

A decorative graphic on the left side of the page consists of three overlapping circles. The top circle contains a mountain range. The middle circle contains a city skyline at night. The bottom circle contains a city skyline at night.

NuScale US460 Plant Standard Design Approval Application

Chapter Seven Instrumentation and Controls

Final Safety Analysis Report

Revision 2

©2025, NuScale Power LLC. All Rights Reserved

COPYRIGHT NOTICE

This document bears a NuScale Power, LLC, copyright notice. No right to disclose, use, or copy any of the information in this document, other than by the U.S. Nuclear Regulatory Commission (NRC), is authorized without the express, written permission of NuScale Power, LLC.

The NRC is permitted to make the number of copies of the information contained in these reports needed for its internal use in connection with generic and plant-specific reviews and approvals, as well as the issuance, denial, amendment, transfer, renewal, modification, suspension, revocation, or violation of a license, permit, order, or regulation subject to the requirements of 10 CFR 2.390 regarding restrictions on public disclosure to the extent such information has been identified as proprietary by NuScale Power, LLC, copyright protection notwithstanding.

Regarding nonproprietary versions of these reports, the NRC is permitted to make the number of additional copies necessary to provide copies for public viewing in appropriate docket files in public document rooms in Washington, DC, and elsewhere as may be required by NRC regulations. Copies made by the NRC must include this copyright notice in all instances and the proprietary notice if the original was identified as proprietary.

TABLE OF CONTENTS

CHAPTER 7 INSTRUMENTATION AND CONTROLS	7.0-1
7.0 Instrumentation and Controls - Introduction and Overview	7.0-1
7.0.1 Regulatory Requirements	7.0-2
7.0.2 Instrumentation and Control System Classification	7.0-2
7.0.3 System Architecture	7.0-2
7.0.4 System Descriptions	7.0-2
7.0.5 References	7.0-20
7.1 Fundamental Design Principles	7.1-1
7.1.1 Design Bases and Additional Design Considerations	7.1-1
7.1.2 Independence	7.1-13
7.1.3 Redundancy	7.1-18
7.1.4 Predictability and Repeatability	7.1-22
7.1.5 Diversity and Defense-in-Depth	7.1-22
7.1.6 Common Cause Failure of Nonsafety Related Controls	7.1-44
7.1.7 Simplicity	7.1-45
7.1.8 Hazards Analysis	7.1-47
7.1.9 References	7.1-55
7.2 System Features	7.2-1
7.2.1 Quality	7.2-1
7.2.2 Equipment Qualification	7.2-28
7.2.3 Reliability, Integrity, and Completion of Protective Action	7.2-31
7.2.4 Operating and Maintenance Bypasses	7.2-36
7.2.5 Interlocks	7.2-39
7.2.6 Derivation of System Inputs	7.2-40
7.2.7 Setpoints	7.2-41
7.2.8 Auxiliary Features	7.2-42
7.2.9 Control of Access, Identification, and Repair	7.2-44
7.2.10 Interaction between Sense and Command Features and Other Systems	7.2-50
7.2.11 Multi-Module Stations	7.2-52
7.2.12 Automatic and Manual Control	7.2-53
7.2.13 Displays and Monitoring	7.2-55

TABLE OF CONTENTS

7.2.14 Human Factors Considerations	7.2-60
7.2.15 Capability for Test and Calibration	7.2-65
7.2.16 Sensors	7.2-68
7.2.17 References	7.2-75

LIST OF TABLES

Table 7.0-1:	NuScale Instrumentation and Controls Design and Applicable Regulatory Requirements Matrix	7.0-22
Table 7.0-2:	Highly Integrated Protection System Topical Report Application Specific Information Cross References	7.0-26
Table 7.0-3:	Classification of Instrumentation and Controls Systems	7.0-28
Table 7.1-1:	Module Protection System Design Basis Events	7.1-57
Table 7.1-2:	Variables Monitored by Module Protection System	7.1-58
Table 7.1-3:	Reactor Trip Functions.	7.1-60
Table 7.1-4:	Engineered Safety Feature Actuation System Functions	7.1-61
Table 7.1-5:	Module Protection System Interlocks / Permissives / Overrides	7.1-64
Table 7.1-6:	Design Basis Event Actuation Delays Assumed in the Plant Safety Analysis	7.1-68
Table 7.1-7:	Summary of Post-accident Monitoring Variables	7.1-69
Table 7.1-8:	Sensor Inputs to Module Protection System	7.1-71
Table 7.1-9:	Intentional Differences Between Field Programmable Gate Array Architecture	7.1-73
Table 7.1-10:	Partial Spurious Actuation Scenarios for Engineered Safety Features Actuation System within Safety Block I.	7.1-74
Table 7.1-11:	Consequences of Partial Spurious Reactor Trip	7.1-75
Table 7.1-12:	Effects of Digital-Based Common Cause Failure of Level Function Type on Sensor Block I	7.1-76
Table 7.1-13:	Effects of Digital-Based Common Cause Failure of Digital-Based Flow Function Type on Sensor Block I and II	7.1-77
Table 7.1-14:	Safety-Related Digital Sensors Used by Safety Block I and II.	7.1-78
Table 7.1-15:	Effect of Field Programmable Gate Array Technology Diversity for Postulated Digital-Based Common Cause Failure of Module Protection System Safety Blocks	7.1-79
Table 7.1-16:	Example: Hazard Conditions	7.1-80
Table 7.1-17:	Example: Safety Functions	7.1-81
Table 7.1-18:	Example: High-level Safety Constraints.	7.1-82
Table 7.1-19:	Example: Safety Constraints Associated with Plant Conditions	7.1-83
Table 7.1-20:	Example: Control Action Analysis	7.1-84
Table 7.1-21:	Example: Identified Hazard Causes.	7.1-85
Table 7.2-1:	Nuclear Steam Supply System Sensor List	7.2-78

LIST OF FIGURES

Figure 7.0-1:	Overall Instrumentation and Controls System Architecture Diagram.	7.0-32
Figure 7.0-2:	Module Protection System Boundaries	7.0-33
Figure 7.0-3:	Module Protection System Safety Architecture Overview	7.0-34
Figure 7.0-4:	Separation Group A Communication Architecture.	7.0-35
Figure 7.0-5:	Separation Group A and Division I Reactor Trip System and Engineered Safety Features Actuation System Communication Architecture	7.0-36
Figure 7.0-6:	Reactor Trip Breaker Arrangement	7.0-37
Figure 7.0-7:	Pressurizer Heater Breaker Arrangement	7.0-38
Figure 7.0-8:	Module Protection System Gateway Diagram	7.0-39
Figure 7.0-9:	Module Protection System Power Distribution.	7.0-40
Figure 7.0-10:	Neutron Monitoring System Ex-Core Block Diagram.	7.0-41
Figure 7.0-11:	Plant Protection System Block Diagram	7.0-42
Figure 7.0-12:	Safety Display and Indication System Boundary	7.0-43
Figure 7.0-13:	Safety Display and Indication Hub	7.0-44
Figure 7.0-14:	Module Control System Internal Functions and External Interfaces	7.0-45
Figure 7.0-15:	Plant Control System Internal Functions and External Interfaces	7.0-46
Figure 7.1-1a:	Module Protection System And Plant Protection System Trip or Bypass Switch Logic	7.1-86
Figure 7.1-1b:	Source Range and Power Range Trips	7.1-87
Figure 7.1-1c:	Power Range High-2 Power Trip and N-2 Interlocks, Low and Low Low RCS Flow Trips.	7.1-88
Figure 7.1-1d:	Power Range and Intermediate Range Rate Trips	7.1-89
Figure 7.1-1e:	Pressurizer Pressure and Level Trips	7.1-90
Figure 7.1-1f:	Reactor Coolant System Hot Temperature Trip, Temperature Interlocks	7.1-91
Figure 7.1-1g:	Pressurizer Level Interlock and Trip, High Containment Pressure, and High Containment Level Trips.	7.1-92
Figure 7.1-1h:	Steam Generator Low and Low Low Main Steam Pressure Trips.	7.1-93
Figure 7.1-1i:	High Main Steam Pressure and Steam Generator Low and High Steam Superheat Trips	7.1-94
Figure 7.1-1j:	Reactor Trip and Reactor Tripped Interlock RT-1	7.1-95
Figure 7.1-1k:	ESFAS - Containment System Isolation and Chemical and Volume Control System Isolation Interlocks	7.1-96

LIST OF FIGURES

Figure 7.1-1l:	ESFAS - Decay Heat Removal System and Secondary System Isolation Actuation, FWIV Interlock	7.1-97
Figure 7.1-1m:	ESFAS - Demineralized Water System Isolation, Pressurizer Heater Trip	7.1-98
Figure 7.1-1n:	ESFAS Emergency Core Cooling System Actuation, Low Temperature Overpressure Protection Actuation	7.1-99
Figure 7.1-1o:	Decay Heat Removal System Valve Actuation	7.1-100
Figure 7.1-1p:	Main Steam Isolation Valve Actuation	7.1-101
Figure 7.1-1q:	Main Steam Isolation Bypass Valve Actuation.	7.1-102
Figure 7.1-1r:	Secondary Main Steam Isolation Valve Actuation	7.1-103
Figure 7.1-1s:	Secondary MSIV Bypass Valve Actuation	7.1-104
Figure 7.1-1t:	Feedwater Isolation Valve Actuation	7.1-105
Figure 7.1-1u:	Feedwater Regulating Valve Isolation	7.1-106
Figure 7.1-1v:	Chemical and Volume Control System RCS Injection and Discharge Valve Actuation.	7.1-107
Figure 7.1-1w:	Chemical and Volume Control System Pressurizer Spray and High Point Degasification Valve Actuation.	7.1-108
Figure 7.1-1x:	Containment Flooding and Drain and Containment Evacuation Valve Actuation	7.1-109
Figure 7.1-1y:	Reactor Component Cooling Water System Valve Actuation	7.1-110
Figure 7.1-1z:	Demineralized Water Supply Valve Actuation	7.1-111
Figure 7.1-1aa:	Emergency Core Cooling System Reactor Vent Valve 1 & 2 Actuation	7.1-112
Figure 7.1-1ab:	Emergency Core Cooling System Reactor Recirculation Valve Actuation	7.1-113
Figure 7.1-1ac:	Reactor Trip Breaker Division I A.	7.1-114
Figure 7.1-1ad:	Reactor Trip Breaker Division I B.	7.1-115
Figure 7.1-1ae:	Pressurizer Heater Breaker Proportional Heater A	7.1-116
Figure 7.1-1af:	Pressurizer Heater Breaker Proportional Heater B	7.1-117
Figure 7.1-1ag:	Loss of AC Power to ELVS Battery Chargers	7.1-118
Figure 7.1-1ah:	Reactor Trip Breaker Division II A	7.1-119
Figure 7.1-1ai:	Reactor Trip Breaker Division II B	7.1-120
Figure 7.1-1aj:	Pressurizer Heater Trip Breaker Backup Heater A	7.1-121
Figure 7.1-1ak:	Pressurizer Heater Trip Breaker Backup Heater B	7.1-122
Figure 7.1-1al:	Actuation Priority Logic Nonsafety Input Control Logic	7.1-123

LIST OF FIGURES

Figure 7.1-2:	Post-Accident Monitoring General Arrangement Drawing	7.1-124
Figure 7.1-3:	Blocks Selected for Defense-in-Depth Analysis.	7.1-125
Figure 7.1-4:	Blocks Selected for Defense-in-Depth Analysis.	7.1-126
Figure 7.1-5:	Four Echelons of Defense within Chosen Blocks	7.1-127
Figure 7.1-6:	Common Cause Failure of Division I Safety Display and Indication System.	7.1-128
Figure 7.1-7:	Common Cause Failure of Safety Block I with Correct Indication	7.1-129
Figure 7.1-8:	Common Cause Failure of Safety Block I with False Indication	7.1-130
Figure 7.1-9:	Common Cause Failure of Nonsafety Monitoring and Indication.	7.1-131
Figure 7.1-10:	Digital-Based Common Cause Failure of Level Function Type in Sensor Block I	7.1-132
Figure 7.1-11:	Digital-Based Common Cause Failure of Flow Function Type in Sensor Block I and II	7.1-133
Figure 7.1-12:	Direction of Information and Signals between Analysis Blocks	7.1-134
Figure 7.1-13:	Basic Control Loop with Example Flawed Control Actions	7.1-135
Figure 7.1-14:	Example Module Protection System High Level Control Structure	7.1-136
Figure 7.1-15:	Example Neutron Monitoring System High Level Control Structure	7.1-137
Figure 7.1-16:	Safety Function Module Low-Level Logic Structure.	7.1-138
Figure 7.1-17:	Basic Module Protection System Configuration.	7.1-139
Figure 7.2-1:	Instrumentation and Controls Safety System Development Processes	7.2-81
Figure 7.2-2:	System and Software Technical Development Life Cycle Processes	7.2-82
Figure 7.2-3:	Software Lifecycle Comparisons	7.2-83

CHAPTER 7 INSTRUMENTATION AND CONTROLS

7.0 Instrumentation and Controls - Introduction and Overview

The instrumentation and control (I&C) systems provide the capability to control the plant systems manually and automatically during normal, steady state, and transient power operations. The systems also provide reactor protection against unsafe plant operations by initiating signals to mitigate the consequences of an anticipated operational occurrence or postulated accident and ensure safe shutdown.

Chapter 7 describes the design of I&C systems, including classification, functional requirements, and architecture, and demonstrates the systems' capability to perform required safety and nonsafety-related functions. The scope of the information provided in Chapter 7 includes instruments that are safety systems as defined in IEEE Std 603-1991 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 7.0-1) and nonsafety-related I&C systems that perform specific regulatory required functions.

Section 7.0 provides an introduction and overview of I&C systems. Systems addressed in Section 7.0 include the following:

- module protection system (MPS)
- neutron monitoring system (NMS)
- plant protection system (PPS)
- safety display and indication system (SDIS)
- module control system (MCS)
- plant control system (PCS)
- in-core instrumentation system (ICIS)
- fixed area radiation monitoring system (RMS)

Section 7.1 describes major functional and design considerations associated with I&C systems, including system design bases and incorporation of fundamental design principles of:

- independence
- redundancy
- predictability and repeatability
- diversity and defense-in-depth

Section 7.1 describes the attributes of integrated hazard analysis, system architecture, and simplicity in the design of the safety-related systems.

Section 7.2 addresses additional I&C system functional and design considerations contained in IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

(Reference 7.0-2), and specific I&C system criteria, sense and command features, and execute features that complement the fundamental design principles discussed in Section 7.1.

7.0.1 Regulatory Requirements

Table 7.0-1 provides a cross-reference of regulatory requirements, guidance, and industry standards with the Chapter 7 subsections in which the requirements and guidance are specifically addressed. The information in this section satisfies the application specific information requirements in the NuScale Power, LLC, topical report TR-1015-18653-P-A, "Design of the Highly Integrated Protection System Platform," (Reference 7.0-3) listed in Table 7.0-2 for Application Specific Action Item Number 1.

7.0.2 Instrumentation and Control System Classification

The I&C structures, systems, and components are classified in accordance with the classification criteria described in Section 3.2. The I&C systems classified as safety-related are the MPS and the NMS. The remaining I&C systems (PPS, SDIS, MCS, PCS, ICIS and RMS) and the human-system interfaces (HSIs), are classified as nonsafety-related, with the exception of the reactor coolant pressure boundary function. Table 7.0-3 provides classification of I&C systems and components.

7.0.3 System Architecture

The architectural design of I&C systems is based on providing clear interconnection interfaces for plant I&C structures, systems, and components. Each NuScale Power Module (NPM) has a dedicated safety-related MPS and NMS, and a dedicated nonsafety-related MCS and ICIS. One nonsafety-related PPS, SDIS, PCS and RMS serve the non-NPM-specific plant systems.

A simplified block diagram of the overall I&C system architecture is provided in Figure 7.0-1 along with the classification of I&C systems.

More detail of the architectural design is provided in Section 7.1 and Section 7.2.

7.0.4 System Descriptions

7.0.4.1 Module Protection System

The primary purpose of the MPS is to monitor process variables and provide automatic initiating signals in response to out-of-normal conditions, ensuring protection against unsafe NPM operation during steady state and transient power operation. Each NPM has a single dedicated MPS. The two major functions that the MPS performs are:

- to monitor plant variables and trip the reactor when specified setpoints based on plant safety analysis analytical limits described in Chapter 15 are reached or exceeded during anticipated operational occurrences. The NPM reactor trip functions for the reactor trip system (RTS) are listed in Table 7.1-3

- to monitor plant variables and actuate engineered safety features actuation system (ESFAS) equipment when specified setpoints based on the plant safety analysis analytical limits described in Chapter 15 are reached or exceeded during anticipated operational occurrences. Actuation of ESFAS equipment prevents or mitigates damage to the reactor core and reactor coolant system components, and ensures containment integrity. The ESFAS functions are summarized in Table 7.1-4

The MPS also transmits status and information signals to the nonsafety-related MCS, maintenance workstations (MWS), PCS, and SDIS, and performs monitoring for post-accident monitoring (PAM) functionality.

The MPS utilizes field programmable gate arrays (FPGAs) based on the highly integrated protection system (HIPS) platform (Reference 7.0-3). The MPS conforms to Reference 7.0-3 with the exception of Diversity and Defense-in-Depth, which is based on the NuScale Design Specific Review Standard Section 7.1 rather than NRC Branch Technical Position (BTP) 7-19 (Section 7.1.5).

The information in this section satisfies the application specific information requirements in Reference 7.0-3 listed in Table 7.0-2 for Application Specific Action Item Numbers 2, 18 and 57.

The MPS includes the following safety-related (except where noted otherwise) elements:

- separation group sensor electronics and input cabinets
- four separation groups of signal conditioning
- four separation groups of trip determination
- manual actuation switches in the main control room (MCR)
- MCR isolation switches located outside control room
- Class 1E components to provide isolation from the nonsafety-related augmented DC power system (EDAS) power supply
- power supplies for sensors and MPS components
- eight nonsafety-related voltage sensors for detecting loss of 480 VAC to the EDAS battery chargers
- four reactor trip breakers and associated cabling
- four pressurizer heater breakers and associated cabling
- two nonsafety-related MWS
- two nonsafety-related MPS gateways
- two divisions of RTS voting and actuation equipment (Section 7.0.4)
- two divisions of ESFAS voting and actuation equipment (Section 7.0.4)
- four under-the-bioshield temperature sensors

- division power distribution cabinets

The MPS boundary is shown in Figure 7.0-2.

7.0.4.1.1 Safety Function Modules

The safety function module (SFM) signal conditioning receives inputs from the process sensors and detectors to measure the process variables shown in Figure 7.0-3. The interconnections of the process sensors and detectors to the signal conditioning block are dedicated copper wires and are routed according to the separation group with which they are associated. Loop power supplies are provided where needed based on the sensor requirements.

A typical separation group architecture showing the interconnection of an SFM to the interfacing modules is shown in Figure 7.0-4.

If an SFM identifies a failure on a communication bus, the SFM generates an alarm and assumes a fail-safe state for that communication bus. The fail-safe state for the SFM on that communication bus is to not respond to the communication bus master (e.g., (scheduling and bypass modules (SBM))). The communication paths and equipment are redundant, making the safety data fault-tolerant to single failures or multiple failures on a single data path. The SBM validates the data and transmits it through isolated, one-way, transmit-only fiber to both divisions of RTS and ESFAS to their respective scheduling and voting modules (SVMs). The SVMs are slaves to the SBMs on the safety data communication buses and slaves to the monitoring and indication bus (MIB) communication module (MIB-CM) on the monitoring and indication communication bus. If an SVM identifies a failure on a communication bus, the SVM generates an alarm and assumes a fail-safe state for that communication bus. The fail-safe state for that communication bus on the SVM is to demand a trip or actuation of protective functions. The fail-safe state for the SVM on the monitoring and indication communication bus is to not respond to the communication bus master. The redundant data for the four separation groups are received by each division of RTS and ESFAS as shown in Figure 7.0-5.

Status and diagnostics information for the SFM and SBM is provided to the MIB. The MIB-CM is the bus master for the MIB and schedules the communications for the MIB. If the SFM identifies a failure on a communication bus, the SFM generates an alarm and assumes a fail-safe state for that communication bus. The fail-safe state for the SFM on that communication bus is to not respond to the bus master. By not receiving a response from an SFM, the MIB-CM also generates an alarm. The MIB-CM provides the status and diagnostics information to the MCS and the MPS gateway through one-way, transmit only, isolated outputs. The MPS gateway sends the data to the MWS and SDIS. The MIB-CM also provides a communication path from the MWS to the SFM through the calibration and test bus (CTB) to allow for calibration and parameter updates for each safety function. The safety function must be out of service and a temporary cable from the MWS to the MIB-CM is required to allow changing parameters or

calibration of a channel. An MWS can only access one separation group at a time using a temporary cable. Additional information on access controls of the MWS is found in Section 7.2.9.

An MIB-CM is included for each separation group and each division. A divisional MIB-CM only serves the function of monitoring and indication as there is no calibration available for the divisional RTS and ESFAS.

7.0.4.1.2 Reactor Trip System

The RTS uses four redundant trip determination signals, one from each separation group, to complete the logic decisions necessary to automatically open the reactor trip breakers as shown in Figure 7.0-3. The analytical limits for the RTS are listed in Table 7.1-3.

When an RTS parameter exceeds a predetermined setpoint as defined by the NuScale TR-122844, "NuScale Instrument Setpoint Methodology Technical Report," (Reference 7.0-4). The SFM for each separation group generates a trip signal that is sent through an SBM to an SVM in both RTS divisions. The SVM performs two-out-of-four coincident logic voting on the trip determination status. If two or more trip determination signals generate a reactor trip, a trip signal is generated in the SVM and sent to the associated equipment interface modules (EIMs) to open the reactor trip breakers.

The EIMs in the RTS are slaves to the SVMs on the safety data communication buses and slaves to the MIB-CM on the monitoring and indication communication bus. If an EIM identifies a failure on a communication bus, the EIM generates an alarm and assumes a fail-safe state for that communication bus. The fail-safe state for that communication bus on the EIM is to demand a trip or actuation of its protective functions. The fail-safe state for protective functions on EIMs is to demand a trip or actuation. The fail-safe state for the EIM on the monitoring and indication communication bus is to not respond to the communication bus master.

Each EIM in the RTS receives redundant trip signals from outputs created in the SFM and provides a trip signal based on two-out-of-three voting from the incoming signals as shown in Figure 7.0-5. Two divisions of RTS circuitry and reactor trip breakers are provided to ensure that a single failure does not cause the loss of an RTS function. The reactor trip breakers are configured in a series-parallel configuration as shown in Figure 7.0-6.

