper (Secretary of the Commission, Office of the [NRC]) (SECY) 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" and Item II.Q of Staff Requirements Memorandum (SRM) on SECY 93-087. Figure 7.8-1 provides a simplified block diagram of the DPS.

The relationships between the ATWS mitigation logic, the DPS, the Q-DCIS and the N-DCIS are discussed in Section 7.1. Figure 7.1-1 provides a simplified network functional diagram of the relationship between the ATWS/SLC System and the Q-DCIS, the DPS, and the N-DCIS.

The ATWS/SLC logic provides a diverse means of emergency shutdown using the SLC System for soluble boron injection. Alternate rod insertion, which hydraulically scrams the plant using the three sets of ARI valves of the Control Rod Drive (CRD) System, is also used for ATWS mitigation. This logic is implemented in the DPS. Detailed ATWS mitigation features are described later in this subsection.

The DPS is a nonsafety-related, triple redundant system powered by redundant nonsafety-related load group power sources. The highly reliable, isolated, and independent DPS provides diverse reactor scram using a subset of the RPS scram signals. The DPS provides diverse emergency core cooling by independently actuating the Emergency Core Cooling System (ECCS). The DPS performs selected containment isolation functions as part of the diverse ESF function. Any DPS manual initiation requires operation of two switches, with each switch requiring two distinct operator actions. Additional DPS features are described in Subsection 7.8.1.2. The design scope of the DPS functions is based on the diversity and defense-in-depth strategy developed via analyses that show the design meets criteria of BTP HICB-19, as outlined in Licensing Topical Report (LTR) NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report." (Reference 7.8-1). A confirmatory analysis supports and validates the DPS design scope requirements of BTP HICB-19. Conformance to BTP HICB-19 is described further in Subsection 7.8.3.5.

Table 7.8-1 provides a summary of the functions, initiators, and interfacing systems used by the diverse I&C systems for ATWS mitigation or for mitigation of design basis events described in

Chapter 15. Table 7.8-2 provides a list of the controls, interlocks, and bypasses used by the diverse I&C systems for ATWS mitigation or for mitigation of design basis events described in Chapter 15. Tables 7.8-3 and 7.8-4 describe additional diverse instrumentation and control features used to ensure that releases during a common mode protection system failure coincident with the design basis events discussed in the Safety Analysis of Chapter 15 do not exceed the radiation guidelines from 10 CFR 52.47(a)(2)(iv).

Mitigation of common mode failures is provided by:

- Manual scram and Main Steam Isolation Valve (MSIV) isolation by the operator in the Main Control Room (MCR) in response to diverse parameter indications;
- Availability of diverse manual initiation of the passive ECCS functions including Gravity-Driven Cooling System (GDCS) squib valve initiation, Safety Relief Valve (SRV) initiation, Depressurization Valve (DPV) initiation, Isolation Condenser System (ICS) initiation, and SLC System squib valve initiation. Manual initiation functions are available in the safety-related systems and in the DPS;
- Core makeup water capability from the Condensate and Feedwater System (C&FS), CRD System, and Fuel and Auxiliary Pools Cooling System (FAPCS) in the Low Pressure Coolant Injection (LPCI) mode;
- Long-term shutdown capability in the two redundant Remote Shutdown System (RSS) panels which are equipped with Division 1 and 2 controls for manual scram and MSIV closure, Division 1 and 2 safety-related Video Display Units (VDUs), and nonsafety-related displays and controls to allow monitoring and control of all plant systems. Local displays of process variables in the RSS system are continuously powered and are available for monitoring at any time;
- Diverse scram, which is different from the safety-related RPS, using diverse hardware and software;
- Diverse ESF initiation logic, which is different from the SSLC/ESF, using diverse hardware and software;
- ATWS mitigation using liquid boron injection for emergency plant shutdown through the SLC system;
- ATWS mitigation using alternate rod insertion (ARI) to hydraulically scram the plant using the three sets of ARI valves of the CRD system;
- Selected Control Rod Run-in (SCRRI) command to the Rod Control and Information System (RC&IS);
- Select Rod Insert (SRI) to hydraulically insert selected control rods with every SCRRI action; and
- Manual initiation capability of the ATWS mitigation functions (ARI/SLC/Feedwater Runback).

7.8.1.1 Anticipated Transients Without Scram Mitigation Functions

The ATWS mitigation control functions are:

- Automatic SLC System initiation, as shown in Figure 7.8-3. The SLC System is described in Subsection 7.4.1.
- Alternate rod insertion, as shown in Figure 7.8-2 and described in Subsections 7.7.2 and 7.8.1.1.2.
- Fine Motion Control Rod Drive (FMCRD) Run-in (or FMCRD Emergency Insertion) associated with the RC&IS, as shown in Figure 7.8-2 and described in Subsections 7.7.2 and 7.8.1.1.2.
- Feedwater runback, as shown in Figure 7.8-3 and described in Subsections 7.7.3, 7.8.1.1.1.1, 7.8.1.1.2, and 7.8.1.2.
- Alternate rod insertion and diverse scram plus delayed Feedwater runback for events where the RPS scram command has been unsuccessful in shutting down the reactor or when the SCRRI/SRI has been unsuccessful in reducing reactor power to an acceptable level, as described in Subsection 7.8.1.1.4.
- Automatic Depressurization System (ADS) Inhibit logic, which interfaces with select Engineered Safety Features to avoid escalation of an ATWS event to more serious events, is described in Subsections 7.8.1.1.1.2 and 7.8.1.2.3.

7.8.1.1.1 ATWS Mitigation Logic Implemented as Safety-Related Logic

The portion of the ATWS mitigation system implemented as safety-related logic is contained within the four divisions of the Reactor Trip and Isolation Function (RTIF) cabinets. The ATWS/SLC logic processing components are separate and diverse from the software-based RPS logic, which is also located in the RTIF cabinets. The RPS is described in Subsection 7.2.1.

ATWS/SLC Analog Trip Modules (ATM), instead of Digital Trip Modules (DTM), perform setpoint comparisons for the automatic trip parameters in each division. Hardware-based discrete digital logic substitutes for software-based trip logic to perform two-out-of-four voting. Therefore, the hardware and software-based logic of this alternate emergency shutdown function is diverse from the hardware and software logic of the RPS function.

7.8.1.1.1.1 Anticipated Transients Without Scram Logic Processors

There is an ATWS logic processor in each of the four divisional RTIF cabinets (Refer to Figure 7.8-3). The ATWS logic processors are separate and diverse from RPS circuitry. Each ATWS logic processor uses discrete programmable logic devices for ATWS mitigation logic processing. The programmable logic devices provide voting logic, control logic, and time delays for evaluating the plant conditions for automatic initiation of SLC boron injection and feedwater runback.

ATWS mitigation functions initiated by the safety-related ATWS/SLC platform are described as follows.

- Automatic initiation of SLC boron injection:
  - High Reactor Pressure Vessel (RPV) dome pressure and a Startup Range Neutron Monitor (SRNM) ATWS permissive (an SRNM signal that is above a specified setpoint) for three minutes or greater; or

- Low RPV water level (Level 2) and an SRNM ATWS permissive for three minutes or greater.

- Automatic initiation of feedwater runback:
  - High RPV dome pressure and SRNM ATWS permissive. A reset is permitted only when both signals drop below their setpoints. This signal is sent to the DPS for transmission to the FWCS.
- Automatic ADS Inhibit logic as described in Subsection 7.8.1.1.1.2.

ATWS mitigation logic processing features are described as follows.

- ATWS Mitigation Logic Processor Functions:
  - Performs the two-out-of-four voting function and additional interlock logic using data from ATMs and the Neutron Monitoring System (NMS).
  - Provides isolated hardwired contact outputs to the SLC System, the SSLC/ESF platform, and FWCS through the DPS.
- ATWS Mitigation Logic Processor Data Handling:
  - Discrete gate logic and hardware timers implement the ATWS mitigation logic. The input signals are hardwired, not multiplexed.
- ATWS Mitigation Logic Processor Status Monitoring and Communication:
  - A programmable logic device in each ATWS mitigation logic division processes the self-test logic. The self-test function is operator initiated and can only be performed with the associated ATWS mitigation logic division bypassed.
  - Fiber optic cables transmit ATWS mitigation logic processor status to external interfaces.
- ATWS Mitigation Logic Processor Alarms:
  - Instrument Inoperative (INOP) to N-DCIS (operating voltage degraded).
  - Division 1, 2, 3, and 4 ATWS SLC System injection logic tripped.
  - Division 1, 2, 3, and 4 ATWS FWCS runback logic tripped.

Manual initiation capability of the ATWS SLC liquid boron injection is provided in the MCR, with SLC, ARI, and feedwater runback initiation occurring from the same manual controls. The ARI and feedwater runback features are described in further detail in Subsection 7.8.1.1.2.

The actuating signals for the SLC System and FWCS are hardwired, rather than multiplexed, to their respective system controllers. If one of the four ATWS mitigation logic processors is inoperable, signals are initiated to bypass the input signals from the out-of-service processor so that the input voting logic changes from two-out-four to two-out-of-three. A manual bypass switch for this function is provided in the MCR.

The ATWS/SLC logic mitigates random failures with the divisional sensor channel and/or output trip channel bypass capability. A bypass places the remaining divisions in a two-out-of-three coincident logic condition so that another failure in a remaining division will not disable system operation.

