HITACHI

GE Hitachi Nuclear Energy

Richard E. Kingston
Vice President, ESBWR Licensing

PO Box 780
3901 Castle Hayne Road, M/C A-65
Wilmington, NC 28402-0910 USA

T 910.819.6192
F 910.362.6192
rick.kingston@ge.com

MFN 09-374 Docket No. 52-010

June 15, 2009

U.S. Nuclear Regulatory Commission
Document Control Desk
Rockville, MD 20852

Subject: **Response to Portion of NRC Request for Additional Information Letter No. 319 Related to ESBWR Design Certification Application - RAI 7.1-139**

Enclosure 1 contains the GE Hitachi Nuclear Energy (GEH) response to Request for Additional Information (RAI) Number 7.1-139 from the U.S. Nuclear Regulatory Commission (NRC) sent by NRC letter dated April 15, 2009 (see Reference 1). Enclosure 2 contains the DCD markup pages associated with the response.

Verified DCD changes associated with this RAI response are identified in the enclosed DCD markups by enclosing the text within a black box. Changes to the DCD figures are identified by a red box.

If you have any questions or require additional information, please contact me.

Sincerely,

Richard E. Kingston

Richard E. Kingston
Vice President, ESBWR Licensing

Reference:

1. MFN 09-259, Letter from U.S. Nuclear Regulatory Commission to Jerald G. Head, *Request for Additional Information Letter No. 319 Related to ESBWR Design Certification Application*, dated April 15, 2009.

Enclosures:

1. Response to Portion of NRC Request for Additional Information Letter No. 319 Related to ESBWR Design Certification Application – RAI Number 7.1-139

2. Response to Portion of NRC Request for Additional Information Letter No. 319 Related to ESBWR Design Certification Application – DCD Markups for RAI Number 7.1-139

cc:

AE Cubbage	USNRC (with enclosures)
JG Head	GEH/Wilmington (with enclosures)
DH Hinds	GEH/Wilmington (with enclosures)
eDRF Section:	0000-0101-5044 (7.1-139)

MFN 09-374

Enclosure 1

Response to Portion of NRC Request for Additional Information Letter No. 319 Related to ESBWR Design Certification Application

RAI Number 7.1-139

NRC RAI 7.1-139

Several instrumentation and control (I&C) issues were raised that might require further clarification during interactions with the Advisory Committee on Reactor Safeguards (ACRS). After further review, the staff has identified the following issues that require clarification by GEH.

1. *The Deluge System is used for severe accident monitoring function. The capability of the power source for the Deluge System should be documented in the DCD. For example, DCD Tier 2, Section 7.3.1.2.2 System Description of Deluge System does not include a discussion about life of the Deluge System batteries, with or without chargers.*

2. *Additional clarification is required in the DCD of the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) and the anticipated transient without scram (ATWS) independent control platform control of the standby liquid control (SLC) system. The DCD is unclear whether the SLC isolation valves are controlled by each of these systems, and if so, which system has priority if concurrent signals occur.*

3. *DCD Tier 2 Figure 7.1-1 shows the elements of the Q-DCIS and the N-DCIS with a very high-level functional representation. During the ACRS meeting, GEH presented additional architectural information, including a simplified diagram with a "safety ring." This level of architectural detail needs to be included in the DCD for the safety systems. Add figures with this level of detail to the DCD with corresponding discussion in the text as applicable.*

4. *Provide additional clarification in DCD Section 7.4.2.2.2 to describe how plant control is transferred from the main control room to remote shutdown station (RSS). If RSS is normally online and with no operators at the panels, clarify the kind of administrative control will be implemented for these panels.*

GEH Response by Questions

Question 1

1. *The Deluge System is used for severe accident monitoring function. The capability of the power source for the Deluge System should be documented in the DCD. For example, DCD Tier 2, Section 7.3.1.2.2 System Description of Deluge System does not include a discussion about life of the Deluge System batteries, with or without chargers.*

GEH Response

The two nonsafety-related deluge system PLCs are powered from different sets of batteries, which are also different from the set of batteries powering the deluge system valves. Each set of batteries is supported by a battery charger operating on nonsafety-related power, and has the capability to provide power for 72 hours with nonsafety-related power lost. This clarification will be added to DCD Subsection 7.3.1.2.2.

DCD Impact

DCD Tier 2, Subsection 7.3.1.2.2 will be revised in DCD Revision 6 as noted in Enclosure 2.

Question 2

2. *Additional clarification is required in the DCD of the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) and the anticipated transient without scram (ATWS) independent control platform control of the standby liquid control (SLC) system. The DCD is unclear whether the SLC isolation valves are controlled by each of these systems, and if so, which system has priority if concurrent signals occur.*

GEH Response

The RAI reference to "SLC isolation valves" is inferred to be a reference to the SLC injection shut-off valves. The SLC injection shut-off (isolation) valves are controlled by the ATWS/SLC platform only. This will be clarified in DCD Subsection 7.4.1.2.2.

DCD Impact

DCD Tier 2, Subsection 7.4.1.2.2 will be revised in Revision 6 as noted in Enclosure 2.

Question 3

3. *DCD Tier 2 Figure 7.1-1 shows the elements of the Q-DCIS and the N-DCIS with a very high-level functional representation. During the ACRS meeting, GEH presented additional architectural information, including a simplified diagram with a "safety ring." This level of architectural detail needs to be included in the DCD for the safety systems. Add figures with this level of detail to the DCD with corresponding discussion in the text as applicable.*

GEH Response

Chapter 7 will be revised to provide revised and additional figures along with corresponding descriptions.

Subsection 7.1 revised figures:

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

Subsection 7.2 new figures:

- Figure 7.2-11a, Reactor Trip and Isolation Function (RTIF) Functional Block Diagram (description in subsection 7.2.1.2.4.4)
- Figure 7.2-11b, Reactor Trip and Isolation Function (RTIF) Functional Block Diagram - Output Logic Unit Detail (description in subsection 7.2.1.2.4.4)
- Figure 7.2-12, Neutron Monitoring System (NMS) Functional Block Diagram (description in subsection 7.2.2.5.3)

Subsection 7.2 revised figures:

- Figure 7.2-2, RPS Interfaces and Boundaries Diagram.

Subsection 7.3 new figures:

- Figure 7.3-6, SSLC/ESF Division 1 Layout (description in subsection 7.3.5.2.1)
- Figure 7.3-7, SSLC/ESF Functional Block Diagram (description in subsection 7.3.5.2.1)
- Figure 7.3-8, SSLC/ESF Interdivisional Communication Detail (description in subsection 7.3.5.2.1)
- Figure 7.3-9,SSLC/ESF Safety-Related VDU Communication Detail (description in subsection 7.3.5.2.1)

- Figure 7.3-10, SSLC/ESF Nonsafety-Related Communication Detail (description in subsection 7.3.5.2.1)

Subsection 7.3 revised figures:

- Figure 7.3-1a, SRV Initiation Logics
- Figure 7.3-1b, GDCS and DPV Initiation Logics
- Figure 7.3-2, GDCS Equalizing Valve Initiation Logics
- Figure 7.3-3, LD&IS System Design Configuration
- Figure 7.3-4, SSLC/ESF Functional Block Diagram
- Figure 7.3-5, SSLC/ESF System Interface Diagram

Subsection 7.4 revised figures:

- Figure 7.4-3, Isolation Condenser System Initiation and Actuation

As a result of answering this RAI and providing additional DCIS design detail, the following conforming changes were also made for completeness, accuracy and consistency:

- Various editorial improvements for readability and consistency with other DCD Chapters and previously submitted RAI responses.

- In DCD Tier 2 Subsection 7.1.5.2.1.4, the description of the nonsafety-related CRD system to maintain the hydraulic control unit (HCU) accumulators at the pressure required to assure a successful scram was clarified.

- In DCD Tier 2 Subsection 7.1.5.2.3.4, clarified that the "one button startup and synchronization sequence" applies to the turbine generator startup.

- In DCD Tier 2 Subsection 7.1.5.2.4.8, the description of 3DMonicore operations was clarified to provide for both automatic and manual data acquisition of parameters and not just automatic as was originally stated.

- In DCD Tier 2 Subsection 7.1.5.3, the description of Auxiliary Fuel Building was changed to Fuel Building to match Chapter 1.

- In DCD Tier 2 Subsection 7.1.6.6, the phrase "HP CRD isolation bypass logic controller" was added for consistency with RAI 21.6-103, Item# 10.

- In DCD Tier 2 Subsection 7.1.6.6.1.13, the phrases "predefined components of" (the nonsafety-related I&C) plus "and other predefined nonsafety-related heat loads" were added to provide clarity and consistency with DCD Chapter 9.

- Throughout the DCD markups, the word "different" was changed to "diverse" or "diversity" for clarity and consistency with the Diversity and Defense in Depth Topical Report (NEDE-33251).

- Throughout the DCD, made corrections for compliance with the DCD Global Acronym List (GAL).

- In DCD Tier 2 Subsection 7.3.4.2, throughout this Section modified or added information associated with the CRHAVS generally and EFU specifically related to (a) low flow detection at the outlet of the operating EFU filter train, (b) safety classification of low flow detection, (c) safety classification of high radiation detection functions, (d) radiation sensor location, and (e) initiation setpoint, to be technically correct and to be consistent with and between Chapters 1, 6, 7, 9, 11, 16, and Tier 1.

- In DCD Tier 2 Subsection 7.3.4.2, modified or added information associated with the CRHAVS generally and the EFU smoke purge ducts specifically related to the intake and exhaust (versus discharge) ducts and the use of four redundant safety-related discharge flow detectors installed in each discharge duct to be technically correct and to be consistent with and between Chapters 1, 9, 16, and Tier 1.

- ·In DCD Tier 2 Subsection 7.4.1.2, replaced "dual keylocked control switches" with "any two of four switches" and added "that will require at least two manual operator actions," for clarity.

- ·In DCD Tier 2 Subsection 7.4.1.3, replaced "dual" with "two of four" for clarity and deleted "The manual SLC system switches are protected by key locks to minimize the likelihood of inadvertent operation," to include use of VDU-based switches.

- ·In DCD Tier 2 Subsection 7.4.2.1, modified existing text to clarify applicability of the RSS to provide the capability to achieve and maintain stable shutdown conditions.

- ·In DCD Tier 2 Subsections 7.4.1.2, 7.4.1.3, 7.4.14, and 7.4.15, replaced the term "accumulator shut-off valves" with "injection shut-off valves" to be consistent with the terms as described in Subsection 9.3.5.

DCD Impact

DCD Tier 2, Chapter 7, Sections 7.1, 7.2, 7.3, and 7.4 will be revised in Revision 6 as shown in Enclosure 2.

Question 4

4. Provide additional clarification in DCD Section 7.4.2.2.2 to describe how plant control is transferred from the main control room to remote shutdown station (RSS). If RSS is normally online and with no operators at the panels, clarify the kind of administrative control will be implemented for these panels.

GEH Response

Remote Shutdown System (RSS) VDUs panels are connected to Q-DCIS or N-DCIS through the same networks serving VDUs in the MCR. All Division 1 and 2 safety-related and all nonsafety-related data/display/control functions available at the MCR are available at the RSS panels. A simplified RSS panel schematic is provided in Figure 7.4-1. Operator activities related to the transfer of plant control between the main control room and RSS panels are controlled by plant procedures. The task is analyzed and procedures are developed as part of the HFE design process. DAC-ITAAC are provided for the HFE design process (refer to Tier 1, Table 3.3-2, items 3, and 7). Access to the RSS and panels therein will be determined as part of the IEEE-603 Criterion 5.9 analysis (refer to Tier 2, Subsection 7.1.6.6.1.10). DAC-ITAAC are provided for this analysis (refer to Tier 1, Table 2.2.15-2, Item 12).

DCD Impact

DCD Tier 2, Chapter 7, subsection 7.4.2.2.1 and Figure 7.4-1 will be revised in Revision 6 to include the two PIP VDUs in the RSS panels, as shown in Enclosure 2.

MFN 09-374

Enclosure 2

Response to Portion of NRC Request for Additional Information Letter No. 319 Related to ESBWR Design Certification Application

DCD Markups for RAI Number 7.1-139

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 ~~A network diagram of the DCIS appears as Figure 7.1-2, which is a~~ functional representation of the ~~design~~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 Defense-In-Depth And Diversity 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.

~~The software for the Q-DCIS and N-DCIS is designed and developed in accordance with the LTRs "ESBWR I&C Software Management Plan," NEDO-33226, NEDE-33226P, and "ESBWR I&C Software Quality Assurance Plan" NEDO-33245, NEDE-33245P. (References 7.1-12 and 7.1-10, respectively.) These plans describe the managerial, design, development, and software quality assurance requirements for the DCIS and address the Nuclear Regulatory Commission (NRC) review guidance provided in the Standard Review Plan.~~

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 independent of each other: ~~NUMAC for the~~ Reactor Trip Isolation Function-Neutron Monitoring System (RTIF-NMS)~~ functions~~, ~~TRICON for~~ Safety System Logic and Control/Engineered Safety Features (SSLC/ESF)~~ functions~~, and the Independent Control Platform (ICP). The ICP provides independent logic control~~lers for~~of the Anticipated Transient Without Scram mitigation and Standby Liquid Control (ATWS/SLC) functions, ~~and~~ 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. ~~Each division is segmented into systems; segmentation allows, but does not require, the systems to operate independently of each other.~~

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

~~Reactor Trip and Isolation Function (RTIF) cabinets.~~ 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

    - ~~Anticipated Transient Without Scram/Standby Liquid Control (ATWS/SLC) functions (Refer to Subsection 7.4.1),~~
    - Suppression Pool Temperature Monitoring (SPTM) ~~subsystem~~ function of the Containment Monitoring System (CMS) (Refer to Subsection 7.2.3).~~, and~~
  - **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).
- ~~Neutron Monitoring System (~~NMS Functions~~) (Refer to Subsection 7.2.2) which includes~~:

  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 ~~(Refer to Subsection 7.3.5) which includes:~~
  - 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),
- Main control room (MCR) wide display panels/consoles that house controls and monitoring,
- 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 Design Basis Events (DBEs) identified in Chapter 15. 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 always 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 example, GDCS, ICS, and ADS)~~.

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 appropriate 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 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.

- 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, SPTM function (of CMS), ~~and~~ 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.

~~Note that a~~Although the RTIF cabinets house the RPS, the ATWS/SLC functions, ~~and~~ the VB isolation ~~valve~~ function~~ systems~~, and the HP CRD isolation bypass function, the logics for the ATWS/SLC, ~~and~~ VB isolation~~ valve function~~, and the HP CRD isolation bypass functions ~~logic~~ use ~~different~~diverse hardware and their designs are not fail-safe. The RPS ~~sensors,~~ hardware/software platform~~,~~ ~~and logic are~~is diverse from the SSLC/ESF~~ logic~~, the VB isolation function~~ logic~~, the ATWS/SLC ~~mitigation logic~~, the HP CRD isolation bypass function, and the ~~Diverse Protection System (~~DPS~~)~~ ~~logic.~~hardware/software platforms; the RPS and DPS sensors are diverse and RPS sensors are not shared with other Q-DCIS or N-DCIS systems.

7.1.2.8.3.2 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 ~~Subsystem~~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~~on independent logic controllers as a Q-DCIS subsystem~~, which is diverse from the RTIF-NMS platform and the SSLC/ESF platform and not susceptible to a common-cause failure~~and uses equipment different from the RPS, NMS, and SSLC/ESF equipment~~. 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. ~~A simplified functional block diagram of the DCIS is shown as part of Figure 7.1-1.~~ 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 ~~part of~~

Figure 7.1-1~~2~~, 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, 4.5, 4.8, and 4.10. 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

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 ~~NUMAC chassis~~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 ~~NUMAC chassis~~RTIF-NMS platform has correctly received the 3D MONICORE data. If a checkback signal is utilized, it is initiated by the ~~NUMAC~~ RTIF-NMS equipment and sent to 3D MONICORE. 3D MONICORE receives the checkback signal, verifies/validates that the information received by the ~~NUMAC~~ RTIF-NMS equipment is what was sent, and then sends a signal back to the ~~NUMAC~~ 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 ~~NUMAC~~ RTIF-NMS platform~~chassis~~ 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~~NUMAC chassis~~ ~~and~~ then entering it manually. The manual process is still possible. After the download is accepted by the RTIF-NMS platform~~NUMAC~~, 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 possibly 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 either centralized control processors or are various cabinets 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 ~~outputs are hardwired directly to the~~ 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~~(IEEE Std. 603, Section 6.5.)~~.

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 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, Section 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~~(IEEE Std. 603, Section 5.7 and 6.5)~~.

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 ~~(IEEE Std. 603, Section 8.1)~~.

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 ~~two~~ three diverse safety-related platforms~~,~~: ~~NUMAC for~~ RTIF-NMS ~~functions~~ (RPS, NMS, and the MSIV isolation function) and ~~TRICON for~~ SSLC/ESF ~~functions (ADS, GDCS, ICS, SLC, LD&IS functions (except MSIV isolation)~~, and ~~CRHS)~~ICP.

~~Both~~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 ~~NUMAC~~RTIF-NMS and ~~TRICON~~SSLC/ESF are qualified as safety-related in conjunction with functional software qualification ~~(IEEE Std. 603, Section 5.7)~~, and also meet the self-diagnostic characteristics for digital computer based protection systems recommended by IEEE Std. 7-4.3.2.

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

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

The ~~TRICON~~SSLC/ESF platform~~,~~ is a Triple Modular Redundant (TMR) system, ~~has~~ 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 ~~NUMAC~~RTIF-NMS and ~~TRICON~~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 (~~TRICON~~SSLC/ESF platform),
- Inter-divisional communication between RPS and NMS logic processors or logic functions~~instruments~~ (~~NUMAC~~RTIF-NMS platform),~~ and~~
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (~~TRICON~~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 ~~NUMAC~~RTIF-NMS~~/~~ or ~~TRICON~~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 periodic testing performed to support surveillance requirements of the Technical Specifications. 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 ~~NUMAC/TRICON~~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 ~~different~~diverse from the safety-related platforms~~NUMAC and TRICON~~. 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 ~~and actuation logic~~ channel performs its intended function. The online self-diagnostic features of the safety-related platforms~~NUMAC and TRICON~~, 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 ~~its logic output contact~~ 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. ~~The logic system functional test is performed from sensor inputs to the actuated devices for all logic components required for operability of a logic circuit. To confirm that the trip logic is functioning, testing requires manual injection of simulated signals in two sensor channels of NUMAC/TRICON.~~

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~~instrument~~ self-diagnostics and the TSM support the performance of the response time test for the safety-related platforms~~NUMAC/TRICON~~. Watchdog timers monitor logic processor or logic function~~instrument~~ internal clocks and alarms for out-of-limit conditions and the completion of application code per logic processor or logic function~~instrument~~ 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~~ (IEEE Std. 603, Section 5.7, 5.10, and 6.5)~~.

The following Q-DCIS displays and alarms, as a minimum, are provided in the MCR~~ (IEEE Std. 603, Section 5.8)~~.

- 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.~~In addition, the Q-DCIS includes neither the sensors, the sensor wiring to the RMUs, nor the RMU output wiring to the actuators.~~

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;

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 comprises of workstations, triple-redundant controllers, and dual-redundant controllers, that execute the following functions~~systems include~~:

- Workstations:~~;3D MONICORE that calculates three dimensional power distribution and thermal limits for the reactor core;~~
  - 3D MONICORE, and
  - SPDS.
- Dual-Redundant Controllers~~Systems that control and monitor control rod motion, including the RC&IS, ATLM, rod worth minimizer (RWM), MRBM, and signal interface unit (SIU)~~:~~;~~
  - RC&IS (includes RSPC, RAPI, FCM),
  - ATLM,

  - Rod worth minimizer (RWM), and
  - Signal interface unit (SIU).
- Triple-Redundant Controllers~~The logic for the Safety Parameter Display System (SPDS);~~:
  - DPS.

~~□The DPS that provides diverse backup to the RPS and SSLC/ESF functions;~~

~~□The nonsafety-related datalinks and gateways that translate and distribute data between the Q-DCIS and the N-DCIS;~~

~~□Operator control and monitoring from the MCR VDUs; and~~

~~□The nonsafety-related portion of the NMS that includes the AFIP subsystem and the MRBM subsystem.~~

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

~~The N-DCIS for~~ T~~t~~he Plant Investment Protection (PIP) network segment comprises two channels (A and B) of dual-redundant controllers that execute the following functions:~~systems (Train A and Train B) provides the control logic for the~~:

- 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 ~~Uninterruptible power supplies (~~UPS~~)~~., ~~and~~

~~□MCR and RSS panel displays.~~

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: ~~provide the logic for systems involved in power generation. These systems control/protect:~~

- Triple-Redundant Controllers:
  - Steam Bypass and Pressure Control (SB&PC),
  - Feedwater Control System,
  - Feedwater Temperature Control System, and
  - Turbine-Generator Control System.

~~□Reactor pressure;~~

~~RPV water level;~~

~~□The Feedwater controlFWCS, including RPV level and feedwater temperature control;~~

- Dual-Redundant Controllers
  - ~~□~~ ~~The PAS~~Turbine auxiliary;
  - ~~□~~ ~~The SB&PC System~~Generator auxiliary controller;
  - ~~□~~ ~~The turbine and generator~~Electrical system main transformer/Unit Auxiliary Transformer (UAT) controller;
  - ~~□~~ ~~The m~~Main condenser ~~and normal heat sink~~controller;
  - ~~□~~ ~~The nonsafety-related plant electrical systems, including protective relaying, that are non-PIP~~Electrical system Reserve Auxiliary Transformer (RAT) controller;
  - ~~□~~ ~~Power generation components such as the moisture separator reheater (MSR) and the CPS~~Normal heat sink controller;
  - ~~□~~ ~~The~~ Condensate~~ and~~ /Feedwater ~~System~~ (~~C&FS~~FW)/drains/extraction controller, including extraction and level control; ~~and~~
  - ~~□~~ ~~Vendor-furnished BOP systems~~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;

~~□MCR and RSS VDUs;~~

- 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/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.

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 ~~usually~~ maintains the hydraulic control unit (HCU) accumulators at the ~~required~~ 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 ~~can~~ also provides a HP CRD ~~“high pressure~~ 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~~One button startup 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~~one button startup and synchronization sequence~~,~~"~~ 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-

- 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, ~~although~~ the ~~automation system can automatically initiate~~ 3D MONICORE system can be updated automatically by the PAS or ATLMs, or manually by the operator~~more often~~.