An EIM is included for each reactor trip breaker in both RTS divisions that are actuated by the MPS. Each reactor trip breaker EIM has two separate logic paths. The primary coil is connected to the undervoltage trip circuit and the secondary coil is connected to the shunt trip circuit for each reactor trip breaker. Each RTS division controls one reactor trip breaker in each parallel path. This configuration allows for either division to accomplish a reactor trip. When a reactor trip signal is generated, the EIM outputs to the undervoltage and shunt trip circuits are de-energized, causing the undervoltage coils and the shunt trip relays to de-energize. When the shunt trip relays drop out, the

shunt trip coils are energized from EDAS-module-specific (EDAS-MS). Either action causes the reactor trip breakers to open. The shunt trip circuit and coil are provided as a nonsafety-related, diverse means to open the reactor trip breakers for increased reliability should de-energization of the undervoltage coil fail to cause a reactor trip breaker to open, and nonsafety-related electrical power from EDAS-MS is still available. Power from the control rod drive power supply is then interrupted and the control rods are inserted into the core by gravity. The undervoltage and shunt trip circuits are shown in Figure 7.1-1ac and Figure 7.1-1ad, and Figure 7.1-1ah and Figure 7.1-1ai for the Division I and II reactor trip breakers, respectively.

The RTS also provides manual trip capability. Manual switches in the MCR allow the operator to manually initiate a reactor trip. Two manual switches, one per division, are provided to manually initiate a reactor trip. The manual switches are input into the actuation and priority logic (APL) associated with the reactor trip system EIM via the hard-wired module (HWM).

The APL accepts commands from the following sources:

- digital trip signal from the SVM
- non-digital manual trip signal from its associated RTS division
- non-digital manual control signals from the MCS

The non-digital signals are diverse from the digital portion of the MPS. Discrete logic is used by the APL for actuating a single device based on the highest priority. Regardless of the state of the digital system, manual initiation can always be performed at the division level. If the enable nonsafety control input is active and there are no automatic or manual actuation signals present, the MCS is capable of operating the reactor trip breaker.

The result from the APL is used to actuate equipment connected to the EIM. Reactor trip breaker status is transmitted to the EIM. Breaker status information is sent to the MIB, along with the status of the safety data bus (SDB) signals.

7.0.4.1.3 Engineered Safety Feature Actuation System

The ESFAS uses four redundant actuation determination signals, one from each separation group, to complete the logic decisions necessary to automatically initiate the operation of necessary engineered safety features (ESFs) as shown in Figure 7.0-3. The analytical limits for the ESFAS are listed in Table 7.1-4.

When an ESFAS parameter exceeds a predetermined setpoint, the SFM for each separation group generates an actuation signal that is sent through an SBM to the SVM in both ESFAS divisions. The SVM performs two-out-of-four coincident logic voting on the trip determination status. If two or more actuation signals generate an actuation of an ESF system, an actuation signal is generated in the SVM. The signal is then sent to the associated EIMs to

de-energize the solenoids or open the breakers of the associated ESF system.

An EIM is included in each division for each ESF component actuated by the MPS. Each EIM has two separate logic paths to allow for connection to separate ESF components. Each component is connected to two separate EIMs, resulting in two EIMs providing redundant control to each component as shown in Reference 7.0-3, Figure 2-20. This configuration allows an EIM to be taken out of service and replaced online without actuating the connected equipment.

The EIMs in the ESFAS are slaves to the SVMs on the safety data communication buses and slaves to the MIB-CM on the monitoring and indication communication bus. If an EIM identifies a failure on a communication bus, the EIM generates an alarm and assumes a fail-safe state for that communication bus. The fail-safe state for the communication bus on the EIM is to demand a trip or actuation of its protective functions. The fail-safe state for protective functions on EIMs is to demand a trip or actuation. The fail-safe state for the EIM on the monitoring and indication communication bus is to not respond to the communication bus master.

When an ESFAS actuation signal is generated in the SVM, four switching outputs from the EIM open, as shown in Reference 7.0-3, Figure 2-19, power is interrupted to the component solenoids, the solenoids are de-energized, and the components change state to their de-energized position. For the pressurizer heater breakers, the EIM outputs to the undervoltage trip and shunt trip circuits are de-energized, causing the undervoltage coils and the shunt trip relays to de-energize. When the shunt trip relays drop out, the shunt trip coils are energized from EDAS-MS. Either action causes pressurizer heater breakers to open. The shunt trip circuit and coil are provided as a nonsafety-related, diverse means to open the pressurizer heater breakers for increased reliability should de-energization of the undervoltage coil fail to cause a pressurizer heater breaker to open, and nonsafety-related electrical power from EDAS-MS is still available. Power is then removed from the pressurizer heaters. The undervoltage and shunt trip circuits are shown in Figure 7.1-1ae and Figure 7.1-1af, and Figure 7.1-1aj and Figure 7.1-1ak for the proportional and backup pressurizer heater breakers, respectively.

Similar to the reactor trip breakers, only one division of pressurizer heater breakers is required to trip to remove power to heaters. The pressurizer heater breakers are configured as two separate series connections as shown in Figure 7.0-7.

The ESFAS also provides manual actuation capability. Manual switches in the MCR allow the operator to manually initiate an ESF function. Two manual switches, one per division, are provided to manually initiate each ESF function. These manual switches are inputs into the APL associated with the engineering safety features actuation system EIM via the HWM.

The APL accepts commands from three sources:

- digital trip signal from the SVM
- non-digital manual trip signal from its own ESFAS division
- non-digital manual control signals from the MCS

The non-digital signals are diverse from the digital portion of the MPS. Discrete logic is used by the APL for actuating a single component based on the highest priority. Regardless of the state of the digital system, manual initiation can always be performed at the division level. If the enable nonsafety control input is active and there are no automatic or manual actuation signals present, the MCS is capable of controlling the ESF components.

The result from the APL is used to control and actuate equipment connected to the EIM. Equipment status is transmitted to each EIM. Equipment status information is sent to the MIB, along with the status of the SDB signals.

7.0.4.1.4

Module Protection System Support Systems

Each MPS separation group and division, as well as the MPS gateway, has a dedicated HWM. The HWM accepts hard-wired signals external to the MPS cabinets and makes them available on the chassis backplane for the other modules. These signals include the manual actuation switches, operating bypasses switches, override switches, and enable nonsafety control switches from the MCR. The operating bypass and override switches are described in Section 7.2.4. Other inputs to the HWM include the SFM trip/bypass switches, MCS control inputs, and component position feedback.

Each division of MPS has a nonsafety-related MWS for the purpose of maintenance and calibration. The one-way, read-only data are connected through the MPS gateway for its division and are available continuously on each division's MWS. The MWS is used to update tunable parameters in the SFMs when the safety function is out of service. Controls are put in place, as described in Section 7.2.9, to prevent modifications to an SFM when it is being relied upon to perform a safety function. The MWS is used for offline maintenance and calibration, using a temporary cable that allows two-way communication to update setpoints and tunable parameters in the SFMs. When an SFM is placed out of service by operating its out-of-service switch, the position of the trip/bypass switch associated with that SFM is read by the SBM and used as the status for the SFM output. Each division of the MPS has a nonsafety-related MWS permanently connected for the purpose of online monitoring, using the MPS gateway through one-way isolated communication ports over point-to-point fiber-optic cables.

Each division of MPS has a nonsafety-related MPS gateway that consolidates the information received from the four separation groups, the two divisions of RTS, and the ESFAS. The MPS gateway also collects equipment status feedback from the HWM for PAM-only mode. The information transmitted to the MPS gateway is consolidated by a single communication module that acts

as a master on the MPS gateway backplane and then transmits the consolidated data through a qualified, isolated, one-way communication path to the MWS and the SDIS hubs as shown in Figure 7.0-8. There is one MPS gateway for each division.

The EDAS is the power source for the MPS as described in Section 8.3. The DC-to-DC voltage converters are used for Class 1E isolation and protection of the MPS equipment. Division I MPS power is generated from power channels A and C through a DC-DC converter for Class 1E isolation, and then distributed to the loads by sharing or auctioneering. Division II power is generated from power channels B and D, similar to Division I. Each of the separation groups is redundantly supplied from a single EDAS channel, and then distributed to the loads by sharing or auctioneering. Configuration of the EDAS channels and DC-to-DC voltage converters for MPS Division I and separation groups A and C are shown in Figure 7.0-9. The MPS Division II and separation groups B and D are similar. The EDAS power channels A and C that supply power to MPS Division I are completely independent from EDAS power channels B and D that supply power to MPS Division II and are shown in Figure 8.3-4a and Figure 8.3-4b.

To ensure EDAS batteries supply power for their mission time, only loads associated with maintaining the ECCS valves closed and PAM instrumentation remain energized during ECCS-hold mode. These loads include the MPS and NMS cabinets, including power to sensors, ECCS valve solenoids, RMS bioshield radiation monitors, and the EDAS battery monitors. If two out of four sensors detect a loss of voltage on both B and C battery charger switchgears, the MPS automatically generates a reactor trip, decay heat removal system (DHRS) actuation, pressurizer heater trip, demineralized water supply isolation, secondary system isolation, chemical and volume control system isolation, containment isolation, de-energizes the MWS for both MPS divisions, and starts the three 24-hour timers per division. For the first 24 hours following a loss of voltage, the four separation groups of MPS equipment and both divisions of ESFAS and RTS remain energized. If an ECCS actuation is not required due to plant conditions, then ECCS is not actuated (ECCS trip solenoid valves remain energized), which is defined as the ECCS-hold mode, to allow time to restore AC power and prevent actuation of ECCS. The ECCS still actuates if the associated ESFAS signal is generated during this 24-hour period.

If AC power is not restored within 24 hours, the 24-hour timers time out (PAM only mode), the RTS chassis, ESFAS chassis, and Separation Groups A and D are de-energized, and the rest of the ESFAS actuations initiate (e.g., ECCS), reducing the load on batteries for buses B and C to support the availability of PAM indications for a minimum of 72 hours.

The MPS actuates ECCS automatically after a specified period of time following an automatic or manual reactor trip. This actuation allows the ECCS supplemental boron to recirculate into the reactor core region before xenon decays from the core, to assure subcriticality without requiring operator actions. The RCS is maintained inert by the actuation of the eight hour ECCS

timer. Operators may manually block the actuation if subcriticality at cold conditions is confirmed and if it is confirmed that sufficient hydrogen concentration will be maintained in the RCS throughout DHRS cooldown to preclude radiolytic generation of combustible gases.

7.0.4.2 Neutron Monitoring System

The neutron monitoring system (NMS) performs the following functions:

- provides neutron flux data to the MPS for various reactor trips
- provides information signals to the MPS for post-accident monitoring
- provides neutron flux signals to the PCS during refueling operations

When the NPM is in transit to or from the refueling bay of the plant, neutron monitoring is not required. Equipment with the potential to cause core alterations, such as control rod drive mechanisms, is disconnected or disabled prior to NPM movement. The NMS consists of NMS-excore, NMS-refuel, NMS-flood, and positioning equipment.

The neutron monitoring system PAM function meets augmented quality and regulatory requirements described in Regulatory Guide 1.97, including Seismic categorization.

The NMS operating bay positioning equipment is safety-related. The nonsafety-related hydraulic power unit and control skid are classified as Seismic Category II, augmented quality.

7.0.4.2.1 Neutron Monitoring System-Excore

Neutron flux level signals generated by the safety-related NMS-excore equipment are used by the MPS to generate appropriate reactor protection trips, operating permissives, indication, and alarms for various modes of reactor operation, including shutdown conditions. The MPS sends neutron flux signals to other systems in order to provide non-protective controls and indication.

The NMS-excore sub-system monitors neutron flux during normal operations, off-normal conditions, design basis events, and the subsequent long-term stable shutdown phase. The NMS-excore sub-system continuously monitors the reactor neutron flux from shutdown to full rated power with wide range detectors for the source range, intermediate range, and power range.

An NMS-excore sub-system includes the following components for each NPM:

- four wide-range excore detectors functioning over the source, intermediate, and power ranges distinguished by processing electronics
- moderator assemblies
- four NMS-excore cabinets with pre-amplifier and electronics needed to monitor flux levels from reactor shutdown to 200 percent full-rated power

- associated cabling
- Class 1E components to provide isolation from the nonsafety-related EDAS power supply

The NMS-excore detectors and moderator assemblies are qualified to Seismic Category I and located within the operating bays of the Reactor Building. They are placed outside the containment vessel. The NMS-excore detectors are located inside moderator assemblies and installed in support mechanisms that are connected to the NPM operating bay structure. During operation, the support mechanisms are positioned to place the NMS-excore detectors and moderator assemblies just outside the containment vessel to monitor neutron flux leakage that is directly proportional to reactor power level.

The NMS positioning equipment retracts the NMS moderator assemblies away from the NPM to provide clearance for module movement during refueling. The moderator assemblies are positioned to their operational locations following refueling for module start-up.

The NMS-excore signal processing cabinets are located in the Reactor Building in the I&C equipment rooms. The separation Group A and C cabinets (Figure 1.2-11) are located in a separate room from the separation Group B and D cabinets (Figure 1.2-12).

Figure 7.0-10 shows the NMS-excore block diagram.

7.0.4.2.2 Neutron Monitoring System-Refuel

The nonsafety-related NMS-refuel detectors are located in the refueling bay of the plant. There is one NMS-refuel subsystem for the plant because each NPM is relocated to the refueling bay for the refueling process, and only one NPM is refueled at a time. The NMS-refuel monitors neutron flux from the point of reactor pressure vessel (RPV) head lift until the replacement of the RPV head.

The NMS-refuel subsystem includes the detector array, pre-amplifiers, NMS-refuel cabinets with electronics, and associated cabling. The NMS-refuel detectors are proportional counter source range detectors located near the core mid-plane. The detectors monitor neutron flux in counts per second over a four decade range from 10^{-1} to 10^3 counts per second.

The NMS-refuel neutron monitoring capability ensures the neutron flux level is continuously monitored during the refueling process and also provides an audible count rate to the operator with the ability to detect and alert a spurious increase in count rate during fuel movement. The NMS-refuel provides neutron flux signals to the PCS.

The NMS-refuel detectors are located on the outside of the RPV. This mounting allows the NMS-refuel to be repeatedly replaced back into the same

location between each use, allowing for the movement of NPMs between the operating bay and refueling bay.

Temporary neutron detectors can be used during fuel loading to provide additional reactivity monitoring and to satisfy Technical Specification requirements.

7.0.4.2.3 Neutron Monitoring System-Flood

The nonsafety-related NMS-flood sub-system monitors neutron flux during specific conditions when the containment vessel is flooded during normal and accident conditions. The NMS-flood sub-system provides indication only; there are no safety-related functions performed by the NMS-flood sub-system.

The NMS-flood sub-system consists of two proportional neutron detectors with sufficient sensitivity to monitor neutron flux when the CNV is flooded, moderator assemblies, pre-amplifiers, cabling and signal conditioning, and processing equipment. The NMS-flood detectors monitor the neutron flux over a range of four decades.

The NMS-flood detectors and moderator assemblies are seismically-qualified and located in the NPM operating bay, level with the reactor core on opposite sides of the NPM 180 degrees apart. The NMS-flood detectors are located inside moderator assemblies and positioned near the outer wall of the CNV in the retractable supporting structure. The NMS-flood detectors and moderator assemblies have the capability to be moved away from the CNV for maintenance. During plant startup, the NMS-flood detectors are verified operational. The NMS positioning equipment retracts the NMS moderator assemblies away from the NPM to provide clearance for module movement during refueling. The moderator assemblies are placed into the position following refueling for module start-up.

The NMS-flood sub-system is powered by the nonsafety-related EDAS, and provides indication for monitoring neutron flux during the specific periods of time when the containment vessel is flooded during normal and accident conditions. The signals from the NMS-flood sub-system are provided to the MPS via isolated inputs to MPS separation groups B and C. The indication for the NMS-flood sub-system is also categorized as a PAM variable (Table 7.1-7) and provided to the SDIS to support PAM of neutron flux levels.

7.0.4.3 Plant Protection System

The PPS monitors common process variables at the plant level and executes actuations in response to normal and off-normal conditions. Selected variables monitored and equipment actuated by the PPS require an augmented level of quality. The PPS consists of two independent and redundant divisions. Either of the divisions is capable of accomplishing PPS functions. Additional design considerations for the PPS are described in Section 7.1.1.2.5. The list of PPS automatic actuation functions for the control room habitability system and normal control room HVAC system can be found in Section 9.4.1.

The PPS is built on the HIPS platform (TR-1015-18653-P-A) and is an FPGA-based system. Figure 7.0-11 displays the system diagram of the PPS architecture.

Division I and Division II of the PPS are located in separate rooms in the Control Building. The boundaries of the PPS extend from the output connections of the sensors and detectors to the input connections of the actuated devices. The low voltage AC electrical distribution system voltage sensors are also classified as part of the PPS. The nonsafety-related displays, which receive data from the PPS, are either part of the SDIS or the PCS as described in Section 7.0.4.4 and Section 7.0.4.6, respectively.

The process sensors measure different process variables, such as radiation, level, and voltage. Separate sensors supply information to the two PPS divisions. Sensors are qualified for the environmental conditions before, during, and after a design basis event. The sensors provide input to the PPS, but are classified as part of the system in which they are installed.

7.0.4.4 Safety Display and Indication System

The SDIS provides accurate, complete, and timely information pertinent to MPS and PPS status and information displays. The SDIS displays PAM variables and meets augmented quality criteria as described in Section 7.1.1.2.4. Display of information is designed to minimize the possibility of ambiguous indications and to enhance the human-system interface (HSI) for the operator.

The principal functions of the SDIS are to:

- provide operators the HSI and data to ensure the plant is operating within the limits defined by safety analyses.
- notify operators when the ESFAS, RTS, and PPS setpoints are reached.
- supply operators with data necessary to ensure the NPM is in a safe condition following an accident.
- provide accurate, complete, and timely information pertinent to the MPS and PPS status and information displays to support post-accident monitoring.

Information regarding process variable values and equipment status is provided to the SDIS from each separation group and each division of the MPS and PPS.

The SDIS consists of two independent divisions of equipment. Each SDIS division consists of communication hubs, display interface modules (DIMs), and display panels. The SDIS boundaries and interfaces are shown on Figure 7.0-12.

The SDIS hub receives data from the MPS gateway and plant protection system monitoring and indication bus (MIB) communication module. Each MPS gateway delivers data to a separate communication module within the SDIS hub. The SDIS hub distributes the data it receives from the MPS and PPS to the DIM associated with the respective NPM or PPS through one-way, optically-isolated, fiber-optic cables. Data from each of the communication modules on the SDIS hub are also

aggregated into a single communication module. This module polls each of the communication modules through the backplane and sends the aggregated information to the PCS through a unidirectional, optically isolated interface.

The SDIS hubs are located in the PPS rooms and are shown in Figure 7.0-13.

The DIM within the SDIS receives data through an isolated fiber-to-copper interface. The received data are converted in an FPGA to a display-ready format. The DIM then sends the display-ready data through a cable to the display panel. The DIM is located in the MCR.

The display panels display the data made available from the MPS and PPS to the plant operators in the MCR. Data from each MPS and PPS are displayed a dedicated monitor, with one monitor per division. Both divisions of MPS and PPS data are displayed on both SDIS divisional displays.

7.0.4.5 Module Control System

The MCS is a distributed control system which allows monitoring and control of NPM-specific plant components that are associated with the NPM balance-of-plant control functions. The MCS includes manual controls and HSIs necessary to provide operator interaction with the process control mechanism. The HSIs are provided in the MCR and remotely as described in Section 7.2.13 and Section 7.2.14.

The principal function of the MCS is to control and monitor nonsafety-related systems and components. The MCS is part of the nonsafety-related network and includes the associated network equipment and appurtenances necessary for network communication.

The MCS provides component-level control and monitoring of safety-related components that are specific to an NPM. The monitoring of the safety-related components is achieved by receiving one-way communications from the MPS to the MCS through isolated one-way communication ports on the MIB communication module. The controls of the safety-related components by the MCS are manual component-level manipulations used for maintenance, testing, or aligning the components following refueling or actuation and not for safety-related purposes. The control signal from the MCS is hard-wired and sent through a qualified isolation device through the HWM to the EIM in the MPS, which contains priority logic that requires a safety-related enable signal prior to allowing control of the device from the MCS.

Figure 7.0-14 represents the MCS internal functions and external interfaces.

The boundary of the MCS is at the terminations on the MCS hardware. The MCS supplies nonsafety-related inputs to the HSIs for nonsafety displays in the MCR, the alternate operator workstations, and other locations where module control system HSIs are necessary. There are two boundaries between MCS and MPS: the fiber-optic isolated portion and the HWM boundary. The MCS has a direct, bi-directional interface with the PCS. The network interface devices for the MCS

domain controller/historian provide the interface between the human-machine interface network layer and the control network layer.

The MCS uses logic processing in the cases where redundant input or output channels are used. Some logic supports the redundant-channel architecture used by the MPS, while other logic directly supports the process systems. The logic processing of multiple channels can include two, three, or four input signals.

COL Item 7.0-1: Not used.

The potential for closed loop MCS subsystems that use reactor power as a control input to cause instabilities is addressed by evaluations in Section 15.9.5. The results in Section 15.9.5 demonstrate that MPS effectively mitigates potential oscillations that have sufficient effect on the primary side conditions prior to the conditions challenging margin to specified acceptable fuel design limits.

Normal operation and power maneuvering control functions are provided by the following MCS functions for each NPM:

- turbine trip, throttle and governor valve control
- turbine bypass valve control
- feedwater pump speed control
- feedwater regulating valve control
- reactor coolant system boron concentration (chemical shim) control
- control rod drive system control
- pressurizer pressure control
- pressurizer level control

The control inputs and functions for each during normal power operation are described below.

Turbine Trip, Throttle and Governor Valve Control

The turbine trip, throttle, and governor controls rely on the following control inputs:

- main turbine control system package sensors (case temperatures, drain valve position, eccentricity, speed sensing, shaft axial position, journal bearing displacement, journal bearing temperature and other sensors)
- demand power level (main turbine generator load or reactor power) from MCS and main turbine control system
- main steam line flow
- turbine inlet steam pressure
- secondary system calorimetric input
- target reactor power and change rate via the MCR operator workstation

- turbine generation limit and load change rate via the MCR operator workstation

During normal power operations, the turbine governor control maintains steam header pressure as a function of reactor power demand. The turbine bypass valve diverts excess steam energy to the main condenser to limit turbine generation to the power generation target. While normal turbine generator power changes are limited to a fixed rate, the turbine generator is capable of loading and unloading by diverting steam flow to and from the turbine bypass valve.