7.8.1.1.1.2 ADS Inhibit ATWS Mitigation Logic

To prevent ATWS events from escalating to more serious events that approach the ADS initiation setpoint, automatic actuations occurring on sustained RPV Level 1 initiation and sustained drywell pressure high initiation by SSLC/ESF platform logic (which is described in Subsections 7.3.1.1.2 and 7.3.1.2.2) is inhibited by the ATWS/SLC logic. This function called the ADS Inhibit uses the following ATWS signals.

- Coincident low RPV water level (Level 2) and Average Power Range Monitor (APRM) ATWS permissive signals (i.e., an APRM signal that is above a specified setpoint from the NMS).
- Coincident high RPV pressure and APRM ATWS permissive signals that persists for 60 seconds.

Since drywell pressure increases that could approach the feedwater isolation setpoint may also occur during ATWS events the ADS Inhibit logic is also used to inhibit the feedwater isolation on high-high drywell pressure logic in the SSLC/ESF platform. The feedwater isolation logic is described in Subsection 7.3.3.3.

MCR controls are provided to manually inhibit the sustained RPV Level 1 initiation signal and sustained drywell pressure high initiation start signal by SSLC/ESF platform logic under ATWS conditions.

7.8.1.1.2 DPS Alternate Rod Insertion ATWS Mitigation Logic

The ARI function of the ATWS mitigation logic is implemented by nonsafety-related logic that is processed by the DPS. The DPS generates the signal to open the ARI valves in the CRD system based on any of the following command signals:

- High RPV dome pressure signal;
- Low RPV water level signal (Level 2); or
- Any diverse scram command identified in Subsections 7.8.1.1.4 or 7.8.1.2.1.

Additionally, a safety-related manual ATWS mitigation signal identified in Subsection 7.8.1.1.1.1 initiates the SLC System, ARI and FWCS runback of feedwater flow. It is sent to the nonsafety-related portions of the ATWS mitigation logic through qualified isolation devices.

On receipt of signals initiating ARI, described above, the DPS generates an additional signal to the RC&IS to initiate electrical insertion (i.e., FMCRD Run-in) of all operable control rods.

The ARI and FMCRD Run-in logic resides in the DPS, which is totally separate and independent from the Q-DCIS with diverse hardware and software. The RPV pressure and level input sensors for the ARI logic are diverse from the sensors used in the Q-DCIS.

7.8.1.1.3 DPS SCRRI/SRI Logic

The DPS processes a SCRRI/SRI signal to hydraulically scram selected control rods and to command the RC&IS to perform the SCRRI function based on any of the following initiators:

- Generator load rejection signal from the Turbine Generator Control System (TGCS) (two-out-of-three logic),
- Turbine trip signal from the TGCS (two-out-of-three logic),
- Loss of feedwater heating based on C&FS and NMS signals (two-out-of-four logic),
- SCRRI/SRI signal from the ATLM (two-out-of-three logic),
- SCRRI signal from the RC&IS (two-out-of-three logic), and
- Oscillation Power Range Monitor (OPRM) thermal neutron flux oscillation signal from the NMS (two-out-of-four logic).

It is also possible to initiate SCRRI and SRI manually from the MCR.

7.8.1.1.4 DPS Diverse Scram ATWS Mitigation Logic

On either a SCRRI/SRI command with power remaining elevated (two-out-of-three logic) or an RPS scram command (two-out-of-four logic) the DPS:

- Initiates a diverse scram (and ARI as indicated previously); and
- Initiates a delayed feedwater runback if elevated power levels persist.

7.8.1.2 DPS Diverse Instrumentation and Control

Diverse I&C functions other than the ATWS mitigation functions described previously are included in the DPS. These functions are outlined in Tables 7.8-3 and 7.8-4.

The DPS has a set of diverse reactor scram and diverse ESF logics that are implemented using diverse hardware and software from that of the RPS and SSLC/ESF.

The DPS transmits the feedwater runback signal from the ATWS mitigation logic to the FWCS. The DPS trips the feedwater pumps on high RPV water level (Level 9) after they have been run back to zero flow on high RPV water level (Level 8) by the Feedwater Control System as described by Subsection 7.7.3.

Additionally, the DPS provides diverse monitoring and indication of critical safety functions and process parameters required to support manual operations and assessment of plant status.

7.8.1.2.1 Diverse Scram Functions

The DPS diverse scram functions provide a diverse means of reactor shutdown and serve as backups to the RPS. A subset of the RPS scram signals is selected for inclusion in the DPS scope, which provides acceptable diverse protection results. This set of diverse protection logics for reactor scram, combined with the ATWS mitigation features, other diverse backup scram protection, and diverse ESF functions provides the necessary diverse protection to meet the required design position. The design position is specified in the SRM on SECY 93-087 and BTP

HICB-19 (Referenced in NUREG 0800 Section 7). The scram signals selected for inclusion in the DPS are:

- High RPV pressure,
- High RPV water level (Level 8),
- Low RPV water level (Level 3),
- High drywell pressure,
- High suppression pool temperature, and
- Closure of the MSIVs.

This diverse set of scram logics resides in diverse hardware and software equipment from the RPS. The sensors that provide input are diverse from those used for the RPS. The diverse logic equipment is nonsafety-related with triple redundant processors processing coincident logic from four sensor channels. The DPS includes a sensor channel bypass capability. If a sensor is bad or bypassed, each of the three processors will revert to two-out-of-three voting logic and if a main processor fails, the output switches will revert to two-out-of-two logic.

The power sources for this diverse equipment are from the nonsafety-related load groups. The diverse scram logic is "energize-to-actuate" with the trip signal applied at the return side of the 120 VAC circuit for the CRD hydraulic control unit (HCU) scram pilot valve solenoids. The RPS scram initiation signal is applied at the supply side of the 120 VAC circuit.

The diverse scram logic is based on two-out-of-four coincident logic processed by two-out-of-three triple redundant processors sent through three isolated fiber optic cables to the scram timing panel. A two-out-of-three vote is performed at the scram timing panel to open the solenoid return power switches.

The DPS also provides the ability to initiate a manual scram from either hardwired switches or DPS displays.

7.8.1.2.2 Diverse Engineered Safety Features Functions

The ESF functions include core cooling provided by the GDCS and the SLC System and the ADS function using SRVs and DPVs. The pressure relief and core cooling function is also provided by the ICS. The ESF functions of the GDCS squib valves, SLC System squib valves, ICS, and ADS (SRVs and DPVs) are included in the DPS to provide diverse initiation of emergency core cooling. The initiating logic is based on low RPV water level (Level 1).

The DPS does not provide automatic initiation of the suppression pool equalizing function of the GDCS because it is not required for approximately 30 minutes. Therefore, manual suppression pool equalization capability is provided.

Manual capability is provided in the DPS logic circuitry to initiate the diverse ECCS functions of the GDCS, SLC System, ICS, and ADS (SRVs and DPVs). The DPS also provides the ability to generate diverse manual ECCS actuation from the DPS displays.

Additionally manual controls are provided for ADS and GDCS injection sequenced initiation. This control feature is provided to mitigate small and medium break LOCA scenarios that do not result in ECCS initiation from low RPV water level. DPS does not provide automatic ADS and

GDCS injection start on sustained high drywell pressure since this function is not required for 60 minutes. Therefore, manual ADS and GDCS injection sequenced initiation capability is provided.

This set of nonsafety-related diverse ESF logics resides in diverse hardware and software equipment from the SSLC/ESF system. The process sensors that provide inputs to this diverse set of logics are diverse from the sensors used in the SSLC/ESF systems. The diverse logic equipment is nonsafety-related with triple redundant processors. The diverse equipment power source is nonsafety-related.

The initiation logic is "energize to actuate" similar to that for the SSLC/ESF. The diverse ECCS automatic initiation signal is based on two-out-of-four coincident logic processed by triple redundant processors. If RPV Level 1 is sustained for 10 seconds, the logic seals in and a DPS ECCS start signal is issued. The manual initiation signal is based on two-out-of-two coincident logic processed by triple redundant processors. A coincident logic trip decision is required from two-out-of-three processors to generate the start signal. Series discrete output switches independently process the two-out-of-three voted start signal. A valid initiation signal from all series output switches is required to generate diverse ECCS actuation. Figure 7.8-4 shows the DPS triple modular redundant logic processing.

For the SRV opening function, three of the four solenoids on each SRV are powered by three of the four divisional safety-related power sources in the ESF ADS. A fourth solenoid on each SRV is powered by the nonsafety-related load group, with the trip logic controlled by the DPS. All ten SRVs in the ADS are controlled by the DPS through the fourth solenoid on each valve.

For the DPV opening function, one of the four squib initiators on each DPV is controlled by and connected to the nonsafety-related DPS logic. However, the three other squib initiators on all of the DPVs are controlled simultaneously by the SSLC/ESF ADS logic. The reliability and availability of DPV initiation by the SSLC/ESF ADS function is not affected by the DPS logic. The typical ADS initiation logic arrangements applied in both the SSLC/ESF and DPS functions are illustrated in Figure 7.3-1a and Figure 7.3-1b. As shown in Figure 7.3-1a and Figure 7.3-1b, the logic contact circuit from the DPS is arranged in parallel with the SSLC/ESF circuit.

As described in Subsections 7.3.1 and 7.3.5, it takes three simultaneous SSLC/ESF trip signals to initiate the DPV squib valve opening. It also takes three simultaneous DPS trip signals in a triple redundant logic path to initiate the DPV squib valve opening. This satisfies the single failure criterion for inadvertent squib valve initiation. With this arrangement, the initiation of the DPVs by DPS logic does not affect the reliability and availability of the DPV initiation function controlled by the SSLC/ESF logic.