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 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, ~~Auxiliary~~ Fuel Building, ~~Auxiliary~~ 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

- 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~~s~~ 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 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

The Q-DCIS meets the integrity requirements described in IEEE Std. 603, Section 5.5. The ~~RPS~~ RTIF – NMS platform functions fail to the tripped state. The SSLC/ESF platform and the independent control platform fail~~s~~ 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.~~ and complete failures of hardware and software do not inhibit manual initiation of reactor scram, MSIV closure or SLC injection. available in the MCR in accordance with More details of system integrity design considerations are included in the system description subsections of the respective safety-related systems as outlined in Table 7.1-2.~~

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 (see Subsection 7.1.3.3.1).~~Communication directly between the four divisions is limited to the minimum, such as trip signals and bypass status signals, and is through proper isolation devices.~~

Electrical Independence

Independence between ~~the~~ safety-related systems ~~and the effects of DBEs~~ is achieved through proper equipment qualification and isolation. ~~Safety-related equipment is qualified for continuous functional capability in the environment at the equipment location, for which DBE~~

~~bypass operation. Only qualified plant personnel are allowed access to other plant operation switches.~~

Keys, passwords, and other security devices (following the guidance of RG 1.152) are used ~~by qualified plant personnel~~ to ~~enter~~ 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.

~~An o~~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. ~~Although it is not possible to bypass more than one division at a time, the Q-DCIS system performs its safety-related functions with three out of four divisions available, in the presence of a single failure.~~

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~~, such as safety-related electrical system equipment including batteries and inverters, satisfy the requirements of~~ 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 ~~for the expected~~ 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. ~~For multiple unit designs only the N-DCIS would have common network components as necessary to control and monitor common hardware and systems. The Q-DCIS of multiple units would have neither shared components nor shared divisions. The operation or failure of shared N-DCIS components does not affect the performance of the Q-DCIS.~~

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- ~~and~~ 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 ~~AOOs and~~ 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, ~~and~~ 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 ~~actuating manual switches~~ 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 manual scram switches directly control the scram air header dump valves~~ 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)~~Additional details of automatic and manual controls at system levels (RTIF, NMS, and SSLC/ESF) are included in Subsections 7.2.1, 7.2.2, and 7.3.5, respectively~~.

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.~~ Additional descriptions of the RTIF, NMS, and SSLC/ESF are included in Subsections 7.2.1, 7.2.2, and 7.3.5, respectively.~~

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. ~~The two RPS sensing inputs that are not~~An example of an indirect measurement~~s of the variables are the RPV water level and~~ is 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 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. 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).~~The RPS initiating circuits and SSLC/ESF logics are described in Subsections 7.2.1 and 7.3.5, respectively.~~

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, ~~and~~ 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).

~~an alarm if water leaks past the piston barrier and collects in the accumulator instrumentation block. An alarm is issued for low CRD charging header pressure that keeps the individual accumulators charged; if the CRD pressure decreases further the reactor is automatically scrammed while there is still hydraulic pressure to do so.~~

~~The SLC system injection status is provided by the MCR indication of accumulator pressure. Operation of the accumulator nitrogen charging and makeup to accommodate small losses is manual. MCR alarms are provided for high, low, and low-low conditions of accumulator pressure and low and low-low conditions of accumulator solution level.~~ 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)

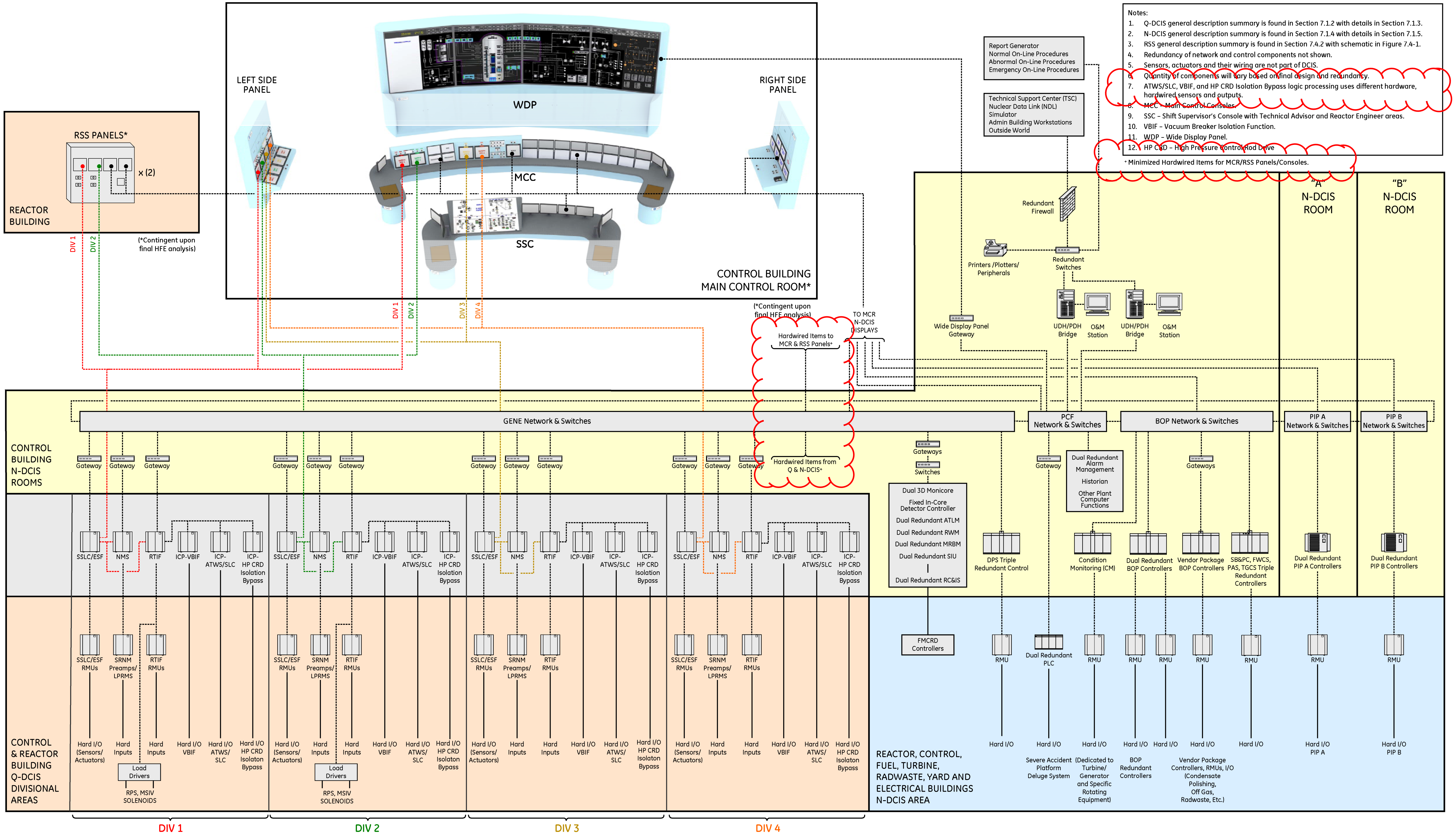
The Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies appropriate to their division with battery backup (per division) for at least 72 hours. The UPS have ~~both an automatic static transfer switch and~~ a manual maintenance switch and either supply (per division) can operate its Q-DCIS division. Using the inverter's ~~automatic or~~ 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 ~~does not~~ 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 ~~in~~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)

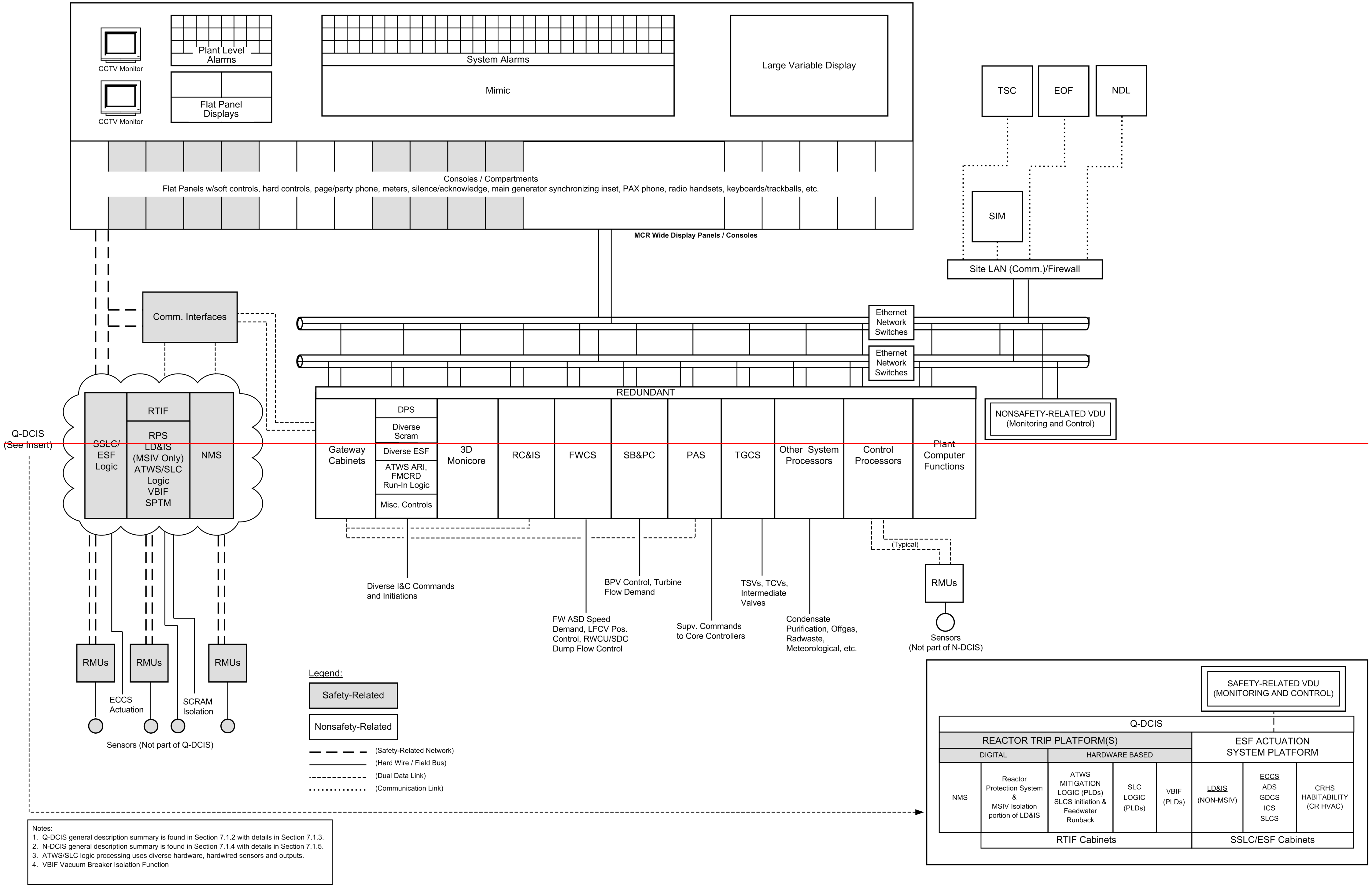
The security measures included in RG 1.152 are evaluated and incorporated in the Q-DCIS design and include plant hardware and software security measures. The software development process plans are developed with the security measures.


RSS PANELS*
x (2)
REACTOR BUILDING
(*Contingent upon final HFE analysis)
DIV 1
DIV 2
LEFT SIDE PANEL
WDP
MCC
SSC
RIGHT SIDE PANEL
CONTROL BUILDING MAIN CONTROL ROOM*
DIV 1
DIV 2
DIV 3
DIV 4
(*Contingent upon final HFE analysis)
Hardwired Items to MCR & RSS Panels+
TO MCR N-DCIS DISPLAYS
Report Generator
Normal On-Line Procedures
Abnormal On-Line Procedures
Emergency On-Line Procedures
Technical Support Center (TSC)
Nuclear Data Link (NDL)
Simulator
Admin Building Workstations
Outside World
Redundant Firewall
Printers /Plotters/ Peripherals
Redundant Switches
Wide Display Panel Gateway
UDH/PDH Bridge
O&M Station
UDH/PDH Bridge
O&M Station
"A" N-DCIS ROOM
"B" N-DCIS ROOM
CONTROL BUILDING N-DCIS ROOMS
GENE Network & Switches
PCF Network & Switches
BOP Network & Switches
PIP A Network & Switches
PIP B Network & Switches
Gateway
Gateway
Gateway
Gateway
Gateway
Gateway
Gateway
Gateway
Gateway
Gateway
Gateway
Gateway
Hardwired Items from Q & N-DCIS+
Gateways
Switches
Dual 3D Monicore
Fixed In-Core Detector Controller
Dual Redundant ATLM
Dual Redundant RWM
Dual Redundant MRBM
Dual Redundant SIU
Dual Redundant RC&IS
Gateway
Dual Redundant Alarm Management
Historian
Other Plant Computer Functions
Gateways
SSLC/ESF
NMS
RTIF
ICP-VBIF
ICP-ATWS/SLC
ICP-HP CRD Isolation Bypass
SSLC/ESF
NMS
RTIF
ICP-VBIF
ICP-ATWS/SLC
ICP-HP CRD Isolation Bypass
SSLC/ESF
NMS
RTIF
ICP-VBIF
ICP-ATWS/SLC
ICP-HP CRD Isolation Bypass
SSLC/ESF
NMS
RTIF
ICP-VBIF
ICP-ATWS/SLC
ICP-HP CRD Isolation Bypass
DPS Triple Redundant Control
Condition Monitoring (CM)
Dual Redundant BOP Controllers
Vendor Package BOP Controllers
SB&PC, FWCS, PAS, TGCS Triple Redundant Controllers
Dual Redundant PIP A Controllers
Dual Redundant PIP B Controllers
SSLC/ESF RMUs
SRNM Preamps/ LPRMS
RTIF RMUs
SSLC/ESF RMUs
SRNM Preamps/ LPRMS
RTIF RMUs
SSLC/ESF RMUs
SRNM Preamps/ LPRMS
RTIF RMUs
SSLC/ESF RMUs
SRNM Preamps/ LPRMS
RTIF RMUs
FMCRD Controllers
RMU
Dual Redundant PLC
RMU
RMU
RMU
RMU
RMU
RMU
RMU
Hard I/O (Sensors/ Actuators)
Hard Inputs
Hard Inputs
Hard I/O VBIF
Hard I/O ATWS/ SLC
Hard I/O HP CRD Isolaton Bypass
Load Drivers
RPS, MSIV SOLENOIDS
Hard I/O (Sensors/ Actuators)
Hard Inputs
Hard Inputs
Hard I/O VBIF
Hard I/O ATWS/ SLC
Hard I/O HP CRD Isolaton Bypass
Load Drivers
RPS, MSIV SOLENOIDS
Hard I/O (Sensors/ Actuators)
Hard Inputs
Hard Inputs
Hard I/O VBIF
Hard I/O ATWS/ SLC
Hard I/O HP CRD Isolaton Bypass
Hard I/O (Sensors/ Actuators)
Hard Inputs
Hard Inputs
Hard I/O VBIF
Hard I/O ATWS/ SLC
Hard I/O HP CRD Isolaton Bypass
Hard I/O
Hard I/O Severe Accident Platform Deluge System
Hard I/O (Dedicated to Turbine/ Generator and Specific Rotating Equipment)
Hard I/O BOP Redundant Controllers
Hard I/O
Hard I/O Vendor Package Controllers, RMUs, I/O (Condensate Polishing, Off Gas, Radwaste, Etc.)
Hard I/O
Hard I/O PIP A
Hard I/O PIP B
CONTROL & REACTOR BUILDING Q-DCIS DIVISIONAL AREAS
REACTOR, CONTROL, FUEL, TURBINE, RADWASTE, YARD AND ELECTRICAL BUILDINGS N-DCIS AREA
DIV 1
DIV 2
DIV 3
DIV 4

Notes:

1. Q-DCIS general description summary is found in Section 7.1.2 with details in Section 7.1.3.
2. N-DCIS general description summary is found in Section 7.1.4 with details in Section 7.1.5.
3. RSS general description summary is found in Section 7.4.2 with schematic in Figure 7.4-1.
4. Redundancy of network and control components not shown.
5. Sensors, actuators and their wiring are not part of DCIS.
6. Quantity of components will vary based on final design and redundancy.
7. ATWS/SLC, VBIF, and HP CRD Isolation Bypass logic processing uses different hardware, hardwired sensors and outputs.
8. MCC – Main Control Consoles.
9. SSC – Shift Supervisor's Console with Technical Advisor and Reactor Engineer areas.
10. VBIF – Vacuum Breaker Isolation Function.
11. WDP – Wide Display Panel.
12. HP CRD – High Pressure Control Rod Drive

+ Minimized Hardwired Items for MCR/RSS Panels/Consoles.


CCTV Monitor
CCTV Monitor
Plant Level Alarms
Flat Panel Displays
System Alarms
Mimic
Large Variable Display
Consoles / Compartments
Flat Panels w/soft controls, hard controls, page/party phone, meters, silence/acknowledge, main generator synchronizing inset, PAX phone, radio handsets, keyboards/trackballs, etc.
MCR Wide Display Panels / Consoles
TSC
EOF
NDL
SIM
Site LAN (Comm.)/Firewall
Ethernet Network Switches
Ethernet Network Switches
Comm. Interfaces
REDUNDANT
Gateway Cabinets
DPS
Diverse Scram
Diverse ESF
ATWS ARI, FMCRD Run-In Logic
Misc. Controls
3D Monicore
RC&IS
FWCS
SB&PC
PAS
TGCS
Other System Processors
Control Processors
Plant Computer Functions
NONSAFETY-RELATED VDU (Monitoring and Control)
Q-DCIS
(See Insert)
SSLC/ESF Logic
RTIF
RPS
LD&IS (MSIV Only)
ATWS/SLC Logic
VBIF
SPTM
NMS
(Typical)
RMUs
Sensors (Not part of N-DCIS)
Diverse I&C Commands and Initiations
BPV Control, Turbine Flow Demand
FW ASD Speed Demand, LFCV Pos. Control, RWCU/SDC Dump Flow Control
Supv. Commands to Core Controllers
TSVs, TCVs, Intermediate Valves
Condensate Purification, Offgas, Radwaste, Meteorological, etc.
RMUs
RMUs
RMUs
ECCS Actuation
SCRAM Isolation
Sensors (Not part of Q-DCIS)
Legend:
Safety-Related
Nonsafety-Related
(Safety-Related Network)
(Hard Wire / Field Bus)
(Dual Data Link)
(Communication Link)
SAFETY-RELATED VDU (MONITORING AND CONTROL)
Q-DCIS
REACTOR TRIP PLATFORM(S)
DIGITAL
HARDWARE BASED
ESF ACTUATION SYSTEM PLATFORM
NMS
Reactor Protection System & MSIV Isolation portion of LD&IS
ATWS MITIGATION LOGIC (PLDs) SLCS initiation & Feedwater Runback
SLC LOGIC (PLDs)
VBIF (PLDs)
LD&IS (NON-MSIV)
ECCS ADS GDCS ICS SLCS
CRHS HABITABILITY (CR HVAC)
RTIF Cabinets
SSLC/ESF Cabinets

Notes:
1. Q-DCIS general description summary is found in Section 7.1.2 with details in Section 7.1.3.
2. N-DCIS general description summary is found in Section 7.1.4 with details in Section 7.1.5.
3. ATWS/SLC logic processing uses diverse hardware, hardwired sensors and outputs.
4. VBIF Vacuum Breaker Isolation Function

Figure 7.1-1. ~~ESBWR Instrumentation and Control~~ Simplified Network/Functional ~~Block~~ Diagram of DCIS

- 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 System (CRDS),
- 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

~~□Direct Current (DC) Power Supply System, and~~

- Raceway System.

The RPS ~~sensors, ~~hardware~~,~~/software platform is~~ and logic are~~ diverse from ~~their counterparts on the ~~SSLC/ESF and DPS~~ platforms~~. RPS has a separate set of sensors from SSLC/ESF, and a diverse set of sensors from DPS.

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. ~~Each RPS division uses two independent, uninterruptible power supplies (UPS) from the same division. ~~Either UPS of the divisional ~~of the ~~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~~ (IEEE Std. 603, Section 5.1)~~.

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 ~~air header dump (~~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 ~~air header dump~~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~~ (IEEE Std. 603, Section 4.4)~~.

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~~ (fulfilling the independence requirement~~

~~of IEEE Std. 603, Section 5.6)~~. 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..

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~~TLU~~ bypass. Each RTIF BPU sends its divisional sensor~~a separate~~ bypass signal ~~for the four channels~~ to the TLU ~~in~~of the same division and an isolated divisional~~for channel~~ sensor~~s~~ bypass signal to the TLUs of the other three divisions. Each ~~RPS~~ RTIF BPU ~~also~~ sends ~~the TLU~~its divisional logic bypass signal to the OLUs of~~in~~ 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 ~~RPS~~ RTIF BPU~~,~~ and trip inputs from the TLU of the same division~~, and manual inputs from switches within 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 ~~air header dump~~ 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 ~~and backup~~ 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~~Load drivers~~ are ~~also~~ used for back~~-~~up scram actuators, scram–follow initiation, and scram reset permissive actuators. When in a tripped state, the output contactors~~load drivers~~ for backup scram cause the ~~air header dump~~ valve solenoids ~~(air header dump)~~ to energize. The ~~load drivers~~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 ~~diverse~~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 ~~air header dump~~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 ~~air header dump~~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 CRDS. 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 ~~(IEEE Std. 603, Section 4.1, 4.2 and 4.4)~~. The system monitoring the associated process condition is found in the system~~is~~ 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),
- ~~Low control rod drive HCU~~Scram accumulator charging water header pressure – low-low (CRDS),
- 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~~loss of~~ power generation bus loss, main condenser pressure high, and manual scram outputs, systems provide sensor outputs through the ~~RPS~~ RTIF RMU.

The MSIV Closure, TSV closure and TCV fast-closure, loss of power generation bus, 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 or high thermal neutron flux level),
- 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 ~~RPS~~ RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate ~~RPS~~ 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 ~~RPS~~ 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 ~~RPS~~ RTIF RMU, which digitizes and conditions the signal before sending it to the appropriate ~~RPS~~ 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 STP high setpoint that is a function of FW temperature.

~~The RPS initiates a scram when the FW temperature further departs from the area allowed by the thermal power vs. FW temperature domain.~~

Simulated Thermal Power Biased Feedwater Temperature: The RPS uses the STP 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 STP. 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 ~~CRDS~~ 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 CRDS. This is an anticipatory scram because it initiates a scram before the ~~HCUs~~scram accumulators have time to depressurize~~ the reactor~~.

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.