Turbine Bypass Valve Control

The turbine bypass valve control relies on the following control inputs:

- turbine trip
- reactor trip
- DHRS passive condenser steam pressure (below approximately 15 percent steam flow)
- turbine inlet steam pressure (above 15 percent steam flow)
- secondary system calorimetric
- target reactor power and change rate via the MCR operator workstation
- turbine generation power limit and load change rate via the MCR operator workstation

During normal power operations, the turbine bypass valve is closed. During load following, operator input via the MCR human-system interface establishes the turbine generation limit. The turbine bypass valve diverts excess steam energy to the main condenser to limit turbine generation to the generation target. On a turbine trip, turbine bypass valve automatically opens to control steam header pressure.

Feedwater Pump Speed Control

The feedwater pump speed control relies on the following control inputs:

- main steam line flow
- feedwater line flow
- feedwater pressure
- turbine inlet steam pressure (above approximately 15 percent steam flow)
- main steam temperature (above approximately 15 percent steam flow)
- secondary system calorimetric
- reactor power from the NMS
- target reactor power and change rate via the MCR operator workstation

- turbine generation limit and load change rate via the MCR operator workstation

Above approximately 25 percent thermal power, feedwater pump speed is controlled to provide feedwater flow to the desired power level. If the control rods are in automatic, then feedwater speed control generates the desired power level as determined by reactor power from the NMS. If the control rods are in manual and reactor power is less than or equal to the desired power level, then the operator can select the control to use the secondary heat balance as the controlled variable. The feedwater regulating valves (FWRVs) remain static and are opened to the optimum position to support feedwater pump speed control.

Feedwater Regulating Valve Control

The FWRV control relies on the following control inputs:

- decay heat removal passive condenser condensate pressure
- decay heat removal passive condenser steam pressure
- main steam line flow
- feedwater line flow
- target reactor power and change rate via the MCR operator workstation
- turbine generation limit and load change rate via the MCR operator workstation

From plant startup to approximately 25 percent reactor power, MCS controls the FWRV position to adjust feedwater flow to maintain DHRS passive condenser steam pressure equal to a saturation pressure slightly below the RCS average coolant temperature. From approximately 25 percent reactor power to 100 percent reactor power, the FWRVs remain static and are opened to the optimum position to support feedwater flow control.

Control Rod Drive System Control

The control rod drive system relies on the following control inputs:

- RCS average coolant temperature
- source, intermediate, and power range nuclear instrumentation

Controls rods are manually and automatically controlled by the control rod drive system to maintain average RCS coolant temperature on a programmed value as a function of reactor power. Rod position is limited by the power dependent insertion limits described in Section 4.3.

Reactor Coolant System Boron Concentration (Chemical Shim) Control

The chemical shim control relies on the following control inputs:

- RCS flow

- RCS boron concentration
- CVCS letdown line flow
- CVCS makeup line flow
- CVCS makeup boron concentration
- boron addition system boron concentration

The CVCS adjusts the boron concentration in the RCS to compensate for changes in core reactivity over the fuel cycle. It also provides the required boration for normal shutdowns. The CVCS makeup pumps inject borated water from the boron addition system to raise RCS boron concentration. CVCS letdown flow is discharged to the liquid radwaste system to maintain a nearly constant volume of reactor coolant (RCS inventory may vary over short time periods within the pressurizer level operating band).

The boron concentration of the RCS is lowered by adding demineralized water from the demineralized water system with the CVCS makeup pumps while discharging coolant to the liquid radwaste system. Routine incremental boron concentration dilution of the RCS by CVCS is performed based on operator permission. The MCS determines a desired dilution rate and quantity, which preserves shutdown margin to achieve a final RCS boron concentration. The operator is required to review and approve the dilution process using the MCR operator workstations and monitor the plant during dilution evolutions.

Pressurizer Pressure Control

The pressurizer pressure control relies on the following control input:

- RCS pressure

During normal operation, pressurizer pressure control is achieved using the pressurizer spray to lower pressurizer pressure, and two groups of pressurizer heaters are used to raise pressurizer pressure based on the deviation from the normal operating pressure. One group of pressurizer heaters uses modulating proportional control, and the other group of pressurizer heaters is either on or off, depending on the deviation of pressurizer pressure from the normal operating pressure.

Pressurizer Level Control

The pressurizer level control relies on the following control inputs:

- pressurizer level
- RCS average coolant temperature

During normal power operation, pressurizer water level control is achieved using CVCS makeup and letdown flows.

Common cause failure analysis of the MCS is provided in Section 7.1.6.

7.0.4.6 Plant Control System

The PCS is a distributed control system which allows monitoring and control of non-NPM-specific plant components. The PCS includes manual controls and HSIs necessary to provide operator interaction with the process control mechanism.

The principal function of the PCS is to control and monitor the nonsafety-related control system components which are not specific to an NPM. The PCS is composed of the central processor or processors, power supplies, mounting racks, input/output racks, and associated networking equipment.

Figure 7.0-15 shows the PCS internal functions and external interfaces.

The boundary of the PCS is at the terminations on the PCS hardware. The PCS supplies nonsafety inputs to the HSIs for nonsafety displays in the MCR, the alternate operator workstations, and other locations where PCS human-system interfaces are necessary. The boundary between the PPS and PCS is at the output connection of the optical isolators in the PPS. The PCS has a direct, bi-directional interface with the MCS. The network interface devices for the PCS domain controller/historian provide the interface between the human-machine interface network layer and the control network layer.

The PCS uses logic processing in the cases where redundant input or output channels are used. Some logic supports the redundant-channel architecture used by the PCS, while other logic directly supports the process systems. The logic processing of multiple channels can include two, three, or four input signals.

Common cause failure analysis of the PCS is provided in Section 7.1.6.

7.0.4.7 In-core Instrumentation System

The ICIS monitors the neutron flux distribution within the reactor core and provides core exit temperature information to the MPS for PAM. The neutron flux information is also used to verify operation and calibrate the NMS-excore detectors. The ICIS can determine a power shape deviation caused by stuck or misaligned control rods when the rod positions cannot be determined by the rod position indication system. The ICIS instrument stringer assembly provides safety-related functions to ensure the integrity of the primary containment pressure boundary and reactor coolant pressure boundary are maintained where the instrument stringer assembly penetrates the CNV and RPV pressure boundaries, respectively.

The ICIS includes:

- self-powered neutron detectors located in the reactor core for monitoring neutron flux.
- thermocouples located at the exit of the core to provide temperature information to the MPS.

- thermocouples located in the reactor core for monitoring core temperature
- instrument stringer assemblies in which the neutron detectors and thermocouples are housed.
- signal conditioning and processing electronics.

The ICIS has a total of six detectors integral to each instrument stringer assembly. There are four self-powered neutron detectors and two thermocouples. The neutron detectors are distributed throughout the vertical height of the reactor core. One thermocouple is located at the inlet of the core, and one thermocouple is located at the exit of the core.

Each NPM has a total of 12 in-core instrumentation guide tubes. These rigid tubes extend from the top of the containment to the bottom of the reactor to provide routing and structural support for the in-core instrumentation stringer assemblies. Section 4.3.2 provides additional information on the in-core instrumentation system. Figure 4.3-14 provides the ICIS core locations.

7.0.4.8 Fixed Area Radiation Monitoring

Radiation monitoring is performed by fixed area radiation monitors and continuous air monitors throughout the plant.

The principal functions of radiation monitoring are:

- monitoring in-plant radiation and airborne radioactivity as appropriate for routine and accident conditions,
- informing plant personnel immediately when predetermined exposure rates are exceeded in various areas within the plant, and
- alerting control room operators of changing plant radiation levels.

Area radiation monitors consist of a detector or detectors that are connected to an electronic control unit in local proximity. The electronic control unit interfaces with the corresponding I&C system depending on functionality. Airborne monitors are self-contained and consist of modular components assembled on an open frame for ease of accessibility. The detectors are connected to a local electronic control unit which interfaces with the corresponding I&C system depending on functionality. Location of area and airborne radiation monitors are provided in Section 11.5.

7.0.5 References

- 7.0-1 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603-1991, Piscataway, NJ.
- 7.0-2 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Standard 7-4.3.2-2003, Piscataway, NJ.

- 7.0-3 NuScale Power, LLC, "Design of the Highly Integrated Protection System Platform," TR-1015-18653-P-A, Revision 2.
- 7.0-4 NuScale Power, LLC, "NuScale Instrument Setpoint Methodology Technical Report," TR-122844-P, Revision 0.

Table 7.0-1: NuScale Instrumentation and Controls Design and Applicable Regulatory Requirements Matrix

Regulatory Requirements and Guidance	Applicable FSAR Sections																				
	7.1- Fundamental Design Principles					7.2 - System Characteristics															
	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8	7.2.9	7.2.10	7.2.11	7.2.12	7.2.13	7.2.14	7.2.15	7.2.16
10 CFR																					
50.34(f)(2)(iv)																		x			
50.34(f)(2)(v)									x									x			
50.34(f)(2)(xi)																		x			
50.34(f)(2)(xvii)																		x			
50.34(f)(2)(xviii)																		x			x
50.34(f)(2)(xiv)					x																
50.34(f)(2)(xix)																		x			
50.36(c)(I)(ii)(A)												x									
50.36(c)(3)												x								x	
50.49							x														x
50.54(jj)						x															
50.55(i)						x															
50.55a(h)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
50.62 (ATWS)					x																
52.137(a)(2)													x								
GDC 1						x															
GDC 2	x						x														x
GDC 4							x														x
GDC 5																					
GDC 10	x															x					
GDC 13		x		x	x							x						x			x
GDC 15	x																				
GDC 16	x																				
PDC 19	x																	x			
GDC 20	x											x									
GDC 21		x	x	x																x	
GDC 22		x			x																
GDC 23	x																				
GDC 24		x	x		x																

Table 7.0-1: NuScale Instrumentation and Controls Design and Applicable Regulatory Requirements Matrix (Continued)

Regulatory Requirements and Guidance	Applicable FSAR Sections																				
	7.1- Fundamental Design Principles					7.2 - System Characteristics															
	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8	7.2.9	7.2.10	7.2.11	7.2.12	7.2.13	7.2.14	7.2.15	7.2.16
GDC 25	x																				
GDC 29				x																	
GDC 64	x																				
App B						x	x														
Regulatory Guides																					
RG 1.22						x															
RG 1.28						x															
RG 1.47									x									x			
RG 1.53			x		x											x					
RG 1.62					x												x				
RG 1.75		x					x							x							
RG 1.89							x														x
RG 1.97	x																	x			
RG 1.105												x									
RG 1.118																				x	
RG 1.151							x														
RG 1.152		x				x	x	x		x				x		x				x	
RG 1.168						x															
RG 1.169						x															
RG 1.170						x															
RG 1.171						x															
RG 1.172						x															
RG 1.173						x															
RG 1.180							x														
RG 1.204							x														
RG 1.209							x														x
IEEE Std 603-1991																					
4.1	x																				
4.2	x																				
4.3	x																				

Table 7.0-1: NuScale Instrumentation and Controls Design and Applicable Regulatory Requirements Matrix (Continued)

Regulatory Requirements and Guidance	Applicable FSAR Sections																				
	7.1- Fundamental Design Principles					7.2 - System Characteristics															
	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8	7.2.9	7.2.10	7.2.11	7.2.12	7.2.13	7.2.14	7.2.15	7.2.16
4.4	x			x																	
4.5	x																				
4.6	x																				
4.7	x																				
4.8	x																				
4.9	x																				
4.10	x			x																	
4.11	x																				
4.12	x																				
5.1			x		x										x						
5.2				x				x													
5.3						x															
5.4							x														
5.5				x				x													
5.6		x																			
5.7																				x	
5.8									x									x			
5.9														x							
5.10														x							
5.11														x							
5.12													x								
5.13																x					
5.14																			x		
5.15								x													
6.1																	x				
6.2																	x				
6.3															x						
6.4											x										
6.5																				x	
6.6									x												

Table 7.0-1: NuScale Instrumentation and Controls Design and Applicable Regulatory Requirements Matrix (Continued)

Regulatory Requirements and Guidance	Applicable FSAR Sections																				
	7.1- Fundamental Design Principles					7.2 - System Characteristics															
	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8	7.2.9	7.2.10	7.2.11	7.2.12	7.2.13	7.2.14	7.2.15	7.2.16
6.7									x						x						
6.8												x									
7.1																	x				
7.2																	x				
7.3								x													
7.4									x												
7.5									x												
NUREG/CR-6303					x																
SECY-93-087 18.II.Q					x													x			
GL 85-06					x																
IEEE Std 7-4.3.2					x	x															
GL 91-04												x									

Table 7.0-2: Highly Integrated Protection System Topical Report Application Specific Information Cross References

HIPS TR Application Specific Action Item Number	Section 7.0 - Introduction and Overview				Section 7.1- Fundamental Design Principles								Section 7.2 - System Characteristics														
	7.0.1	7.0.2	7.0.3	7.0.4	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.1.7	7.1.8	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8	7.2.9	7.2.10	7.2.11	7.2.12	7.2.13	7.2.14	7.2.15	
1	x				x																						
2				x																							
3 ¹					x																						
4 ¹					x							x															
5 ¹					x																						
6 ¹					x				x																		
7															x												
8						x																					
9						x			x																		
10									x																		
11									x											x							
12							x																				
13							x																				
14							x																			x	
15														x													
16												x															
17													x														
18				x									x	x													
19								x						x													
20						x																					
21							x																				
22						x														x							
23						x							x														
24																										x	
25																										x	
26																										x	
27																								x			
28																								x			
29																								x			
30																								x			
31																				x							
32							x													x						x	
33																				x							
34																			x								

**Table 7.0-2: Highly Integrated Protection System Topical Report Application Specific Information
Cross References (Continued)**

HIPS TR Application Specific Action Item Number	Section 7.0 - Introduction and Overview				Section 7.1- Fundamental Design Principles							Section 7.2 - System Characteristics														
	7.0.1	7.0.2	7.0.3	7.0.4	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.1.7	7.1.8	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8	7.2.9	7.2.10	7.2.11	7.2.12	7.2.13	7.2.14	7.2.15
35																						x				
36																									x	
37														x												
38																							x			
39																							x			
40																					x					
41																	x									
42															x											
43															x											
44																		x								
45															x											
46						x																				
47												x							x							x
48	Not applicable.																									
49												x							x							x
50												x														x
51												x														x
52						x																				
53						x														x						
54																				x						
55						x																				
56								x																		
57				x																						
58																				x						
59								x																		
60						x																				
61						x																				
62									x																	
63									x																	
64									x																	
65									x																	

Note 1: For application specific action items 3 through 6, the overall conformance of the MPS to IEEE Std 603-1991, IEEE Std 7-4.3.2-2003, Digital I&C ISG-04 and SRM for SECY-93-087 is described in Section 7.1.1.

Table 7.0-3: Classification of Instrumentation and Controls Systems

SSC (Note 1)	SSC Classification (A1, A2, B1, B2)	QA Program Applicability (Note 2)	Augmented Design Requirements (Note 3)	Seismic Classification (Ref. RG 1.29 or RG 1.143)
MPS, Module Protection System				
All components (except as listed below)	A1	Q	None	I
- Separation Group A - Safety Function Module: - Leak Detection into Containment - Separation Group B and C - Safety Function Module for PAM indication functions - Separation Group D - Safety Function Module: - Leak Detection into Containment	B2	AQ	- IEEE 497-2016 (Note 4) - EMI/RFI - Environmental Qualification - Power from Vital Instrument Bus 10 CFR 50.55a(1) 10 CFR 50.55a(h) - IEEE 603-1991 - Independence - Single Failure Criterion - Common-Cause Failure - Location of Indicators and Controls - Multi-Module Considerations	I
- Division I and Division II: - Engineered Safety Features Actuation System - Equipment Interface Module for low AC voltage to battery chargers function - Engineered Safety Features Actuation System Monitoring and Indication Bus, Communication Module - MPS Gateway - Reactor Trip System Monitoring and Indication Bus - Communication Module - Separation Group A, B, C, and D: - Monitoring and Indication Bus - Communication Module - Separation Group B and C - Safety Function Modules for PAM indication functions	B2	AQ	- IEEE 497-2016 (Note 4) - EMI/RFI - Environmental Qualification - Power from Vital Instrument Bus	I
Division I and II Maintenance Workstations	B2	AQ	None	II

Table 7.0-3: Classification of Instrumentation and Controls Systems (Continued)

SSC (Note 1)	SSC Classification (A1, A2, B1, B2)	QA Program Applicability (Note 2)	Augmented Design Requirements (Note 3)	Seismic Classification (Ref. RG 1.29 or RG 1.143)
NMS, Neutron Monitoring System				
• Excore Neutron Detectors • Excore Separation Group A/B/C/D - Power Isolation, Conversion and Monitoring Devices • Excore Signal conditioning and processing equipment	A1	Q	None	I
• Flood Neutron Detectors • Flood Signal conditioning and processing equipment	B2	AQ	IEEE 497-2016 (Note 4)	I
• Refuel Neutron Detectors • Refuel Signal conditioning and processing equipment	B2	AQ	None	II
SDIS, Safety Display and Indication System				
All components (except as listed below)	B2	AQ	IEEE 497-2016 (Note 4)	I
Division I and Division II Hub PCS Communication Modules	B2	None	None	I
MCS, Module Control System				
• MCR MCS HMI	B2	AQ	IEEE 497-2016 (Note 4)	II
• MCS Domain Controllers • Controllers • I/O Modules • Gateway from MPS • Gateway to PCS	B2	AQ	IEEE 497-2016 (Note 4)	III
• Controllers (other than above) • I/O Modules (other than above)	B2	None	None	III
ICIS, In-Core Instrumentation System				
In-core instrument stringer sheath (Table 3.2-2)	-	-	-	-
In-core instrument stringer/ temperature sensors	B2	AQ	IEEE 497-2016 (Note 4)	I
In-core instrument stringer/ flux sensors	B2	None	None	II
Signal Conditioning and Processing Electronics	B2	None	None	II

Table 7.0-3: Classification of Instrumentation and Controls Systems (Continued)

SSC (Note 1)	SSC Classification (A1, A2, B1, B2)	QA Program Applicability (Note 2)	Augmented Design Requirements (Note 3)	Seismic Classification (Ref. RG 1.29 or RG 1.143)
PCS, Plant Control System				
• Controllers • I/O Modules • PCS Domain Controllers • PCS Alternate Operator Workstations • Gateway from MCS • Gateway from PPS	B2	AQ	IEEE 497-2016 (Note 4)	III
• MCR PCS HMI	B2	AQ	IEEE 497-2016 (Note 4)	II
• WMCR PCS HMI • MMC PCS HMI • Controllers (other than above) • I/O Modules (other than above)	B2	None	None	III
PPS, Plant Protection System				
Division I and Division II: • Monitoring and Indication Bus Communication Modules • Safety Function Modules for Spent Fuel Pool Level Indication	B2	AQ	• IEEE 497-2016 (Note 4) • 10CFR50.155 • Protected from Natural Phenomena per GDC 2	I
Division I and Division II Equipment Interface Modules	B2	AQ	• IEEE 497-2016 (Note 4) • Environmental Qualification	I
Division I and Division II: • ELVS Voltage Sensors • Manual CRHS Actuation Switches • Enable Nonsafety Control Switches • Scheduling and Bypass Modules • Hard-Wired Modules • Safety Function Modules for: - ELVS Voltage Sensors - CRE Air Duct Air Radiation Monitors - CRE Air Duct Toxic Gas Sensors	B2	AQ	Environmental Qualification	I

Table 7.0-3: Classification of Instrumentation and Controls Systems (Continued)

SSC (Note 1)	SSC Classification (A1, A2, B1, B2)	QA Program Applicability (Note 2)	Augmented Design Requirements (Note 3)	Seismic Classification (Ref. RG 1.29 or RG 1.143)
Division I and Division II: • CTB Communication Modules • Maintenance Workstations • Safety Function Modules for CRHS Sensors	B2	None	None	I
RMS, Radiation Monitoring System				
RM system that monitors PAM B, C & F variables	B2	AQ	IEEE 497-2016 (Note 4)	I
Radiation monitors that monitors Type E variables	B2	AQ	IEEE 497-2016 (Note 4)	III
Area airborne radiation monitors that monitors Type E Variable	B2	AQ	• IEEE 497-2016 (Note 4) • ANSI/HPS N13.1-2011	III
Area airborne radiation monitors in: • Radioactive Waste Building • Reactor Building	B2	AQ	ANSI/HPS N13.1-2011	III
Radiation monitors in: • Radioactive Waste Building • Reactor Building • Turbine Buildings	B2	None	None	III

Note 1: Acronyms used in this table are listed in Table 1.1-1.

Note 2: QAP applicability codes are as follows:

- Q = indicates quality assurance requirements of 10 CFR 50 Appendix B are applicable in accordance with the QAP (Section 17.5).
- AQ = indicates that pertinent augmented quality assurance requirements for nonsafety-related SSC are applied to ensure that the function is accomplished when needed based on that functionality's regulatory requirements. Note that in meeting regulatory guidance, codes, and standards, those applicable SSC may also have quality assurance requirements invoked by said guidance (e.g., RG 1.26, RG 1.143, IEEE 497, RG 1.189).
- None = indicates no specific QAP or augmented quality requirements are applicable.

Note 3: Augmented design requirements are applied in addition to the Quality Group, and seismic classification requirements, where applicable.