The logic application to the GDCS squib valves from the SSLC/ESF and from the DPS is similar to that of the DPV logic application described above. Short term injection via the GDCS squib valves can be initiated both by the SSLC/ESF logic and by the DPS logic. For the GDCS squib valve-opening function, one of the four squib initiators on each GDCS valve is controlled by and connected to the nonsafety-related DPS logic. The DPS logic requires three simultaneous GDCS trip initiation signals to initiate a GDCS squib valve opening.

The logic application to the SLC System squib valves from the SSLC/ESF and from the DPS is similar to that of the DPV logic application described above, except that there is a dual instead of a triple logic path. However, the SLC System squib valves are actuated by two independent safety-related divisions with one valve per loop that is also actuated by the DPS. This configuration allows the flow path of both SLC System loops to be available through activation from the DPS and from any safety-related division (Refer to Subsection 7.4.1 for a description of the SLC System).

The ICS logic is configured to allow the availability of each ICS loop flow path from the four safety-related divisions and the DPS.

7.8.1.2.3 ATWS Mitigation Logic to Inhibit ADS Initiation by DPS

To prevent ATWS events from escalating to more serious events (as described in Subsection 7.8.1.1.1.2), the DPS sustained RPV Level 1 logic is inhibited by the following signals.

- Coincident low RPV water level (Level 2) and SRNM ATWS permissive signals (i.e., an SRNM signal from the NMS that is above a specified setpoint).
- Coincident high RPV pressure and SRNM ATWS permissive signals that persist for 60 seconds.

DPS – ADS Inhibit also inhibits the ADS and GDCS Injection sequenced initiation from occurring via DPS logic.

The DPS – ADS Inhibit logic is also used to inhibit the DPS feedwater isolation on high-high drywell pressure (described in Subsection 7.8.1.2.4).

MCR controls are provided to inhibit the sustained RPV Level 1 logic, ADS and GDCS Injection sequenced initiation, and feedwater isolation on high-high drywell pressure logic within DPS under ATWS conditions.

7.8.1.2.4 Diverse Isolation Logic by DPS

The DPS also provides the following major isolations using two-out-of-four sensor logic and two-out-of-three processing logic. The isolation functions performed as part of the diverse ESF are “energize to actuate.”

- Closure of the MSIVs on detection of high steam flow rate, low RPV pressure, or low RPV water level (Level 2). The isolation function is performed by contacts in the 120 VAC MSIV solenoid return circuit. The logic is enabled when the reactor is in Run mode.
- Closure of the Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) isolation valves on high differential flow rate.
- Isolation of the feedwater lines on a feedwater line break inside containment or LOCA conditions that pose a challenge to containment design pressure. The line break is sensed by differential pressure between feedwater lines coincident with high drywell pressure. A feedwater isolation also occurs on high-high drywell pressure or high drywell pressure coincident with high drywell water level. The DPS trips the main feedwater pump adjustable speed drive (ASD) motor circuit breakers and closes the feedwater containment isolation valves.

- Isolation of CRD high pressure makeup water injection (HP CRD) on high drywell pressure coincident with high drywell level, or low level in two out of three GDCS pools.

7.8.1.2.5 Additional Functions of DPS

The following additional functions are performed by the DPS.

- With logic similar to the SSLC/ESF, the DPS initiates the ICS on high RPV dome pressure, low RPV water level (Level 2), or MSIV closure to provide core cooling.
- The DPS trips the feedwater pumps on high RPV water level (Level 9).
- The DPS opens pool cross-connect valves between the equipment storage pool and the IC/PCCS expansion pools when a low level condition is detected in either of the IC/PCCS inner expansion pools. DPS uses the four nonsafety-related level sensors in each IC/PCCS inner expansion pool which are part of FAPCS (Subsection 9.1.3.5).

The diverse protection logics for ESF function initiation, in combination with the ATWS mitigation feature, other diverse backup scram protection, and selected diverse RPS logics provide the diverse protection necessary to satisfy the design position specified in BTP HICB-19.

7.8.1.3 Diverse Manual Controls and Displays

All safety-related systems have displays and controls located in the MCR that provide manual system-level actuation of their safety-related functions and monitoring of parameters that support those safety-related functions.

In addition to the manual controls and displays for the safety-related reactor protection and SSLC/ESF functions, the DPS also has displays and manual control functions that are independent and diverse from those of the safety-related protection and SSLC/ESF functions. They are not subject to the same common mode failure as the safety-related protection system components. The manual controls permit manual initiation of the SRV, DPV, GDCS, and SLC System valves, and the ICS.

The operator is provided with a set of diverse displays separate from those supplied through the safety-related software platform. The displays that provide independent confirmation of the status of major process parameters include:

- Reactor pressure,
- Reactor pressure high alarm,
- RPV water level,
- RPV water level high alarm,
- RPV water level low alarm,
- Drywell pressure,
- Drywell pressure high alarm,
- Drywell water level,
- Drywell water level high alarm,

- Suppression pool temperature,
- Suppression pool temperature high alarm,
- SRV solenoid-controlled valves opening,
- DPV squib-initiation valves opening,
- GDCS squib-initiation valves opening,
- GDCS pool level,
- GDCS pool level low alarm,
- SLC System squib injection valves opening, and
- ICS operation.

In addition to the controls provided by the primary safety-related systems, the RSS provides manual control of shutdown cooling functions and continuous local display of monitored process parameters.

7.8.2 Common Mode Failure Defenses Within Safety-Related System Design

7.8.2.1 Design Techniques for Optimizing Safety-Related Hardware and Software

In addition to the DPS, other techniques ensure safety-related system reliability by minimizing both random and common mode failure probabilities. They are:

- The total amount of hardware is minimized;
- Microprocessors with a simple operating system are used;
- High quality components are used;
- Self-diagnostics are implemented;
- The man-machine interface (MMI) is implemented so that the equipment is structured into small units with sufficient diagnostics that a user can repair equipment by replacing modules and can operate the equipment by following straightforward instructions;
- The software design process specifies modular code;
- Software modules have one entry and one exit point and are written using a limited number of program constructs;
- Code is segmented by system and function:
  - Program code for each safety-related system resides in independent modules that perform setpoint comparison, voting, and interlock logic;
  - Code for calibration, signal input/output, online diagnostics, and graphical displays are common to all systems;
  - Fixed message formats are used for plant sensor data, equipment activation data, and diagnostic data. Thus, corrupted messages are readily detected by error-detecting software in each digital instrument;

- Software design uses recognized defensive programming techniques, backed up by self-diagnostic software and hardware watchdog timers;
- Software for control programs is permanently embedded as firmware in controller Read Only Memory (ROM);
- Commercial development tools and languages with a known history of successful applications in similar designs are used for software development;
- Automated software tools aid in verification and validation (V&V), and
- [*Reliable software is implemented by ensuring that the quality of the design and requirements specification is controlled under the formal V&V program which is discussed in the LTR "ESBWR - Software Quality Assurance Program Manual (SQAPM)," NEDO-33245, NEDE-33245P. (Reference 7.8-3.)*]*

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7.8.2.2 Defense Against Common Mode Failure

In addition to the DPS and the ATWS mitigation features, safety-related logic processing systems used in the RPS and SSLC/ESF perform the following simple and repetitive tasks. These tasks are performed continuously and simultaneously in four independent and redundant divisions of logic. They are:

- Setpoint comparison;
- Two-out-of-four voting logic processing;
- Control and interlock logic processing;
- Input/output signal processing; and
- Self-testing.

The development of common software modules for many of these functions offers advantages that:

- Produce reliable programs,
- Promote standardization and code reusability,
- Minimize program design errors, and
- Minimize timing differences among channels.

The V&V program reduces the probability of common mode failure to a very low level. The simple modules used in each division can be thoroughly tested during the validation process. In addition to software V&V, the RPS and SSLC/ESF contain system level and functional level defenses against common mode failure, including defenses within the software itself.

7.8.2.2.1 System Level Defenses

Operational defenses include:

- Asynchronous operation of multiple protection divisions. Timing signals are not exchanged among divisions;
- Automatic error checking on all multiplexed transmission paths. Only the last valid data is used for logic processing. If a permanent fault is detected, the channel alarms and a trip is initiated for the RPS and MSIV isolation functions;
- Continuous cross-checking of redundant sensor inputs;
- Continuous on-line surveillance of trip functions with divisional bypass capability for the RPS and MSIV isolation functions; and
- Continuous self-test with alarm outputs in all system devices.

Functional defenses include:

- Automatic error detection. This permits early safe shutdown or bypass before common mode effects occur. Instantaneous, simultaneous, and undetected failure on a common mode error is unlikely; and
- Separation and independence requirements that protect against global effects resulting from such factors as Electromagnetic Interference (EMI) and thermal conditions.

Software defenses:

The functional program logic in the RPS and SSLC/ESF controllers provides protection against common mode failures using:

- Redundant sensors. Data messages from the sensors have unique identifications in each division;
- Identical modules that provide simple, readily verifiable functions such as setpoint comparison and two-out-of-four logic; and
- Standard protocols for multiplexing and other data transmission functions that are verified to industry standards and are qualified to safety-related standards.

7.8.3 Safety Evaluation

The DPS is designed as a highly reliable nonsafety-related system that meets the probabilistic risk assessment (PRA) requirements to minimize failures on demand and to minimize inadvertent operation. The DPS components are designed to ensure that reliability goals and system design requirements are met. The sensors and actuation devices that interface directly with safety-related structures, systems, and components (SSC) are qualified to meet the Seismic Category I classification.