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 ~~CRD~~ 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 ~~CRD~~ 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 ~~air header dump~~ valves of the CRD system ~~(backup scram valves)~~ 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 "~~Low CRD~~ Scram Accumulator Charging Water Header Pressure - Low" trip signal or when any ~~CRD~~ 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,
- ~~CRD HCU~~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 STP trip,
- ~~CRD HCU~~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),
- ~~CRD~~ Scram accumulator~~-~~ charging~~-~~ water header~~-~~ pressure - low-low trip bypass,

- Any ~~CRD~~ 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 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 RPS configuration and communication paths.

The RPS 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, RPS to NMS and RPS to SSLC/ESF communication. Since the RPS 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 extend their address space (memory) to include the memory on the communications (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 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.

Finally, there are two "counter rotating" rings within each division of RPS. 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 RPS 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 hardwired 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. 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.~~Safety-related systems are designed to conform to Regulatory Guide (RG) 1.153 and IEEE Std. 603. Separation and isolation are preserved both mechanically and electrically in accordance with IEEE Std. 603, Section 5.6 and RG 1.75. The RPS is divisionalized and is designed with redundancy so that failure of any instrument does not interfere with the system operation. Electrical separation is maintained between the redundant divisions~~
  - 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

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

7.2.1.3.5 Branch Technical Positions

~~BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service:~~

- ~~Conformance: Because there is no reactor coolant pump, BTP HICB-3 does not apply.~~

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. 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. 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.

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 ~~(IEEE Std. 603, Sections 6.6 and 7.4)~~. 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 ~~alarmed~~indicated in the MCR.

- ~~CRD HCU~~Scram accumulator charging water header ~~low~~ 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 ~~CRD~~ scram accumulator charging water header ~~low~~ 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 ~~low CRD HCU~~scram accumulator charging water header pressure – low-low trip can be bypassed manually in each division of trip logic by separate, manual ~~CRD HCU~~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 ~~CRD~~ scram accumulator charging water header pressure is below the trip setpoint. The ~~low~~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 ~~alarmed~~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 ~~CRD~~ 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 ~~alarmed~~indicated in the MCR.

- ~~Loss of p~~Power generation bus loss trip bypass (indicated operational bypass): The ~~Loss of~~ 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~~alarmed~~ 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, and the coincident/non-coincident NMS trip remains in the non-coincident position, the non-coincident NMS scram trip functions are automatically disabled (bypassed). This logic is an NMS function.

  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.

  The non-coincident NMS trip function is automatically removed when the Reactor Mode Switch is in the Run position. If the coincident/non-coincident NMS trip selection switch is in the non-coincident position when the Reactor Mode Switch is in the Run position, there is an alarm in the MCR. When the reactor is in Shutdown, Refuel, or Startup mode, the non-coincident NMS trip can be bypassed manually by a separate "non-coincident trip disable" switch. These logics are NMS functions.

- 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~~alarmed~~ 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~~alarmed~~ 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~~ (IEEE Std. 603, Sections 6.7 and 7.5)~~. 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~~alarmed~~ 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~~alarmed~~ 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 ~~RPS~~ 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

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~~ and in detail in Reference 7.2-2. This Topical Report addresses the CIM function, communication data link, data flow, and isolation requirements of IEEE Std. 603. ~~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~~ (IEEE Std. 603, Section 6.8)~~. 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~~ is in~~ the coincident mode and, if the coincident/non-coincident switch is still in the non-coincident mode, an alarm will be generated. For each division, the three SRNM scram trip signals are combined to form a

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, 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~~ (IEEE Std. 603, Section 6.8)~~. 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. This scheme assures that each quadrant will always have at least two unbypassed SRNMs for startup range flux monitoring~~into four bypass groups. A logic processor allows only one SRNM at a time to be bypassed in each bypass group, allowing up to four SRNM channels~~

~~to be bypassed at any one time~~. 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 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. The individual unbypassed SRNM power signals are combined and averaged to form a divisional SRNM power signal. 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 setpoint is lowered ~~(IEEE Std. 603, Section 6.8)~~ 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).

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)~~signal output interface units~~ 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

- 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. The Reactor Mode Switch not in Run mode equates to a non-coincident mode for the NMS. 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 RPS 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 extend their address space (memory) to include the memory on the communications (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 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.

Finally, 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 hardwired.

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. 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~~, a subsystem~~ 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.

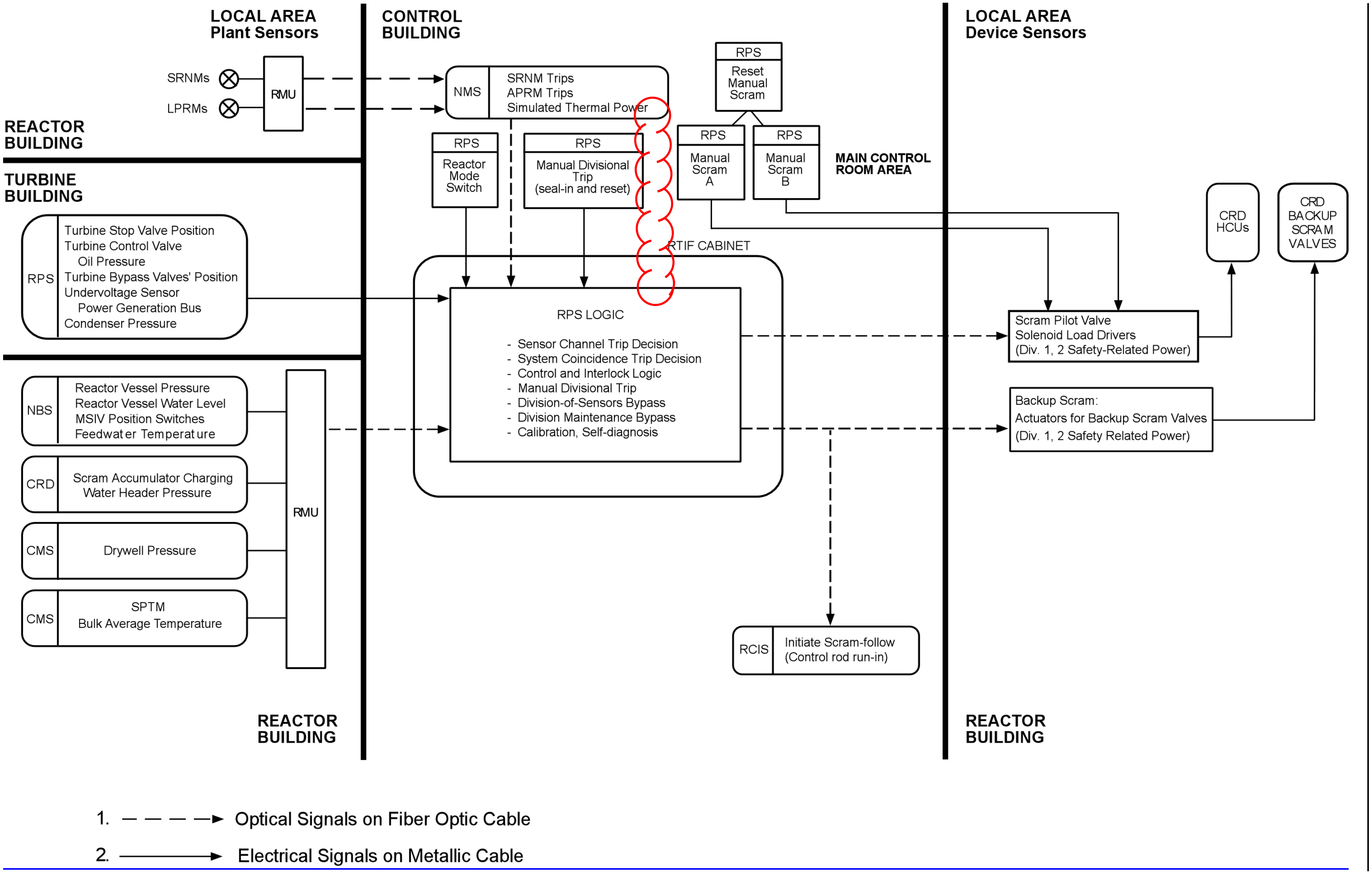
The SPTM function is ~~a~~physically implemented by the safety-related four-divisional subsystem, designed for Seismic Category I requirements.

The SPTM function also provides:

- Safety-related inputs to the MCR for indication.~~;~~

~~□Input for nonsafety-related suppression pool automatic cooling mode initiation; and~~

~~□Information for display, alarm, and recording inputs to the DPS.~~


LOCAL AREA
Plant Sensors
CONTROL
BUILDING
LOCAL AREA
Device Sensors
SRNMs
LPRMs
RMU
NMS
SRNM Trips
APRM Trips
Simulated Thermal Power
RPS
Reset
Manual
Scram
REACTOR
BUILDING
RPS
Reactor
Mode
Switch
RPS
Manual Divisional
Trip
(seal-in and reset)
RPS
Manual
Scram
A
RPS
Manual
Scram
B
MAIN CONTROL
ROOM AREA
TURBINE
BUILDING
CRD
HCUs
CRD
BACKUP
SCRAM
VALVES
RPS
Turbine Stop Valve Position
Turbine Control Valve
Oil Pressure
Turbine Bypass Valves' Position
Undervoltage Sensor
Power Generation Bus
Condenser Pressure
RTIF CABINET
RPS LOGIC
- Sensor Channel Trip Decision
- System Coincidence Trip Decision
- Control and Interlock Logic
- Manual Divisional Trip
- Division-of-Sensors Bypass
- Division Maintenance Bypass
- Calibration, Self-diagnosis
Scram Pilot Valve
Solenoid Load Drivers
(Div. 1, 2 Safety-Related Power)
NBS
Reactor Vessel Pressure
Reactor Vessel Water Level
MSIV Position Switches
Feedwater Temperature
Backup Scram:
Actuators for Backup Scram Valves
(Div. 1, 2 Safety Related Power)
CRD
Scram Accumulator Charging
Water Header Pressure
RMU
CMS
Drywell Pressure
CMS
SPTM
Bulk Average Temperature
RCIS
Initiate Scram-follow
(Control rod run-in)
REACTOR
BUILDING
REACTOR
BUILDING
1. Optical Signals on Fiber Optic Cable
2. Electrical Signals on Metallic Cable

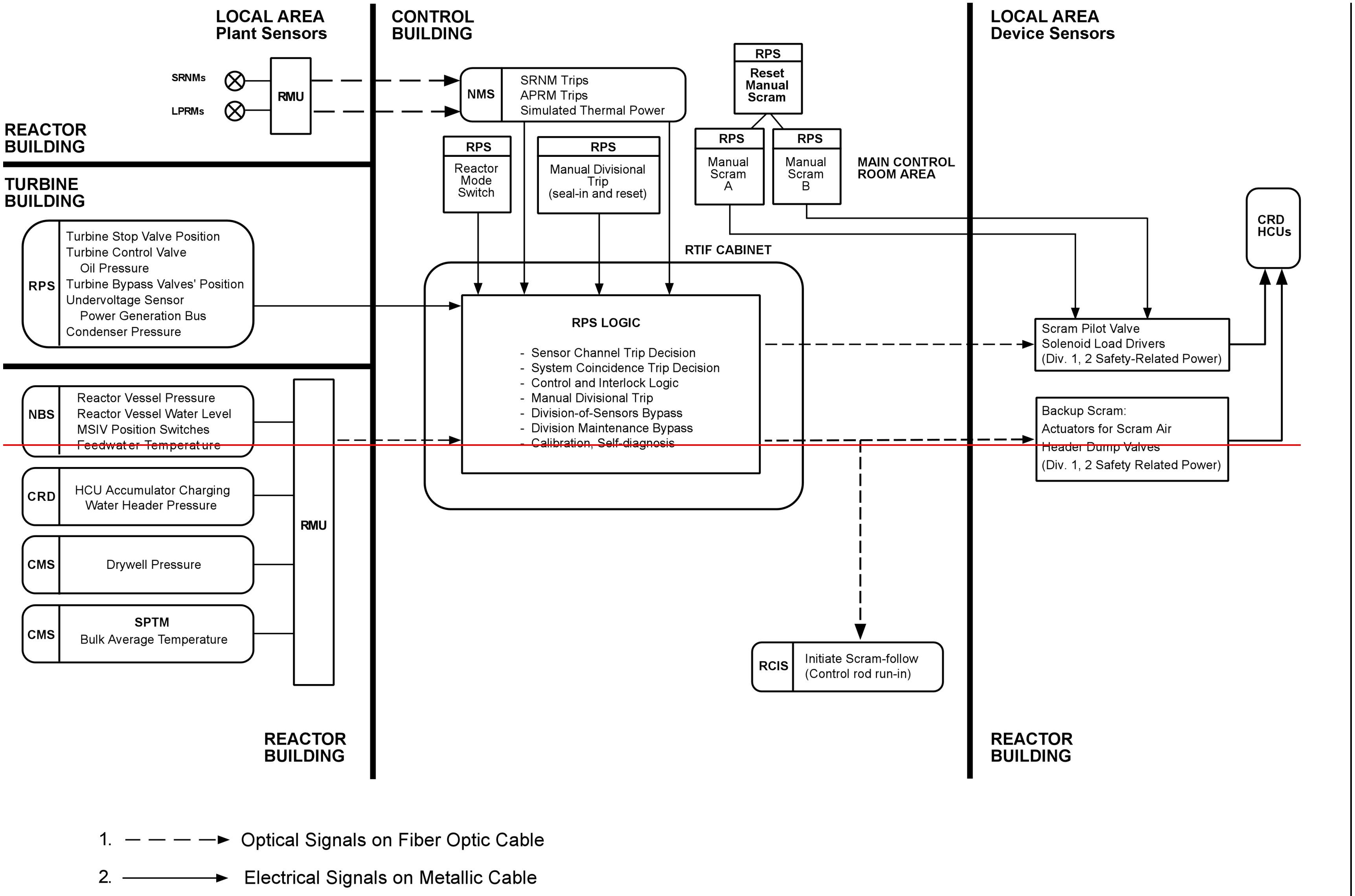


Figure 7.2-2. RPS Interfaces and Boundaries Diagram

(Typical of four divisions)

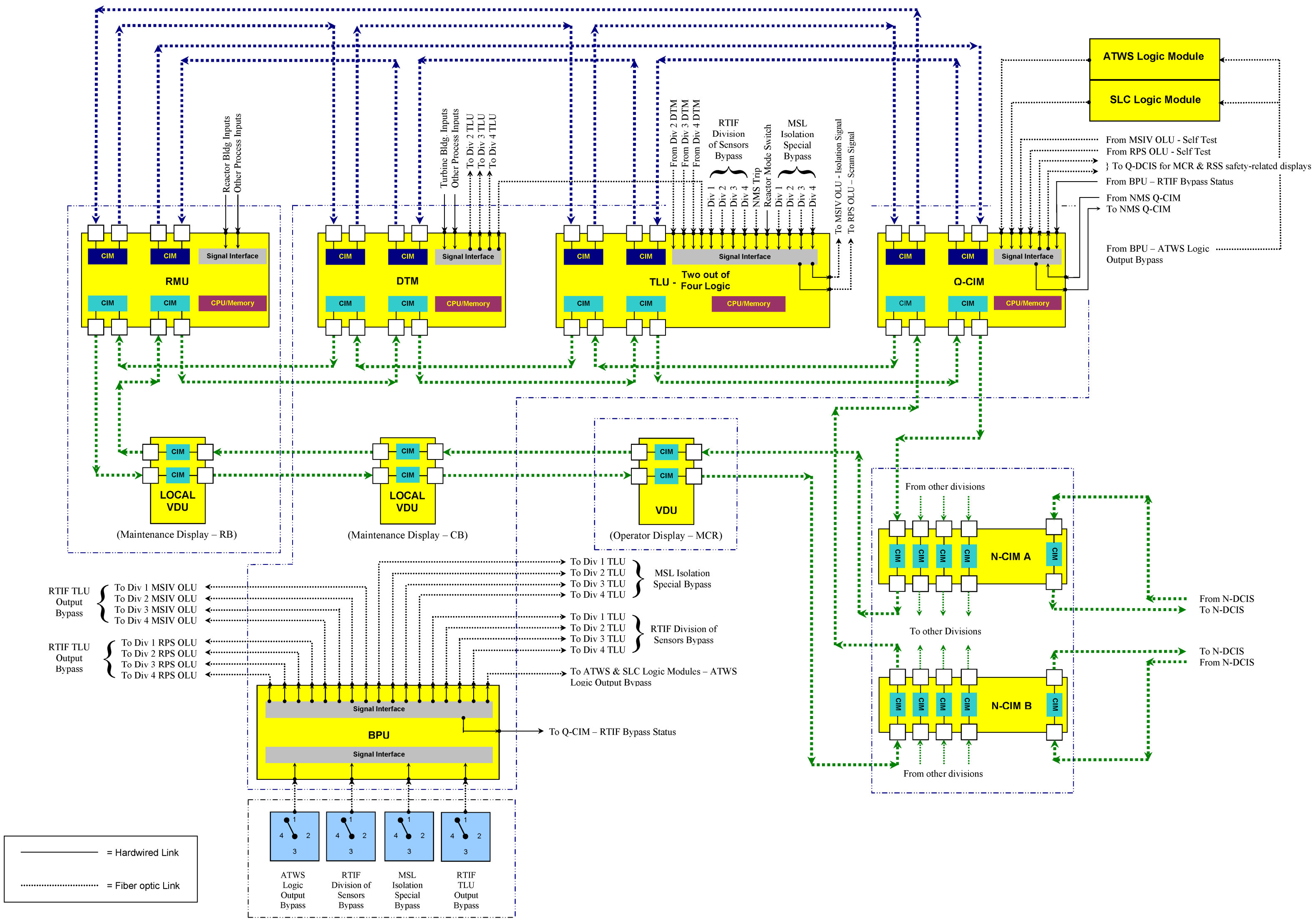


Figure 7.2-11a. Reactor Trip and Isolation Function (RTIF) Functional Block Diagram

(Four Divisions Shown)

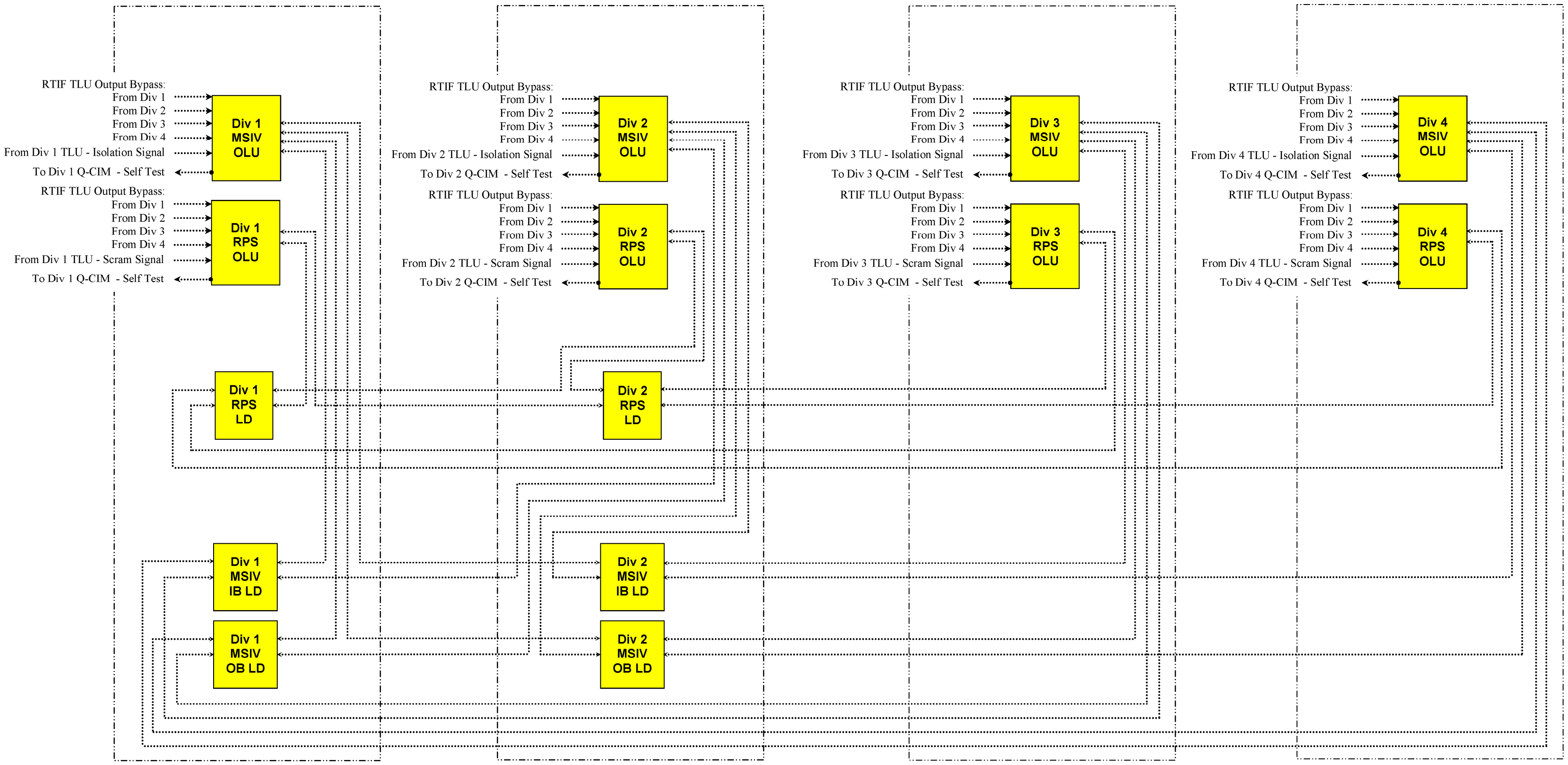


Figure 7.2-11b. Reactor Trip and Isolation Function (RTIF) Functional Block Diagram – Output Logic Unit Detail