Note 4: IEEE Std 497-2016 as endorsed by RG 1.97 and implemented as described in Table 1.9-2

Figure 7.0-1: Overall Instrumentation and Controls System Architecture Diagram

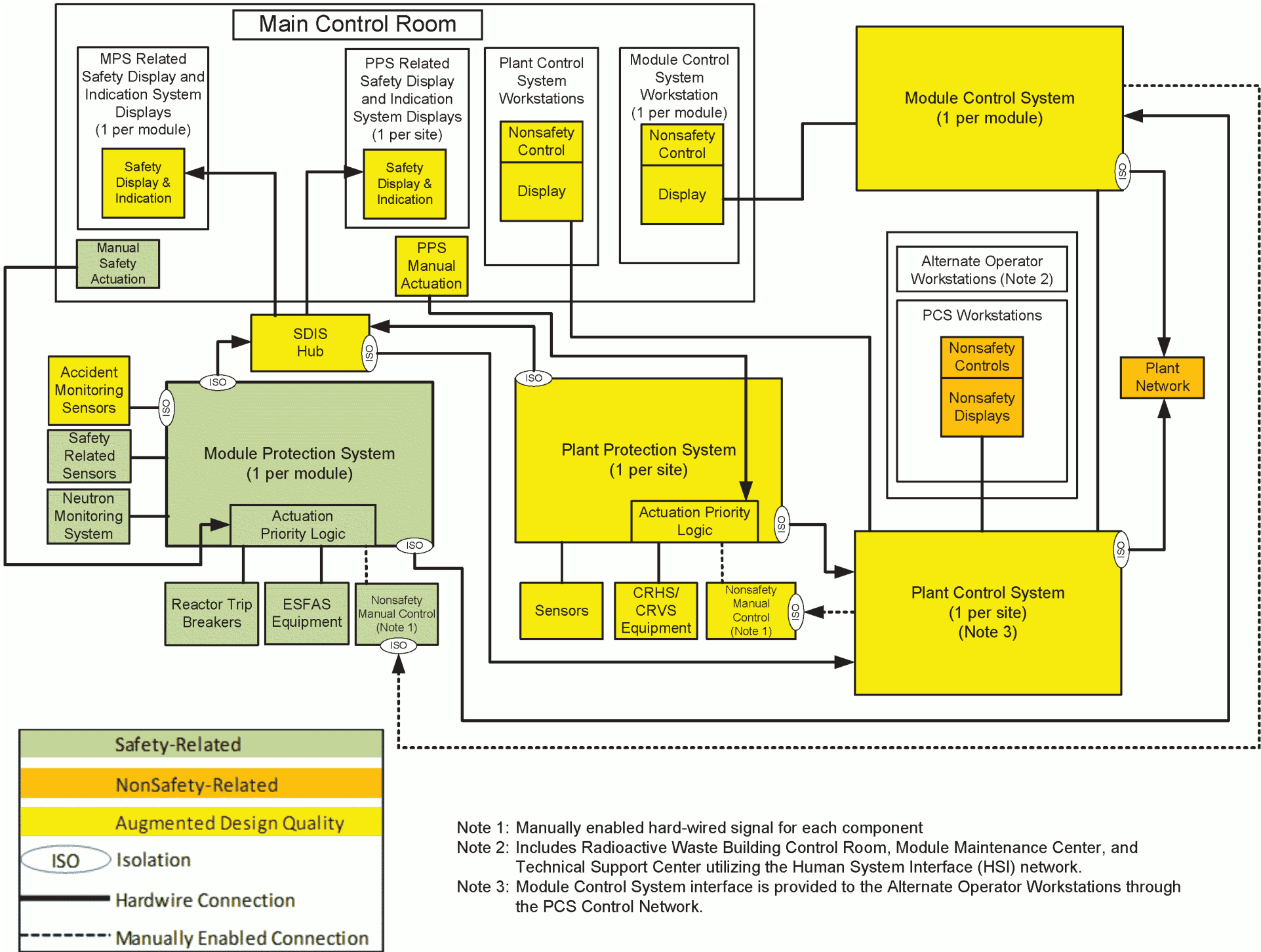


Figure 7.0-2: Module Protection System Boundaries

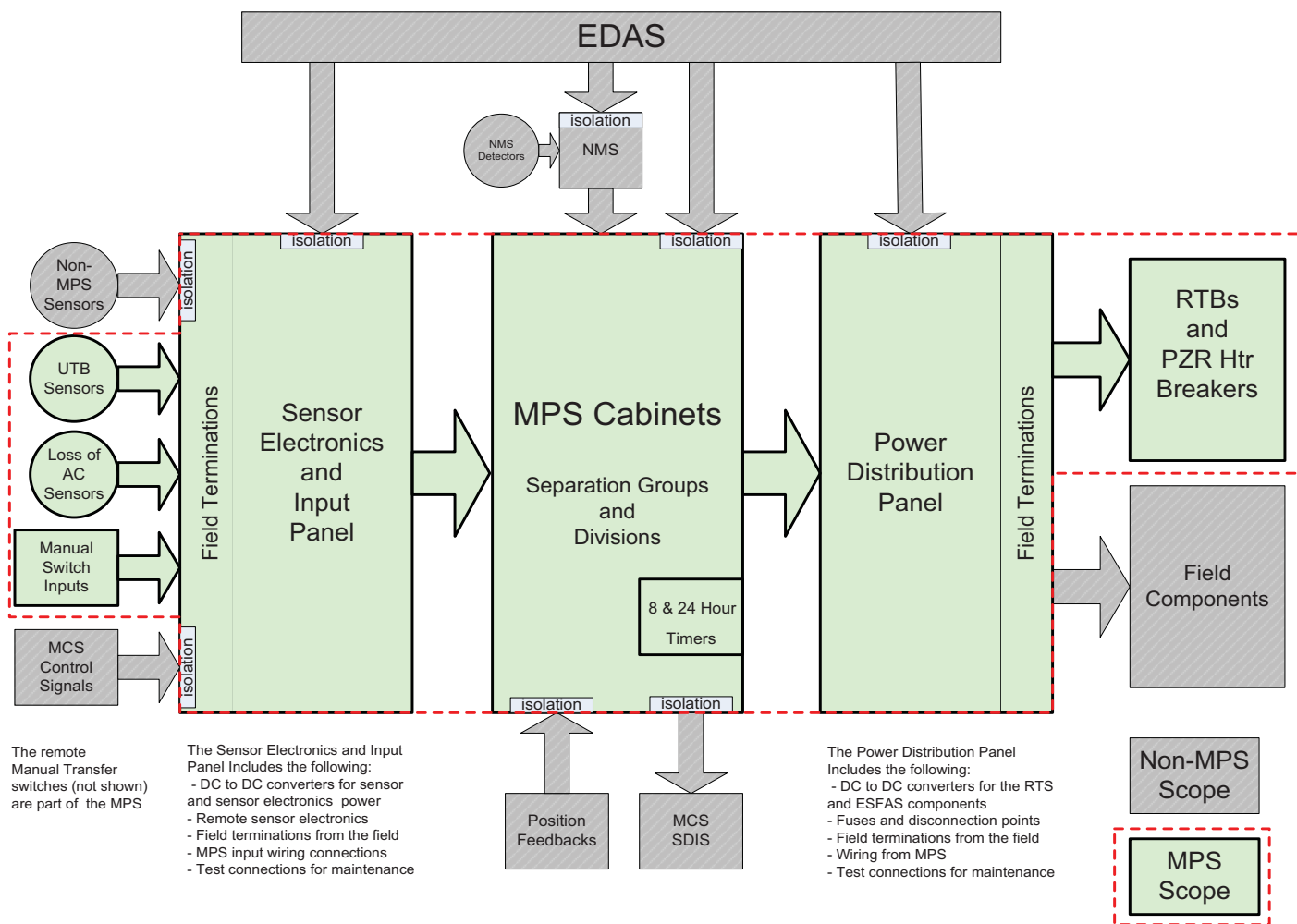
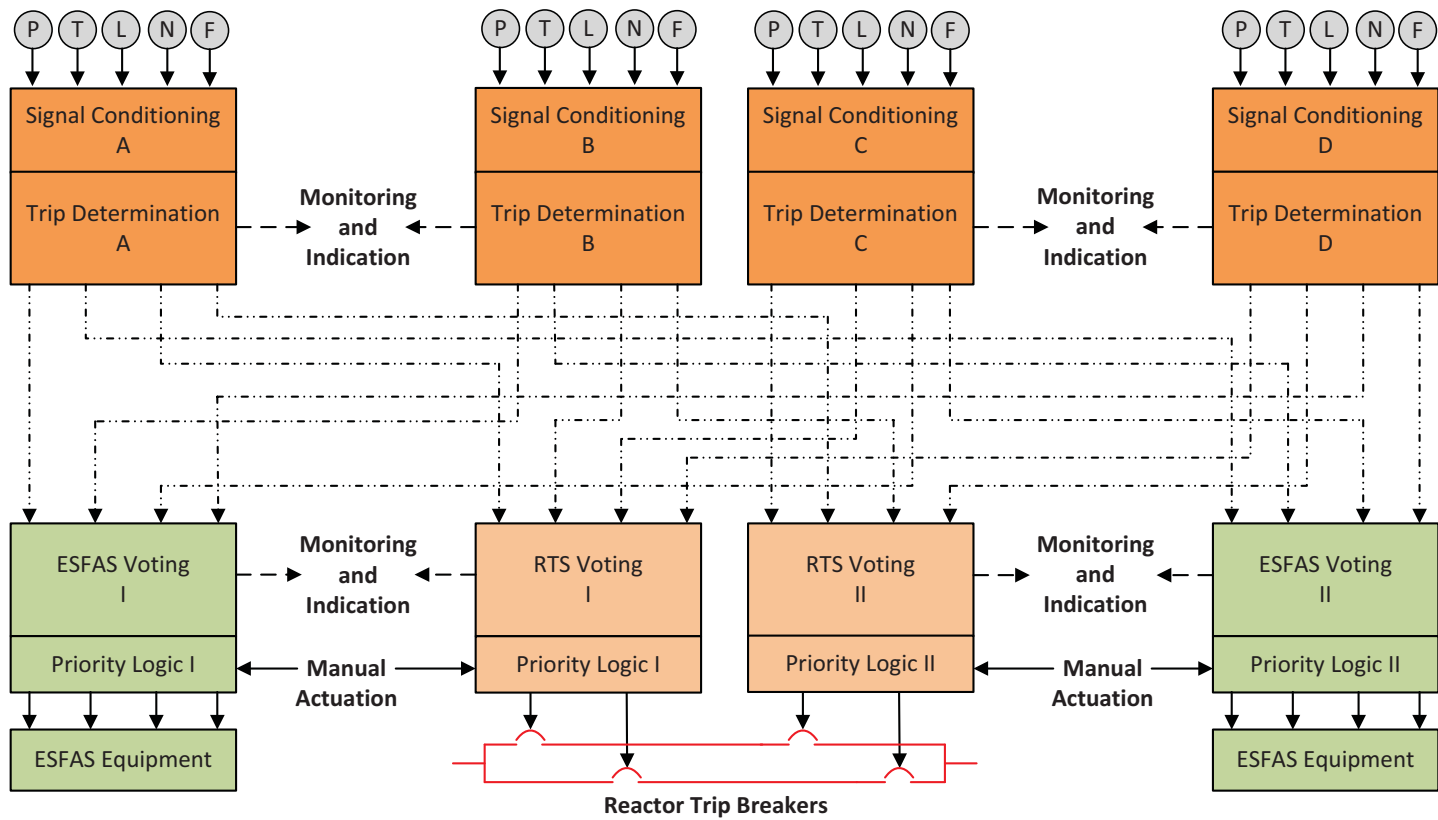


Figure 7.0-3: Module Protection System Safety Architecture Overview



Revision 2

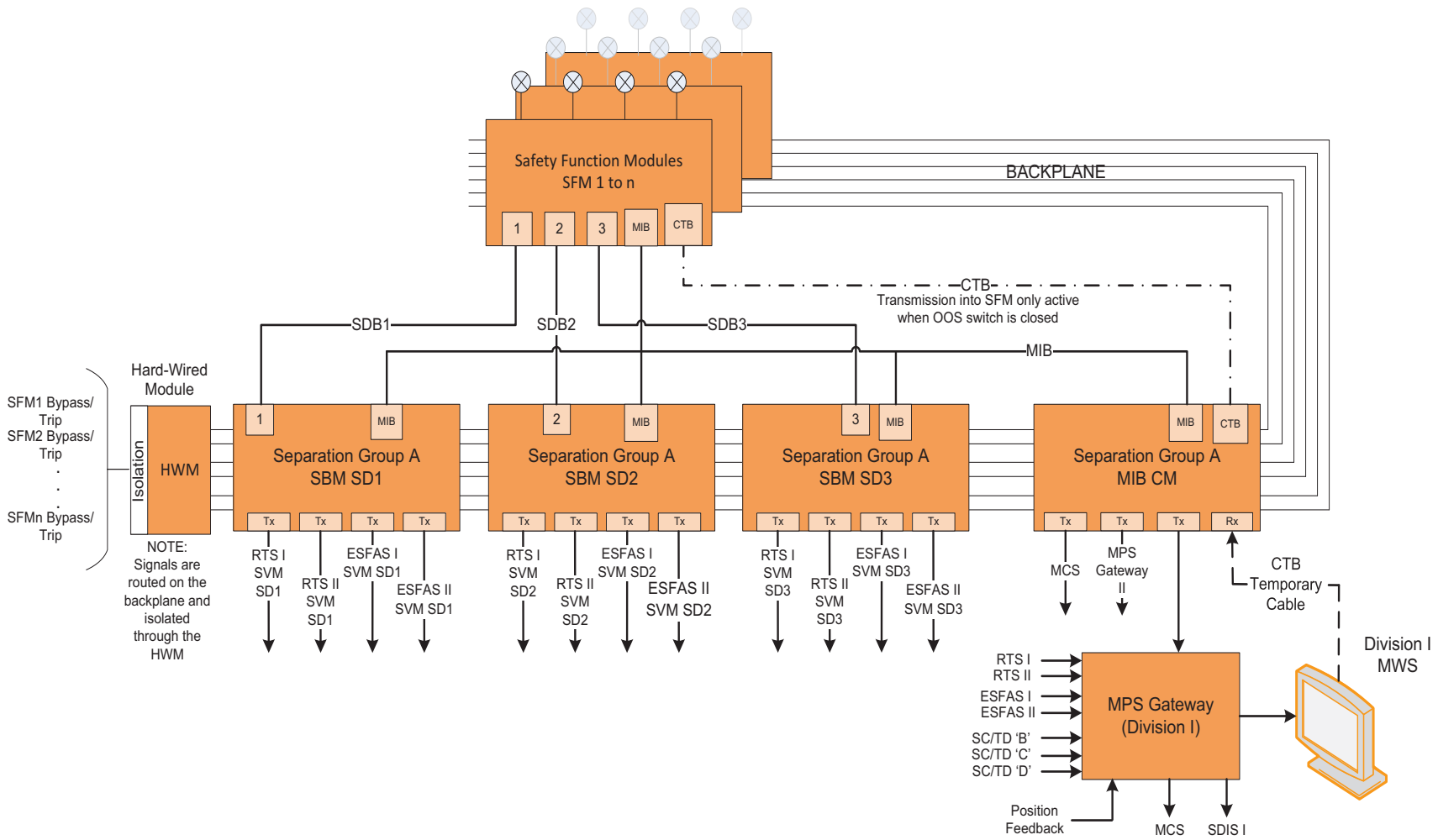


Figure 7.0-5: Separation Group A and Division I Reactor Trip System and Engineered Safety Features Actuation System Communication Architecture