Consistent with the guidance in IEEE Std. 603, Section 5.6 and IEEE Std. 384, the nonsafety-related DPS is designed to avoid adverse interaction with the protection systems with which it interfaces. Because the DPS logic does not communicate with the RPS logic, credible DPS failure modes do not prevent the RPS from performing a reactor scram. The DPS cannot cause the RPS to initiate a reactor scram prematurely. Credible DPS failure modes cannot prevent the SSLC/ESF actuation system from initiating ECCS functions and/or performing fission product barrier isolation functions. Additionally, credible DPS failure modes cannot result in premature operation of these protection systems.

The ATWS/SLC logic is designed to mitigate a failure of the normal reactor trip system to function and is diverse from and independent of the RPS. The ATWS/SLC logic platform is designed as a safety-related system with four independent divisions powered from divisionally separated safety-related power sources. Each redundant division of ATWS/SLC logic, which uses two-out-of-four voting logic, is capable of performing ATWS mitigation during reactor operation.

A quality assurance program that meets or exceeds the guidance contained in NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," is applied to all diverse I&C systems and components described in this section. Software used in diverse instrumentation and control systems is designed and developed in accordance with the requirements of Reference 7.8-3.

The guidance contained in the SRM on SECY 93-087 Item II.Q, SRP BTP HICB-19, and Generic Letter 85-06 is applicable to the DPS and to all portions of the systems shown in Figure 7.8-1 and identified in Table 3.2-1 that are required to perform sense and actuate functions in support of the diverse instrumentation and control functions described in this Section.

Table 7.1-1 identifies the diverse I&C and the associated codes and standards applied, in accordance with the SRP. This subsection addresses I&C systems conformance to regulatory requirements, guidelines, and industry standards.

7.8.3.1 Code of Federal Regulations

10 CFR 50.55a(a)(1), Quality Standards for Systems Important to Safety:

- Conformance: The diverse I&C systems design conforms to these standards.

10 CFR 50.55a(h), Protection and Safety Systems, compliance with IEEE Std. 603:

- Conformance: The safety-related portions of the diverse I&C conform to IEEE Std. 603. Conformance information is found in Subsections 7.1.6.6.1 through 7.1.6.6.1.27. Additional information concerning how the diverse I&C conforms to IEEE Std. 603 is discussed below.
  - Section 4.2 (Safety-related Functions): See Subsection 7.8.1.1.
  - Section 4.3 (Permissive Conditions for Operating Bypasses): Permissive conditions for operating bypasses are for the Diverse I&C system are described in Tables 7.8-1 and 7.8-2.
  - Section 4.6 (Spatially Dependent Variables): Spatial dependency of monitored variables is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.1.
  - Section 5.2 (Completion of Protective Actions): Completion of Protective Actions is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.3.
  - Section 5.7 (Capability for Test and Calibration): Capability for Test and Calibration is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.8.

- Section 6.2 and 7.2 (Manual Control): Manual Control is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.18.
- Section 6.4 (Derivation of System Inputs): Derivation of System Inputs is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.20.
- Section 6.5 (Capability of Test and Calibration): Capability for Test and Calibration is not applicable to the Diverse I&C system beyond that discussed in Subsection 7.1.6.6.1.8.
- Section 6.6 and 7.4 (Operating Bypasses): Operating Bypasses are for the Diverse I&C system are described in Table 7.8-2.
- Section 6.7 and 7.5 (Maintenance Bypasses): Maintenance bypasses for the Diverse I&C system are not applicable beyond that discussed in Subsection 7.1.6.6.1.23.
- Section 8.2 (Non-Electrical Power Sources): Non-Electrical power sources for the Diverse I&C system are not applicable beyond that discussed in Subsection 7.1.6.6.1.26.
- Section 8.3 (Maintenance Bypasses): Maintenance bypasses for the Diverse I&C system power sources are not applicable beyond that discussed in Subsection 7.1.6.6.1.27.

10 CFR 50.34(f)(2)(iii) [I.D.1], Human Factors Principles for Control Room Design:

- Conformance: The diverse I&C systems design conforms to these requirements.

10 CFR 50.34(f)(2)(iv) [I.D.2], Minimum Set of Parameters on a Safety Display Console Defining the Safety Status of the Plant:

- Conformance: The diverse I&C systems design conforms to these requirements.

10 CFR 50.34(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication:

- Conformance: The safety-related ATWS mitigation logic conform to these requirements by providing automatic indication of bypassed and inoperable status.

10 CFR 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for reduction of risk from ATWS events for light-water cooled nuclear power plants:

- Conformance: The ATWS mitigation functions described in Subsection 7.8.1.1 are designed in accordance with the requirements of 10 CFR 50.62.

10 CFR 52.47(a)(21), Resolution of Unresolved and Generic Safety Issues:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(b)(1), ITAAC in Design Certification Applications:

- Conformance: ITAACs are provided for the diverse I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(25), Interface Requirements:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47, Level of Detail:

- Conformance: The level of detail provided for the diverse I&C functions within the DCD conforms to this requirement.

10 CFR 52.47(c)(2), Innovative Means of Accomplishing Safety Functions:

- Conformance: The diverse I&C systems design does not use innovative means for accomplishing safety functions.

7.8.3.2 General Design Criteria

General Design Criteria (GDC) 1, 2, 4, 13, 19, and 24:

- Conformance: The DPS design conforms to these GDC.

General Design Criteria (GDC) 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, and 29:

- Conformance: The safety-related ATWS mitigation logic design conforms to these GDC.

The design of the diverse I&C systems does not compromise the ability of the RPS and SSLC/ESF actuation system to meet the requirements of 10 CFR 50 Appendix A, "General Design Criteria for Nuclear Power Plants," Section III, "Protection and Reactivity Control Systems."

7.8.3.3 Staff Requirements Memorandum

Item II.Q, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) of SECY-93-087 and SRM on SECY 93-087 (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and ALWR Designs):

- Conformance: The SRM requirements applicable to the diverse I&C functions state that, "If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure as the safety system shall be required to perform either the same function as the safety system function that is vulnerable to common mode failure or a different function." It also states, "The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions." With respect to manual control and display functions, it states, "A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer systems."

The implementation of the DPS and the ATWS mitigation features as described in Subsection 7.8.1, in conjunction with the RPS and ESF designs, conforms to the above SRM requirements.

7.8.3.4 Regulatory Guides

RG 1.22, (Safety Guide 22) Periodic Testing of Protection System Actuation Functions:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.22. This RG is not applicable to the nonsafety-related DPS.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.47. Automatic indication is provided in the MCR to inform the operator that the system is inoperable or a division is bypassed. This RG is not applicable to the nonsafety-related DPS.

RG 1.53, Application of the Single-Failure Criterion to Nuclear Power Protection Systems:

- Conformance The safety-related ATWS mitigation logic is organized into four physically and electrically isolated divisions that use the principles of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related system designs' conformance to the single-failure criterion.. This RG is not applicable to the nonsafety-related DPS.

RG 1.62, Manual Initiation of Protection Actions:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.62. This RG is not applicable to the nonsafety-related DPS.

RG 1.75, Physical Independence of Electric Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.75. This RG is not applicable to the nonsafety-related DPS.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: .See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97-Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.105, Instrument Setpoints for Safety Systems:

- Conformance: The safety-related ATWS mitigation logic setpoints are consistent with this guide. The guidance in RG 1.105 is also applied to any portions of the nonsafety-related DPS used for maintaining automatic initiation function required by the Technical Specifications. Reference 7.8-4 provides a detailed description of the GEH setpoint methodology.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.118. This RG is not applicable to the nonsafety-related DPS.

RG 1.151, Instrument Sensing Lines:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in RG 1.151. Sections of endorsed standard ANSI/ISA-S67.02.01 on design practices for tubing, vents, and drains also apply to sensing lines that support DPS.

RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The diverse I&C conforms to the guidance in RG 1.152.

RG 1.153, Criteria for Power Instrumentation and Control Portions of Safety Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to 10 CFR 50.55a(h). This RG is not applicable to the nonsafety-related DPS.

RG 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The diverse I&C conforms to the guidance in RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The diverse I&C conforms to the guidance in RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The diverse I&C conforms to the guidance in RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The diverse I&C conforms to the guidance in RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The diverse I&C conforms to the guidance in RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants:

- Conformance: The diverse I&C conforms to the guidance in RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance provided in RG 1.204.

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.8.3.5 Branch Technical Position

BTP HICB-8, Guidance on Application of RG 1.22:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-8. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: The ESBWR I&C conforms to RG 1.97. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.

BTP HICB-11, Application and Qualification of Isolation Devices:

- Conformance: The safety-related ATWS mitigation logic conforms to BTP HICB-11. BTP HICB-11 is not applicable to the nonsafety-related DPS because all interfacing isolation devices are part of the safety-related systems.

BTP HICB-12, Establishing and Maintaining Instrument Setpoints:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-12. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-14, Software Reviews for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-14. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail for the diverse I&C systems conform to BTP HICB-16.

BTP HICB-17, Self-Test and Surveillance Test for Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-17. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-18, Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-18. This BTP is not applicable to the nonsafety-related DPS.

BTP HICB-19, Guidance for evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: Reference 7.8-1 details the echelons of defense used in the design that conforms to BTP HICB-19. This document also discusses the basis for selection of the DPS functions used as backups for the RPS and SSLC/ESF. A failure modes and effects analysis based on the Guidance in NUREG/CR-6303 (Reference 7.8-2) is performed to ensure the radiation guidelines from 10 CFR 52.47(a)(2)(iv) are not exceeded in the event of a common mode failure of the RPS or SSLC/ESF software platform during the design basis events discussed in the Safety Analyses.