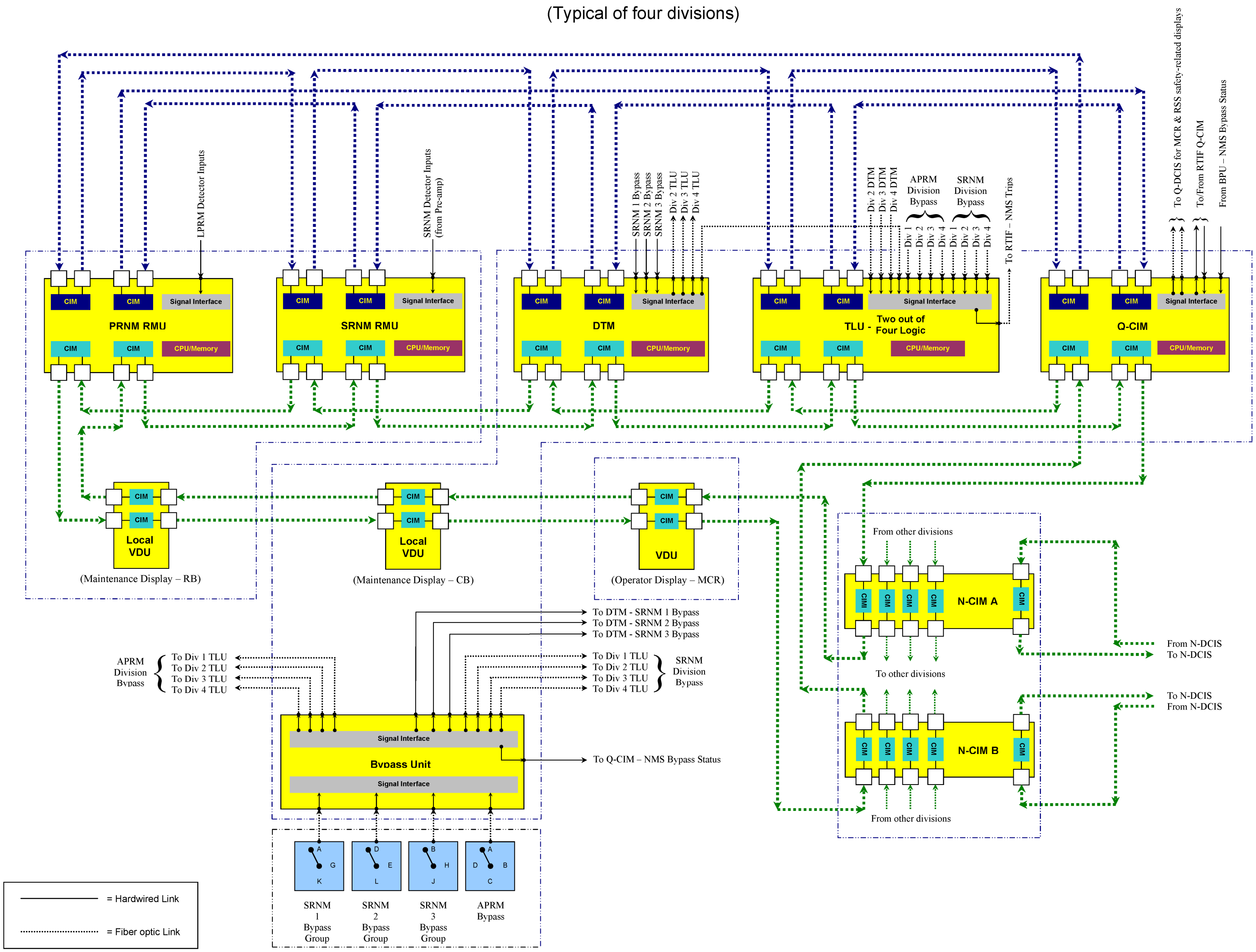


Figure 7.2-12. Neutron Monitoring System (NMS) Functional Block Diagram

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 ~~block~~ diagram of the ~~Q-~~DCIS is included as ~~part of~~ Figure 7.1-1.~~ and a functional network diagram appears as Figure 7.1-2.~~ This~~ese~~ diagram~~s~~ 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~~ (IEEE Std. 603, Sections 6.1 and 7.1)~~, 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 ~~different~~diverse from the Diverse Protection System (DPS) wide range level transmitters.

When ~~attainment of~~ 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 ~~separate from those used in the primary ECCS functions.~~ 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~~logic function (IEEE Std. 603, Sections 5.8, 6.2 and 7.2)~~. 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~~ (IEEE Std. 603, Section 5.2)~~. 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 the SSLC/ESF has two trains of two-out-of-four trip logic (except the DPV logic, which has three trains) 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). Each initiating logic has access to one channel of wide range level sensing for the Level 1 trip decision. The four divisional water levels and their trip setpoints are continuously monitored for consistency by the N-DCIS plant computer functions (PCF). An inconsistency results in an alarm. The separate logic of each train issues the ECCS trip signal, if the RPV water drops below Level 1.~~ 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 ECCS trip signal actuates a~~ timer ~~(see Table 7.3-2). If the trip signal resets (as, for example, from an instrument column transient), the timer resets and restarts when the next ECCS trip signal is received. If the ECCS trip signal persists for 10 seconds, the logic seals in and issues an "initial start" signal (IEEE Std. 603, Section 5.2). The initial start signal also is transmitted to the SSLC/ESF (Subsection 7.3.5) , ICS (Subsection 7.4.4), and GDCS (Subsection 7.3.1.2). The initial start signal specifically actuates five timers in each of the two two-out-of-four trip logic trains (per division) of ADS logic.~~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 the two load driver/discrete output circuits, followed by a continuity monitor and a disable switch all arranged in series, and located in the appropriate divisional Remote Multiplexing Units (RMUs) and DPS RMUs in the Reactor Building (RB). Because there is the division of sensors bypass, and there are multiple trains of two-out-of-four logic, no additional division of trip logic bypass is implemented in the SSLC/ESF logic.~~ 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 ~~(IEEE Std. 603, Section 5.1)~~.

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

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~~)~~]~~, and 10 CFR 50.34(f)(2)(xiv)(II.E.4.2)~~ 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 trip logic units (~~TLUs~~VLU function) continuously self-tests~~ (IEEE Std. 603, Sections 4.12, 5.7 and 6.5)~~~~, as shown in Table 7.3-1~~. 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~~ (IEEE Std. 603, Section 5.8)~~ 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,~~ and~~
  - 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 ~~(IEEE Std. 603, Sections 4.1, 4.2, 4.5, 5.1, 5.8, 6.2, 7.2, and 7.3)~~ 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~~two~~ 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 ~~initial start~~ 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 ~~the eight GDCS squib valves on the injection lines are actuated~~. 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 initial start signal to open the GDCS equalization valves is also given after a time delay (Table 7.3-4)~~. ~~When t~~The GDCS equalizing valves initiatin 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~~surface drops~~ decreases below RPV Level 0.5 (1m above TAF).~~,~~ ~~t~~Th~~e~~is action results in the actuation of the four equalizing squib valves mounted on the suppression pool equalizing lines~~ are actuated~~. 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 ~~to~~ 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 ~~(IEEE Std. 603, Section 5.2)~~. 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 ~~(IEEE Std. 603, Sections 5.8, 6.2 and 7.2)~~. 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~~ (IEEE Std. 603, Sections 5.8, 6.2 and 7.2)~~. 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~~portion of the~~ Q-DCIS, outside the drywell containment. The ~~NBS~~ RPV level transmitters and the ~~CMS~~ drywell pressure sensors used to initiate GDCS~~ are part of the NBS~~, ~~and~~ are located on racks outside the drywell.

~~The SSLC/ESF logic sends an initial start signal to the GDCS logic that automatically initiates the GDCS following reactor depressurization under LOCA conditions.~~

~~Each of the two trains per division is presented with the initial start signal from the same SSLC/ESF logic initiating the ADS. The SSLC/ESF logic adds a time delay (Table 7.3-4) to the initial start signal, and then operates all of the GDCS injection valves. Once the initial start signal is given to both ADS and GDCS (starting the various timers), the sequence is sealed in and cannot be aborted by the plant operator.~~

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 ~~sensors~~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~~diverse~~ from the ~~sensors~~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 ~~initial start~~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 there is a discrepancy in outputs a sensor trip signal is sent both to its own division and to each of the other divisions by appropriately isolated fiber optic cables.~~If the measured parameter is at or past the setpoint, a divisional 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 ~~therefore has two separate trip logics that can independently perform a~~uses triply redundant logic to perform the two-out-of-four vote on the four divisional~~sensor~~ trip~~s~~ 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 ~~(IEEE Std. 603, Section 5.1)~~.

For the eight GDCS injection squib valves logic, ~~each of the two (per division) initial start signals actuates an~~ 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 ~~with~~at a preset time delay (as specified in Table 7.3-4). After the time delay, ~~each of the two timers outputs~~ 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. ~~Each of the two timers must transmit a trip signal to the corresponding series load driver/discrete output. The effect is that both two-out-of-four trip voters, both timers, and all of the load drivers/discrete outputs must operate to fire the squib initiator, making the design single failure proof against inadvertent actuation~~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 squib initiator, each of the two equalization valve timers and two Level 0.5 outputs must transmit a trip signal to the corresponding series load driver/discrete outputs. The effect is that both two-out-of-four trip Level 0.5 voters, both timers, and all of the load drivers/discrete outputs must all operate to fire the squib initiator, making the design single-failure proof against inadvertent actuation.~~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 .5 and two-out-of-four vote the resulting divisional 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 ~~thermocouples and associated~~ 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.

- 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 ~~(IEEE Std. 603, Sections 5.1, 5.2, 5.6, 5.7, 5.9, 6.1, and 6.8)~~.

- 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, ~~and~~
- 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 ~~differential~~ temperature, and
- RCCWS intersystem leakage radiation.

~~Drywell sump levels and flow rates are used to quantify identified and unidentified leakages.~~

- 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~~3~~.

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 ~~discharge~~ intake duct, the smoke purge exhaust duct, and the restroom exhaust duct in the CRHA~~CHRA~~ 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 ~~discharge~~ duct, the smoke purge exhaust duct, and in the restroom exhaust duct are 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 ~~the~~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, ~~behind~~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~~ion~~ 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.~~(starting the intake air handling unit), the SSLC/ESF produces an actuation signal to energize all four solenoid valves to open redundant air operated isolation dampers. The dampers open simultaneously with manual energization of one of the nonsafety-related air supply air handling units and its nonsafety-related air operated damper 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 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.

- 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;~~,~~
- ~~t~~The ADS functions of the NBS for SRV and DPV control;~~,~~
- ~~t~~The ECCS, and decay heat removal – safe, stable ~~functions of the GDCS and SLC system, the ECCS and~~ shutdown ~~cooling~~ and reactor pressure control functions of the ICS;~~, and~~
- tThe control room isolation function of the CRHS.~~ The SSLC/ESF architecture is presented Reference 7.3-1 and Reference 7.3-5.~~
- 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 ~~trains of~~ 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.

~~There are two independent and redundant VLU functional trains (three for the DPV actuation logic) in each division of the SSLC/ESF equipment. The vote logic trip signals from each VLU functional train are transmitted to the RMU, where a two-out-of-two (or three-out-of-three) confirmation is performed. The redundant trains within a division are necessary to prevent single failures within a division from causing a squib initiator to fire; as a result each VLU logic train is required to operate to produce an output. Self-tests within the SSLC/ESF determine whether any one VLU function has failed, and such a failure is alarmed in the MCR.~~ 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,~~ a failed VLU function cannot be bypassed for any of the ECCS logic for squib valves initiation~~ 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

~~For a fail-safe design, a division-out-of-service bypass inhibits the trip output in a division from affecting the output load drivers/discrete outputs by maintaining that division's load drivers/discrete outputs in an energized state~~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;~~there are multiple trains of two-out-of-four VLU logic,~~ no additional division trip logic bypass is required~~implemented~~. ~~Each of the VLU trip outputs is directly applied to one of the load drivers/discrete outputs in series. Each VLU trip is required to prevent inadvertent trip initiation of the squib valves. It is undesirable to perform the VLU logic bypass activities with the RMU electrically connected to the valve~~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,
- ~~Establish containment isolation~~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 ~~vendor furnished microprocessor-based~~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: ~~Safety-related systems are designed to conform to RG 1.153 and IEEE Std. 603 as discussed in Subsection 7.2.1.3.4.~~ 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.

- 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-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service:~~

~~□Conformance: BTP HICB-3 is not applicable because there is no reactor coolant pump.~~

~~BTP HICB-4, Guidance on Design Criteria for Auxiliary Feedwater Systems:~~

~~□Conformance: BTP HICB-4 is not applicable to the SSLC/ESF.~~

~~BTP HICB-6, Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode:~~

~~□Conformance: There is no recirculation pump and no active ECCS pumps. Therefore, BTP HICB-6 is not applicable.~~

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.

  ~~Defined diverse and hardwired p~~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-13, Guidance on Cross Calibration of Protection System Resistance Temperature Detectors:~~

- ~~Conformance: BTP HICB-13 does not apply to the SSLC/ESF because this system does not use resistance temperature detector-type sensors.~~

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 ~~I&C~~ Software Management ~~Plan~~Program Manual," NEDO-33226, NEDE-33226P and "ESBWR ~~I&C~~ Software Quality Assurance ~~Plan~~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 ~~microprocessor-based~~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 ~~(IEEE Std. 603, Sections 5.7 and 6.5)~~. 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.

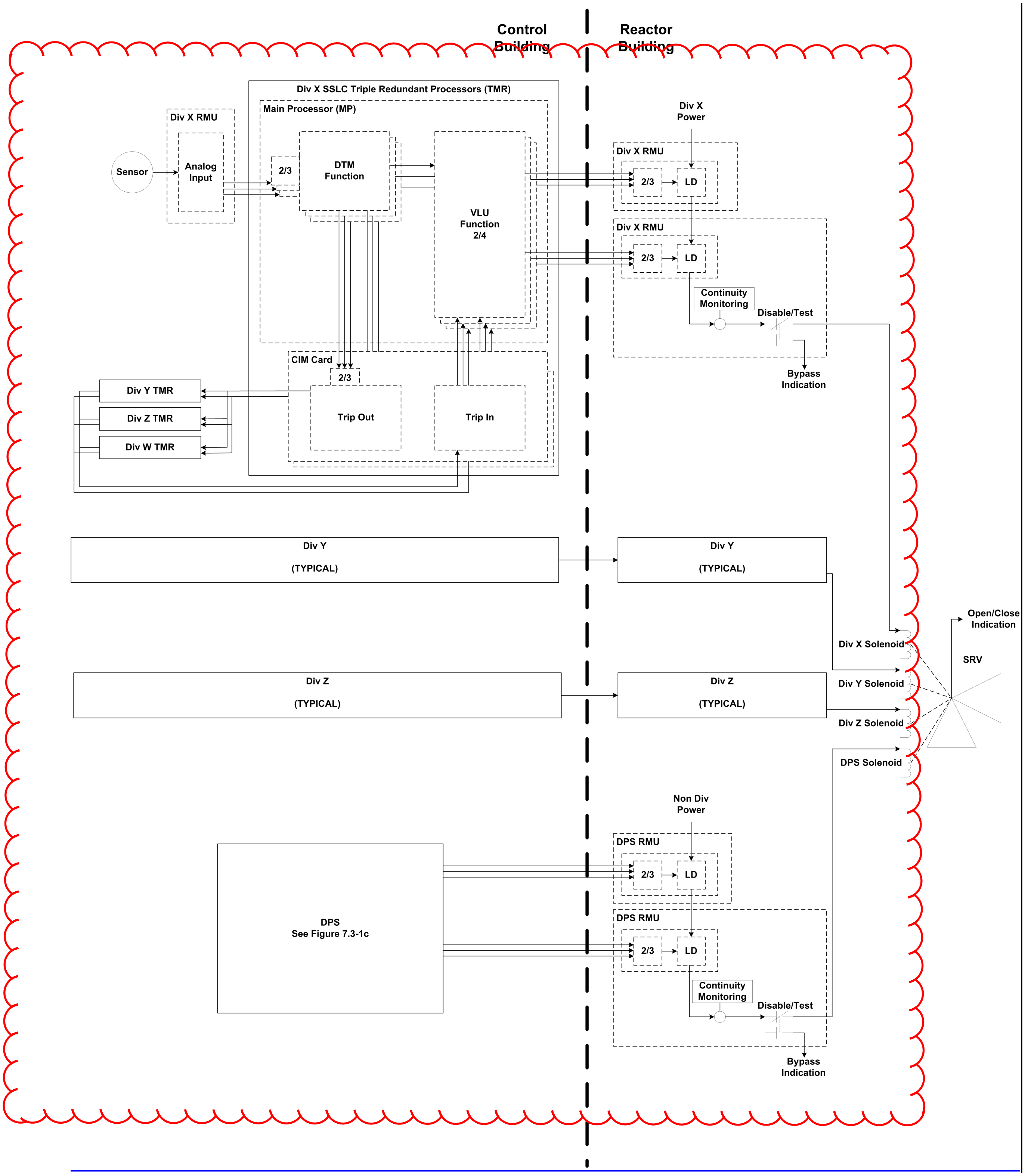
Table 7.3-1
Automatic Depressurization System Parameters

Parameter	Value
Number of ADS divisions	4
~~Number of separate logics (trains)~~Processor/logic redundancy per division	~~2~~3
Number of ~~logic (trains)~~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~~logic (trains)~~ within a division used to actuate the separate igniter circuits on each squib-actuated DPV	~~2~~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)~~Trip logic units self-test time interval~~	~~8 sec~~

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 ~~confirm~~ a sustained RPV Level 1 ~~ECCS-LOCA~~ signal	10 sec
Time delay to a sustained Drywell Pressure High signal	60 min
Time after a sustained RPV Level 1 ~~ECCS-LOCA confirmed initiating~~ signal or a sustained Drywell Pressure High signal before signaling Group 1 SRVs to open	0 sec
Time after a sustained RPV Level 1~~ECCS-LOCA confirmed initiating~~ 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.


Control Building
Reactor Building
Div X SSLC Triple Redundant Processors (TMR)
Main Processor (MP)
Div X RMU
Sensor
Analog Input
2/3
DTM Function
VLU Function 2/4
CIM Card
2/3
Trip Out
Trip In
Div Y TMR
Div Z TMR
Div W TMR
Div X Power
Div X RMU
2/3
LD
Div X RMU
2/3
LD
Continuity Monitoring
Disable/Test
Bypass Indication
Div Y
(TYPICAL)
Div Y
(TYPICAL)
Div Z
(TYPICAL)
Div Z
(TYPICAL)
Div X Solenoid
Div Y Solenoid
Div Z Solenoid
DPS Solenoid
Open/Close Indication
SRV
Non Div Power
DPS RMU
2/3
LD
DPS RMU
2/3
LD
Continuity Monitoring
Disable/Test
Bypass Indication
DPS
See Figure 7.3-1c

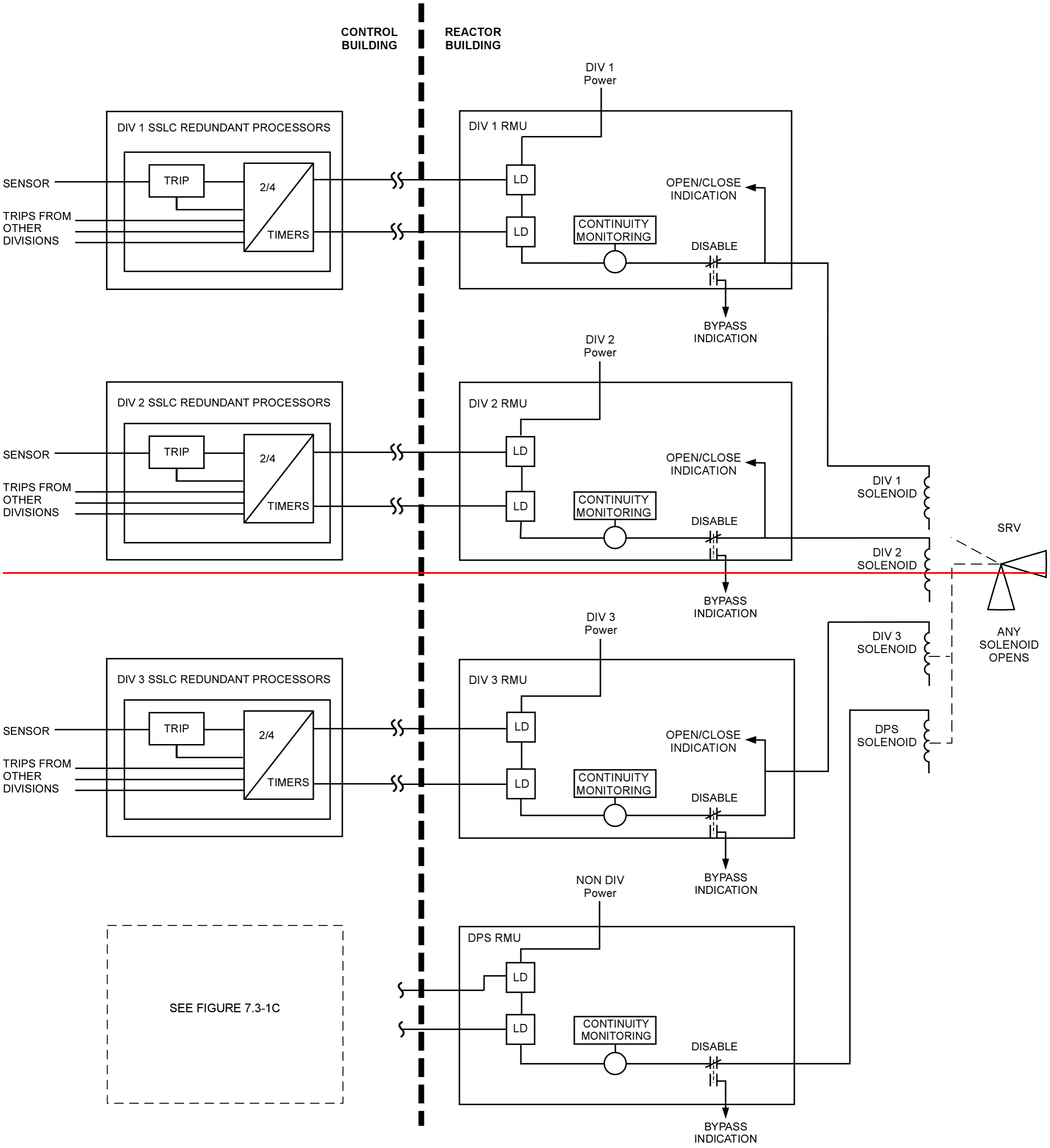
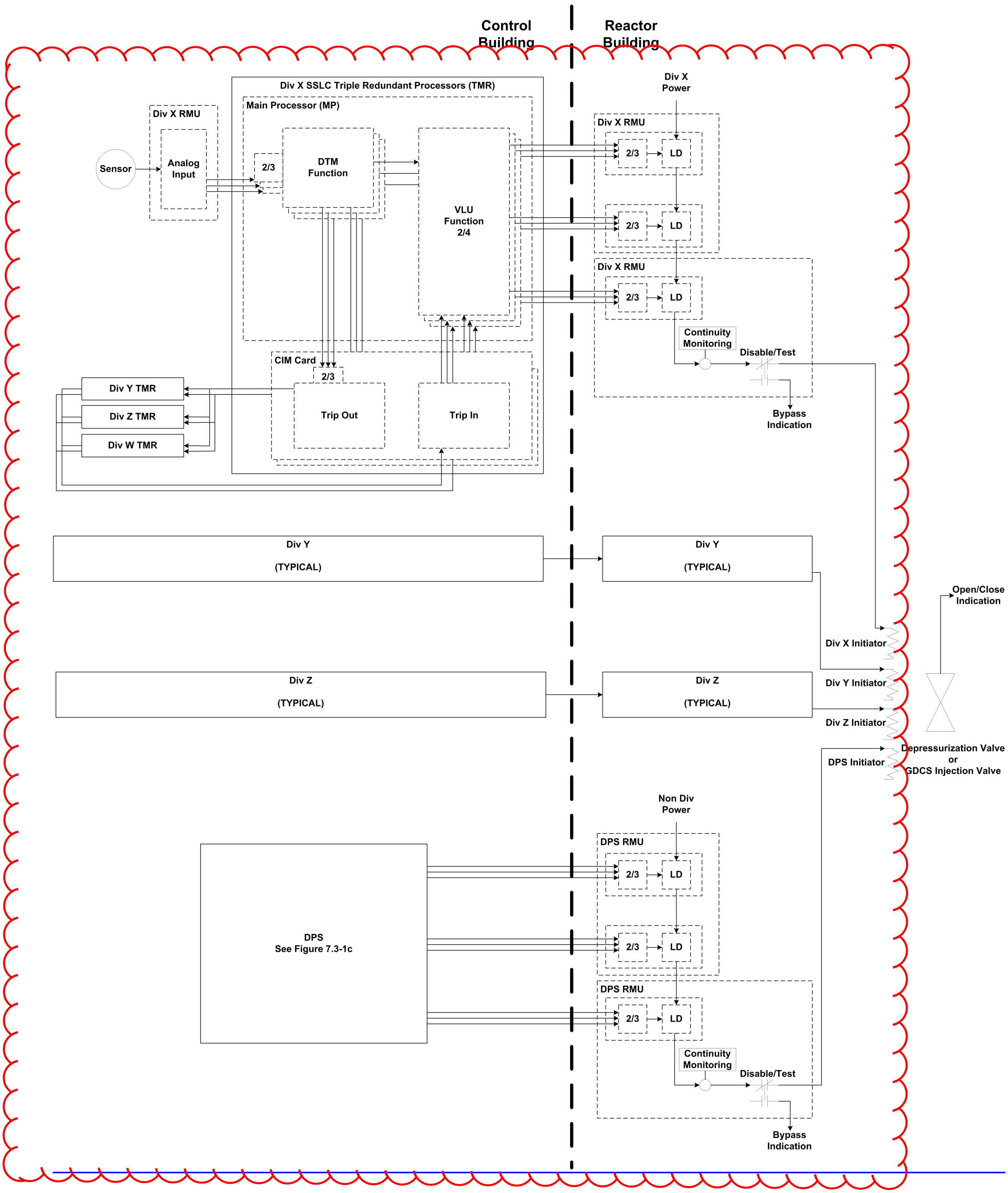