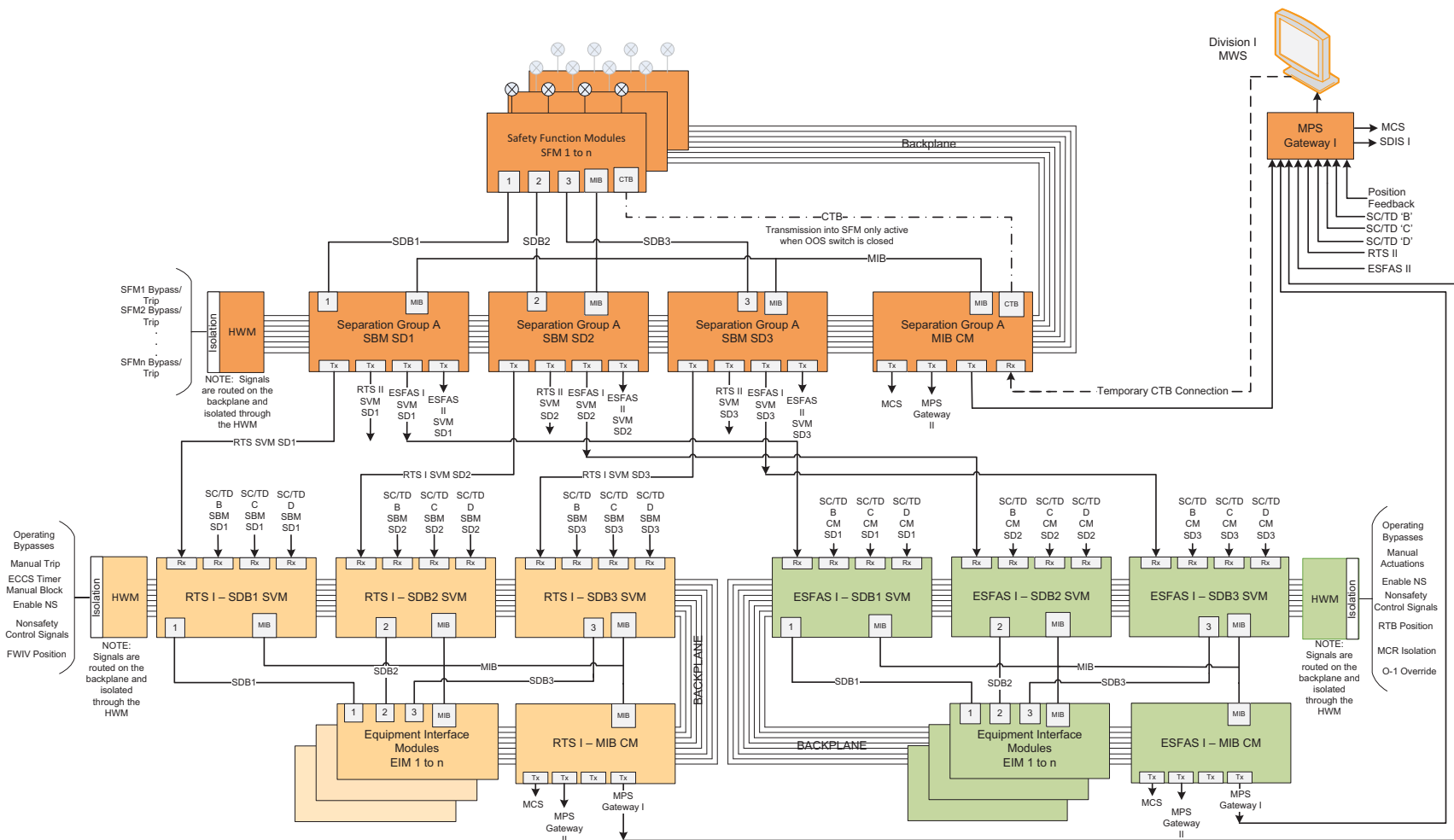


Figure 7.0-6: Reactor Trip Breaker Arrangement

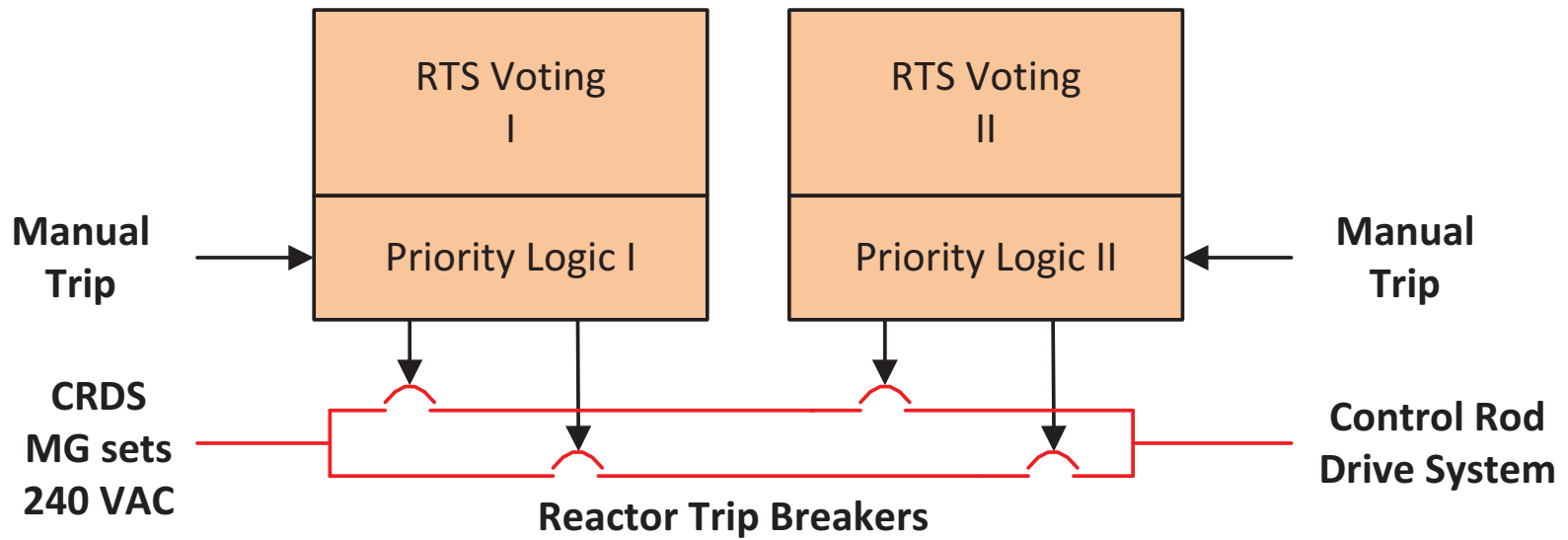


Figure 7.0-7: Pressurizer Heater Breaker Arrangement

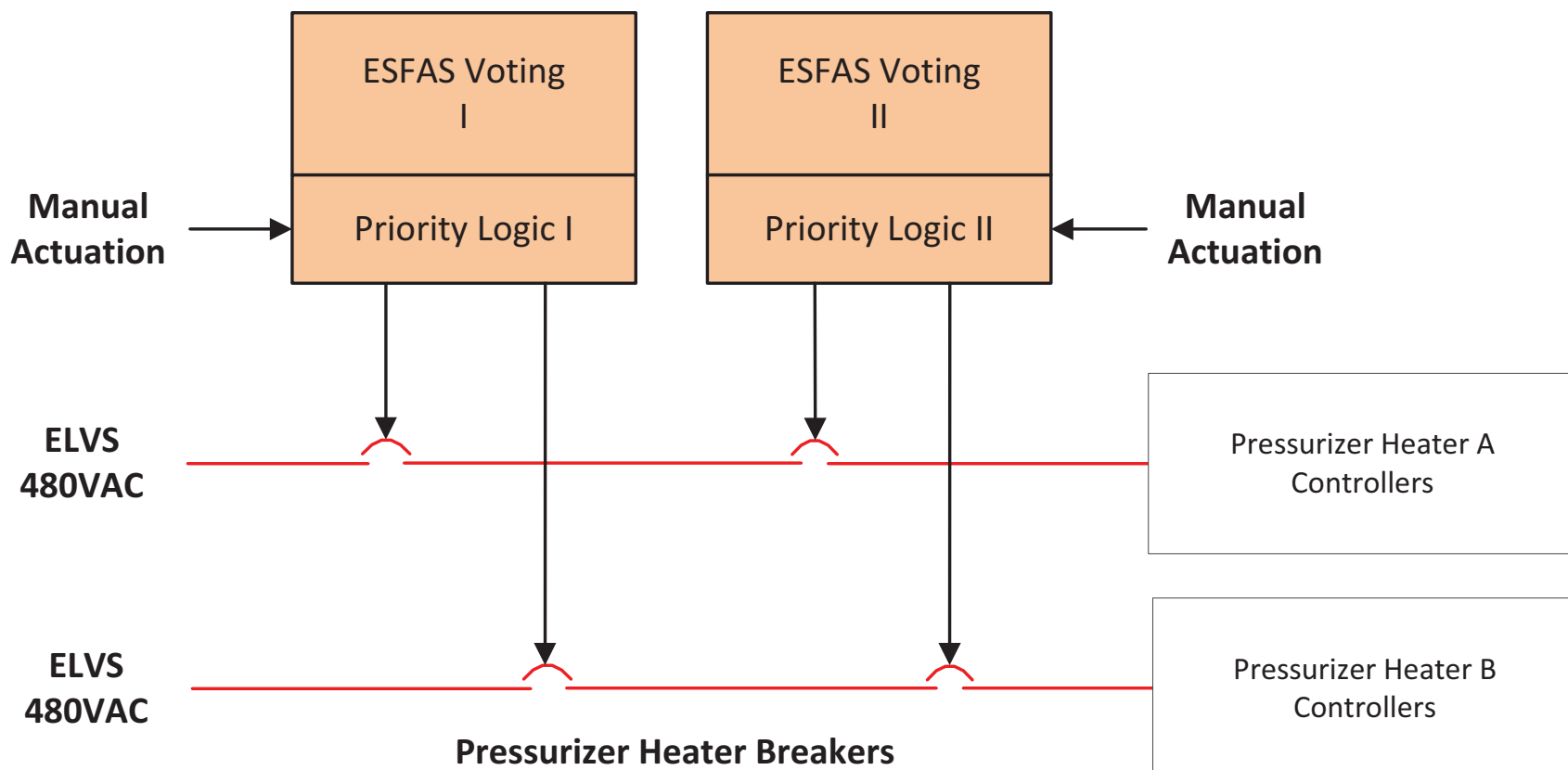


Figure 7.0-8: Module Protection System Gateway Diagram

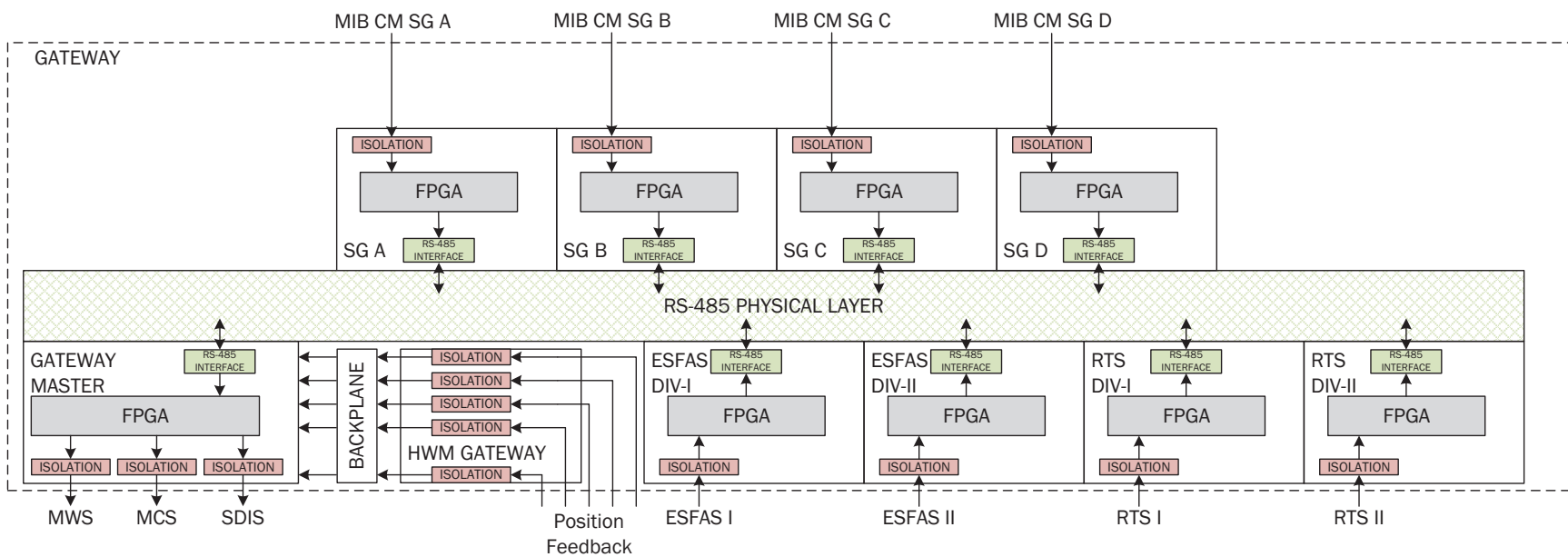
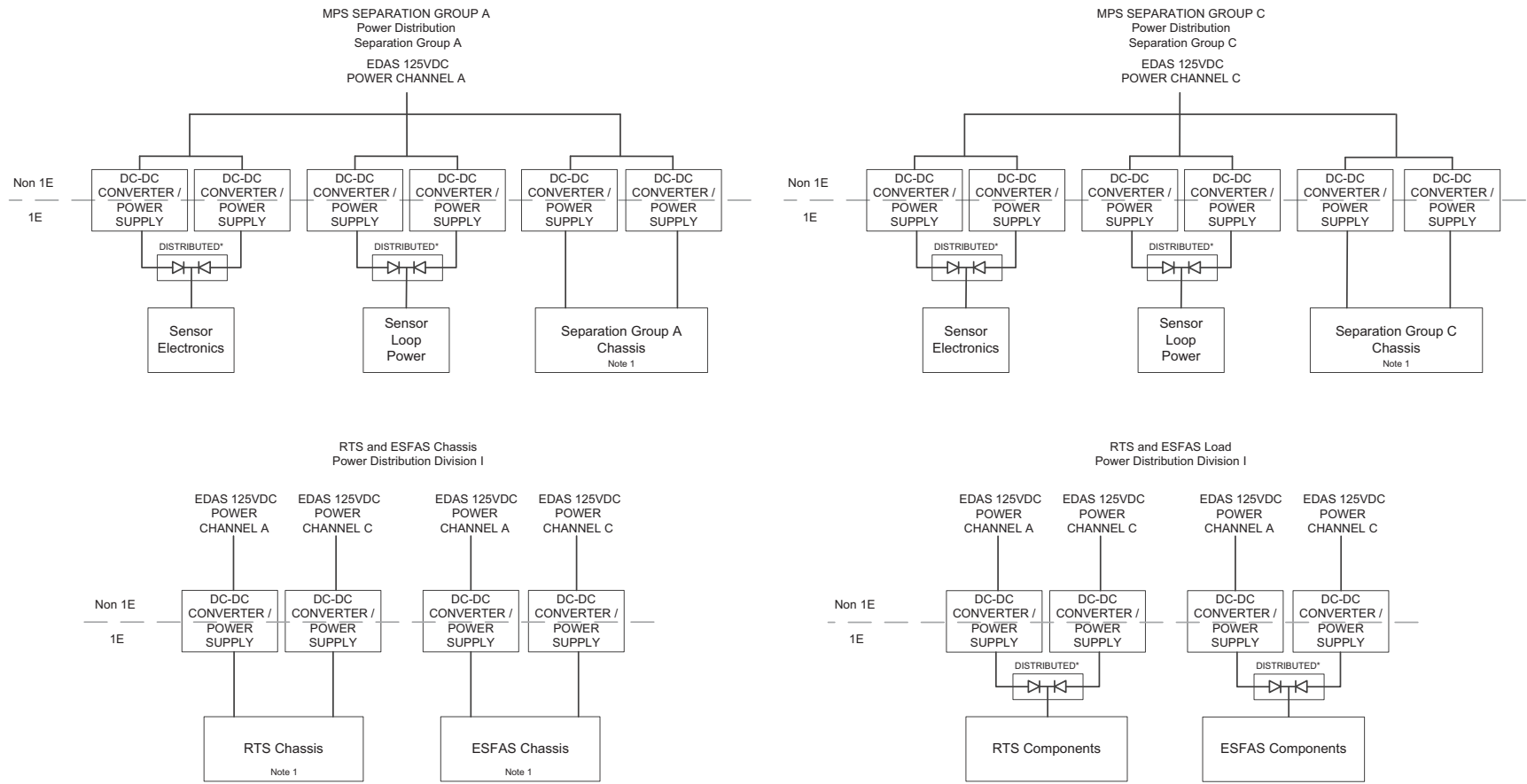


Figure 7.0-9: Module Protection System Power Distribution



Note 1: The two power sources to the chassis are auctioneered on each module in the chassis.

Note 2: Separation Groups B and D are similar.

*Shared or auctioneered

Figure 7.0-10: Neutron Monitoring System Ex-Core Block Diagram

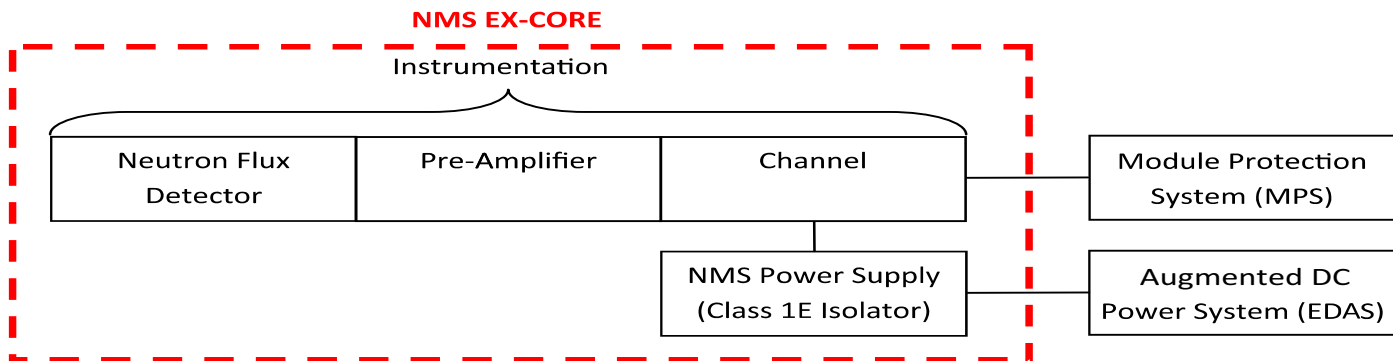


Figure 7.0-11: Plant Protection System Block Diagram

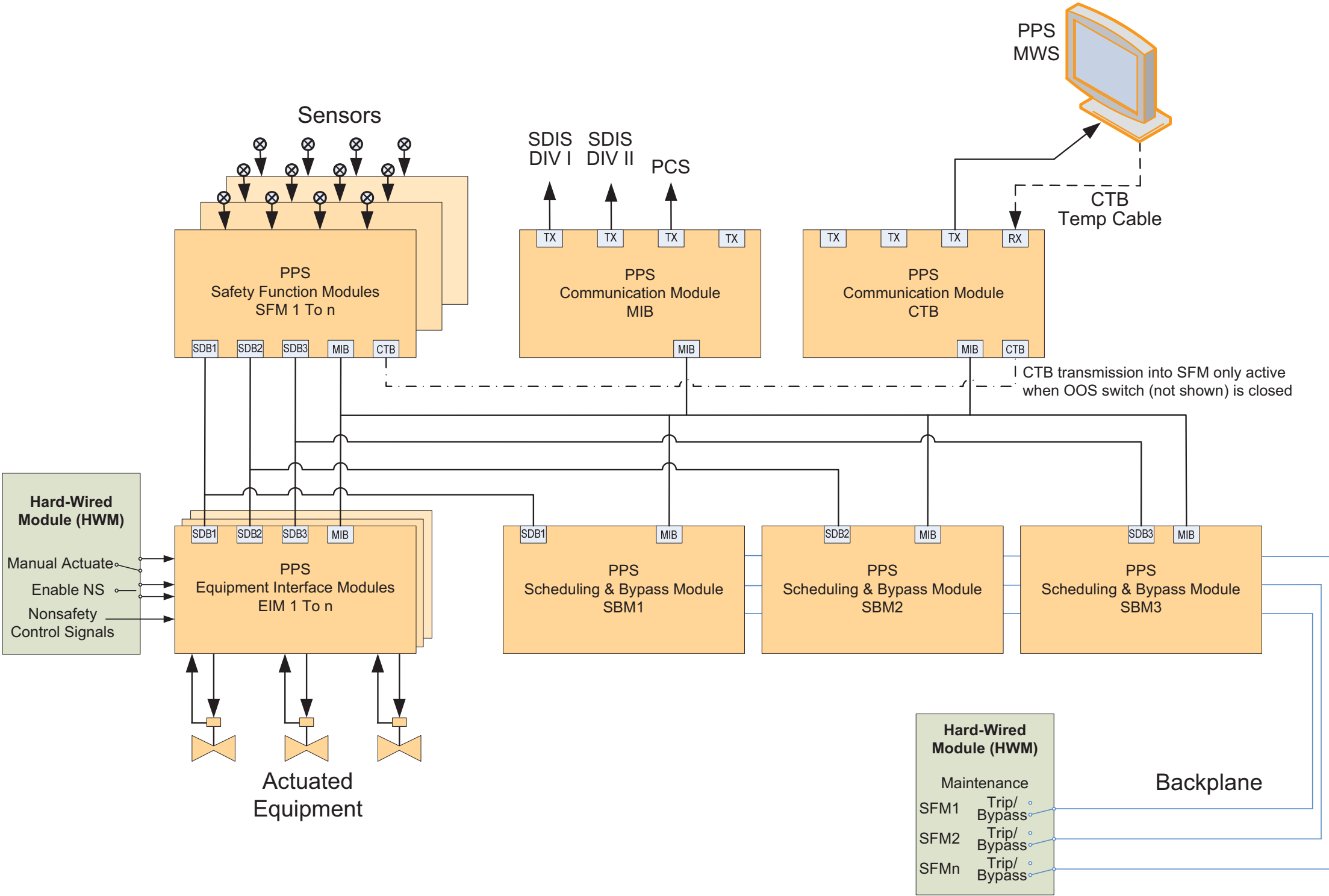
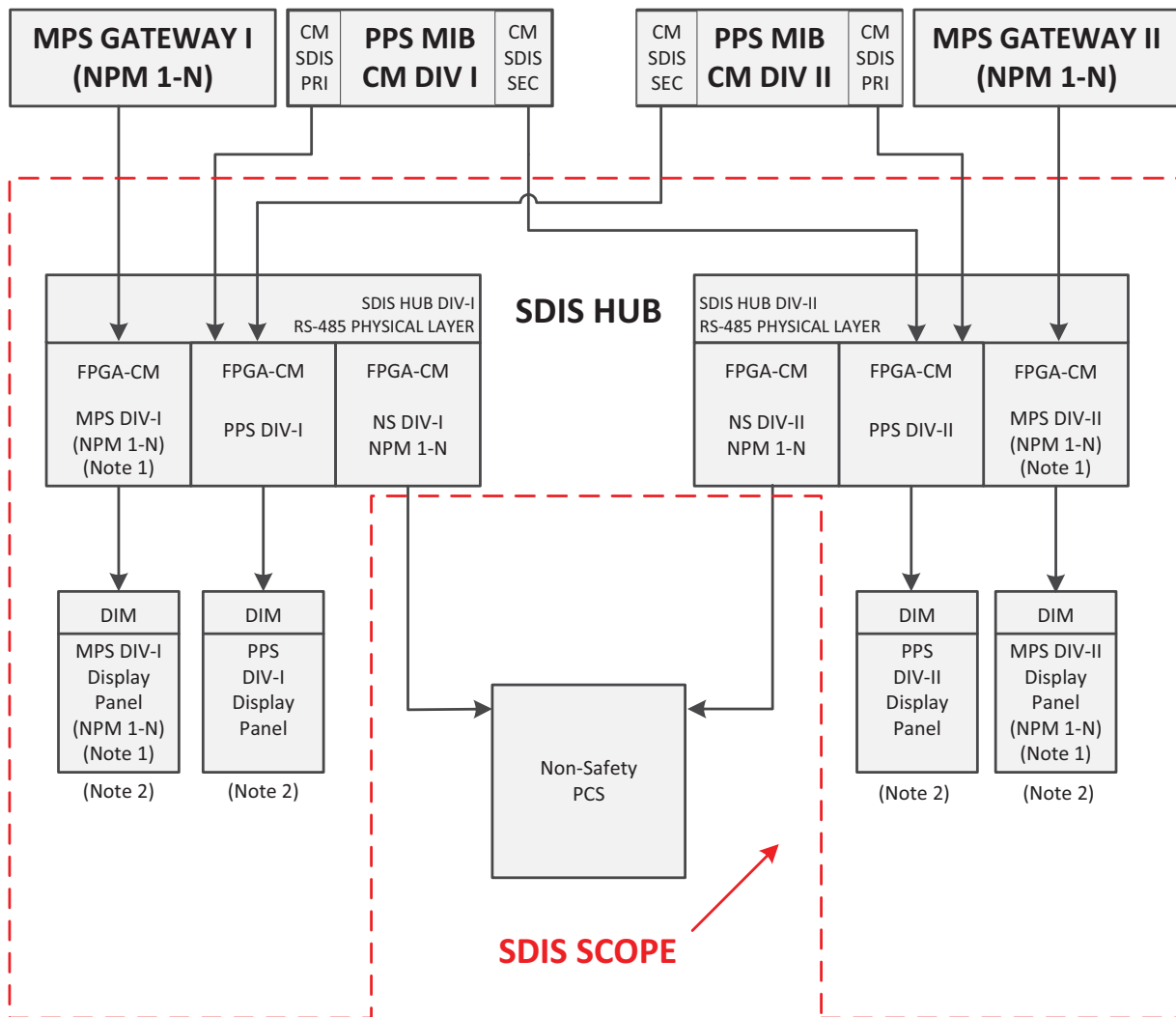


Figure 7.0-12: Safety Display and Indication System Boundary



Notes:

1. The module protection system (MPS) gateway, FPGA-CM, DIM, & Display Panels shown are typical for NMP 1-6.
2. DIMs and display panels will be separate for each NPM. Separate display panels will provide common-plant information from PPS. Although no cabling is shown, there is a cable connection between the DIM and the display panels.