BTP HICB-21, Guidance on Digital System Real-Time Performance:

- Conformance: The safety-related ATWS mitigation logic conforms to the guidance in HICB-21. This BTP is not applicable to the nonsafety-related DPS.

7.8.4 Testing and Inspection Requirements

Periodic testing to verify proper operation of the ATWS/SLC logic is performed. Periodic testing to verify proper operation of the DPS logic is also performed.

7.8.5 Instrumentation and Control Requirements

The ATWS/SLC uses logic that is diverse from the RPS. Logic and controls for ATWS/SLC are located in divisional RTIF cabinets. Operating status is available to the operator in the MCR. Division of sensors bypass capability is provided for the ATWS/SLC logic. Communication with external interfaces is through isolation devices. Provisions are made to allow testing of the ATWS/SLC logic and maintenance of the ATWS/SLC equipment.

The DPS uses triple redundant microprocessor-based automatic actuation logic that is diverse from the RPS and SSLC/ESF automatic actuation logic.

The information available to the operator from the diverse I&C systems is described in Subsection 7.8.1.3.

7.8.6 COL Information

None.

7.8.7 References

7.8-1 GE Hitachi Nuclear Energy, “ESBWR I&C Diversity and Defense-In-Depth Report”, NEDO-33251, Class I (Non-proprietary), Revision 2, May 2009.

7.8-2 NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, December 1994

7.8-3 [*GE Hitachi Nuclear Energy, "ESBWR - Software Quality Assurance Program Manual (SQAPM),"* NEDE-33245P, Class III (Proprietary), Revision 3, July 2009, and *NEDO-33245, Class I (Non-proprietary), Revision 3, July 2008*.]*

7.8-4 GE-Hitachi Nuclear Energy, "GEH ABWR/ESBWR Setpoint Methodology," NEDE-33304P, Class III (Proprietary), Revision 1, November 2008, and NEDO-33304, Class I (Non-proprietary), Revision 1, November 2008.

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

Table 7.8-1

Diverse Instrumentation and Control Systems

Functions, Initiators, and Interfacing Systems

for ATWS Mitigation or Chapter 15 Design Basis Events[1]

Function	Initiator	Interfacing System
SLC system initiation (ATWS/SLC)	RPV dome pressure high and Startup Range Neutron Monitor (SRNM) signal greater than ATWS setpoint (SRNM ATWS permissive) with time delay	NMS, NBS, SLC
	RPV water level low (Level 2) and SRNM ATWS permissive with time delay	NBS, NMS, SLC
Feedwater Runback (ATWS/SLC)	RPV dome pressure high and SRNM ATWS permissive	NBS, NMS, FWCS
ADS inhibit (ATWS/SLC)	RPV water level low (Level 2) and APRM ATWS permissive	NBS, NMS, SSLC/ESF, LD&IS
	RPV dome pressure high and APRM ATWS permissive with time delay	NBS, NMS, SSLC/ESF, LD&IS
SCRRI/SRI (DPS)	Generator load rejection signal	TGCS, RPS, RC&IS
	Turbine trip signal	TGCS, RPS, RC&IS
	Loss of Feedwater heating	C&FS, NMS, RPS, RC&IS
	ATLM SCRRI/SRI signal	RPS, RC&IS
	RC&IS SCRRI signal	RC&IS, RPS
	OPRM thermal neutron flux oscillation	NMS, RPS, RC&IS
Delayed Feedwater Runback (DPS)	SCRRI/SRI signal and power levels remain elevated	NMS, RC&IS, FWCS
	RPS scram command and power levels remain elevated	RPS, NMS, FWCS

Table 7.8-1

Diverse Instrumentation and Control Systems

Functions, Initiators, and Interfacing Systems

for ATWS Mitigation or Chapter 15 Design Basis Events[1]

Function	Initiator	Interfacing System
ATWS ARI and FMCRD motor run-in (DPS)	RPV dome pressure high	NBS, CRD, RC&IS
	RPV water level low (Level 2)	NBS, CRD, RC&IS
	Diverse scram command	CRD, RC&IS

1 Implementing system is shown in parentheses

Table 7.8-2

Diverse Instrumentation and Control Systems

Controls, Interlocks and Bypasses

for ATWS Mitigation or Chapter 15 Design Basis Events[1]

Control	Manual initiation of ATWS SLC (ATWS/SLC)
	Manual initiation of ATWS ARI (ATWS/SLC)
	Manual initiation of ATWS Feedwater Runback (ATWS/SLC)
	Manual initiation of FMCRD Run-in (DPS)
	Manual inhibit of sustained RPV Level 1 initiation logic and sustained drywell pressure high initiation logic under ATWS conditions[2] (ATWS/SLC)
	Manual inhibit of feedwater isolation under ATWS conditions[2] (ATWS/SLC)
Interlock	SRNM ATWS Permissive (ATWS/SLC)
	APRM ATWS Permissive (ATWS/SLC)
	Time Delays
Bypass	Division of sensor bypass (ATWS/SLC)
	Sensor channel bypass (DPS)

1 Implementing system is shown in parentheses.

2 For applicable ATWS conditions, refer to Initiator column, Table 7.8-1, for the Function "ADS inhibit (ATWS/SLC)."

Table 7.8-3

Diverse Instrumentation and Control Systems

Functions, Initiators, and Interfacing Systems to Address BTP HICB-19[1]

Function	Initiator	Interfacing System
Diverse Scram (DPS)	RPV dome pressure high	NBS, RPS
	RPV water level high (Level 8)	NBS, RPS
	RPV water level low (Level 3)	NBS, RPS
	Drywell pressure high	CMS, RPS
	Suppression pool temperature high	CMS, RPS
	MSIV closure	NBS, RPS
	RPS Scram	RPS
	SCRRI/SRI command with power levels remaining elevated	NMS, RC&IS, RPS
ADS initiation (DPS)	RPV water level low (Level 1)	NBS
GDCS initiation (DPS)	RPV water level low (Level 1)	NBS, GDCS
ICS initiation (DPS)	RPV water level low (Level 1)	NBS, ICS
	RPV water level low (Level 2)	NBS, ICS
	MSIV closure	NBS, ICS
	RPV dome pressure high	NBS, ICS
SLC system initiation (DPS)	RPV water level low (Level 1)	NBS, SLC
MSIV closure (DPS)	Steam flow high	NBS
	RPV pressure low	NBS
	RPV water level low (Level 2)	NBS

Table 7.8-3

Diverse Instrumentation and Control Systems

Functions, Initiators, and Interfacing Systems to Address BTP HICB-19[1]

Function	Initiator	Interfacing System
RWCU/SDC isolation valve closure (DPS)	Differential flow rate high	RWCU/SDC
Feedwater Isolation (DPS)	Line differential pressure high coincident with drywell pressure high	C&FS, CMS
	Drywell pressure high coincident with drywell water level high	CMS
	Drywell pressure high-high	CMS
Feedwater Pump Trip (DPS)	RPV water level high (Level 9)	NBS, FWCS
IC/PCCS expansion pool to equipment storage pool cross-connect valve opening (DPS)	Low IC/PCCS expansion pool water level	FAPCS, ICS
ADS inhibit[2] (DPS)	RPV water level low (Level 2) and SRNM ATWS permissive	NBS, NMS
	RPV dome pressure high and SRNM ATWS permissive with time delay	NBS, NMS

1 Implementing system is shown in parentheses

2 Inhibits logic within DPS only

Table 7.8-4

Diverse Instrumentation and Control Systems

Controls, Interlocks and Bypasses to Address BTP HICB-19[1]

Control	Manual initiation of ADS (DPS)
	Manual initiation of ICS (DPS)
	Manual initiation of GDCS squib-initiated injection valves (DPS)
	Manual initiation of GDCS squib-initiated equalization valves (DPS)
	Manual scram (DPS)
	Manual MSIV isolation (DPS)
	Manual inhibit of the sustained RPV Level 1 logic and ADS and GDCS injection sequenced initiation controls under ATWS conditions[2] (DPS)
	Manual inhibit of feedwater isolation on drywell pressure high-high under ATWS conditions[2] (DPS)
	Manual SCRRI/SRI (DPS)
Interlock	SRNM ATWS Permissive (DPS)
	Reactor Mode (RPS, DPS)
	Time Delays
Bypass	Sensor channel bypass (DPS)