Figure 7.3-1a. SRV Initiation Logics


Control Building
Reactor Building
Div X SSLC Triple Redundant Processors (TMR)
Main Processor (MP)
Div X RMU
Sensor
Analog Input
2/3
DTM Function
VLU Function 2/4
CIM Card
2/3
Trip Out
Trip In
Div Y TMR
Div Z TMR
Div W TMR
Div X Power
Div X RMU
2/3
LD
2/3
LD
Div X RMU
2/3
LD
Continuity Monitoring
Disable/Test
Bypass Indication
Div Y
(TYPICAL)
Div Y
(TYPICAL)
Div Z
(TYPICAL)
Div Z
(TYPICAL)
Open/Close Indication
Div X Initiator
Div Y Initiator
Div Z Initiator
DPS Initiator
Depressurization Valve or GDCS Injection Valve
Non Div Power
DPS RMU
2/3
LD
2/3
LD
DPS RMU
2/3
LD
DPS
See Figure 7.3-1c
Continuity Monitoring
Disable/Test
Bypass Indication

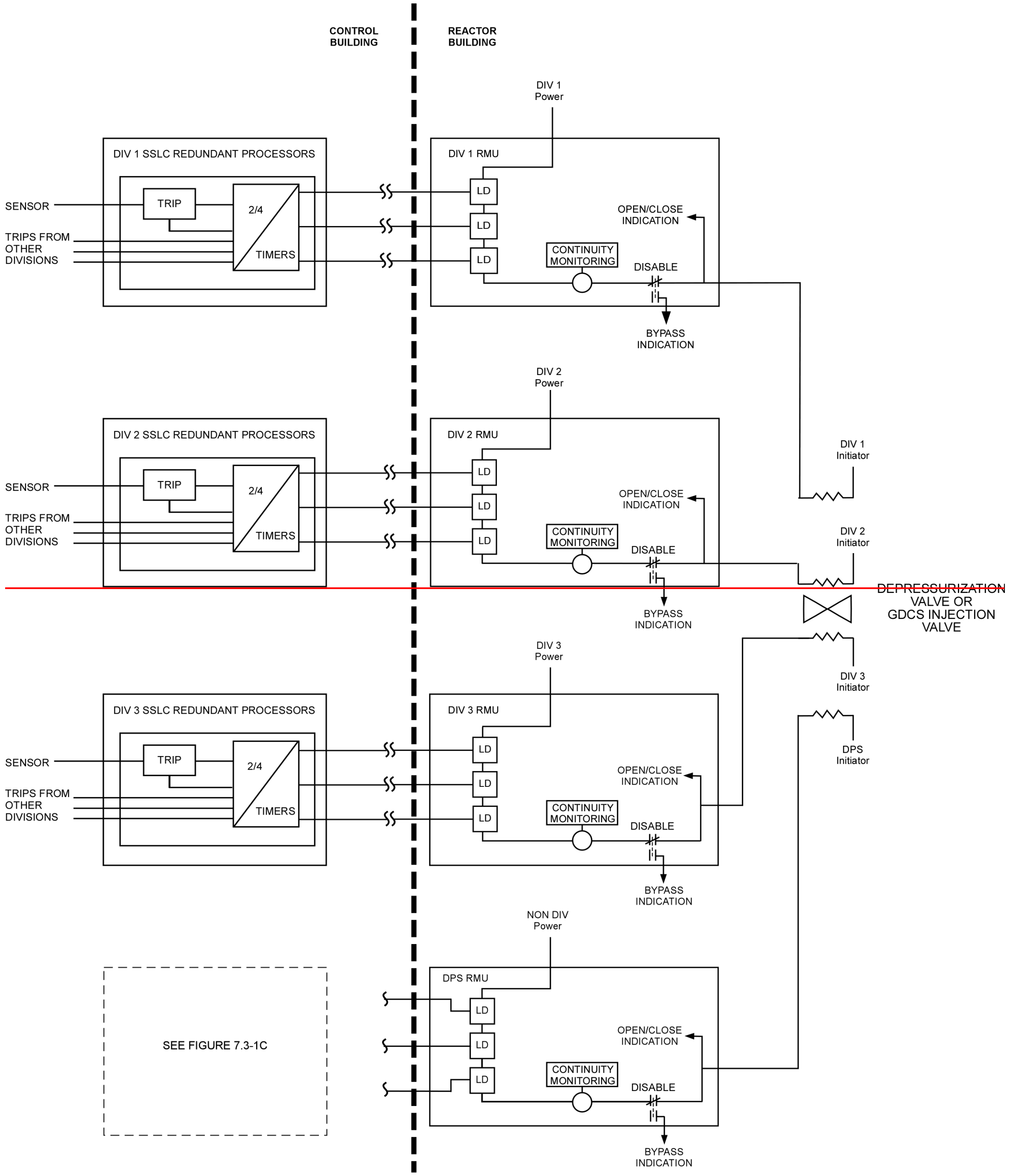
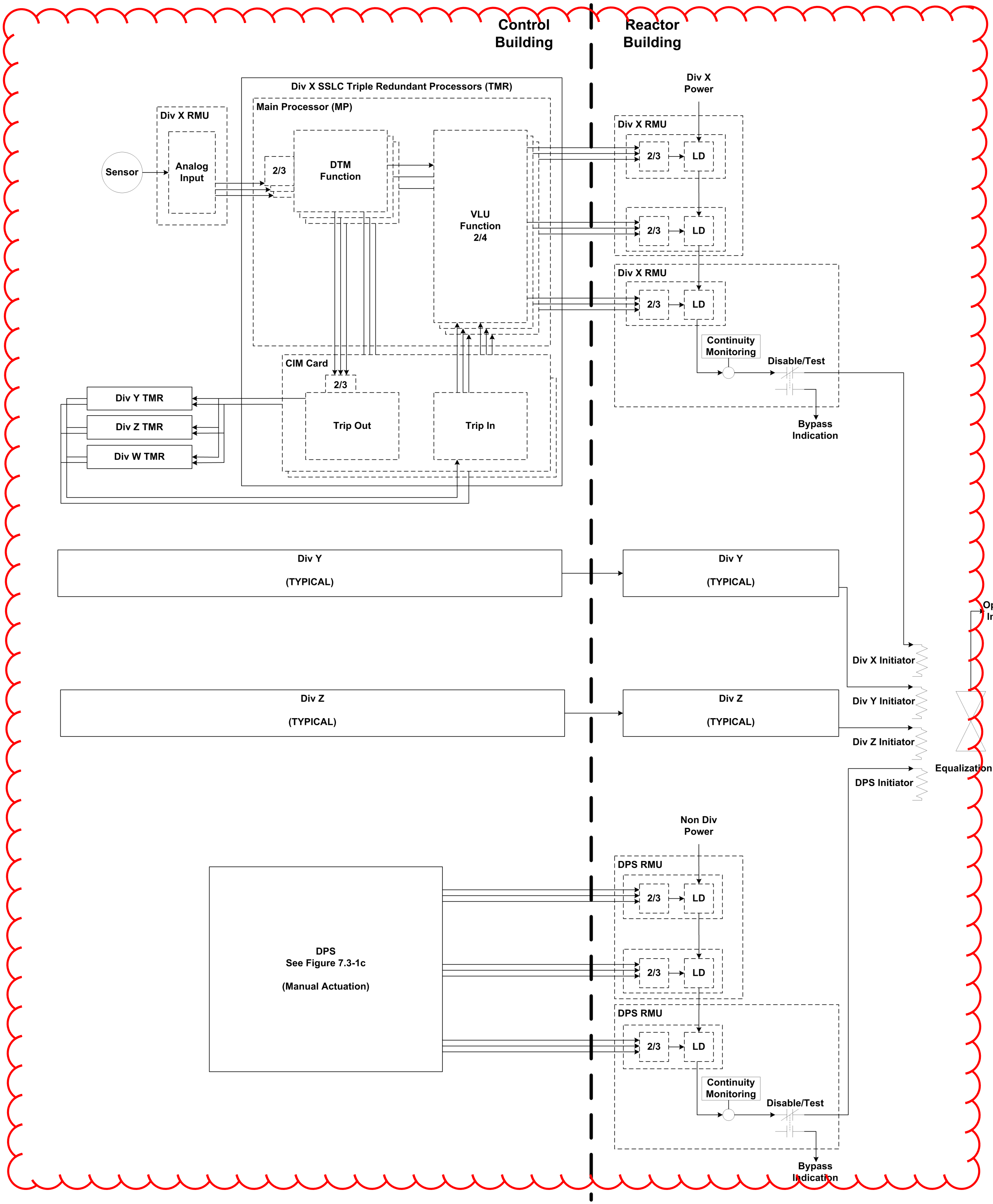


Figure 7.3-1b. GDCS and DPV Initiation Logics


Control Building
Reactor Building
Div X SSLC Triple Redundant Processors (TMR)
Main Processor (MP)
Div X RMU
Sensor
Analog Input
2/3
DTM Function
VLU Function 2/4
CIM Card
2/3
Trip Out
Trip In
Div Y TMR
Div Z TMR
Div W TMR
Div X Power
Div X RMU
2/3
LD
2/3
LD
Div X RMU
2/3
LD
Continuity Monitoring
Disable/Test
Bypass Indication
Div Y
(TYPICAL)
Div Y
(TYPICAL)
Div Z
(TYPICAL)
Div Z
(TYPICAL)
Open/Close Indication
Div X Initiator
Div Y Initiator
Div Z Initiator
DPS Initiator
Equalization Valve
Non Div Power
DPS RMU
2/3
LD
2/3
LD
DPS RMU
2/3
LD
DPS
See Figure 7.3-1c
(Manual Actuation)
Continuity Monitoring
Disable/Test
Bypass Indication

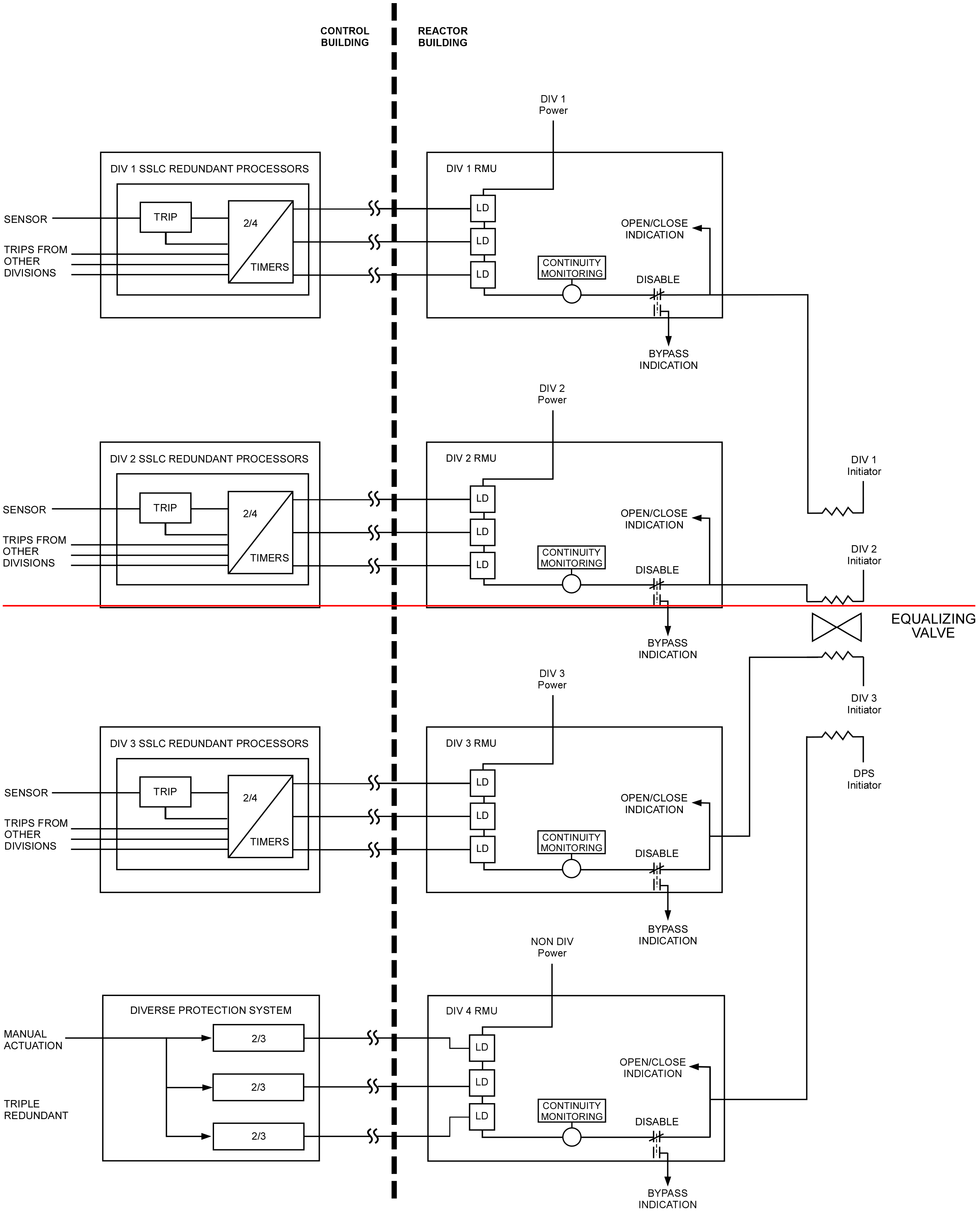
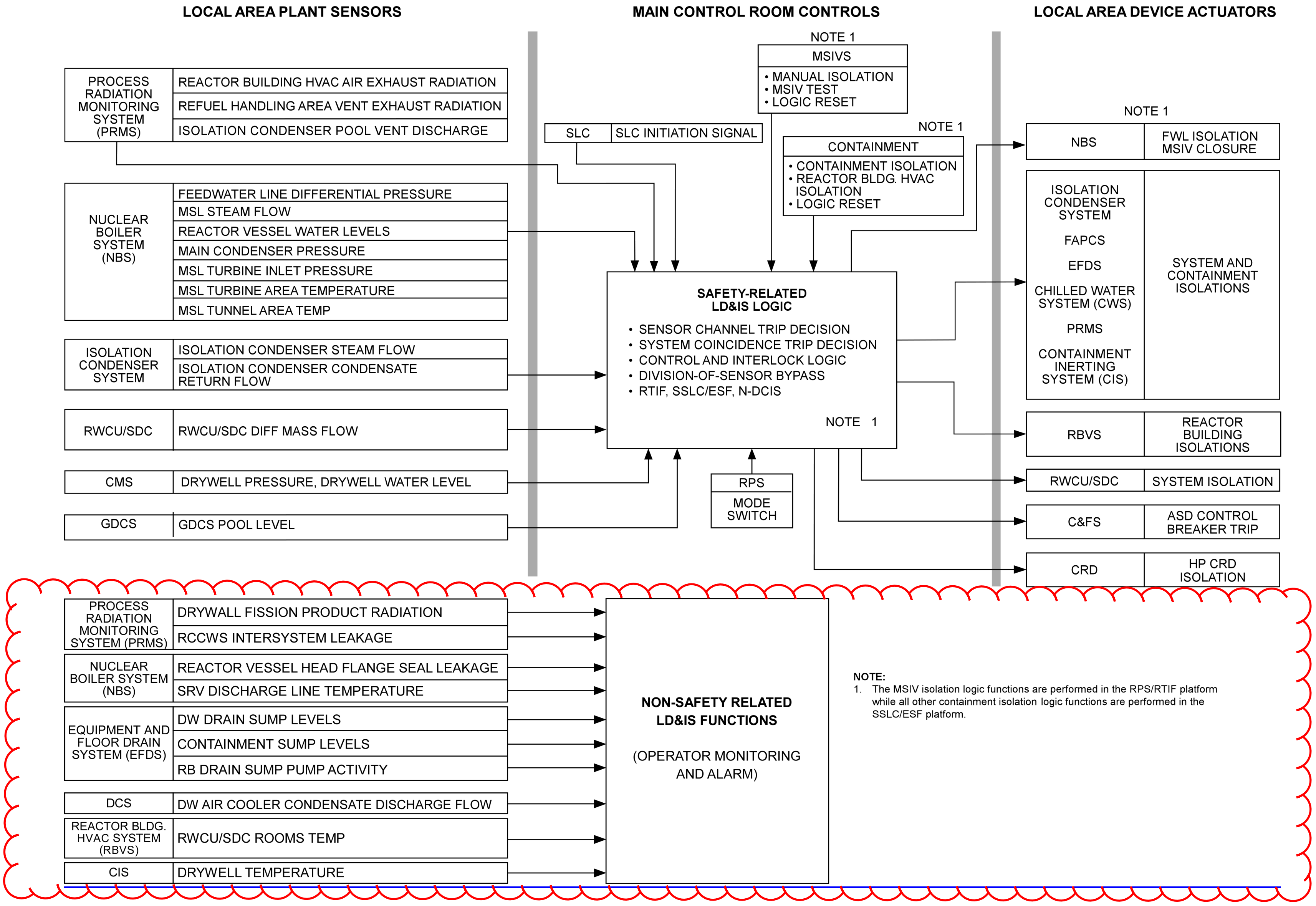
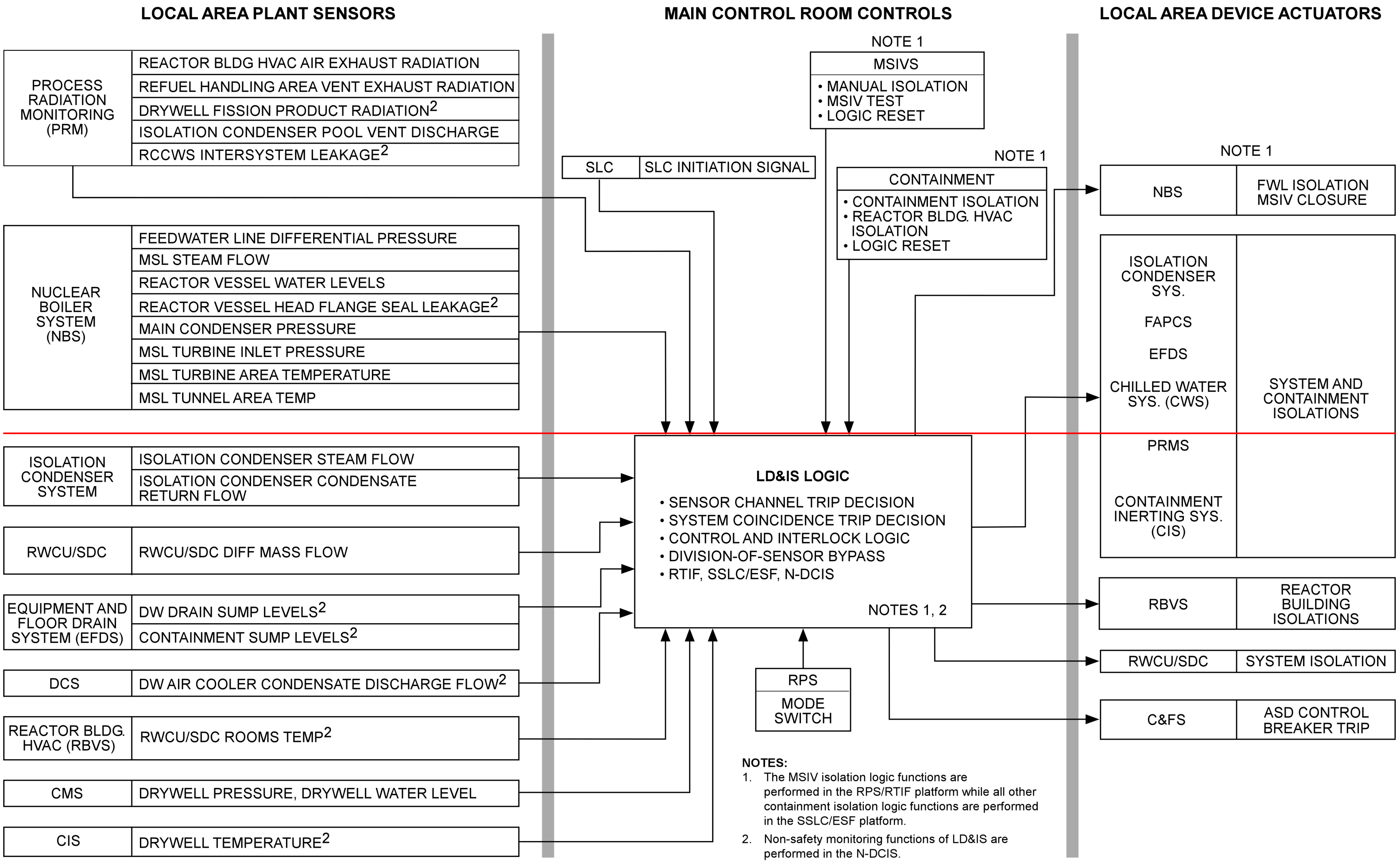