Figure 7.0-13: Safety Display and Indication Hub

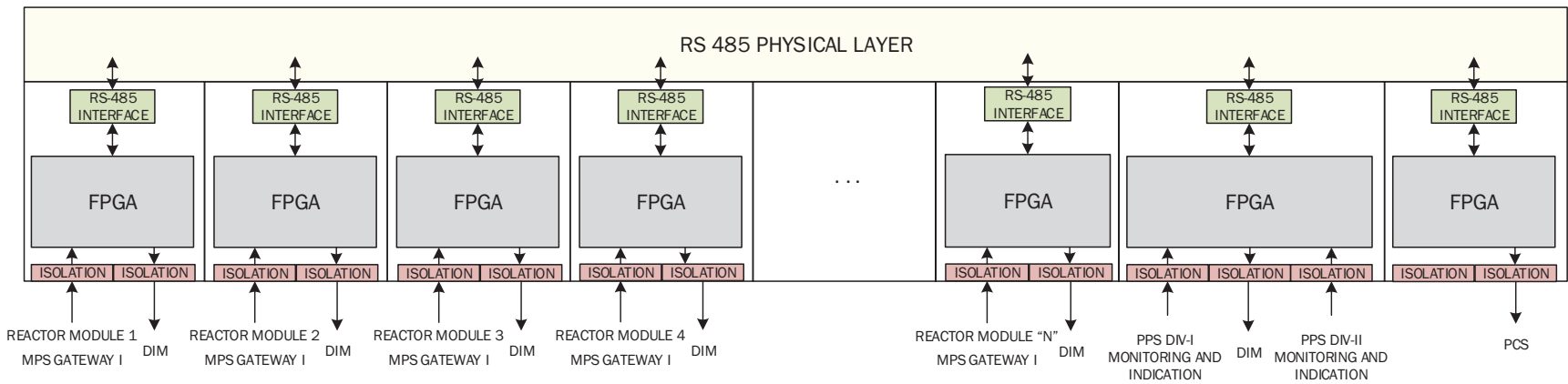


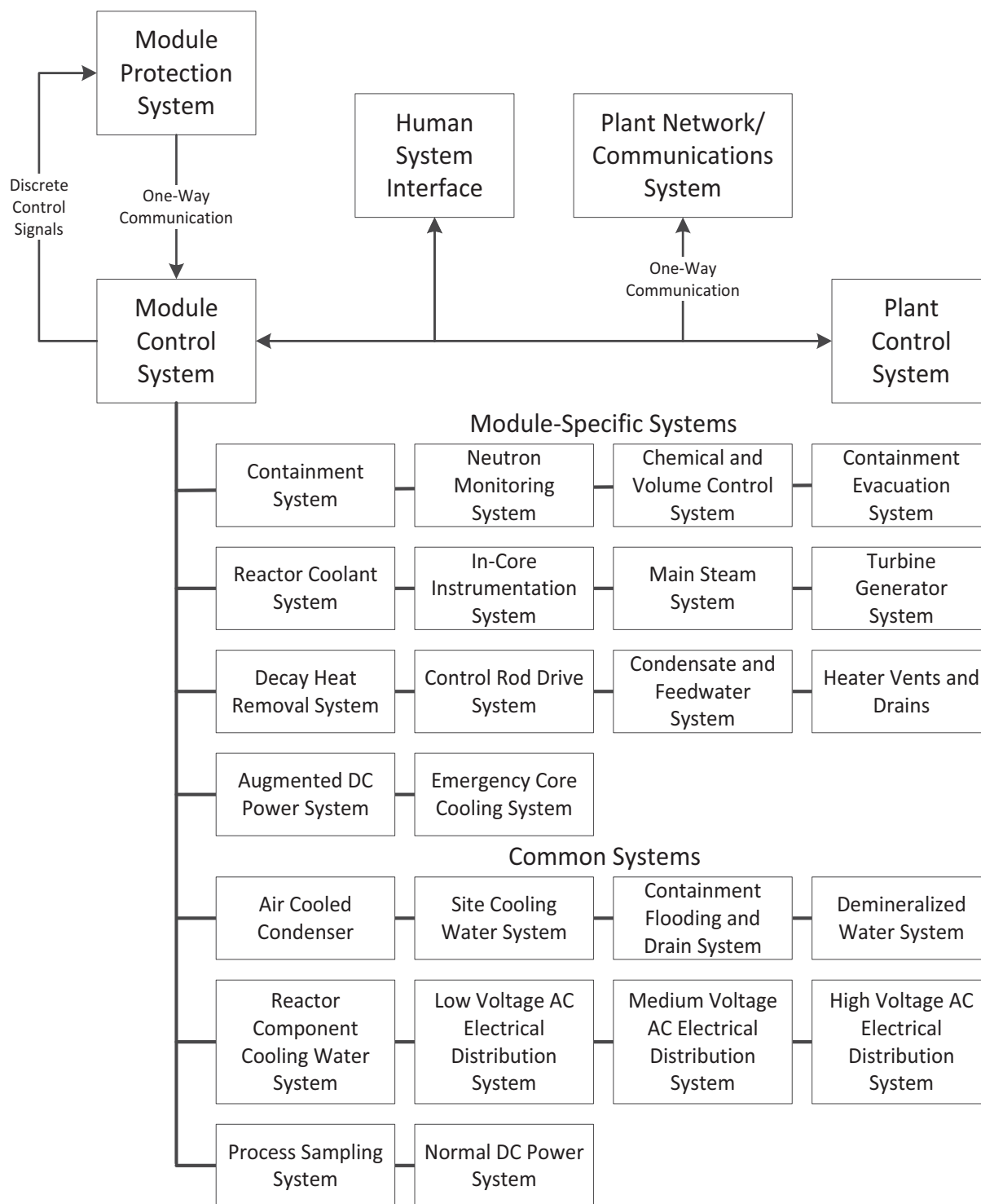
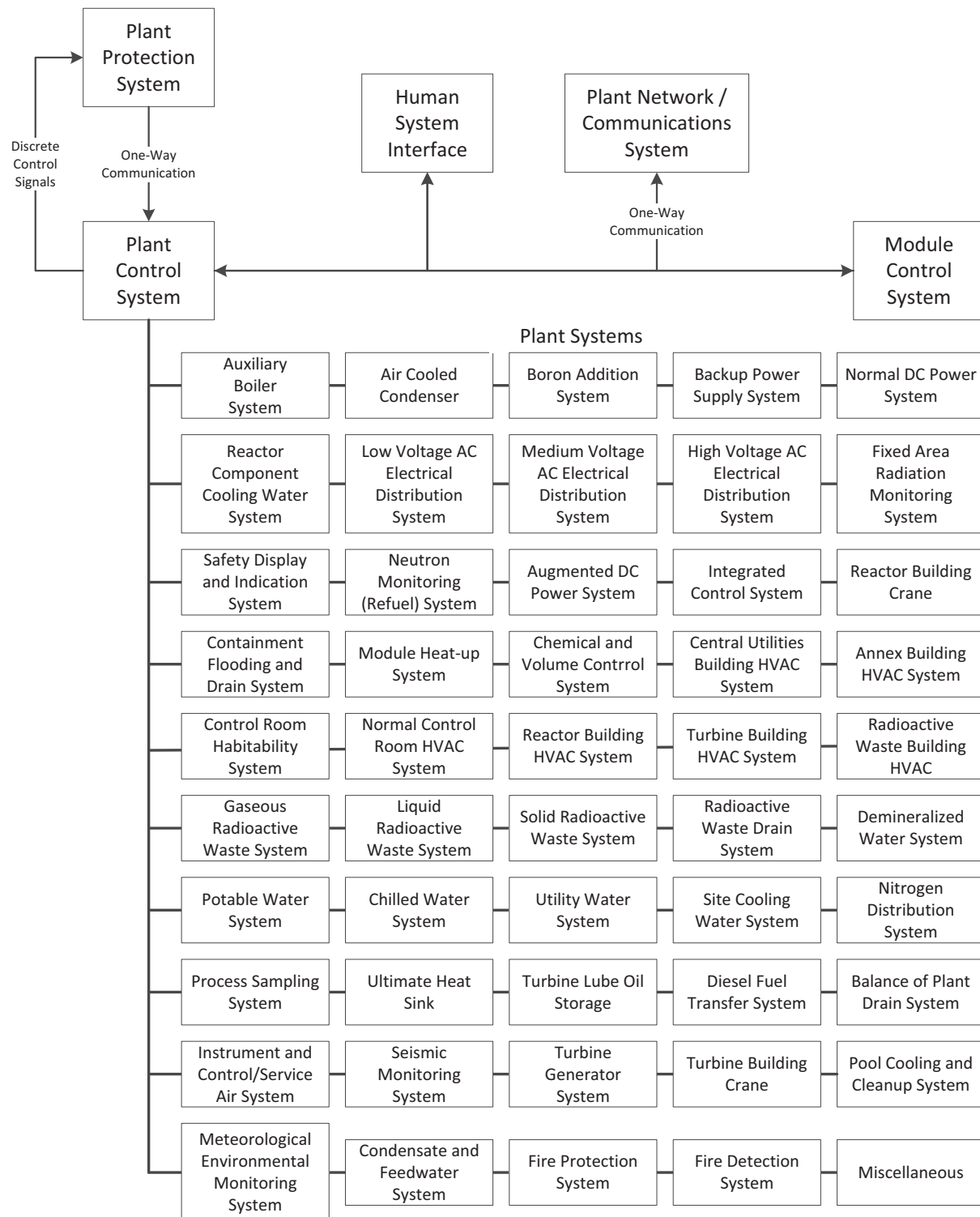
Figure 7.0-14: Module Control System Internal Functions and External Interfaces

Figure 7.0-15: Plant Control System Internal Functions and External Interfaces



7.1 Fundamental Design Principles

The design of safety-related instrumentation and control (I&C) systems is based on four fundamental design principles:

- independence
- redundancy
- predictability and repeatability
- diversity and defense-in-depth (D3)

Section 7.1.1 describes the safety-related I&C system design bases and additional design considerations.

Section 7.1.2 through Section 7.1.5 describe how the four fundamental design principles are incorporated into the I&C system design. Functional block diagrams showing I&C architectures are provided as part of the system descriptions in Section 7.0.4.

Section 7.1.6 describes common cause failure analysis of I&C systems.

Section 7.1.7 describes the cross-cutting design attribute of simplicity and how it is incorporated into the design of safety-related I&C systems.

Section 7.1.8 describes how hazard analyses have been used to examine the safety-related I&C systems, subsystems, and components to identify unintended or unwanted I&C system operation that could adversely affect required safety-related functions.

7.1.1 Design Bases and Additional Design Considerations

The safety-related module protection system (MPS) uses the highly integrated protection system (HIPS) platform described in topical report TR-1015-18653-P-A (Reference 7.1-1). This topical report describes the HIPS platform and demonstrates conformance to NRC Regulatory Guides (RGs) and Institute of Electrical and Electronics Engineers (IEEE) standards applicable to safety-related I&C applications. Specifically, the HIPS platform conforms to RG 1.153, which endorses IEEE Std 603-1991 (Reference 7.1-2) and the correction sheet dated January 30, 1995.

Because the HIPS platform uses programmable digital devices, the following were also used for the HIPS platform design:

- RG 1.152
- IEEE Std 7-4.3.2-2003 (Reference 7.1-3)
- Digital I&C Interim Staff Guidance 04 (DI&C ISG-04)
- Staff Requirements Memorandum for SECY-93-087

The information in this section satisfies the application-specific information requirements in TR-1015-18653-P-A listed in Table 7.0-2 for application-specific action item (ASAI) numbers 1, 3, 4, 5, and 6.

7.1.1.1 Design Bases

This section identifies regulatory requirements that govern the I&C system design.

Consistent with General Design Criterion (GDC) 1, I&C systems are designed to the Quality Assurance Program (QAP) described in Section 7.1.1, Section 7.1.2, and Section 17.5. The quality and safety classifications of Seismic Category I and pressure-retaining structures, systems, and components (SSC) are identified in Section 3.2.

Consistent with GDC 2, the SSC required to function during natural phenomena events are located within structures that protect them against natural phenomena (Section 7.2.2).

Consistent with GDC 4, the I&C systems are designed for environmental conditions associated with normal operation, maintenance, testing, and postulated accidents to which they may be subjected and required to function in (Section 7.2.2).

Consistent with GDC 5, the MPS, neutron monitoring system (NMS), module control system (MCS) and in-core instrumentation system (ICIS) are not shared among NuScale Power Modules (NPMs). The plant control system (PCS) and plant protection system (PPS) monitor parameters common to NPMs and are designed to not adversely affect the ability of I&C systems that perform safety-related functions (Section 7.2.11).

Consistent with GDC 10, the MPS provides the reactor trip and engineered safety features (ESF) actuations based on analytical limits with appropriate margin to ensure specified acceptable fuel design limits are not exceeded during conditions of normal operation, including the effects of anticipated operational occurrences (AOOs). The MPS also monitors NPM variables and provides signals to the MCS and SDIS for control and indication. The NMS monitors and provides neutron flux levels to the MPS.

Consistent with GDC 13, the I&C systems monitor variables and systems over their anticipated ranges for normal operations, AOOs, and accident conditions to ensure adequate safety (Section 7.1.2, Section 7.1.4, Section 7.1.5, Section 7.2.7, and Section 7.2.13).

Consistent with GDC 15, the MPS and NMS provide appropriate controls to the NPM and initiate safety-related functions with sufficient margin to ensure the design conditions of the reactor coolant pressure boundary (RCPB) are not exceeded during normal operations or as a result of an AOO.

Consistent with GDC 16, the MPS initiates containment isolation and safety-related functions to ensure containment design conditions are not exceeded for the duration of a postulated accident. In addition, the MPS removes power to the secondary main steam isolation valves (MSIVs) and the main feedwater regulating valve upon decay heat removal system (DHRS) actuation, providing a backup containment isolation function.

Consistent with principal design criterion (PDC) 19, the I&C systems are designed to ensure the ability to control each NPM during normal and accident conditions. The main control room (MCR) is designed with the ability to place the reactors in safe shutdown in case of a fire requiring an MCR evacuation and for safe shutdown to be maintained without operator action thereafter. Before evacuating the MCR, operators trip the reactors, initiate decay heat removal, and initiate containment isolation. These actions result in passive cooling that achieves safe shutdown of the reactors. Operators can also achieve safe shutdown of the reactors from outside the MCR in the I&C equipment rooms within the Reactor Building (RXB). Following shutdown and initiation of passive cooling from either the MCR or the I&C equipment rooms, the design does not rely on operator action, instrumentation, or controls outside the MCR to maintain the safe shutdown condition. There are no remote displays, alarms, or controls necessary to monitor or maintain the modules in a safe shutdown condition.

Consistent with GDC 20, the MPS, with inputs from the NMS, senses when specified parameters are exceeded and initiates reactor trips and ESF actuations to ensure specified fuel design limits are not exceeded as a result of AOOs, and to sense accident conditions to initiate the operation of appropriate systems and components (Section 7.2.7).

Consistent with GDC 21, MPS and NMS have sufficient redundancy and independence to ensure no single failure results in the loss of the protection function. Individual MPS and NMS components can be removed from service without loss of protection functions to permit periodic testing during operation, including the capability to test channels independently to determine failures and losses of redundancy that may have occurred (Section 7.1.2, Section 7.1.3, Section 7.1.4, and Section 7.2.15).

Consistent with GDC 22, the MPS and NMS have sufficient functional diversity and component diversity to prevent loss of a protection function during operations, maintenance, testing, and postulated accidents, and to withstand the effects of natural phenomena (Section 7.1.5).

Consistent with GDC 23, the MPS has sufficient functional diversity to prevent the loss of a protection function, to fail into a safe state or into a state demonstrated to be acceptable if conditions such as disconnection of the system, loss of power, or postulated adverse environments are experienced.

Consistent with GDC 24, the MPS has physical, electrical, communication, and functional independence within the system and from associated nonsafety-related systems and components. The MPS has sufficient separation of the protection and the control systems to satisfy reliability, redundancy, and independence requirements even with a component or channel failed or removed from service (Section 7.1.2, Section 7.1.3, and Section 7.1.5).

Consistent with GDC 25, the MPS initiates reactor trip functions to ensure specified fuel design limits are not exceeded for a single malfunction of the reactivity control system (Section 4.6.2).

Consistent with GDC 29, the MPS and NMS are designed with redundancy and diversity to ensure a high probability their safety-related functions are performed in the event of AOOs (Section 7.1.3).

Consistent with GDC 64, the MCS and PCS monitor radioactivity releases, the reactor containment atmosphere, and plant environments for radioactivity that may be released from normal operations, AOOs, and postulated accidents.

Consistent with 10 CFR 52.137(a)(2), the design of the I&C systems and auxiliary features of the I&C system design are discussed in Section 7.0.4 and Section 7.2.8, respectively.

Consistent with 10 CFR 50.34(f)(2)(iv), the I&C systems provide the capability to display key plant variables over their anticipated ranges for normal operation, AOOs, and accident conditions (Section 7.2.13).

Consistent with 10 CFR 50.34(f)(2)(v), the MCS provides bypassed and operable status indication of safety systems in the MCR (Section 7.2.4 and Section 7.2.13).

Consistent with 10 CFR 50.34(f)(2)(xi), the displays in the MCR indicate reactor safety valve position (Section 7.2.13).

Consistent with 10 CFR 50.34(f)(2)(xiv)(C), the MPS initiates containment isolation and ensures isolation valves do not re-open upon isolation signal reset (Section 7.1.5 and Section 7.2.3.3).

Consistent with 10 CFR 50.34(f)(2)(xvii), I&C systems are designed to display appropriate variables in the MCR for monitoring specified containment variables and site radioactive gaseous effluents from potential accident releases. The design supports an exemption from the hydrogen monitoring requirement of 10 CFR 50.34(f)(2)(xvii)(C).

Consistent with 10 CFR 50.34(f)(2)(xviii), the I&C systems provide MCR indications of inadequate core cooling (Section 7.2.13).

Consistent with 10 CFR 50.34(f)(2)(xix), the I&C systems provide instrumentation for monitoring plant conditions following an accident, including potential core damage (Section 7.2.13).

Consistent with 10 CFR 50.36(c)(1)(ii)(A), the MPS initiates automatic protective actions before exceeding a safety limit (Section 7.2.7).

Consistent with 10 CFR 50.36(c)(3), the I&C systems meet surveillance requirements to ensure the necessary quality of SSC is maintained such that operation is within safety limits and limiting conditions of operations are met (Section 7.2.7 and Section 7.2.15).

Consistent with 10 CFR 50.49, the I&C equipment that performs the functions in 10 CFR 50.49(b) remains functional during and following design-basis events (DBEs) (Section 7.2.2).

Consistent with 10 CFR 50.54(jj) and 10 CFR 50.55(i), I&C systems are designed, tested, and inspected to quality standards commensurate with the safety function to be performed (Section 7.2.1).

Consistent with 10 CFR 50.55a(h), the MPS and NMS meet the requirements for protection systems and safety systems in accordance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995, as described in Section 7.1 and Section 7.2.

As described in Table 1.9-5, the design supports an exemption from the power supply requirements for pressurizer level indication included in 10 CFR 50.34(f)(2)(xx).

An anticipated transient without scram is considered in the design of I&C systems as it relates to the design provisions of 10 CFR 50.62(c)(1). The design meets the intent of 10 CFR 50.62 by demonstrating the redundancy and diversity of the MPS design, which avoids common cause failures and reduces the probability of a failure to scram (Section 15.8).

Therefore, the design supports an exemption from the portion of 10 CFR 50.62(c)(1) requiring diverse equipment to initiate a turbine trip under conditions indicative of an anticipated transient without scram. The portion of 10 CFR 50.62(c)(1) requiring diverse and automatic auxiliary feedwater system initiation is not applicable to the design.

7.1.1.2 Additional Design Considerations

7.1.1.2.1 Protection Systems

The protection systems facilitate protective actions of the MPS (i.e., reactor trip and ESF functions) in response to monitored variables exceeding pre-established setpoints. Table 7.1-1 identifies specific DBEs for which MPS protective actions are credited in Chapter 15 analyses. The DBEs, including AOOs, infrequent events, and postulated accidents for the design are listed in Table 15.0-1. The MPS functional logic diagrams are shown in Figure 7.1-1a through Figure 7.1-1al.

Table 7.1-2 identifies the specific NPM variables that provide input to the MPS and includes the instrument range for covering normal, abnormal, and accident conditions, and the nominal operating value at 100 percent rated thermal power (RTP).

The NMS-excore subsystem monitors the continuous reactor neutron flux from shutdown to full-rated power using the source range, intermediate range, and power range.

Some monitored variables are relied upon to execute protective actions when setpoints based on the analytical limits are exceeded. The analytical limits and permissive conditions for operating bypasses are summarized in Table 7.1-3 and Table 7.1-5 for the reactor trip system (RTS) and Table 7.1-4 and

Table 7.1-5 for the engineered safety features actuation system (ESFAS). Table 7.1-5 provides additional information on the MPS interlocks and permissives. The NMS provides safety-related input to the MPS to support its functions.

The ESFAS delays assumed in the plant safety analysis are a combination of sensor response time, MPS timing budget allocation, and actuation device delays. The sensor response delays are defined in Table 7.1-6. The delay times in Table 7.1-6 associated with ESFAS signals do not include the delay times associated with the actuation device (e.g., valve stroke times) except opening the pressurizer heater breakers.

There are manual trip or actuate switches for each automatic trip or actuate function in the MCR. The manual actuation for the pressurizer line isolation function is accomplished using the manual chemical and volume control system isolation actuation switches. These switches are connected to the hard-wired modules (HWMs) in the RTS and ESFAS chassis where the signals are isolated and converted to logic-level signals and placed on the backplane. These signals are provided to the associated equipment interface module (EIM) actuation priority logic circuits downstream of the field programmable gate array (FPGA) programmable logic.

Variables monitored by the MPS listed in Table 7.1-2 are sent to the safety display and indication system (SDIS) and the MCS to be displayed in the MCR as required by those systems. These variables include those needed for reactor trip and ESF actuations, and post-accident monitoring (PAM) variables. When allowed by plant procedures to reconfigure systems after a reactor trip or an ESF actuation, the components can be repositioned using the nonsafety-related MCS when the enable nonsafety control switch is activated and no automatic or manual safety actuation signal is present.

Required protective actions by the MPS are automatic. There are no credited manual actuations required for the MPS to accomplish its safety functions; however, manual initiation at the division level of the automatically initiated protective actions is provided in the MCR. The MCR environmental conditions during manual operation are described in Section 9.4.1.

Each MPS and NMS variable used to initiate a protective action is monitored by four independent separation groups, with one or more sensors in each separation group. The separation of redundant sensors creates a potential for spatial dependence for some variables as discussed below.

The physical separation of redundant MPS pressure and level sensors is not a spatial dependence concern. Pressure and level are distributed within the vessel or pipe so that redundant sensors do not see varying process conditions as a function of location.

The location of NMS redundant neutron flux detectors in separate quadrants of the NPM during operation does not result in spatial dependence concerns because of core radial symmetry.

The reactor coolant system (RCS) temperature is measured by resistance temperature detectors (RTDs) located in thermowells on the side of the reactor pressure vessel (RPV).

The RCS narrow range T_{hot} is measured by one RTD in each MPS separation group. One RTD separation group is located in each RPV quadrant at the top of the downcomer.

The RCS narrow range T_{cold} is measured by one RTD in each MPS separation group. One RTD separation group is located in each RPV quadrant in the lower downcomer.

The RCS flow is measured by four sets of digital-based flow transducers mounted in the RPV wall in the downcomer region, one set in each MPS separation group. Each of the four redundant sets of transducers are located in a separate quadrant of the RPV. Reactor coolant flow is expected to be thoroughly mixed as it passes through the SG tube region of the downcomer, so that radial flow variations among RPV quadrants are negligible.

Each NPM contains two steam headers. Main steam temperature is measured by four RTDs in each steamline, one per separation group, for a total of eight. The measurement of main steam temperature is not spatially dependent because the RTDs are located in the same section of vertical pipe where steam flow is uniform.

The MPS and NMS are designed to operate during normal, abnormal, AOO, infrequent events, and accident conditions for a minimum of 72 hours during a loss of alternating current (AC) power. The MPS operates in PAM-only mode after a loss of AC power for 24 hours. These systems are designed to function during a loss of heating ventilation and air conditioning (HVAC). Protection from natural phenomena is provided by the location of the MPS and NMS cabinets in the RXB, which is a Seismic Category I, reinforced concrete structure. Separation Groups A and C and Division I equipment, and Separation Groups B and D and Division II equipment are in different rooms in the RXB and protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids that may result from equipment failures, and from events and conditions outside the nuclear power plant.

The MPS and NMS rack-mounted equipment is installed in a mild environment. The I&C equipment rooms provide an environment that would at no time be more severe than the environment that would occur during normal plant operation, including AOOs. The environmental qualification requirements for the MPS and NMS rack-mounted equipment are identified in Section 3.11.

A failure modes and effects analysis (FMEA) is conducted for both the MPS and the NMS. This is a systematic procedure for addressing failures for components of a system and for evaluating the consequences. The essential function of an FMEA is to consider each part of the system, how it may fail,

and what the effect of the failure on the system would be in the presence of a single failure.

There are no failure modes that are undetectable or would prevent

- the MPS from performing its RTS and ESFAS functions
- the NMS from performing its safety functions
- accident monitoring functions

The MPS automatically initiates a reactor trip or ESF function when the associated setpoint is exceeded. Once initiated, safety functions continue until completed. The completion of the safety function is satisfied once equipment is in the actuated position and the plant conditions are stabilized. The MPS can be returned to normal when the initiating condition is no longer present. Deliberate and separate operator action is required to return the MPS to a normal configuration as described in Section 7.2.3.3. The NMS does not initiate a protective function; it only provides safety-related input to the MPS.

The MPS and NMS do not contain protective provisions that could prevent either system from accomplishing its safety function.

7.1.1.2.2 Post-Accident Monitoring

Post-accident monitoring is a nonsafety-related function. The PAM instrumentation includes the required functions, range, and accuracy for each variable monitored. The selection of each type of variable follows the guidance provided in IEEE Std 497-2016 "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations" (Reference 7.1-6), as modified by RG 1.97.