1 Implementing system is shown in parentheses.

2 For applicable ATWS conditions, refer to Initiator column, Table 7.8-3, for the Function "ADS inhibit (DPS)."

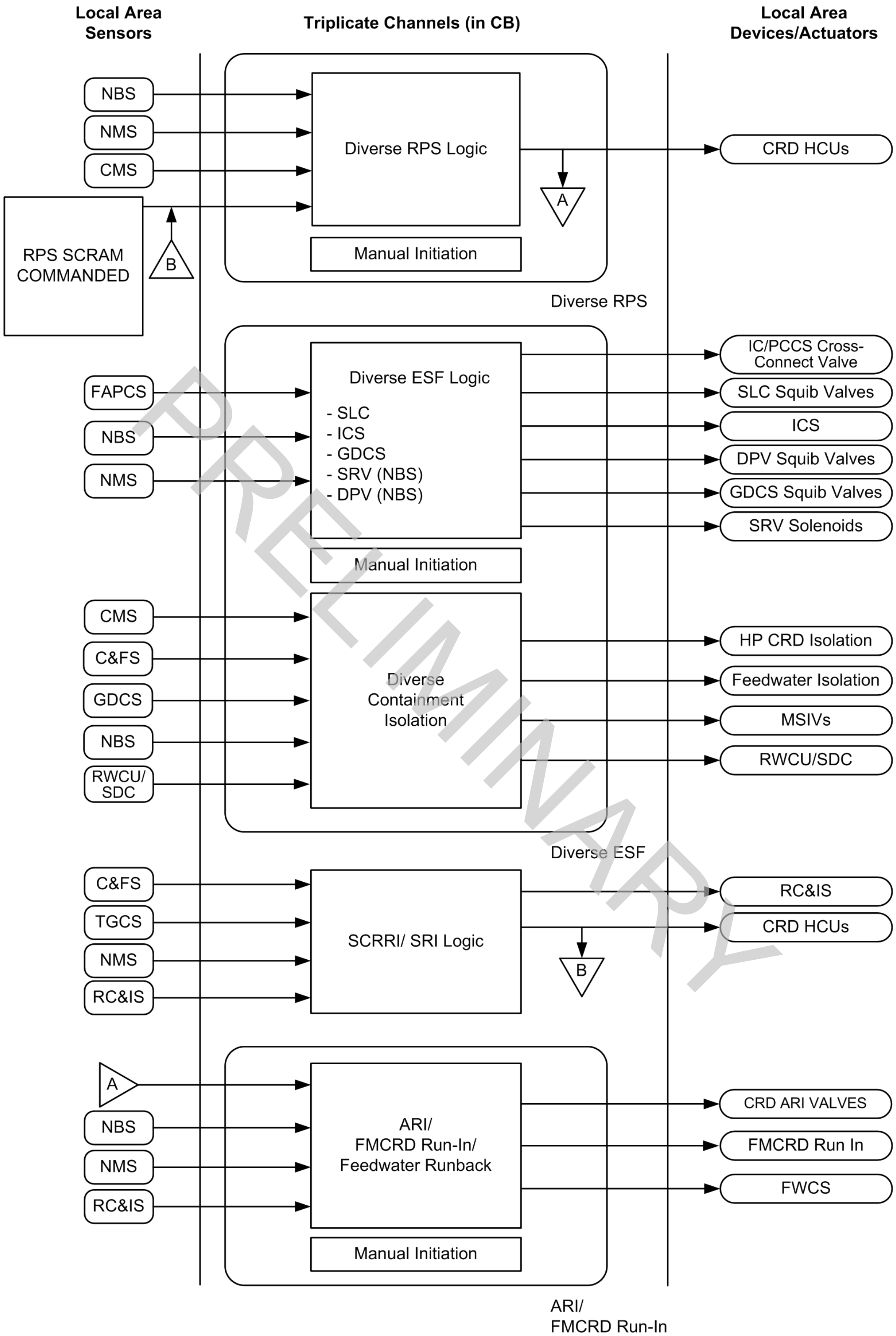
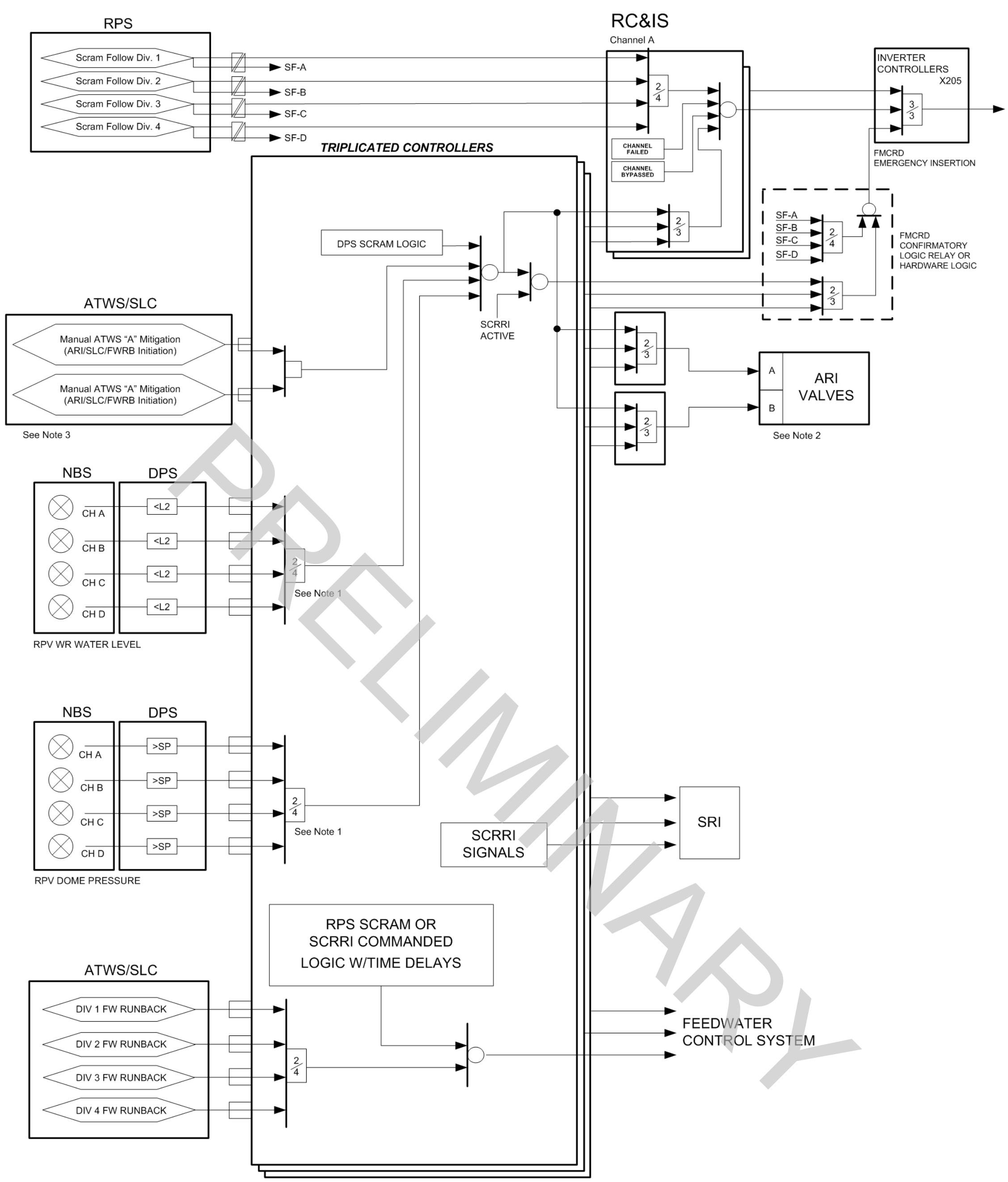
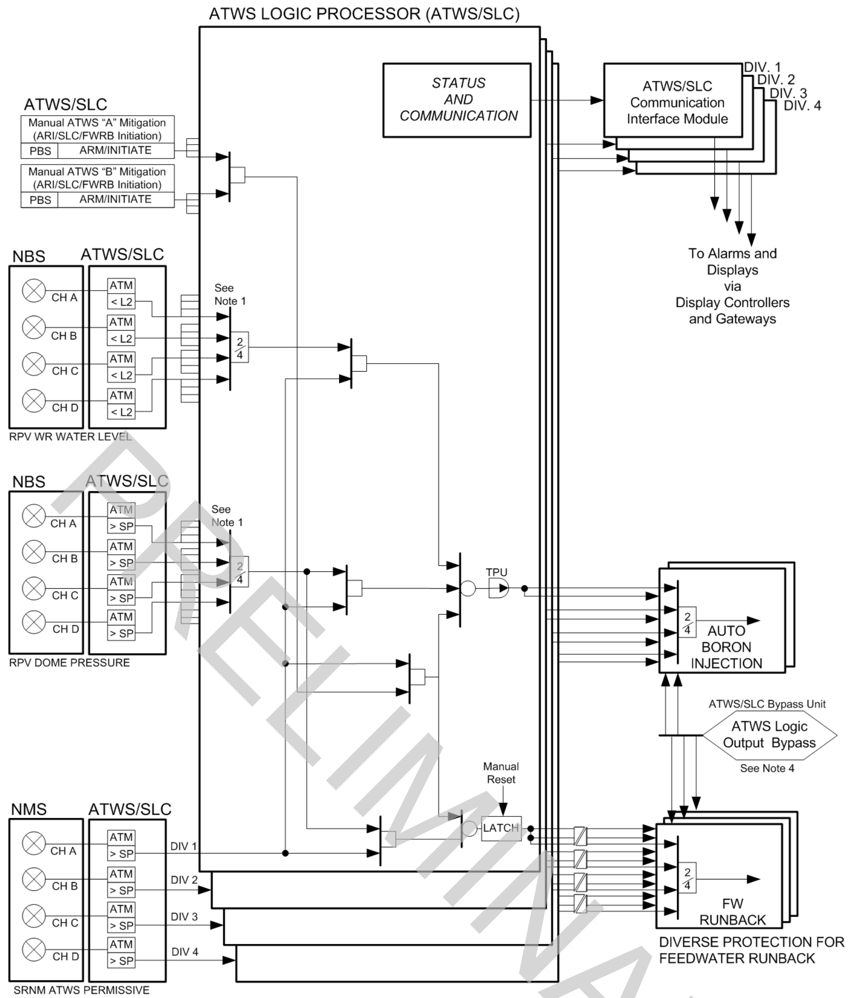


Figure 7.8-1. Simplified DPS Block Diagram



Note:
1. Comparison is part of ARI logic.
2. The ARI valves are part of CRD System.
3. Both manual pushbutton switches armed to initiate

Figure 7.8-2. Alternate Rod Insertion & FMCRD Run-in Logic



NOTES:
1. DIVISION-OF-SENSORS BYPASS INPUTS AND LOGIC NOT SHOWN.