Figure 7.3-2. GDCS Equalizing Valve Initiation Logics


LOCAL AREA PLANT SENSORS
MAIN CONTROL ROOM CONTROLS
LOCAL AREA DEVICE ACTUATORS
PROCESS RADIATION MONITORING SYSTEM (PRMS)
REACTOR BUILDING HVAC AIR EXHAUST RADIATION
REFUEL HANDLING AREA VENT EXHAUST RADIATION
ISOLATION CONDENSER POOL VENT DISCHARGE
NUCLEAR BOILER SYSTEM (NBS)
FEEDWATER LINE DIFFERENTIAL PRESSURE
MSL STEAM FLOW
REACTOR VESSEL WATER LEVELS
MAIN CONDENSER PRESSURE
MSL TURBINE INLET PRESSURE
MSL TURBINE AREA TEMPERATURE
MSL TUNNEL AREA TEMP
ISOLATION CONDENSER SYSTEM
ISOLATION CONDENSER STEAM FLOW
ISOLATION CONDENSER CONDENSATE RETURN FLOW
RWCU/SDC
RWCU/SDC DIFF MASS FLOW
CMS
DRYWELL PRESSURE, DRYWELL WATER LEVEL
GDCS
GDCS POOL LEVEL
NOTE 1
MSIVS
• MANUAL ISOLATION
• MSIV TEST
• LOGIC RESET
SLC
SLC INITIATION SIGNAL
NOTE 1
CONTAINMENT
• CONTAINMENT ISOLATION
• REACTOR BLDG. HVAC ISOLATION
• LOGIC RESET
SAFETY-RELATED LD&IS LOGIC
• SENSOR CHANNEL TRIP DECISION
• SYSTEM COINCIDENCE TRIP DECISION
• CONTROL AND INTERLOCK LOGIC
• DIVISION-OF-SENSOR BYPASS
• RTIF, SSLC/ESF, N-DCIS
NOTE 1
RPS
MODE SWITCH
NOTE 1
NBS
FWL ISOLATION MSIV CLOSURE
ISOLATION CONDENSER SYSTEM
FAPCS
EFDS
CHILLED WATER SYSTEM (CWS)
PRMS
CONTAINMENT INERTING SYSTEM (CIS)
SYSTEM AND CONTAINMENT ISOLATIONS
RBVS
REACTOR BUILDING ISOLATIONS
RWCU/SDC
SYSTEM ISOLATION
C&FS
ASD CONTROL BREAKER TRIP
CRD
HP CRD ISOLATION
PROCESS RADIATION MONITORING SYSTEM (PRMS)
DRYWELL FISSION PRODUCT RADIATION
RCCWS INTERSYSTEM LEAKAGE
NUCLEAR BOILER SYSTEM (NBS)
REACTOR VESSEL HEAD FLANGE SEAL LEAKAGE
SRV DISCHARGE LINE TEMPERATURE
EQUIPMENT AND FLOOR DRAIN SYSTEM (EFDS)
DW DRAIN SUMP LEVELS
CONTAINMENT SUMP LEVELS
RB DRAIN SUMP PUMP ACTIVITY
DCS
DW AIR COOLER CONDENSATE DISCHARGE FLOW
REACTOR BLDG. HVAC SYSTEM (RBVS)
RWCU/SDC ROOMS TEMP
CIS
DRYWELL TEMPERATURE
NON-SAFETY RELATED LD&IS FUNCTIONS
(OPERATOR MONITORING AND ALARM)

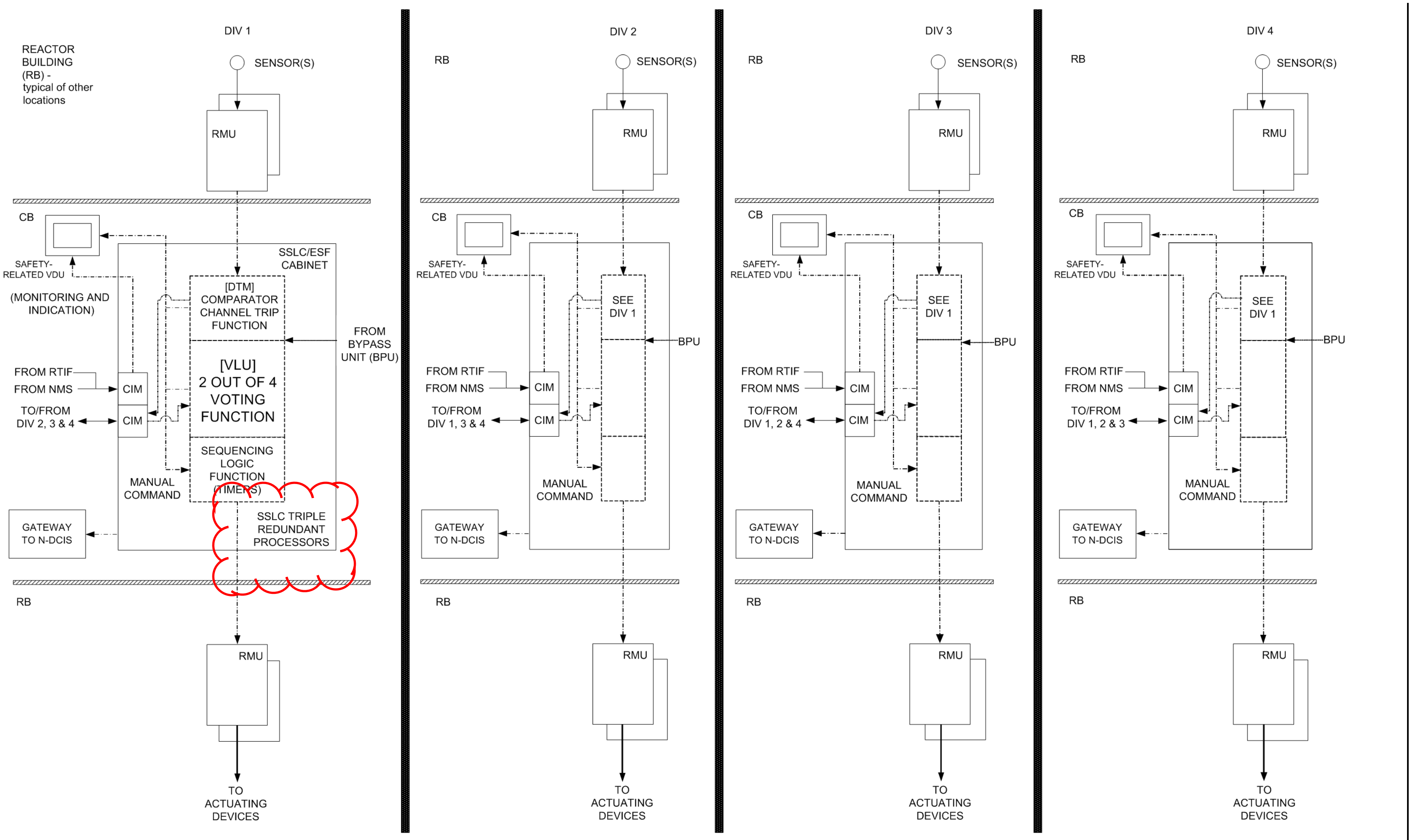
NOTE:
1. The MSIV isolation logic functions are performed in the RPS/RTIF platform while all other containment isolation logic functions are performed in the SSLC/ESF platform.


LOCAL AREA PLANT SENSORS
MAIN CONTROL ROOM CONTROLS
LOCAL AREA DEVICE ACTUATORS
PROCESS RADIATION MONITORING (PRM)
REACTOR BLDG HVAC AIR EXHAUST RADIATION
REFUEL HANDLING AREA VENT EXHAUST RADIATION
DRYWELL FISSION PRODUCT RADIATION2
ISOLATION CONDENSER POOL VENT DISCHARGE
RCCWS INTERSYSTEM LEAKAGE2
NUCLEAR BOILER SYSTEM (NBS)
FEEDWATER LINE DIFFERENTIAL PRESSURE
MSL STEAM FLOW
REACTOR VESSEL WATER LEVELS
REACTOR VESSEL HEAD FLANGE SEAL LEAKAGE2
MAIN CONDENSER PRESSURE
MSL TURBINE INLET PRESSURE
MSL TURBINE AREA TEMPERATURE
MSL TUNNEL AREA TEMP
ISOLATION CONDENSER SYSTEM
ISOLATION CONDENSER STEAM FLOW
ISOLATION CONDENSER CONDENSATE RETURN FLOW
RWCU/SDC
RWCU/SDC DIFF MASS FLOW
EQUIPMENT AND FLOOR DRAIN SYSTEM (EFDS)
DW DRAIN SUMP LEVELS2
CONTAINMENT SUMP LEVELS2
DCS
DW AIR COOLER CONDENSATE DISCHARGE FLOW2
REACTOR BLDG. HVAC (RBVS)
RWCU/SDC ROOMS TEMP2
CMS
DRYWELL PRESSURE, DRYWELL WATER LEVEL
CIS
DRYWELL TEMPERATURE2
NOTE 1
MSIVS
• MANUAL ISOLATION
• MSIV TEST
• LOGIC RESET
SLC
SLC INITIATION SIGNAL
NOTE 1
CONTAINMENT
• CONTAINMENT ISOLATION
• REACTOR BLDG. HVAC ISOLATION
• LOGIC RESET
LD&IS LOGIC
• SENSOR CHANNEL TRIP DECISION
• SYSTEM COINCIDENCE TRIP DECISION
• CONTROL AND INTERLOCK LOGIC
• DIVISION-OF-SENSOR BYPASS
• RTIF, SSLC/ESF, N-DCIS
NOTES 1, 2
RPS
MODE SWITCH
NOTE 1
NBS
FWL ISOLATION MSIV CLOSURE
ISOLATION CONDENSER SYS.
FAPCS
EFDS
CHILLED WATER SYS. (CWS)
PRMS
CONTAINMENT INERTING SYS. (CIS)
SYSTEM AND CONTAINMENT ISOLATIONS
RBVS
REACTOR BUILDING ISOLATIONS
RWCU/SDC
SYSTEM ISOLATION
C&FS
ASD CONTROL BREAKER TRIP

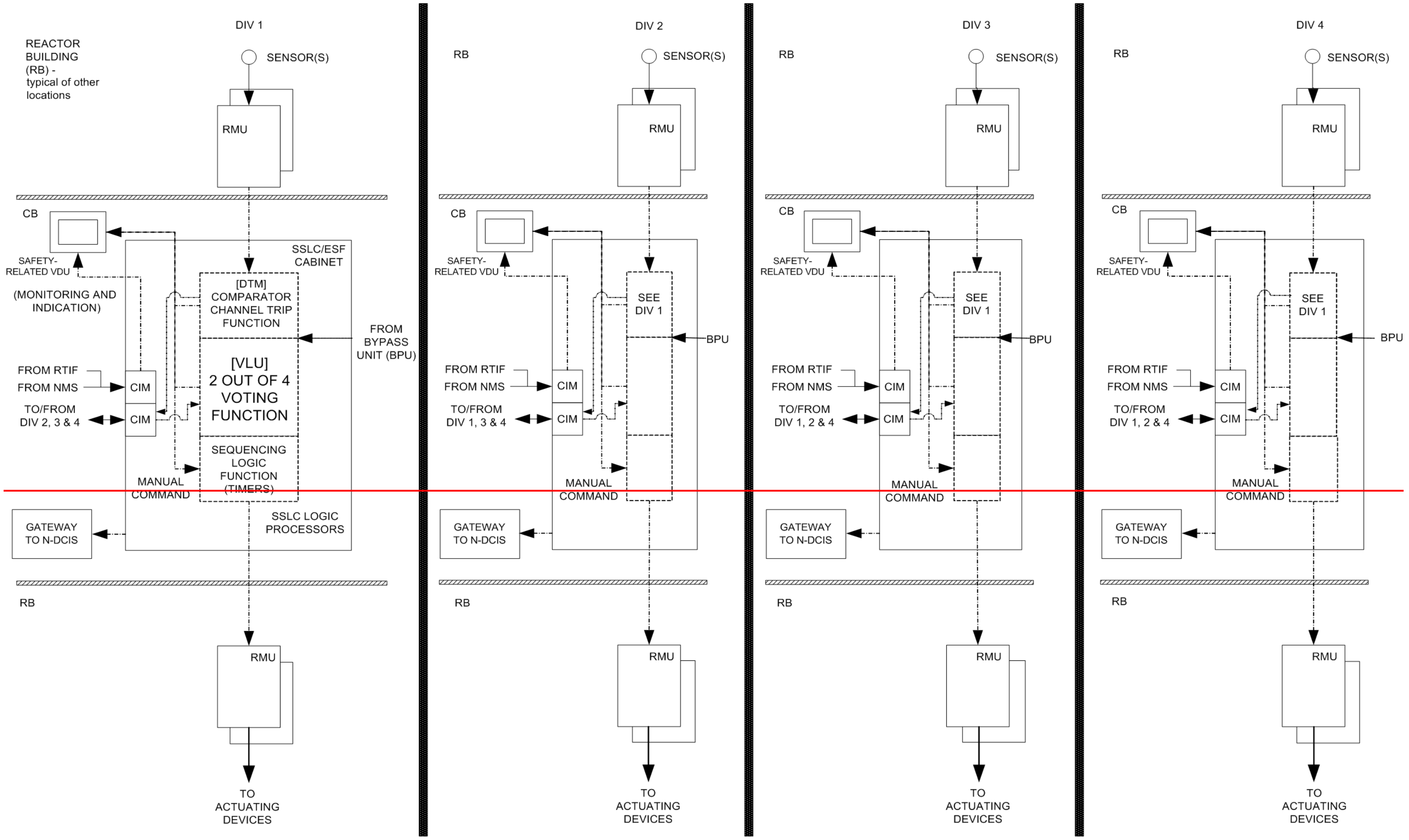
NOTES:

1. The MSIV isolation logic functions are performed in the RPS/RTIF platform while all other containment isolation logic functions are performed in the SSLC/ESF platform.
2. Non-safety monitoring functions of LD&IS are performed in the N-DCIS.

Figure 7.3-3. LD&IS System Design Configuration



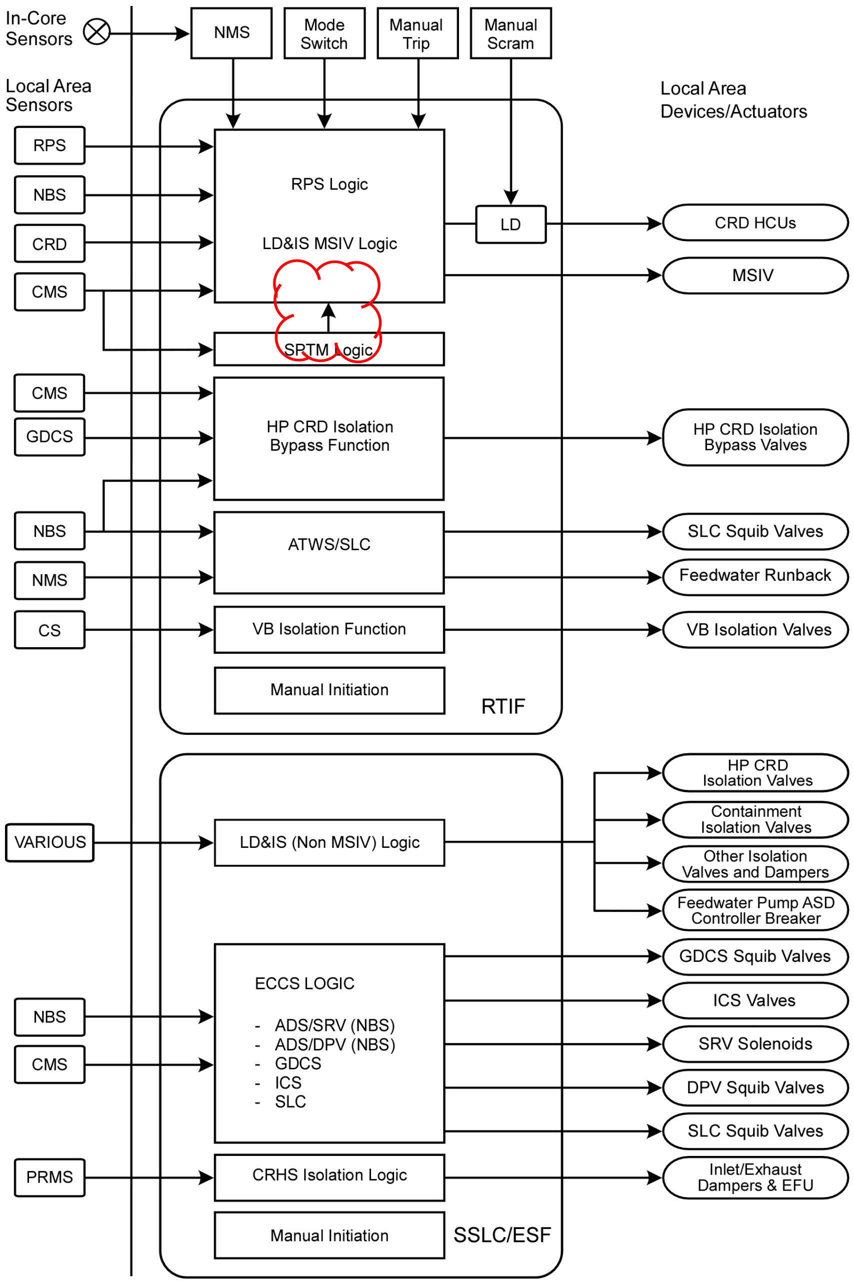
NOTES:
Redundant DIV 1 and 2 VDUs are located at the Remote Shutdown Panels
CIM=COMMUNICATION INTERFACE MODULE-ISOLATOR



NOTES:
FOR ECCS FUNCTION, THE VLU CONTAINS DUAL REDUNDANT 2-out-of-4 LOGIC WITH TWO INDEPENDENT TRIP OUTPUTS
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



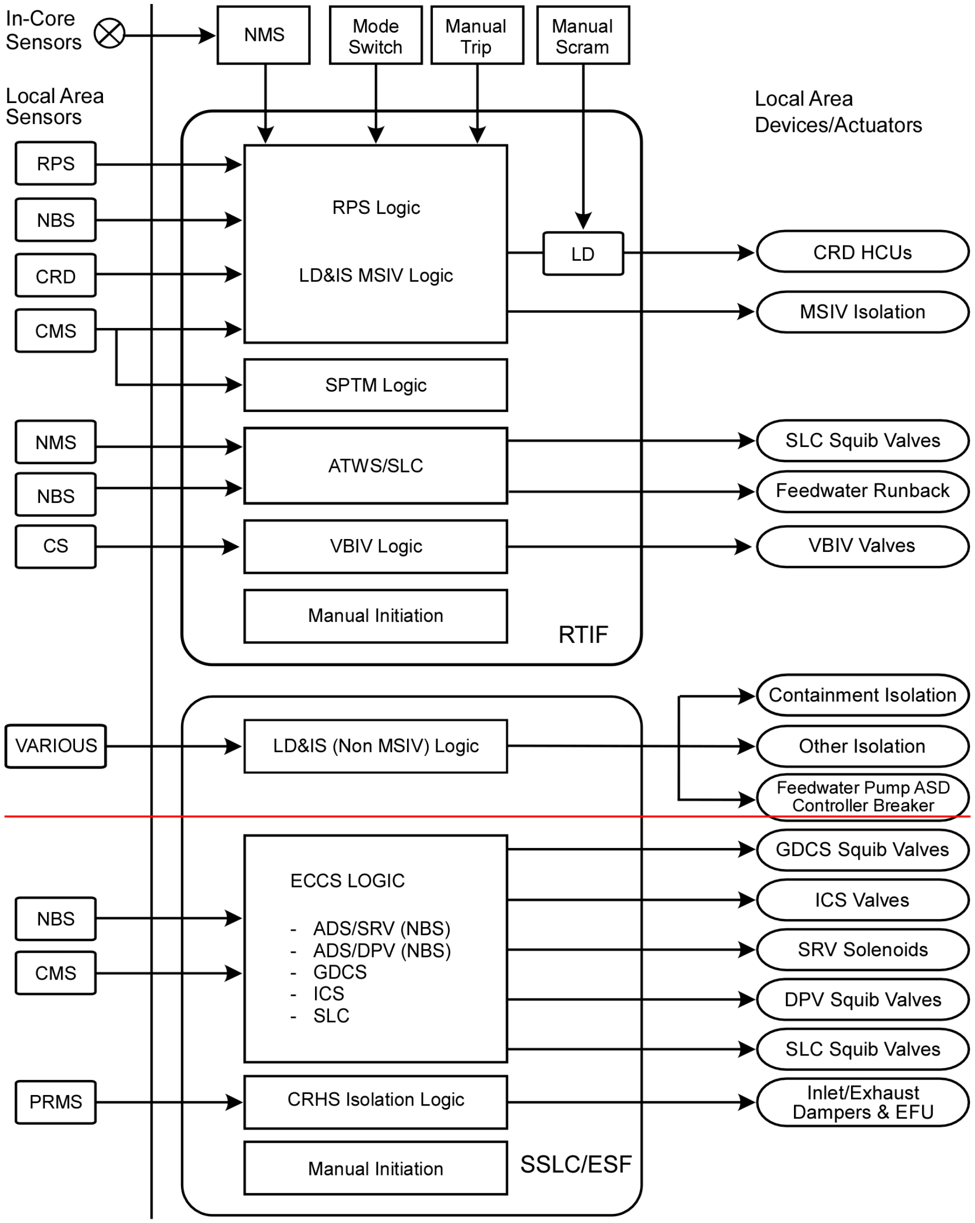
Notes: 1) Local area sensors include:

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.