Variables and their type classification are based on their accident management function as identified in abnormal operating procedures, emergency operating procedures, and emergency procedure guidelines. Because the abnormal and emergency operating procedures and guidelines have not been developed, NuScale developed an approach to identify PAM variables as described below.

The approach and basis for identification and categorization of the variables listed in Table 7.1-7 is:

- review of systems with radiation monitoring equipment and potential effluent release paths.
- operator actions assumed in the probabilistic risk assessment (PRA) (Section 19.1).
- operator actions identified during human factors engineering (HFE) task analysis (Section 18.4).
- industry operating experience.
- engineering judgment.

- the identification process and its results reviewed by a multidisciplinary group (Section 7.2.13.2).

The PAM Type B, C, D, E, and F variables are summarized in Table 7.1-7. Figure 7.1-2 shows the system on which the PAM variable is displayed and the power supplies for each PAM variable. The associated system that processes the sensor input is also provided in Table 7.1-7 and Figure 7.1-2. The reactor design has no Type A variables because there are no operator actions credited in any Chapter 15 anticipated operational occurrences, infrequent events, or postulated accidents, nor the station blackout or ATWS analysis.

The only important human actions modeled in the PRA are in response to multiple failures of automatic safety systems and the actions are not required to meet the assumptions of an accident analysis licensing basis.

Type B Variables

Type B variables provide primary information to the control room operators to assess the critical safety functions that have been defined for the plant. These are accomplishing or maintaining the following three critical safety functions selected based on plant design:

- reactivity control
- remove fuel assembly heat
- containment integrity

The critical safety function for containment integrity has been modified to include the aspects of radioactive effluent control. The “remove fuel assembly heat” critical safety function includes the aspects of RCS integrity. This is because of the integral nature of emergency core cooling system (ECCS) and RCS integrity. Actuating ECCS opens valves to allow steam release to the containment and return of water back to the RCS to maintain core cooling and protect the fuel clad fission product barrier. ECCS is automatically actuated when there is a loss of RCS integrity.

The Type B variables identified in Table 7.1-7 are those necessary to implement the plant abnormal operating procedures, emergency operating procedures, and functional restoration procedures, and to maintain the plant critical safety functions described below.

Reactivity Control Safety Function Variables

The Type B variables that provide direct indication and are used to assess the process of accomplishing or maintaining reactivity control are neutron flux and core exit temperature.

Remove Fuel Assembly Heat Critical Safety Function Variables

The Type B variables selected that provide direct indication and are used to assess the process of accomplishing or maintaining the combined remove fuel assembly heat and RCS integrity critical safety functions are core exit temperature, RPV riser water level, wide range RCS pressure, and wide-range RCS hot temperature.

Maintain Containment Integrity Critical Safety Function Variables

Maintain containment integrity is both a critical safety function and a fission product barrier (Containment) that serves as the primary means to control radioactive effluent releases. The same variables used to provide direct indication and support the containment integrity critical safety function are wide range containment pressure, containment isolation valve position, RPV riser level, and inside the bioshield area radiation level.

Type C Variables

Type C variables identified in Table 7.1-7 provide primary information to the control room operators to indicate the potential for breach or the actual breach of fission product barriers: fuel cladding, reactor coolant system, and containment pressure boundary.

These variables are a minimum set of plant variables that provide the most direct indication of the integrity of the three fission product barriers and provide the capability for monitoring beyond the design limits (extended range).

Fuel Cladding Fission Product Barrier Variables

Core exit temperature and inside the bioshield radiation level are the variables related to monitoring of the fuel cladding fission product barrier. Core exit temperature is the most direct measure of the thermodynamic state of the core; it is used to infer when fuel clad damage is occurring. The inside bioshield area radiation monitor is the primary method used to assess the extent of the fuel cladding breach and to identify fuel cladding breaches.

Reactor Coolant System Fission Product Barrier Variables

The primary variables used to assess the status of the RCS fission product barrier are the RPV riser level and wide range RCS pressure. The RPV riser level can show a loss of boundary through a loss of inventory, resulting in a reduced level. Wide-range RCS pressure is used to assess challenges to the barrier from overpressure and as an alternate variable to RPV riser level for primary assessment.

Containment Fission Product Barrier Variables

Containment is both a critical safety function (containment integrity) and a fission product barrier that serves to control effluent releases. The same

variables identified for the containment integrity critical safety function are also used to support the containment fission product barrier monitoring: wide-range containment pressure, and containment isolation valve position.

Type D Variables

The Type D variables identified in Table 7.1-7 are required in procedures and licensing basis documentation to perform the following:

- indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of DBEs.
- indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
- verify safety system status.

The Type D variables listed in Table 7.1-7 are based upon the plant accident analysis licensing basis and those necessary to implement the plant abnormal operating procedures, emergency operating procedures, and functional restoration procedures.

Type E Variables

Type E variables listed in Table 7.1-7 are used in determining the magnitude of the release of radioactive materials and continually assessing such releases. The variable identification was made on the following criteria:

- Variables identified and related to pathways for release of radioactive material.
- Variables identified and related to environmental conditions used to determine the impact of radiological releases.
- Variables identified and related to the control room and plant areas where access may be required for plant recovery.
- Variables identified and related to monitoring magnitude of releases.
- Variables identified and related to monitoring radiation levels and radioactivity in the plant environs (e.g., boundary environs radiation).

Type F Variables

Type F variables provide primary information to accident management personnel to indicate fuel damage and the effects of fuel damage.

The Type F variables identified and listed in Table 7.1-7 are based upon the plant accident analysis licensing basis and those necessary to implement the plant abnormal operating procedures, emergency operating procedures, and functional restoration procedures.

7.1.1.2.3 Alternate Operator Workstation Controls and Monitoring

If the MCR is evacuated, the alternate operator work stations located at various locations provide confirmation for the operators to monitor the NPMs in a safe shutdown condition with DHRS in service for each NPM. The alternate operator workstations provide D3 capability to monitor the plant from outside the MCR and control balance of plant equipment to support asset protection and long-term plant recovery in case the MCR becomes uninhabitable. An MCR evacuation occurrence is a special event and is not postulated to occur simultaneously with a DBE; it does not cause fuel damage or result in consequential loss of function of the RCPB or primary containment barriers.

The control room habitability system is designed to allow continuous occupancy in the MCR during radiation, hazardous chemical, or hazardous gas release (Section 6.4). In addition, the MCR is protected in case of a security event.

Events for which operators are assumed to evacuate the MCR include fire in the MCR and loss of the Control Building as part of a loss of a large area.

At the onset of an MCR evacuation, the operators trip the reactors, and initiate decay heat removal and containment isolation for each reactor before leaving the MCR. Following evacuation of the MCR, the ability to isolate the MPS manual switches to prevent spurious actuations is provided outside the MCR. An alarm is annunciated in the MCR when the MCR hard-wired switches are isolated using the MCR isolation switches (Figure 7.1-1j).

The MPS manual isolation switches are mounted in a Seismic Category I enclosure to allow them to remain functional following an earthquake. Controls are available outside the MCR in the associated I&C equipment rooms that provide the capability to trip the reactors, to initiate DHRS, and to initiate containment isolation, which initiates passive cooling, and places and maintains the NPMs in safe shutdown. The alternate operator workstations provide nonsafety-related human-system interfaces (HSIs) and direct readings of process variables that allow operators to monitor the NPMs.

The alternative shutdown capability is independent of specific fire areas and accommodates post-fire conditions when offsite power is available and when offsite power is not available for 72 hours, dependent on the conditions described in the fire hazards analysis as described in Appendix 9A.

7.1.1.2.4 Safety Display and Indication System

The SDIS described in Section 7.0.4.4 provides HSI for the MPS and PPS to monitor and display PAM variables and status information. The SDIS is a nonsafety-related system. The SDIS is designed to meet augmented requirements in accordance with RG 1.97 for accident monitoring instrumentation.

7.1.1.2.5 Plant Protection System

The PPS described in Section 7.0.4.3 provides monitoring and control of common plant systems. The PPS is a nonsafety-related system. The PPS is designed to meet augmented requirements in accordance with RG 1.97 for accident monitoring instrumentation.

The variables monitored by the PPS are sent to the SDIS and the PCS to be displayed in the MCR as required by those systems.

7.1.1.2.6 Module Control System

The MCS described in Section 7.0.4.5 is a nonsafety-related control system that provides monitoring and control of NPM-specific components, including manual controls and HSIs necessary for operator interaction. The MCS is designed to meet augmented requirements in accordance with RG 1.97 for accident monitoring instrumentation.

7.1.1.2.7 Plant Control System

The PCS described in Section 7.0.4.6 is a nonsafety-related control system that provides monitoring and control of plant system components, including manual controls and HSIs necessary for operator interaction. The PCS is designed to meet augmented requirements in accordance with RG 1.97 for accident monitoring instrumentation.

7.1.1.2.8 In-Core Instrumentation System

The ICIS described in Section 7.0.4.7 is a nonsafety-related system (with the exception of containment pressure boundary and RCPB functions) that monitors neutron flux distribution and core temperature. The ICIS is designed to the augmented quality requirements of RG 1.97, including Seismic Category I. The ICIS stringer assembly provides safety-related functions to ensure the integrity of the primary containment pressure boundary and the RCPB are maintained where the instrument assembly penetrates the containment vessel (CNV) and RPV pressure boundaries, respectively. The SSC associated with maintaining the RCPB and primary containment pressure boundary that perform safety-related functions meet the quality assurance requirements of 10 CFR 50 Appendix B in accordance with the QAP.

7.1.2 Independence

The physical, electrical, communications, and functional independence attributes of the I&C systems are discussed in this section.

The independence design principles for the I&C systems meet the criteria for independence in IEEE Std 603-1991, Section 5.6 and GDC 13, 21, 22, and 24, as described in this section. The systems that perform PAM functions for Type B and C variables include the MPS and SDIS, which are designed to meet the criteria for

independence in IEEE Std 497-2016, as endorsed by RG 1.97, with the exception that physical and electrical independence is designed to meet the guidance in RG 1.75.

The physical and electrical independence attributes of the MPS and NMS meet the guidance in RG 1.75, which endorses IEEE Std 384-1992 "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 7.1-7).

The communication independence attributes of the MPS meet the guidance in RG 1.152 Rev. 3, which endorses IEEE Std 7-4.3.2-2003.

The information in this section satisfies the application-specific information requirements in TR-1015-18653-P-A listed in Table 7.0-2 for ASAI numbers 8, 9, 20, 22, 23, 46, 52, 53, 55, 60, and 61.

7.1.2.1 Physical Independence

The MPS structures, systems, and components that comprise a separation group or division are independent and physically separated to retain the capability of performing required safety functions during and following a DBE.

Separation group and division independence is maintained throughout the system, extending from the sensor to the devices actuating the protective function. Physical separation provides independence between redundant sensors. Wiring for redundant divisions uses physical separation and isolation to provide independence of the circuits. Separation of wiring is achieved using separate wireways and cable trays. Separate power feeds energize redundant protection divisions. The MPS Separation Groups A, C, and Division I equipment are located in I&C equipment rooms on a different elevation of the RXB than Separation Groups B, D, and Division II equipment (Figure 1.2-11 and Figure 1.2-12, respectively). The I&C equipment rooms are seismically qualified and located in separate fire zones. Division I MPS and NMS equipment are located in a different room than Division II MPS and NMS equipment.

The NMS separation groups are physically independent and separate. The NMS-excore neutron detectors are installed 90 degrees equidistant around the NPM, and the associated cabling is routed in physically separate cable trays and raceways. The NMS hardware and signal processing equipment associated with the MPS divisions is installed in separate I&C equipment rooms. The NMS Separation Group A and C signal processing equipment is located in the I&C equipment room with MPS Separation Group A, C and Division I (Figure 1.2-11), and NMS Separation Group B and D signal processing equipment is located in the I&C equipment room with MPS Separation Groups B, D, and Division II (Figure 1.2-12).

The SDIS has two separate and independent hubs located in the Control Building (Figure 1.2-18) in the same divisionally separate rooms as the PPS.

Safety-related and nonsafety-related SSC are physically separated in accordance with NuScale electrical design guidelines and meet the criteria established in IEEE Std 384-1992, which is endorsed by RG 1.75 Rev. 3.

7.1.2.2 Electrical Independence

The MPS electrical isolation devices used as a safety system boundary are considered part of the MPS and are qualified in accordance with IEEE Std 384-1992. The isolation devices are tested to confirm credible failures on the nonsafety side of the isolation device do not prevent MPS from performing its safety function.

Electrical isolation between the safety-related MPS and associated nonsafety-related systems is provided by the following devices (Figure 7.0-2):

- Nonsafety-related sensor inputs. The safety function module (SFM) provides Class 1E isolation by galvanic isolation between the nonsafety sensors inputs to the MPS. Section 4.2 of TR-1015-18653-P-A provides additional information.
- Safety-related to nonsafety-related communication interface. Communication to nonsafety-related systems is provided through transmit-only or receive-only fiber optic ports. These ports provide Class 1E electrical isolation for either receive or transmit data through uni-directional communication links. The monitoring and indication bus (MIB) communications module provides Class 1E isolation from the safety-related MPS to nonsafety-related MCS by using four copper-to-fiber optic ports on the device. Three of the copper-to-fiber data ports for the MIB communications module in the separation groups and the RTS and ESFAS Divisions are configured for transmit-only and send information to the MCS, the Division I MPS gateway, and the Division II MPS gateway. The remaining copper-to-fiber data port on the separation group MIB communications module is configured as receive-only and receives information from the maintenance workstation (MWS) through a temporary cable that is connected during maintenance activities.
- Hard-wired inputs to MPS. The HWM receives signals from the manual switches in the MCR; from the discrete, hard-wired, nonsafety-related control signals from MCS; and from the trip/bypass switch panels. The HWM is constructed of discrete logic components only; there are no programmable devices. The HWM provides direct current (DC)-to-DC and galvanic isolation between the safety-related MPS and nonsafety-related MCS.
- Electrical power supply. The MPS receives electrical power from the nonsafety-related, augmented DC power system (EDAS). The MPS provides Class 1E isolation from the nonsafety-related EDAS by using Class 1E isolation devices that are part of the MPS and are used as the safety system boundary (Figure 7.0-2). The DC-to-DC voltage converters are used for Class 1E isolation and protection of the MPS equipment. The DC power sources are redundant and an alarm is generated if one of the redundant supplies fails (Figure 7.0-9).

The NMS separation groups receive isolated, independent power supplied by the EDAS through Class 1E isolation devices that are qualified as part of the NMS.

The PPS, SDIS, ICIS, MCS, and PCS are nonsafety-related SSC and are separated from safety-related SSC in accordance with the NuScale Electrical Design Criteria.

7.1.2.3 Communication Independence

The safety-related MPS architecture uses the communication independence principles described in the design concepts in Section 4 of TR-1015-18653-P-A.

With the exception of interdivisional voting, the communication within the MPS separation group is independent and does not rely on communication from outside the respective separation group or division to perform a safety function. The MPS separation groups perform independent signal conditioning and trip determination and provide that input to the scheduling and bypass module (SBM), which provides inputs to the schedule and voting module (SVM) for the two-out-of-four voting logic.

Permanent MPS communication to nonsafety-related systems is provided by one-way, isolated data communication paths through the MIB. The communication from the safety-related MPS to the nonsafety-related MCS is through the MIB communications module and MPS gateway for each MPS division. The MPS provides communications from a temporary connection using a temporary cable from the nonsafety-related component MWS to an SFM for the purpose of updating tunable parameters. The communication is only allowed when the SFM is taken out of service by placing the out of service switch in the "out of service" position.

The MPS interdivisional communication is performed using point-to-point fiber optic communications through the safety data bus (SDB) connections between the SBM and SVMs.

Independence between safety-related and nonsafety-related systems is maintained by establishing one-way communications from the MPS to the respective nonsafety-related systems. The MPS provides for input and processing of nonsafety-related sensors for the purposes of PAM. Communication independence within the MPS between the safety-related and nonsafety-related sensor data is described in Section 4.2 of TR-1015-18653-P-A.

One-way, isolated communication links are provided from the MPS to the MCS through isolation devices that are components of the MPS. This is accomplished by the MIB communications module within the separation group and RTS and ESFAS division. Isolated communication links between the MPS and the nonsafety-related MWS and SDIS hubs are provided by the MPS gateway. The MPS gateway consolidates the information received from the four separation groups, RTS, and ESFAS, and provides a qualified isolated one-way communication path to the MWS and the SDIS hubs. There are two

nonsafety-related MPS gateway chassis that are qualified as part of the MPS, one for each division of MPS.

The NMS is an analog system with no digital communication protocols; therefore, communications independence in the NMS is maintained by implementing hard-wired connections directly to the MPS.

Independence between the PPS and PCS is maintained by establishing one-way communications from PPS to PCS through isolation devices that are components of the PPS.

7.1.2.4 Functional Independence

Functional independence is a means to achieve isolation between redundant systems.

The safety-related MPS architecture uses the functional independence principles described in the design concepts in Section 4 of TR-1015-18653-P-A. The RTS and ESFAS protective functions listed in Table 7.1-3 and Table 7.1-4 are assigned to a single, separate SFM within the MPS. The MPS separation group components (SFM, SBM, and MIB-CM, and HWM) are functionally independent from the division components (SVM, EIM, MIB Communications Module) and installed in physically separate cabinets providing functional independence between the separation group components and division components.

There are no shared functions between the MPS separation groups or divisions. The MPS separation groups and divisions are self-reliant and have no dependency on functions outside the separation groups or divisions. The MPS communication architecture is isolated between the separation groups and other nonsafety-systems, which supports functional independence.

The MPS maintains functional independence throughout the system using various methods. To support functional independence with the SFM configurations within the MPS there are two rules that are applied.

- First, sensor inputs to the input sub-module (ISM) on an SFM have the same safety classification (i.e., an SFM is configured with all safety-related sensor inputs or all nonsafety-related sensor inputs to keep nonsafety-related sensor inputs on separate SFMs from safety-related inputs).
- Second, for SFMs with multiple inputs, only process variable inputs that are related to the same function are assigned to the same SFM.

To support functional independence in the EIM configurations within the MPS, there are three rules that are applied.

- First, if one of the two groups of field components is used to perform a safety-related function, the other group also performs a safety-related function. This prevents a group that only performs nonsafety-related functions from being actuated by an EIM performing a safety-related function.

- Second, an EIM performs the same actuation on each group of field components regardless of which protective action is demanded. This ensures an EIM performs the same sequence of actuations on all configured outputs; it does not matter which safety function is demanded.
- Third, where the primary group of components has a backup group, the primary and backup groups are actuated by different EIMs. The intent is to keep backup groups separate from primary groups.

Functional independence is maintained throughout the MPS. The safety functions required for the MPS are distributed across SFMs based on the function and classification of their inputs. The SBMs have a separate function of collecting and transmitting trip determination data. The SVMs have a separate function of collecting trip determination data, voting, and initiating protective actions. The allocation of field components to EIMs is based on maintaining functional independence of the safety functions for each EIM.

7.1.3 Redundancy

The redundancy design principle is incorporated into the design of the I&C systems, and conforms to the single-failure criterion in IEEE Std 603-1991, Section 5.1 and the criteria of IEEE Std 497-2016, Section 6.1 for Type B and C PAM variables. The I&C system design also conforms to GDC 21 and 24. Additionally, the redundancy attributes of the safety-related I&C systems are designed to meet the guidance in RG 1.53, which endorses IEEE Std 379-2000 “IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems” (Reference 7.1-4).

The information in this section satisfies the application-specific information requirements in TR-1015-18653-P-A listed in Table 7.0-2 for ASAI numbers 12, 13, 14, 21, and 32.

Redundancy is used to achieve system reliability goals and to demonstrate the safety-related I&C systems can perform the required safety functions during a DBE while also incurring

- single detectable failures within the safety systems concurrent with identifiable but non-detectable failures.
- failures caused by the single failure.
- failures and spurious system actions that cause or are caused by the DBE.

7.1.3.1 Redundancy in Module Protection System Design

The MPS incorporates redundancy into the design as summarized in Section 5 of TR-1015-18653-P-A.

Redundancy within the MPS is achieved by using four separation groups of sensors, detectors, and trip determination, and using two divisions of RTS and ESFAS voting and actuation circuitry.

The MPS uses two-out-of-four voting so that a single failure of an initiation signal or trip determination does not prevent a reactor trip or ESF actuation signal from occurring when required. The two-out-of-four design also ensures a single failure does not cause spurious or inadvertent reactor trips or ESF actuations.

The MPS is designed to eliminate non-detectable failures through a combination of continuous self-testing and periodic surveillance testing. The actuation priority logic is the only portion of the MPS that does not have built-in self-testing capabilities and is periodically tested in accordance with the plant technical specifications (Section 8.2.6 of TR-1015-18653-P-A). This test strategy ensures detectable failures are identified.

The self-test features provide a comprehensive diagnostic system ensuring system status is continually monitored. Detectable failures are identified and an indication of the impact of the failure is provided to determine the overall status of the system. The self-test features maintain separation group and division independence through the use of self-testing circuitry for each separation group and division. A comprehensive discussion of the overall calibration and testing features are provided in Section 8.0 of TR-1015-18653-P-A.

The MPS is designed to allow repair and testing of components while still maintaining the required level of redundancy such that the MPS remains capable of performing its safety function during repair and testing. Section 7.2.4 provides more detail regarding the design of the MPS operating and maintenance bypass functions.

The MPS is evaluated to determine where and how the MPS structures, systems and components could fail, and to assess the impact of the failures on the safe operation of the plant.

The MPS is divided into four groups to evaluate the effect of a single failure. The first group consists of those components in the MPS common to both the RTS and ESFAS. The second group is made up of the associated RTS functions. The third group is analyzed based on the ESFAS functions. The last group analyzes the external communications and supporting functions associated with the MPS.