2. THE ATWS LOGIC PROCESSOR SHALL INCLUDE DIVISION-OF-SENSORS BYPASS EXCLUSIONARY LOGIC THAT RESULTS IN A "NO BYPASS" CONDITION FOR ALL DIVISIONS IF TWO OR MORE BYPASS INPUTS ARE RECEIVED.

3. THE ATWS LOGIC PROCESSOR SHALL INCLUDE DIVISION-OF-SENSORS BYPASS LOGIC THAT BYPASSES TRIP INPUTS FROM ALL SENSORS IN ONE DIVISION WHEN DIVISION-OF-SENSORS FOR THAT DIVISION IS PRESENT.

4. SEE ATWS/SLC LOGIC DIAGRAM FOR ATWS OUTPUT BYPASS LOGIC.

5. SLC FUNCTIONS IN ATM NOT SHOWN. SEE SLC LOGIC DIAGRAM.

Figure 7.8-3. ATWS Mitigation Logic (SLC System Initiation, Feedwater Runback)

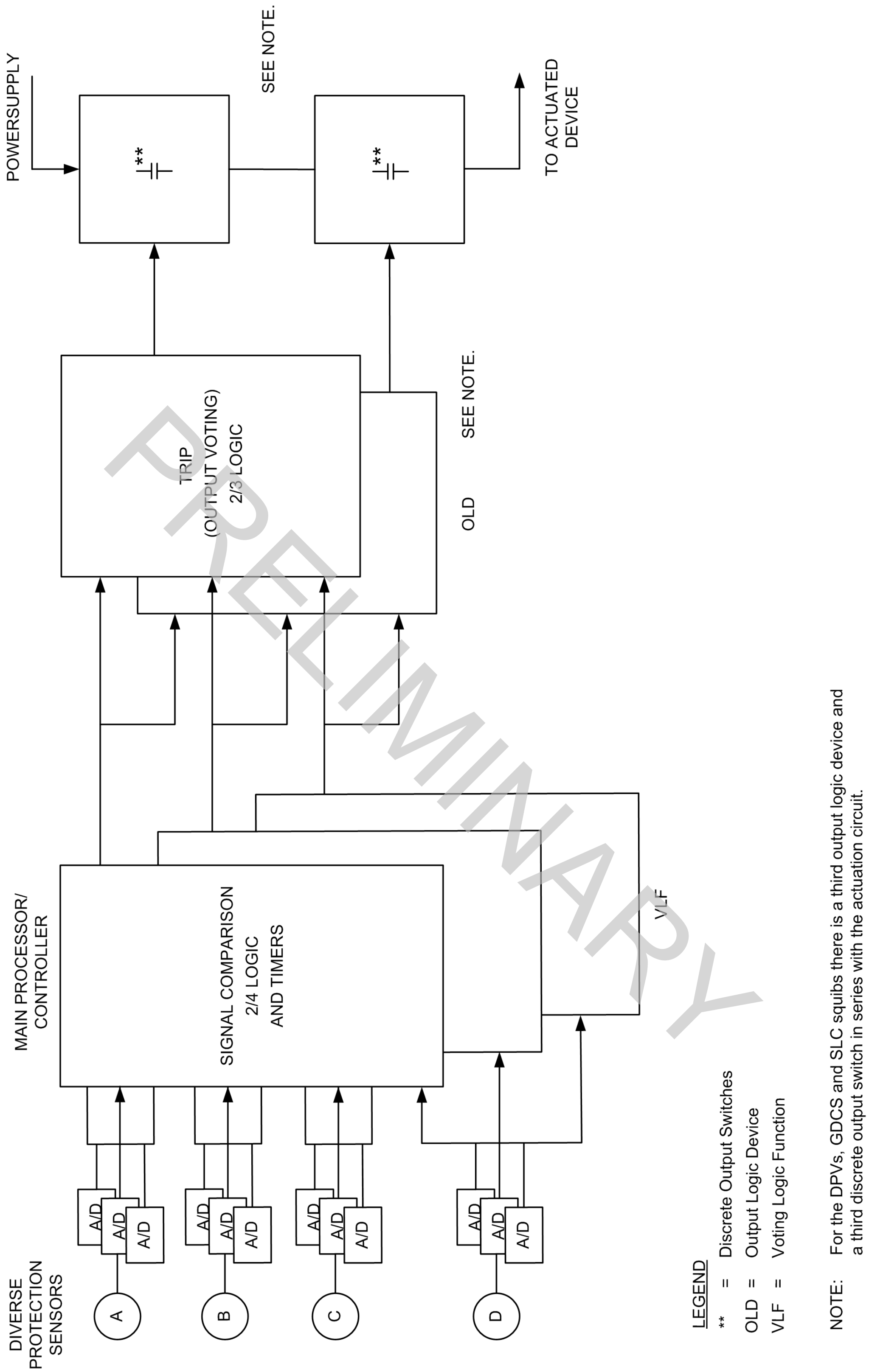


Figure 7.8-4. Diverse ESF Triple Redundant Logic

7.9 (DELETED)

7A. (DELETED)

7B. SOFTWARE DEVELOPMENT

7B.1 SOFTWARE DEVELOPMENT

The safety-related Distributed Control and Information Systems (Q-DCIS) comprise the platforms that are defined in Table 7B-1. The nonsafety-related Distributed Control and Information Systems (N-DCIS) comprise the network segments that are defined in Table 7B-2. These platforms and network segments comprise systems of integrated software and hardware elements. Software projects are developed for the various platforms and network segments.

[*Project software plans control the development of each platform and network segment using a software life cycle process. The ESBWR Software Management Program Manual (SMPM, reference 7B.3-1) and ESBWR Software Quality Assurance Program Manual (SQAPM, reference 7B.3-2) provide the bases for developing project software plans and the software life cycle model that will control the software development process. The ESBWR Cyber Security Program Plan (CySPP) (reference 7B.3-3) provides the bases for the project Cyber Security Programs (CySP). These software plans and programs comprise the data that define the platform and network segment design processes.*

A software life cycle phase baseline review process regulates the passage of the platform and network segment design from one software life cycle phase to the next software life cycle phase. A software life cycle phase baseline review record comprises a software life cycle phase requirements traceability analysis report, a software life cycle phase software safety analysis report, a software life cycle phase verification and validation report, a software life cycle phase cyber security analysis report, a software life cycle configuration management assessment, and a software life cycle phase baseline review team report. Baseline review records exist at the end of each software life cycle phase and conclude that the design process has been followed and that the design elements are adequate to pass through to the next software life cycle phase. The summary baseline review records provides assurance that the project software plans are implemented and producing adequate results at the end of each software life cycle phase. The platform and network segment baseline review record documentation will support closure of ITAAC including {{Design Acceptance Criteria}} ITAAC.

A multiple-phase test process, using a series of overlapping tests, confirms that the as-built platform and network segment performs as designed. The Factory Acceptance Test confirms that each part of a platform and network segment performs as designed. The Site Acceptance Test confirms that the platforms and network segments are capable of operating as shown in the Factory Acceptance Test and operate as designed as an integrated ESBWR instrumentation and control system]*

In support of the above described software development process, the following software design commitments are made:

(1) The platform software plans, network segment software plans, and cyber security programs for each platform software project and network segment software project are developed in accordance with the following design acceptance criteria shown for each software development software life cycle phase plan and cyber security program:

a. Software Management Plan (SMP):

- [*Establish project management activities, which include but are not limited to the following activities:*
  - *Project planning and scheduling*
  - *Project monitoring and control*
  - *Project execution*
  - *Post delivery and closeout*]*
- [*Define the organization and responsibilities of individuals or groups involved in the various design and V&V activities*]*
- [*Define risks management process*]*
- [*Establish the methods and tools for project management*]*
- [*Define financial (budget) responsibilities and controls*]*
- [*Define security (including cyber security) requirements*]*
- [*Define training requirements and qualification of project personnel*]*

b. Software Development Plan (SDP)

- [*Describes the plan for technical project development of the I&C software which performs the monitoring, control, and protection functions for all modes of plant operation*]*
- [*Describes the software development process for each phase of the software product's software life cycle process, i.e., Planning, Requirements, Design, Implementation, Test, Installation, Operations & Maintenance (O&M), and Retirement*]*
- [*Establishes the standards, methods, tools, and procedures for the software design and development process*]*
- [*Defines the activities performed for each phase of the software development*]*
- [*Defines how requirements are traced to lower levels of the software life cycle phases from planning phase to test phase*]*
- [*Specifies how the safety-related requirements are documented, evaluated, reviewed, verified, and tested during the design process to minimize unknown, unreliable, and abnormal conditions*]*
- [*Describes the organization and responsibilities of individuals or groups involved in the various V&V and review activities*]*
- [*Addresses metrics that include error tracking, cyber security tracking, and resolution*]*

c. Software Integration Plan (SIntP)