Note: 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 Monitoring - control room inlet ventilation

NBS: MSIV position (for RTIF only), RPV pressure, water level

CRD: HCU accumulator charging water header pressure

CMS: Drywell pressure, drywell level, suppression pool temperature

CS: (Containment System) Wetwell and drywell temperature sensors

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

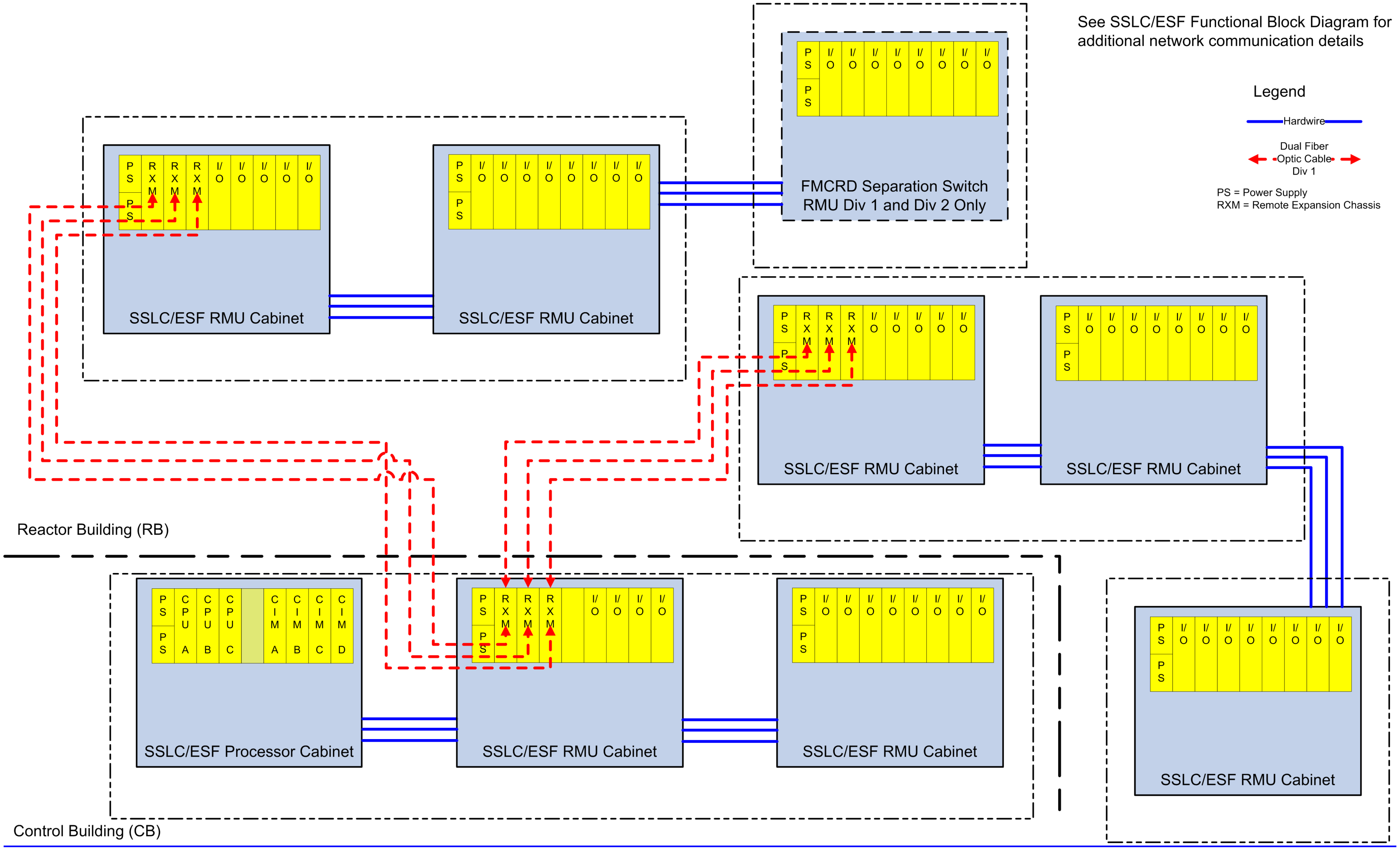


Figure 7.3-6. SSLC/ESF Division 1 Layout

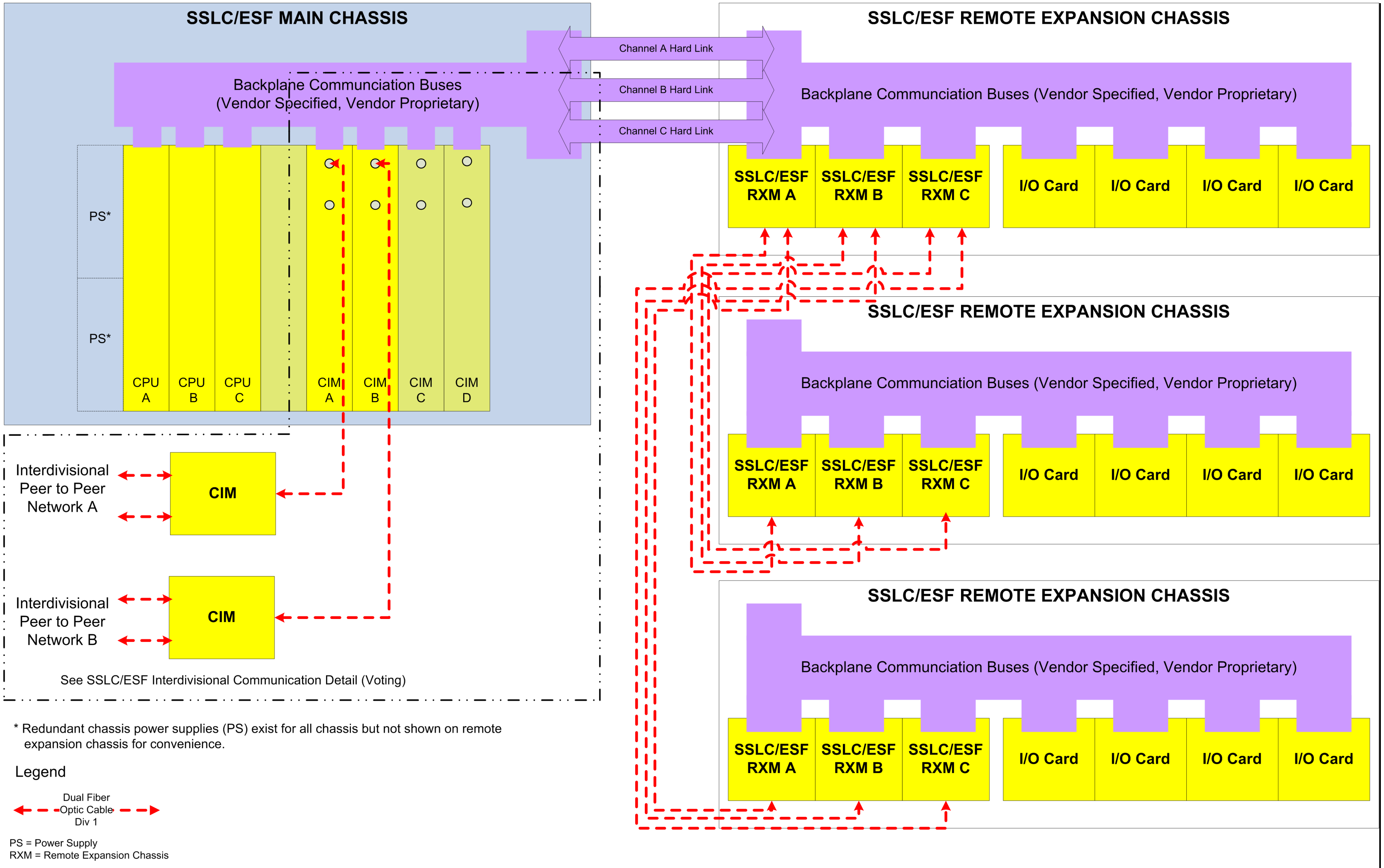

SSLC/ESF MAIN CHASSIS
Backplane Communciation Buses
(Vendor Specified, Vendor Proprietary)
PS*
PS*
CPU A
CPU B
CPU C
CIM A
CIM B
CIM C
CIM D
Channel A Hard Link
Channel B Hard Link
Channel C Hard Link
SSLC/ESF REMOTE EXPANSION CHASSIS
Backplane Communciation Buses (Vendor Specified, Vendor Proprietary)
SSLC/ESF RXM A
SSLC/ESF RXM B
SSLC/ESF RXM C
I/O Card
I/O Card
I/O Card
I/O Card
SSLC/ESF REMOTE EXPANSION CHASSIS
Backplane Communciation Buses (Vendor Specified, Vendor Proprietary)
SSLC/ESF RXM A
SSLC/ESF RXM B
SSLC/ESF RXM C
I/O Card
I/O Card
I/O Card
I/O Card
SSLC/ESF REMOTE EXPANSION CHASSIS
Backplane Communciation Buses (Vendor Specified, Vendor Proprietary)
SSLC/ESF RXM A
SSLC/ESF RXM B
SSLC/ESF RXM C
I/O Card
I/O Card
I/O Card
I/O Card
Interdivisional Peer to Peer Network A
CIM
Interdivisional Peer to Peer Network B
CIM
See SSLC/ESF Interdivisional Communication Detail (Voting)
* Redundant chassis power supplies (PS) exist for all chassis but not shown on remote expansion chassis for convenience.
Legend
Dual Fiber Optic Cable Div 1
PS = Power Supply
RXM = Remote Expansion Chassis

Figure 7.3-7. SSLC/ESF Functional Block Diagram

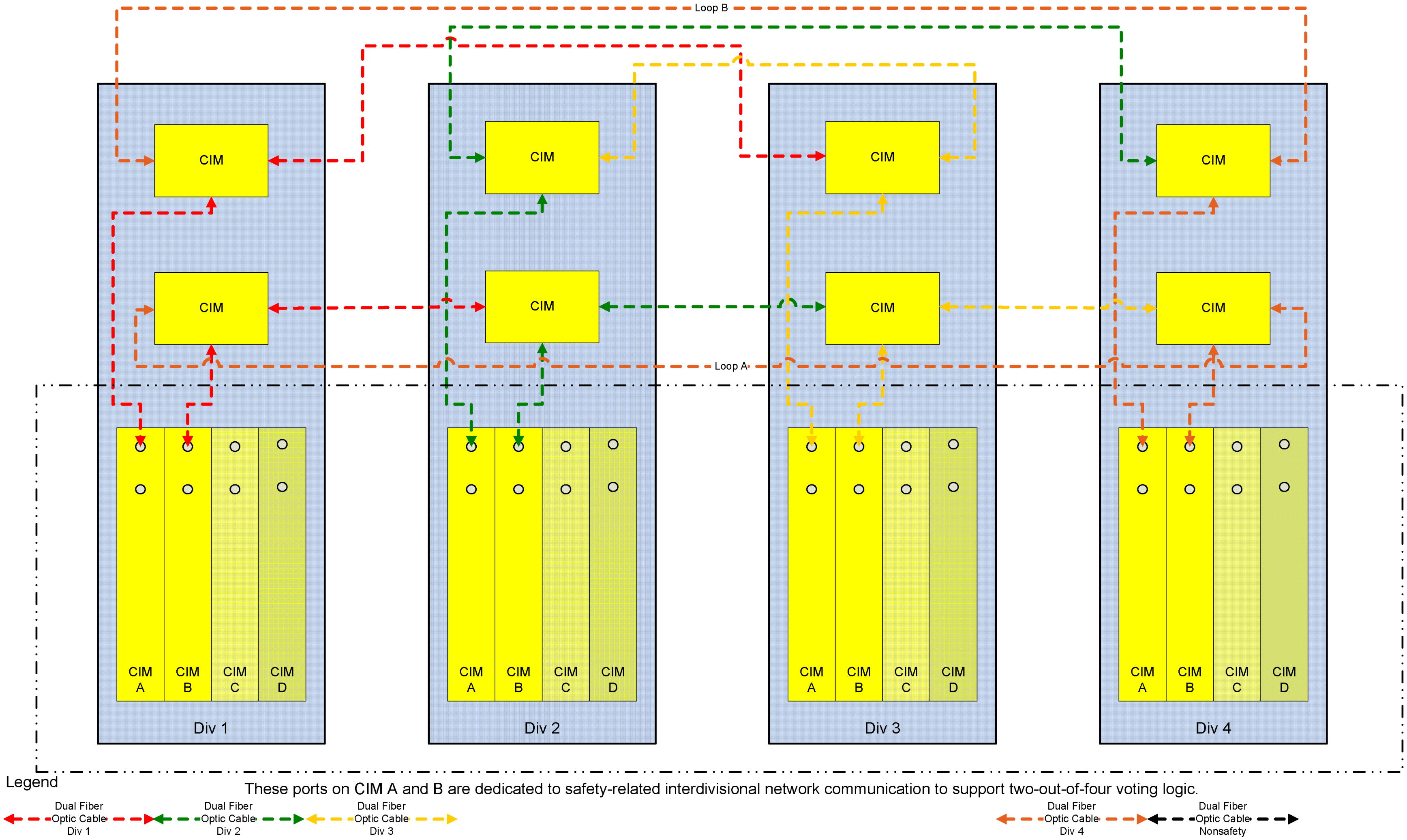

Loop B
Loop A
CIM
CIM
CIM A
CIM B
CIM C
CIM D
Div 1
Div 2
Div 3
Div 4
Legend
These ports on CIM A and B are dedicated to safety-related interdivisional network communication to support two-out-of-four voting logic.
Dual Fiber Optic Cable Div 1
Dual Fiber Optic Cable Div 2
Dual Fiber Optic Cable Div 3
Dual Fiber Optic Cable Div 4
Dual Fiber Optic Cable Nonsafety

Figure 7.3-8. SSLC/ESF Interdivisional Communication Detail

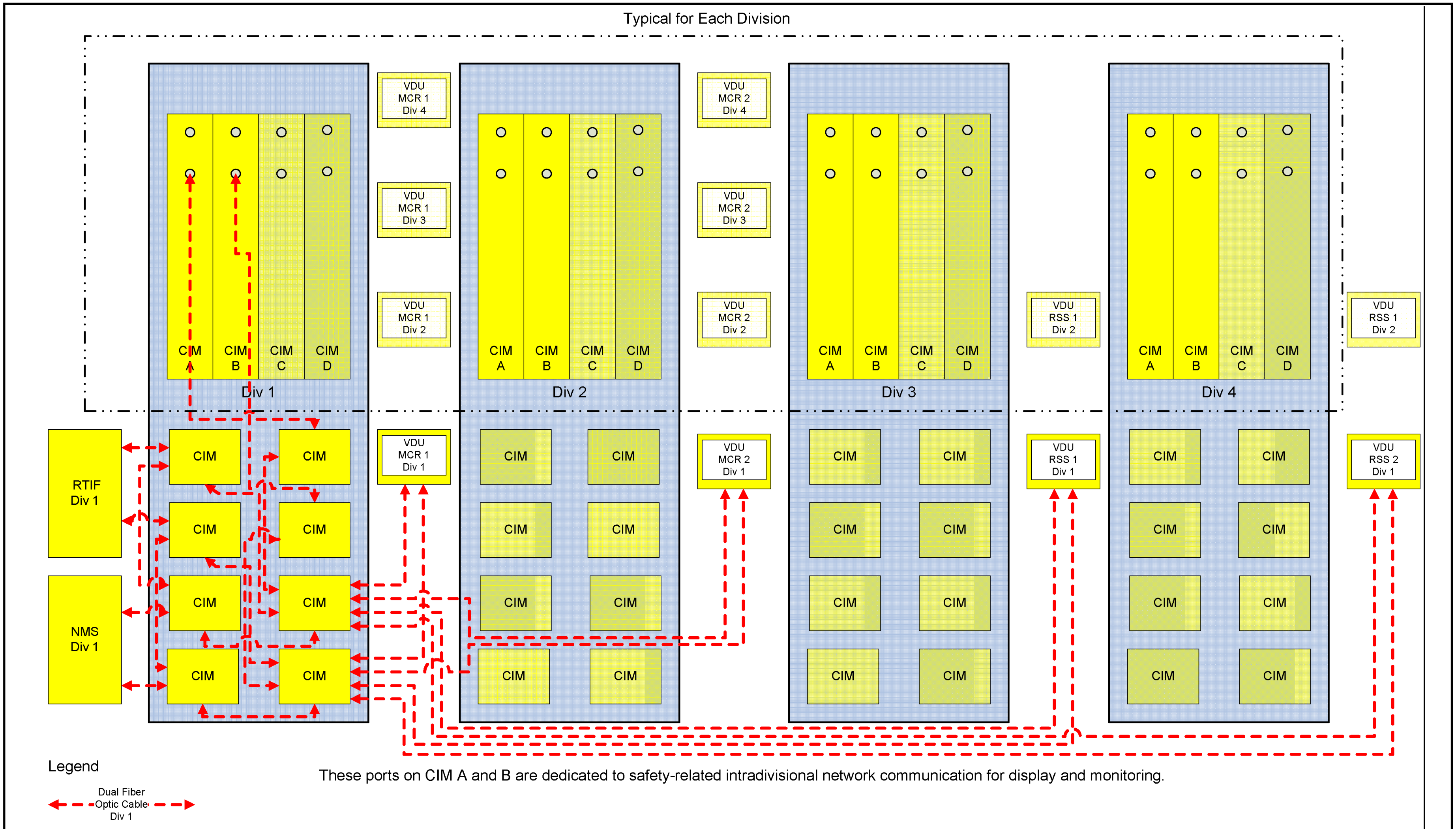
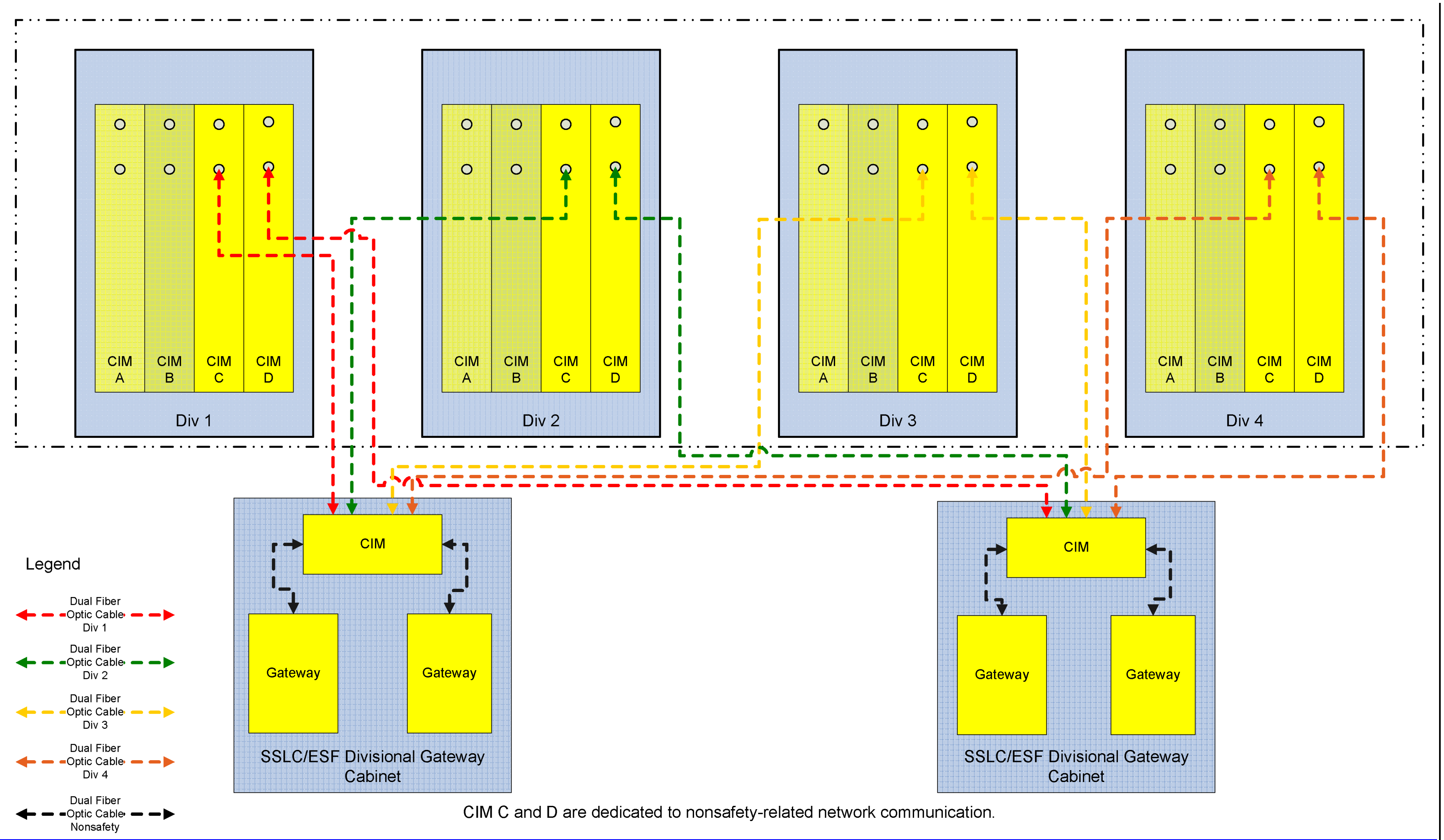


Figure 7.3-9. SSLC/ESF Safety-Related VDU Communication Detail


CIM A
CIM B
CIM C
CIM D
Div 1
Div 2
Div 3
Div 4
CIM
Gateway
Gateway
SSLC/ESF Divisional Gateway Cabinet
CIM
Gateway
Gateway
SSLC/ESF Divisional Gateway Cabinet
Legend
Dual Fiber Optic Cable Div 1
Dual Fiber Optic Cable Div 2
Dual Fiber Optic Cable Div 3
Dual Fiber Optic Cable Div 4
Dual Fiber Optic Cable Nonsafety

CIM C and D are dedicated to nonsafety-related network communication.

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." However, some I&C systems performing cold shutdown functions 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~~ (IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10)~~.