- [*Describes the process for integrating the various software modules together to form single programs*]*
- [*Describes the process for integrating the software module integration result with the hardware and instrumentation*]*
- [*Describes the process for validating the resulting integrated product*]*
- [*Describes the organization and responsibilities of individuals or groups involved in the test activities*]*
- [*Describes software test management (e.g., scheduling, resource planning, security, risks and contingency planning, anomaly, problem reporting, and training needs)*]*
- [*Describes the methods for software testing*]*
- [*Provides the requirements and guidelines necessary to prepare, execute, and document software tests*]*
- [*Defines required software test documentation*]*
- [*Defines measurements and metrics for error tracking and resolution, and assess the success or failure of the software integration and software test effort*]*

d. Software Installation Plan (SIP)

- [*Describes the software installation process and activities performed during the Installation phase*]*
- [*Defines the installation phase activities*]*
- [*Describes the installation procedures*]*
- [*Describes the software installation management. This includes, but is not limited to, scheduling, resource planning, security, risks and contingency planning, anomaly and problem reporting, and training needs*]*
- [*Provides the requirements and guidelines necessary to prepare, execute, and document software installation*]*

e. Software Operation and Maintenance Plan (SOMP)

- [*Defines requirements, methods, and considerations for problem reporting, disposition of change request, backup media maintenance and disaster recovery operations during the Operation and Maintenance Phase*]*
- [*Addresses the activities required to support the licensee during the Operation and Maintenance phase*]*

f. Software Training Plan (STrngP)

- [*Describes the software training activities to be carried out before and during the operation of software products for the plant*]*
- [*Addresses management, implementation and resource characteristics*]*

- [*Defines the requirements and methods used to develop the training program and manual*]*
- [*Defines the training needs of appropriate plant staff, including operators, I&C engineers, and technicians*]*
- [*Defines a general description of the training facilities*]*
- [*Defines the organization supporting the training effort including interfaces and responsibilities*]*

g. Software Quality Assurance Plan (SQAP)

- [*Defines the management organization, techniques, procedures, and methodologies used to assure the delivery of software which meets specified requirements*]*
- [*Assures that software development, evaluation and acceptance standards, are implemented, documented, and followed*]*
- [*Assures that the results of software quality reviews and audits will be given to appropriate management within the scope of the SQAPM*]*
- [*Assures that test results adhere to acceptance standards*]*

h. Software Safety Plan (SSP)

- [*Establishes the processes and activities to ensure that the safety concerns of the software products are properly considered during the software development*]*
- [*Describes the roles and responsibilities of the Software Safety Team (SST)*]*
- [*Describes the Software Safety Analysis (SSA) process*]*
- [*Ensures that all system safety-critical requirements have been satisfied by the software life cycle phases*]*
- [*Ensures that no additional hazards have been introduced by the work done during the software life cycle activity*]*

i. Software Verification & Validation Plan (SVVP)

- [*Establishes the V&V tasks for the software designed and developed for software products*]*
- [*Ensure that the developed software meets its specified requirements, performs its intended functions correctly, and does not perform any unintended function*]*
- [*Ensure that the final software product meets the contract requirements, required industry and regulatory standards, and licensing commitments*]*
- [*Ensure that the final software product is correct, complete, accurate, and traceable to requirements specified in the design documents and outputs*]*

j. Software Configuration Management Plan (SCMP)

- [*Establishes the Software Configuration Management (SCM) activities during the design and development of the software products*]*

- [*Describes the individual with the overall responsibility and authority for the SCM and organizations responsible for supporting the SCM activities*]*
- [*Defines the SCM tasks, including methods, timing, and responsibility for the implementation of design control and design change control*]*
- [*Identifies the tools, procedures, and individuals needed to execute or support each SCM task*]*
- [*Identifies the SCM required schedule and coordination with the design activities and the Quality tasks described in this SQAPM*]*

k. Software Test Plan (STP)

- [*Prescribes the scope, approach, resources, and schedule of the testing activities associated with the software development process*]*
- [*Identifies the items being tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with this plan*]*
- [*Defines the purpose, format and content for each test document*]*

l. Cyber Security Program (CySP)

- [*Provides guidance for developing the ESBWR Cyber Security Program (CySP) for critical digital assets (CDAs)*]*·
- [*Provides a framework for managing a cyber security program that includes description of roles and responsibilities, development of policies and procedures, development of cyber security defensive model, evaluation of third party networks, development training and awareness program, development of contingency and disaster recovery plans, performance of periodic threat and vulnerability review, and preparation of cyber security assessment report*]*
- [*Provides specific guidance for the implementation of cyber security requirements throughout the life cycle phases of software development*]*·
- [*Addresses cyber security quality assurance requirements*]*·
- [*Provides requirements for an incident response and recovery plan*]*

(2) Implementation of the software projects for each platform and network segment in accordance with the approved software plans ensures that adequate software products are produced at the conclusion of each software life cycle phase baseline as documented by the following software life cycle phase Summary Baseline Review Records.

a. [*Planning Phase Summary baseline review records are produced for each hardware and software platform or network segment accordance with the criteria described in the SMPM, Section 5.6.5 (Reference 7B.3-1)*]*

b. [*Requirements Phase Summary baseline review records are produced for each hardware and software platform or network segment in accordance with the criteria described in the SMPM, Section 5.7.12 (Reference 7B.3-1)*]*

c. [*Design Phase Summary baseline review records are produced for each hardware and software platform or network segment in accordance with the criteria described in the SMPM, Section 5.8.3.13 (Reference 7B.3-1)*]*

d. [*Implementation Phase Summary baseline review records are produced for each hardware and software platform or network segment in accordance with the criteria described in the SMPM, Section 5.9.3.10 (Reference 7B.3-1)*]*

e. [*Test Phase Summary baseline review records are produced for each hardware and software platform or network segment in accordance with the criteria described in the SMPM, Section 5.10.9 (Reference 7B.3-1)*]*

(3) A multiple-phase test process performed as part of the installation phase will be used to confirm that each as-built platform or network segment performs in accordance with its defined criteria.

a. [*Installation Phase Summary baseline review records are produced for the each software project in accordance with the criteria described in the SMPM, Section 5.11.10 (Reference 7B.3-1). The Installation Phase baseline review will assess the results summary report for the Factory Acceptance Test to ensure the Factory Acceptance Test was performed in accordance with the criteria described in the SQAPM, Sections 7.4 and 7.5 (Reference 7B.3-2), and confirms that each part of the as-built software project performs as designed. The Factory Acceptance Test is documented in two parts in accordance with the SQAPM, Section 7.7 (Reference 7B.3-2), such that, a Factory Acceptance Test and a cyber security Factory Acceptance Test will be performed on each platform or network segment.*]*

b. [*Installation Phase Summary baseline review records are produced for the each software project in accordance with the criteria described in the SMPM, Subsection 5.11.10 (Reference 7B.3-1). The Installation Phase baseline review will assess the results summary report for the Site Acceptance Test and will confirm, using overlapping tests during Site Acceptance Test, that the as-built platforms or network segments, when integrated, are capable of operating as designed as a complete ESBWR instrumentation and control system with sensors and actuators.*]*

Text sections that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

7B.2 TREATMENT OF SYSTEMS DESIGNATED AS RTNSS

Table 19A-2 defines the structures, systems, and components (SSC) that perform significant safety, special event, or post-accident recovery functions that will be subject to additional regulatory oversight under the RTNSS program. The N-DCIS network segment SSC that perform these RTNSS functions are identified Table 7B-2. RTNSS SSC are subject to Maintenance Rule (10 CFR 50.65), the Availability Control Manual (ACM; Chapter 19, Appendix ACM), and verification by the inspections, tests, analyses, and acceptance criteria (ITAAC) in Tier 1. RTNSS SSC follow existing design processes. Thus, the software development process does not distinguish between RTNSS and non-RTNSS SSC. RTNSS SSC are developed using the software classification assigned to the network segment. The SQAPM (reference 7B.3-2) describes software classification.

7B.3 REFERENCES

7B.3-1 [*GE Hitachi Nuclear Energy, "ESBWR – Software Management Program Manual," NEDO-33226, Class I (Non-proprietary); and NEDE-33226P, Class III (Proprietary), Revision 4, May 2009.*]*

7B.3-2 [*GE Hitachi Nuclear Energy, "ESBWR – Software Quality Assurance Program Manual," NEDO-33245, Class I (Non-proprietary); and NEDE-33245P, Class III (Proprietary), Revision 3, July 2008.*]*

7B.3-3 [*GE-Hitachi Nuclear Energy, "ESBWR Cyber Security Program Plan," NEDO-33295, Class I (Non-proprietary); and NEDE-33295P, Class III (Proprietary), Revision 0, October 2007.*]*

References that are bracketed and italicized with an asterisk following the brackets are designated as Tier 2. Prior NRC approval is required to change.

Table 7B-1

Q-DCIS Platforms

Platform	Software Project
Reactor Trip & Isolation System Function Neutron Monitoring System (RTIF-NMS)	RTIF
	NMS
Safety System Logic & Control / Engineered Safety Features (SSLC/ESF) Platform	SSLC/ESF
Independent Control Platform (ICP)	VBIF
	ATWS/SLC
	HP CRD Isolation Bypass Function

Table 7B-2

N-DCIS Network Segments†

GENE (DPS)
PIP A and PIP B (FAPCS and supporting systems)
BOP
PCF

†Network segments are described in Subsection 7.1.4.8. RTNSS components of the network segments are identified in parentheses.

Table 7B-3

(Deleted)

Table 7B-4

(Deleted)

Table 7B-5

(Deleted)

Table 7B-6

(Deleted)

Table 7B-7

(Deleted)

Table 7B-8

(Deleted)