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. DBE mitigation crediting the SLC system is discussed in Chapter 15, "Safety Analyses." ~~(IEEE Std. 603, Sections 4.1, 4.2, 4.5, 4.8, and 4.10).~~

The SLC system initiation functions ~~is~~are part of a group of systems collectively called the Safety-Related Distributed Control and Information System (Q-DCIS). A simplified network functional ~~block~~ diagram of the ~~Q-~~DCIS is included as ~~part of~~ Figure 7.1-1.~~,~~ ~~and a functional network diagram appears as Figure 7.1-2.~~ Thise~~se~~ diagram~~s~~ 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~~dual, key-locked control~~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.~~ (IEEE Std. 603, Section 4.5)~~

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~~confirmed LOCA. The SLC actuation sequence corresponds to the first Depressurization Valve (DPV) actuation~~ (as described in the Automatic Depressurization System [ADS] logic discussion in Subsection 7.3.1~~.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 ~~sensors,~~ 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~~accumulator~~ shut-off valves on (a voted two-out-of-four) low accumulator level. The SLC system processors of the ATWS/SLC independent control~~mitigation logic~~ 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 ~~(IEEE Std. 603, Sections 5.12, 8.1, and 8.2)~~.

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. ~~(IEEE Std. 603, Section 5.2).~~

- An open signal is provided to the normally open ~~accumulator~~injection shut-off valves to support the ~~ECCS~~ 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 SLC 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 ~~(IEEE Std. 603, Section 4.8~~). 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~~ (IEEE Std. 603, Section 5.4)~~. Inter-division communication (and communication with nonsafety-related interfaces) occurs through qualified isolation devices~~ (IEEE Std. 603, Section 5.6)~~. 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).

~~The o~~Only the automatic actuation logic originating from within the SLC system logic processors transmits the low accumulator-level isolation signals for the ~~accumulator~~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 ~~mitigation logic~~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~~ (IEEE Std. 603, Section 5.1)~~. Division of sensors bypass capability allows a safety-related SLC sensor to be removed from service, while maintaining a high level of reliability~~ (IEEE Std. 603, Section 5.7, 6.5, and 6.7)~~. Alarmed indication of the bypass condition provides off-normal condition status monitoring~~ (IEEE Std. 603, Section 5.8)~~. 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~~Redundant~~ 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 ~~dual~~two of four control switches, with each switch requiring two distinct operator actions.~~ The manual SLC system switches are protected by key-locks to minimize the likelihood of inadvertent operation.~~

In addition to squib injection valve continuity monitoring, status indication of squib injection and ~~accumulator~~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. Separation and isolation is maintained both mechanically and electrically in accordance with IEEE Std.~~

~~BTP HICB-18, Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and control Systems:~~

- ~~Conformance: The SLC system design conforms to BTP HICB-18.~~

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, injection would occur. Testing of the squib injection and ~~accumulator~~injection shut-off valve logic is performed periodically to verify operability.

Routine testing, monitoring of critical system parameters, and surveillances ensure operability with an acceptably low probability of demand failure ~~(IEEE Std. 603, Section 5.7)~~.

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~~accumulator~~ shut-off valves. An open indication for these valves is required to ensure SLC system operation ~~(IEEE Std. 603, Section 5.8)~~.

Pressure-level and solution-level alarms and indications for each accumulator ~~(IEEE Std. 603, Section 5.8)~~ 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 if it becomes uninhabitable. 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 ~~bring the plant to (and maintain) a~~ cold shutdown conditions.

7.4.2.2 System Description

7.4.2.2.1 General

The RSS has two redundant and independent panels. ~~All p~~Parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from any of the two RSS panels ~~(IEEE Std. 603, Section 5.8)~~. 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~~Nonsafety-related VDU~~, and
- Nonsafety-related Communications Equipment.

~~All d~~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, ~~all~~ 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 ~~block~~ diagram of the Q-DCIS and N-DCIS is included as ~~part of~~ Figure 7.1-1.~~;~~ ~~and a functional network diagram appears as Figure 7.1-2.~~ This~~ese~~ diagram~~s~~ indicates the relationships of safety-related ~~or~~ 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

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 ~~(IEEE Std. 603, Sections 4.1 and 4.2)~~. 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 ~~block~~ diagram of the ~~Q-~~DCIS is included as ~~part of~~ Figure 7.1-1.~~, and a functional network diagram appears as Figure 7.1-2.~~ This~~ese~~ diagram~~s~~ indicates the relationships of the SSLC/ESF ~~ICS~~ 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~~IC~~ 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 ~~ICS automatically~~ open~~s~~ ~~equalizing valves between the equipment storage pool and the IC/PCC expansion pools~~ 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 ~~to support~~ 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.

- 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

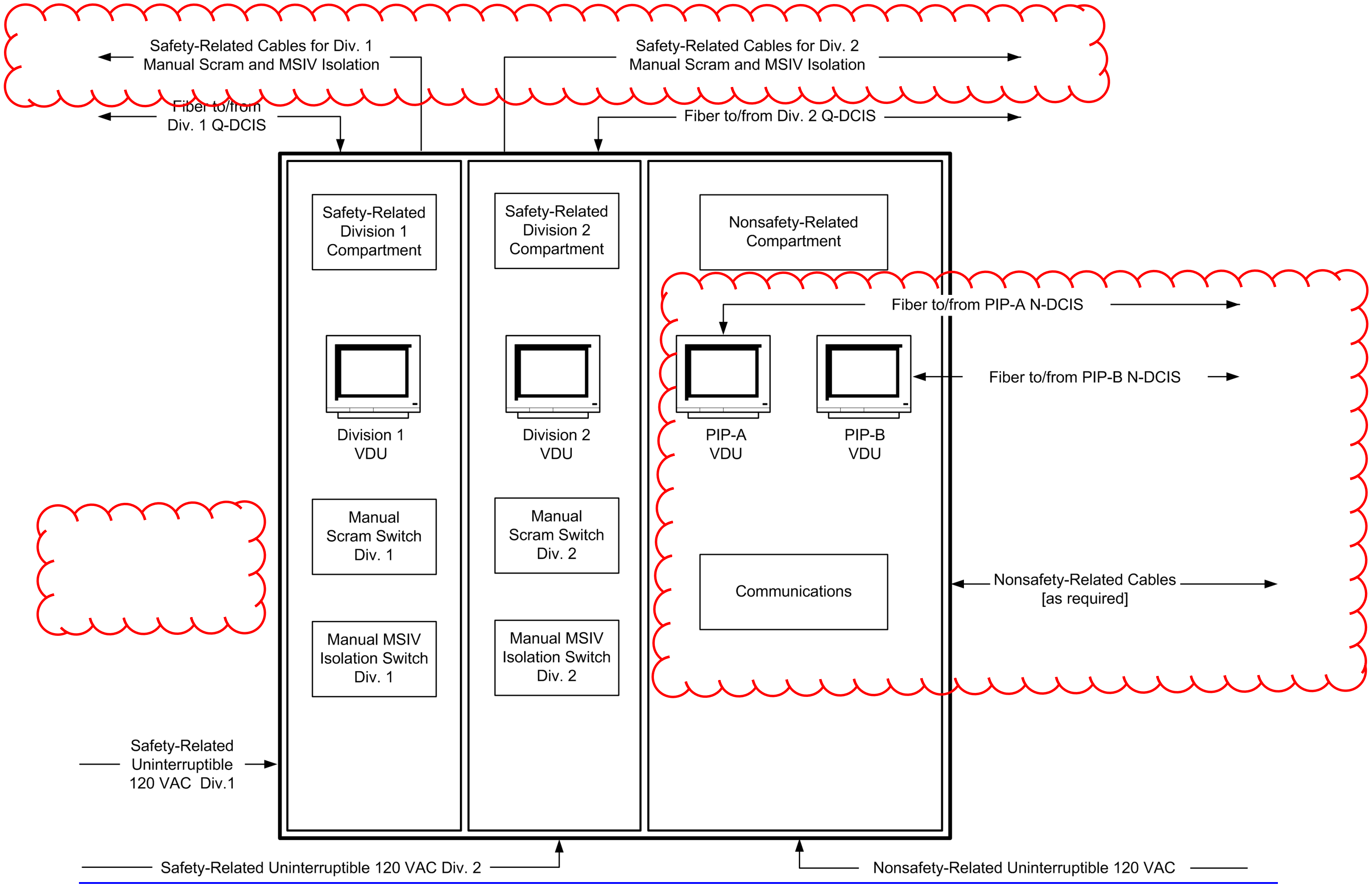
HP CRD Isolation Bypass Function has the following requirements and 10 CFR 50.2 Design Bases.

- 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.


Safety-Related Cables for Div. 1
Manual Scram and MSIV Isolation
Safety-Related Cables for Div. 2
Manual Scram and MSIV Isolation
Fiber to/from
Div. 1 Q-DCIS
Fiber to/from Div. 2 Q-DCIS
Safety-Related
Division 1
Compartment
Safety-Related
Division 2
Compartment
Nonsafety-Related
Compartment
Fiber to/from PIP-A N-DCIS
Fiber to/from PIP-B N-DCIS
Division 1
VDU
Division 2
VDU
PIP-A
VDU
PIP-B
VDU
Manual
Scram Switch
Div. 1
Manual
Scram Switch
Div. 2
Communications
Nonsafety-Related Cables
[as required]
Manual MSIV
Isolation Switch
Div. 1
Manual MSIV
Isolation Switch
Div. 2
Safety-Related
Uninterruptible
120 VAC Div.1
Safety-Related Uninterruptible 120 VAC Div. 2
Nonsafety-Related Uninterruptible 120 VAC

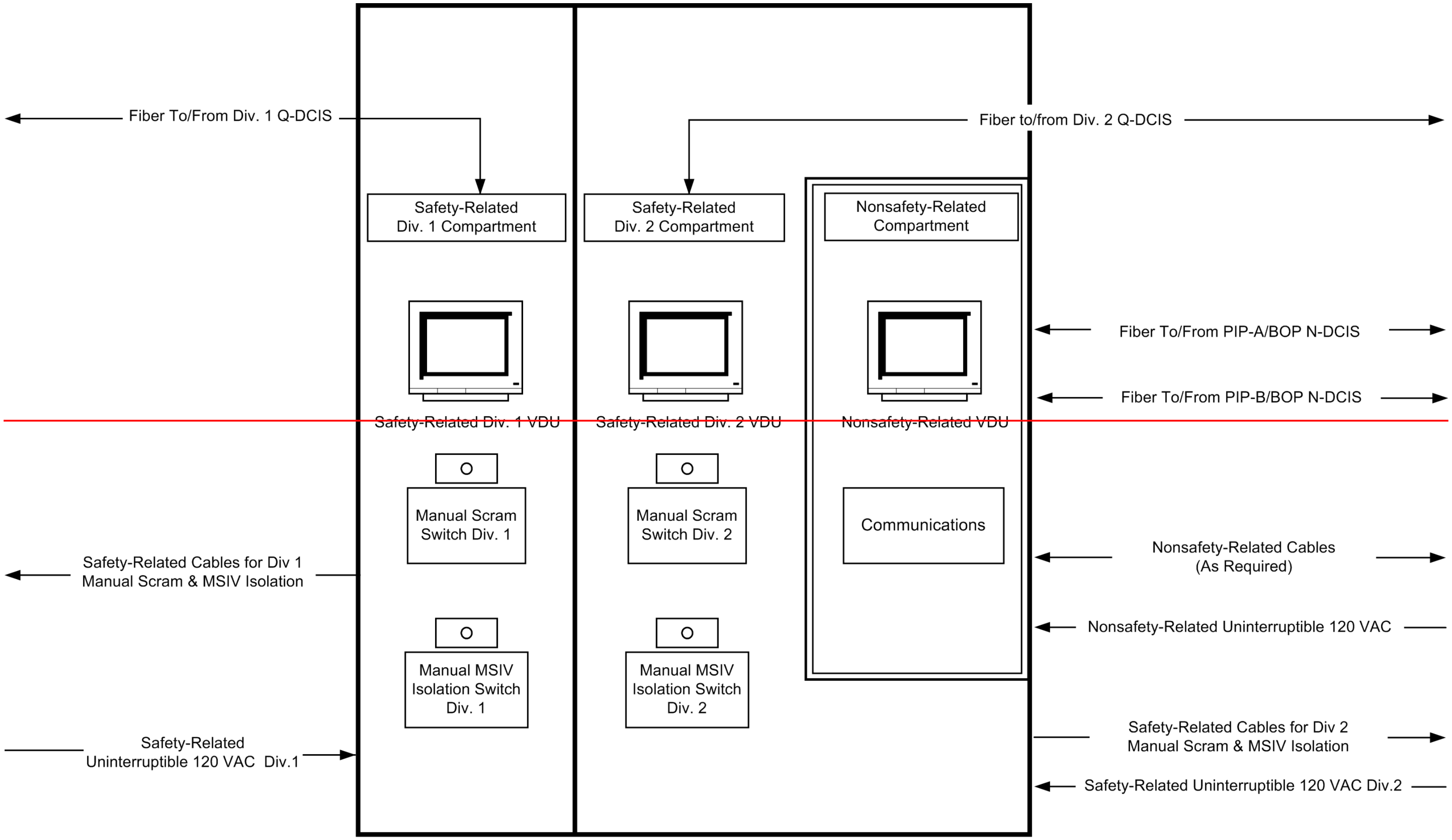
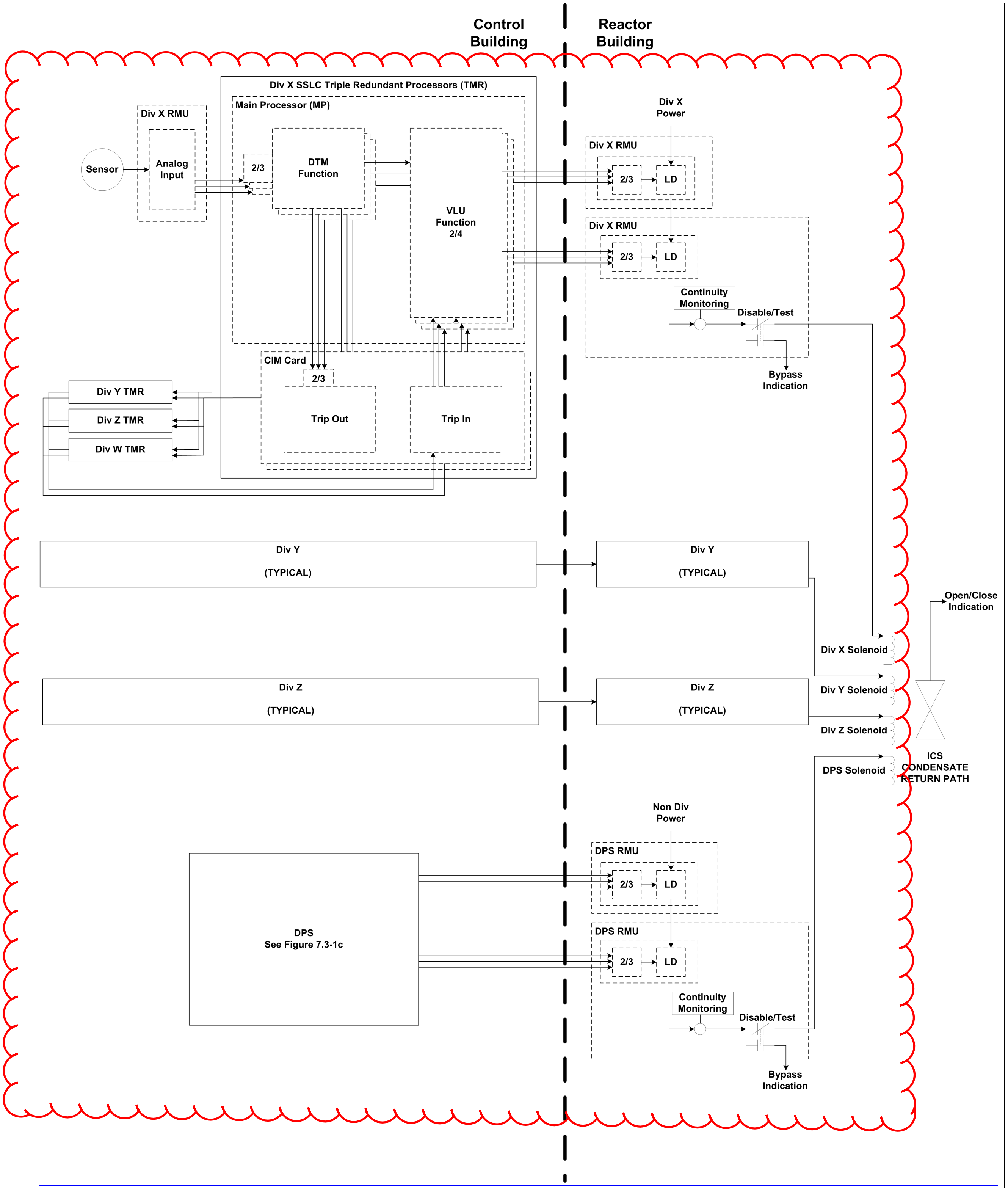

Fiber To/From Div. 1 Q-DCIS
Fiber to/from Div. 2 Q-DCIS
Safety-Related Div. 1 Compartment
Safety-Related Div. 2 Compartment
Nonsafety-Related Compartment
Fiber To/From PIP-A/BOP N-DCIS
Fiber To/From PIP-B/BOP N-DCIS
Safety-Related Div. 1 VDU
Safety-Related Div. 2 VDU
Nonsafety-Related VDU
Manual Scram Switch Div. 1
Manual Scram Switch Div. 2
Communications
Safety-Related Cables for Div 1 Manual Scram & MSIV Isolation
Nonsafety-Related Cables (As Required)
Nonsafety-Related Uninterruptible 120 VAC
Manual MSIV Isolation Switch Div. 1
Manual MSIV Isolation Switch Div. 2
Safety-Related Uninterruptible 120 VAC Div.1
Safety-Related Cables for Div 2 Manual Scram & MSIV Isolation
Safety-Related Uninterruptible 120 VAC Div.2

Figure 7.4-1. Remote Shutdown System Panel Schematic


Control Building
Reactor Building
Div X SSLC Triple Redundant Processors (TMR)
Main Processor (MP)
Div X RMU
Sensor
Analog Input
2/3
DTM Function
VLU Function 2/4
CIM Card
2/3
Trip Out
Trip In
Div Y TMR
Div Z TMR
Div W TMR
Div X Power
Div X RMU
2/3
LD
Div X RMU
2/3
LD
Continuity Monitoring
Disable/Test
Bypass Indication
Div Y
(TYPICAL)
Div Y
(TYPICAL)
Div Z
(TYPICAL)
Div Z
(TYPICAL)
Open/Close Indication
Div X Solenoid
Div Y Solenoid
Div Z Solenoid
DPS Solenoid
ICS CONDENSATE RETURN PATH
Non Div Power
DPS RMU
2/3
LD
DPS RMU
2/3
LD
DPS
See Figure 7.3-1c
Continuity Monitoring
Disable/Test
Bypass Indication

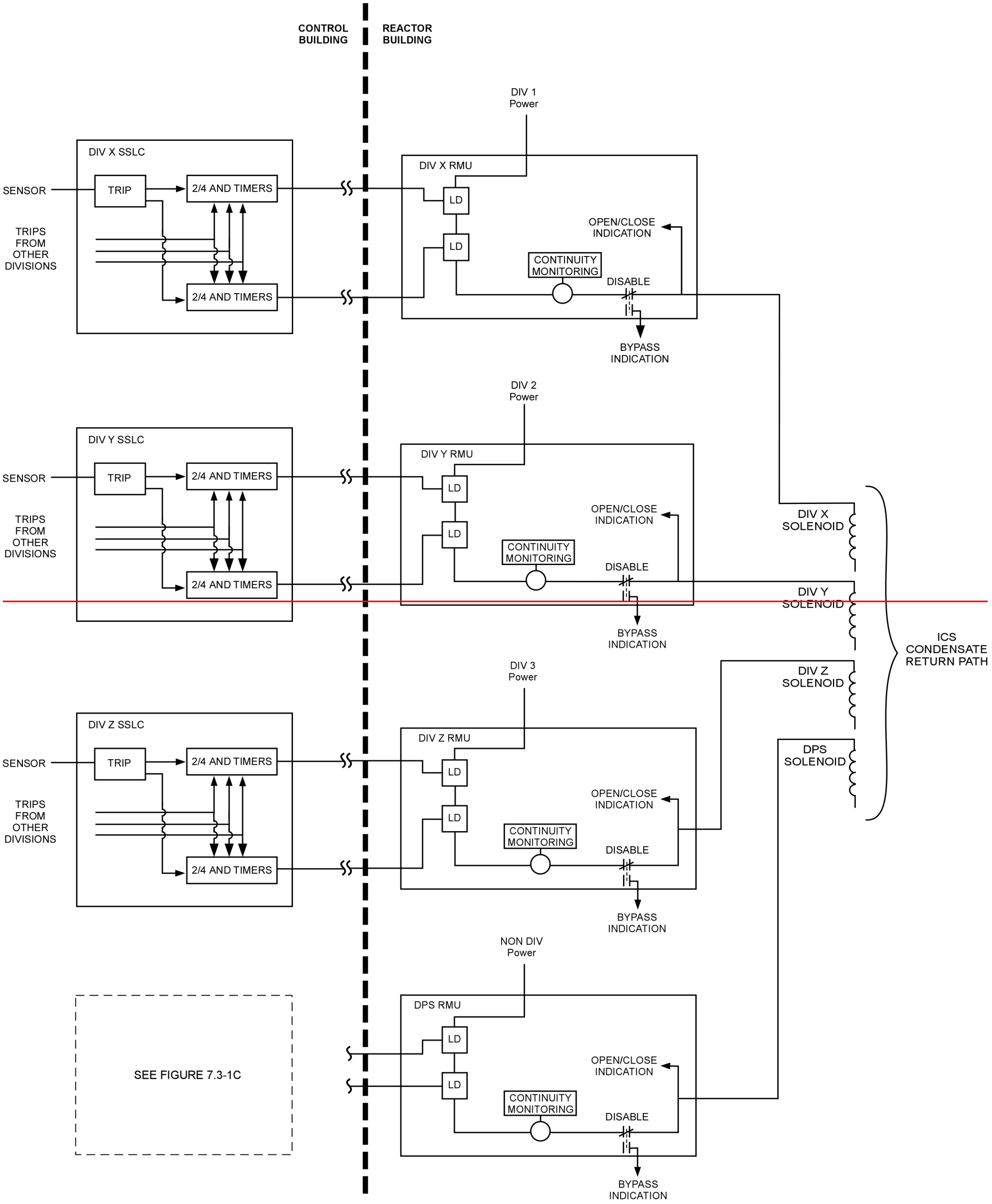


Figure 7.4-3. Isolation Condenser System Initiation and Actuation