Group 1 - Common Components:

- separation group analog sensor/detector associated with monitored systems
- separation group SFM - signal conditioning
- separation group SFM - trip determination
- separation group SBM
- divisional SVM
- divisional EIM
- divisional EIM actuation priority logic
- DC-to-DC converter power supply and power distribution components

- low voltage AC electrical distribution system undervoltage - loss of AC power (normally open contact)
- under-the-bioshield temperature sensors

Group 2 - Reactor Trip Functions:

- divisional safety-related manual trip switch
- divisional reactor trip function EIM
- divisional reactor trip breakers (RTBs)
- divisional automatic RTS

Group 3 - Engineered Safety Features Functions:

- divisional safety-related manual actuation switch
- divisional automatic ESFAS
- divisional pressurizer heater breakers
- divisional ECCS timer block switch

Group 4 - External Communication and Supporting Functions:

- MIB communication module (separation group and divisional)
- HWM - trip/bypass switches (only when out of service (OOS) is active)
- HWM - operating bypass switches
- HWM - operating override switches
- SFM - OOS switches
- HWM - enable nonsafety control switches
- MWS
- MPS gateway

Single failures were considered and evaluated for the MPS design. No coincident failures were assumed to occur to the system. Failures related to incorrect transmission of test or calibration information assume a test or calibration was initiated, successfully completed, and communicated as failed. A test or calibration failing and being communicated as successful would only result from two concurrent failures (whatever caused the test or calibration to fail and incorrectly communicating the results as successful). Therefore, the MPS evaluation did not assume failures caused by errors associated with improper tests.

The power supplied to the MPS by the EDAS is monitored by the MPS Class 1E isolation devices. Therefore, failures of the EDAS are bounded by the MPS FMEA portions of the system bounded by the analysis for the Class 1E isolation devices.

There are no single failures or non-detectable failures that can prevent the MPS from performing its required safety functions.

7.1.3.2 Redundancy in the Neutron Monitoring System Design

The NMS consists of four independent, redundant separation groups. A single failure within the independent separation group does not prevent the NMS from performing required safety functions. The separation groups generate NMS signals that are sent to the MPS, and the trip determination and voting logic is then performed within the MPS.

No single failures exist within the NMS that would prevent the NMS from performing its primary safety function. A failure of one channel (separation group) of the NMS still allows the MPS to perform its required safety function because of the two-out-of-four coincidence voting logic used by the MPS. The following NMS components were evaluated to ensure the NMS remains functional in the presence of a single failure:

- NMS-excore detector and integrated mineral insulated cables
- NMS-excore pre-amplifier and soft coaxial cabling
- NMS-excore channel signal processing equipment
- NMS-excore power supply/Class 1E isolation device

7.1.3.3 Redundancy in Nonsafety Instrumentation and Control System Design

The MCS and PCS are designed with redundant control networks as described in Section 7.0.4.5 and Section 7.0.4.6, respectively. The MCS and PCS architectures incorporate redundancy into the nonsafety I&C architecture design at the human machine interface layer, the control network layer, the controllers, and the remote input/output (I/O) network layer. The flow of data is uninterrupted by a single component, cable, or device failure. In addition, process system equipment redundancy is assessed and incorporated as part of the process system design activities and supported by the PCS and MCS through the use of separate I/O modules and signal segregation.

Redundancy for remote monitoring is accomplished by providing redundant MCS and PCS operator workstations for plant monitoring when the MCR is evacuated. When the operators evacuate the MCR, two manual isolation switches for the MPS divisions are provided to isolate the MPS manual actuation switches in the MCR to prevent fires in the MCR from causing spurious actuations of associated equipment.

The PPS consists of two independent and redundant divisions. A single failure within either division does not prevent the PPS from performing required protection functions. The PPS FMEA also considered the effects of cascaded failures expected as a consequence of a single failure. Either of the PPS divisions is capable of accomplishing the PPS functions.

The SDIS receives inputs from the MPS and PPS through communication modules. The SDIS consists of two independent divisions of data paths to the display panels. A single failure within either division does not prevent the SDIS

from performing required functions. Either of the SDIS divisions is capable of accomplishing the SDIS function.

7.1.4 Predictability and Repeatability

Predictability and repeatability design principles for the I&C systems are designed to meet the criteria for system integrity in IEEE Std 603-1991, Section 5.2 and 5.5 and GDC 13, 21, and 29 as described in this section. The information in this section satisfies the application-specific information requirements in TR-1015-18653-P-A listed in Table 7.0-2 for ASAI numbers 19, 56, and 59.

The MPS architecture uses the HIPS platform. This platform is designed to produce the same outputs for a given set of input signals within well-defined response time limits. Section 7.0 of TR-1015-18653-P-A describes how the platform and components function, and provides functional block diagrams to demonstrate how it meets the criteria for predictability and repeatability.

The MPS response time analysis demonstrates the MPS performs and completes its required safety functions in a predictable and repeatable manner. Section 7.7 of TR-1015-18653-P-A describes the calculation used to determine worst-case digital time response for an MPS channel.

The actuation delays assumed in the plant safety analysis are listed in Table 7.1-6. The RTS timing analysis is defined from the point in time when the monitoring process variable exceeds its predetermined setpoint to when the RTBs open. The MPS digital portion of the RTS function is accounted for in the safety analysis. For the RTS protective function, the MPS response time is composed of the analog input delay plus the digital time response delay plus the analog output delay and includes the time for the RTBs to open. The MPS digital time response delay is described in Section 7.7 of TR-1015-18653-P-A.

For the ESFAS protective functions, the actuation delays in Table 7.1-6 are assumed in the plant safety analysis and are defined as the time from when the monitored process variable exceeds the predetermined setpoint until the EIM output is de-energized. The MPS portion of the ESFAS functions is accounted for in the safety analysis. This time allocation budget is composed of the analog input delay plus the digital time response delay plus the analog output delay and is defined from the sensor input to the SFM input terminals to the EIM output command to the final actuation device. For the pressurizer heater trip function, this time requirement includes the time for the pressurizer heater breakers to open.

7.1.5 Diversity and Defense-in-Depth

The use of digital safety-related sensors is limited to the pressurizer level and the RCS flow sensors. The D3 analysis of digital sensor common cause failure (CCF) concludes there is sufficient diversity between Sensor Block I and II to prevent Type 3 failures from affecting all pressurizer level sensors; as such, no coping analysis is needed to address the CCF of the pressurizer level sensors.

A coping analysis was performed to demonstrate a Type 3 failure of the RCS flow sensors concurrent with an AOO or protective action does not result in radiation release exceeding the dose limits or violate the integrity of the primary coolant pressure boundary and the containment. The coping analysis considered complete or partial spurious initiation of protective actions by the MPS. The coping analysis concluded acceptable diversity of MPS is demonstrated without the need for additional functional diversity or operator intervention.

The I&C system design includes features and processes to mitigate a CCF in the MPS because of digital-based failures that could disable a safety function.

The D3 assessment of the I&C design is consistent with the guidelines in NUREG/CR-6303. This assessment focused on the MPS, which is the only safety-related digital I&C system. The assessment is summarized in Section 7.1.5.1.

The D3 coping analysis methodology and results for postulated digital-based CCF vulnerabilities are summarized in Section 7.1.5.2.2. Coping strategies include identification of signals or components unaffected by the postulated CCF that can be used to perform the safety function, different functions that can provide adequate protection, or justification for taking no action based on meeting analytical acceptance criteria without diverse mitigation actuation.

Conformance to the applicable regulatory guidance from the staff requirements memorandum to SECY 93-087 is summarized in Section 7.1.5.3. Section 15.8 provides discussion on anticipated transients without scram.

The information in this section satisfies the application-specific information requirements in TR-1015-18653-P-A listed in Table 7.0-2 for ASAI numbers 6, 9, 10, 11, 62, 63, 64, and 65.

7.1.5.1 Application of NUREG/CR-6303 Guidelines

NUREG/CR-6303 provides an acceptable method for performing a D3 assessment. The following sections describe the application of those guidelines to the D3 of the I&C system design.

7.1.5.1.1 Guideline 1 - Choosing Blocks

An overview and description of the MPS is provided in Section 7.0.4.1.

For the purpose of the MPS defense-in-depth assessment, the blocks identified in Figure 7.1-3 represent a level of detail that simplifies system examination. Blocks have been selected to represent a physical subset of equipment and software whose internal failures can be assumed not to propagate to other blocks based on respective attributes that are discussed in Guideline 2 (Section 7.1.5.1.2).

Nonsafety Monitoring and Indication Block

The Nonsafety Monitoring and Indication block represents the soft controls and digital displays available to the operator in the MCR for module-specific systems controlled by the MCS. These displays and controls are used by the operators for day-to-day operations.

These operator workstations exist on a human machine interface network that is separate from the MCS control network, and are a physical subset of equipment and software in the MCS. As a result, internal failures, including the effects of software errors, do not propagate to other equipment or software.

Safety Display and Indication and Manual Controls Blocks

The SDIS and manual controls blocks represent the respective division of SDIS and manual controls available to the operators. As mentioned in Section 7.0.4.4, each division of SDIS receives information from the gateway associated with the respective MPS division. Each gateway contains information from the four separation groups and both MPS divisions of RTS and ESFAS. The SDIS displays are for indication only and do not provide control functionality. Each protective action automatically initiated by MPS can be manually actuated at the division level by safety-related manual switches except the pressurizer line isolation which is a subset of the CVCSI. For example, there is a Division I containment system (CNTS) isolation switch that closes Division I containment isolation valves (CIVs). There is also a Division II CIV switch that closes Division II CIVs. Successful closure of one Division completes the intended safety function.

Safety Blocks

Safety Blocks I and II in Figure 7.1-3 encompass the MPS with the exception of the manual controls in the MCR. Each block represents a different programmable technology. Safety Block I includes Separation Group A and C, and Division I of RTS and ESFAS. Safety Block II includes Separation Group B and D, and Division II of RTS and ESFAS. Figure 7.1-4 provides a visual representation using the MPS architecture overview from Figure 7.0-3; however, for purposes of clarity, some communication lines from the separation groups have been removed.

Because each separation group provides a trip determination status to both divisions of RTS and ESFAS, links between both safety blocks are required. Additionally, information from the safety block is provided to the SDIS blocks.

The safety-related manual controls within the manual controls blocks provide division-level initiation of safety-related components; however, component-level control of these safety-related components requires that control logic within the actuation priority logic of the EIM is enabled by a safety-related switch as described in Section 7.0.4.1. If the operator has enabled this control logic in the actuation priority logic of an EIM and there are

no active manual or automatic actuation signals present, the operator can use MCS to control safety-related components.

Sensor Blocks

Sensor Blocks I and II encompass the sensors used as inputs to the MPS. The inputs to MPS are summarized in Table 7.1-8. For the purpose of the D3 assessment, the evaluation of Sensor Block I and II is focused on digital sensors that have safety-related functions. Variables that are calculated by MPS (e.g., high power range positive rate) are not included as part of the sensor blocks. Analog and discrete sensors are identified for completeness, but they are not considered to be vulnerable to digital-based CCF.

Module Control System

The MCS provides for NPM-specific control of nonsafety-related systems and, with the appropriate permissives, control of safety-related equipment. The MCS block provides information to the operators and receives input from the operators through the Nonsafety Monitoring and Indication block. The MCS block consists of the control network, controllers, remote I/O network, and remote I/O modules.

7.1.5.1.2 Guideline 2 - Determining Diversity

The identification of blocks in the previous section allows for diversity assessment against the following six diversity attributes:

- design diversity
- equipment diversity
- functional diversity
- human diversity
- signal diversity
- software diversity

Two types of diversity assessments were performed: diversity attributes within a block and diversity attributes between blocks.

Diversity Attributes within a Block

Safety Block I or II

Software Diversity

Each safety block is composed of three types of FPGA-based modules: SFMs, communications modules, and EIMs. Because each type of module performs different functions, the logic implementations differ. For example, the logic implemented for trip determination on an SFM is different than the logic implemented for two-out-of-four voting on an SVM.

Design Diversity

Implementation of inter-divisional and intra-divisional communication within a safety block uses design diversity. Inter-divisional communication from SBMs, EIMs, SVMs, and MIB communications module uses copper-to-fiber conversion and one-way communication. Intra-divisional communication between SFM and SBM uses a virtual point-to-point connection with the SBM acting as the bus master and the SFMs operating as slaves on the communication bus. Intra-divisional communication between SVMs and EIMs uses a point-to-multipoint communication protocol that results in SVMs not having to request information from EIMs.

Each EIM implements a digital and discrete method for initiating protective actions. The automatic signal actuation is generated within the digital portion (FPGA) of the EIM. The manual signal actuation originates from the physical switches in the manual controls blocks. In the EIM, both manual and automatic actuation signals are used by the actuation priority logic that is implemented using discrete logic components as described in Section 7.0.4.1 and TR-1015-18653-P-A.

Functional Diversity

The SFMs are configured and programmed for different purposes. The safety function or group of safety functions implemented within an SFM is based on its inputs. For example, one SFM only monitors and makes a trip determination on containment pressure, while another SFM monitors and makes a trip determination on steamline conditions. Some SFMs are not required to perform a trip determination. Instead, these SFMs are used only to provide monitoring information to the SDIS blocks through the separation group MIB communications modules.

Each EIM can control two groups of field components. The EIMs are configured for functions only associated with those groups of components by limiting the number of components that an EIM can control. For example, an EIM may be required to close valves on a CNTS isolation signal while another EIM is dedicated to tripping a breaker on a low pressurizer level signal. Although there are instances where EIMs implement different safety functions, there are EIMs that implement more than one safety function.

Sensor Block I or II

Assessment of diversity within this block is intended to demonstrate how a digital-based CCF of a safety-related sensor would be limited to a single function type.

The safety-related digital sensors from Table 7.1-8 can be grouped into the following function types:

- digital-based level measurements
- digital-based flow measurement

Equipment Diversity

Each function type depends on different physical effects that require unique processing algorithms to obtain the desired variable (e.g., flow, level). Within a sensor block, each function type is based on different designs from different manufacturers.

Design Diversity

The equipment diversity within each sensor block creates inherent design diversity. Each function type is based on a different architecture (i.e., arrangement and connection of components).

Functional Diversity

Each function type is used for a particular function: digital based level and flow sensors are used for these process measurements.

Human Diversity

Within a sensor block, each function type represents sensors from a different design organization (i.e., company).

Software Diversity

Each function type relies on different physical effects that require different algorithms and logic to obtain the desired variable.

Signal Diversity

The equipment diversity within each sensor block creates inherent signal diversity. Each function type represents different process variables sensed by different physical effects.

Division I or II of Safety Display and Indication System

There are no diversity attributes within this block.

Division I or II of Manual Controls

There are no diversity attributes within this block.

Nonsafety Monitoring and Indication Block

There are no diversity attributes within this block.

Module Control System

Functional Diversity

The MCS block provides a degree of functional diversity by segmenting control functions to different controllers or different control environments. For example, the chemical and volume control system (CVCS) control function is separate from the control rod drive system control function.

Diversity Attributes between Blocks

Equipment Diversity

Initiation of protective actions can be done manually by operators using physical switches or done automatically by Safety Block I or II.

Between Safety Block I and II, different FPGA technology is used to achieve equipment diversity. The FPGA equipment diversity in the form of two different FPGA technologies coupled with the different development tools is an effective solution for the digital-based CCF vulnerabilities present in the MPS, as described in TR-1015-18653-P-A. Table 7.1-15 describes the effect of a digital-based CCF across diverse FPGA technologies between each safety block.

Between Sensor Block I and II, there are two sets of digital-based level measurement sensors and each set is from a different design organization (i.e., company). Although the process variable is sensed by the same physical effect, the digital processing electronics from different companies result in different designs. When compared to a digital I&C platform, digital-based level measurement sensors have a simpler and specific function. As a result, equipment diversity is an effective solution for the digital-based CCF vulnerability that may be present in the digital-based level measurement electronics.

Design Diversity

To limit the potential for and the consequences of a digital-based CCF, Safety Block I and Division I SDIS block use a different FPGA chip architecture than Safety Block II and Division II SDIS block. The diverse FPGA technologies have additional design diversity attributes, as described in TR-1015-18653-P-A and summarized in Table 7.1-9.

The MCS block and Nonsafety Monitoring and Indication blocks are based on a programmable technology diverse from Safety Block I and II, and Division I and II SDIS. Along with other attributes discussed below, different hardware designs have different failure modes that reduce the possibility of a digital-based CCF affecting more than one block.

Human Diversity

The use of different I&C platforms creates inherent human diversity between blocks. The SDIS and safety blocks are based on an FPGA platform while the Nonsafety Monitoring and Indication block and MCS block are based on a microprocessor-based or computer-based platform as described in Section 7.0.4.5.

Human diversity is an implicit attribute of the FPGA equipment, chip design, and software tool diversity of the SDIS and safety blocks; however, it is neither explicitly defined nor verified for these blocks.

Similar to the SDIS and sensor blocks, human diversity is an implicit attribute of the digital-based level measurements provided by different companies; however, it is neither explicitly defined nor verified for these blocks.

Software Diversity

Software diversity is a subset of design diversity and is the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals (NUREG/CR-6303).

Because of the design diversity discussed for the FPGA equipment, the use of different programmable technologies results in the use of different design tools that would not introduce the same failure modes.

Functional Diversity

Functional diversity is introduced by having different purposes and functions between blocks.

Safety Blocks I and II form the MPS. These blocks initiate a reactor trip and ESF actuations to mitigate a DBE.

The monitoring and indication blocks allow an operator to monitor and control both safety and nonsafety systems. The operator can maintain a plant within operating limits or initiate necessary protective actions.

The MCS provides automatic control of systems to maintain the plant within operating limits including constraining operational transients.

Sensor Block I and II function to provide process variable information to Safety Block I or II.

Signal Diversity

Between blocks, signal diversity is provided by having automatic and manual means of actuating equipment and protective actions. The MCS and Nonsafety Monitoring and Indication blocks provide control at the

component-level while the manual controls blocks provide control at the division-level.

7.1.5.1.3 Guideline 3 - System Failure Types

Type 2 and 3 system failures as described in NUREG/CR-6303 are considered in Guidelines 10, 11, and 12. Type 1 system failures are considered in Guideline 12.

7.1.5.1.4 Guideline 4 - Echelon Requirement

In order to provide blocks representing a level of detail that simplifies MPS examination, the four conceptual echelons of defense are combined and divided into separate blocks as shown in Figure 7.1-5.

The monitoring and indication echelon consists of five blocks: Division I SDIS, Division I Manual Controls, Division II SDIS, Division II Manual Controls, and Nonsafety Monitoring and Indication.

Separation groups and the divisions of RTS, and ESFAS were grouped into Safety Block I or II according to the programmable technology their modules are based on; however, the RTS and ESFAS echelon span across both safety blocks. Because some separation group SFMs are required for both reactor trip and ESFAS actuation, separation groups are considered to be part of the RTS and ESFAS echelon.

The control system echelon is the MCS block. As described in Section 7.1.5.1.1, the MCS block and the control system echelon represent a subset of the actual MCS. The soft controls and digital displays available to the operator in the MCR are a subset of MCS components; however, they are considered to be part of the monitoring and indication echelon.

7.1.5.1.5 Guideline 5 - Method of Evaluation

Blocks chosen in Guideline 1 are considered as "black boxes" so that a credible failure required to be postulated produces the most detrimental consequence when analyzed in accordance with Guideline 9.

Incredible Failures

The actuation priority logic within the EIMs for both Safety Block I and II are the same; however, the actuation priority logic is composed of discrete logic components and is not considered to be vulnerable to digital-based CCFs. The actuation priority logic within an EIM receives commands from the automatic actuation voting logic and external hard-wired signals as described in Section 7.0.4.1. The actuation priority logic responds to commands from the automatic actuation voting logic whether they are valid or spuriously generated.

The HWM for both Safety Block I and II is the same; however, it is also composed of discrete logic components and not vulnerable to digital-based CCF.

Manual controls provided by Division I and II Manual Controls are physical switches and not vulnerable to digital-based CCF.

When enabled by the operator in the MCR, the Nonsafety Monitoring and Indication block is used for component-level control of safety-related components to permit periodic testing. It is not considered credible to have a CCF of the Nonsafety Monitoring and Indication block at the same time the operator has enabled component-level control. Enabling the component-level control of safety-related controls is expected to be for short periods of time.

Sufficient diversity exists within a sensor block to limit a digital-based CCF to one function type.

7.1.5.1.6

Guideline 6 - Postulated Common Cause Failure of Blocks

The possible output signals for a given block are postulated below.

Division I or II Safety Display and Indication System and Manual Controls Blocks

The SDIS and manual controls blocks involve a combination of digital components (e.g., HSIs, display interface modules, communication modules) and analog hardware (i.e., manual controls). The SDIS blocks are designed for indication only and do not have the capability to control equipment. The manual controls in each manual controls block provide the operator the ability to initiate, at the division-level, protective actions automatically performed by Safety Block I or II. Control of ESF equipment at the component level is provided by the Nonsafety Monitoring and Indication block and the MCS block if nonsafety controls are enabled from the manual controls blocks.

With the indication and manual control being different hardware (i.e., digital vs. physical hard-wired switches), a CCF can be assumed to affect only those components relied on to generate or obtain display information. There are no credited manual actions for mitigating DBEs; however, the displays are used for accident monitoring.

A fail-as-is condition within one block before the start of a DBE results in one Division of operator displays indicating false safe operating conditions; however, this would not prevent protective actions from being automatically initiated by Safety Block I or II. Because the digital equipment within the block has no control capability, a CCF would not automatically cause a spurious actuation. Instead, with a digital-based CCF, the operator spends time determining which of the displays is valid. To resolve the information discrepancy, the operator can use the Nonsafety Monitoring and Indication block. The information provided to the SDIS blocks from the safety blocks is

also provided to the Nonsafety Monitoring and Indication block through the MCS block.

Another possible scenario is a CCF that falsely indicates a transient occurring without automatic initiation of protective actions. In this scenario, the operator still has the redundant SDIS block available as well as the Nonsafety Monitoring and Indication block. The operator is able to resolve the discrepancy in indication.

Figure 7.1-6 identifies the assumed CCF in red and shows in green outline the available blocks and signals used to resolve information discrepancy if, for example, Division I SDIS had a CCF.

Safety Blocks I or II

The actuation priority logic within an EIM is composed of discrete components and is not vulnerable to a digital-based CCF. The remaining portions of an EIM and the other modules within a safety block are postulated to have a digital-based CCF.

The most significant consequences for a digital-based CCF within a Safety Block are:

Scenario 1 - Spurious initiation of protective action(s) with correct indication.

Scenario 2 - Spurious initiation of protective action(s) with false indication.

Scenario 3 - Failure to initiate protective action(s) with correct indication.

Scenario 4 - Failure to initiate protective action(s) with false indication.

Initiation and successful completion of a protective action is considered to be a complete spurious actuation. Spurious actuation signals from separation group modules within a safety block would result in a complete spurious actuation in the opposite safety block because of the two-out-of-four voting performed by each safety block. Partial spurious actuation is credible for digital-based CCF postulated in the EIMs of a safety block. To identify the extent of partial spurious actuations due to digital based CCF, the EIMs are evaluated and grouped by the protective action(s) configured on the EIM. The EIMs that only perform decay heat removal actuation are considered to be unaffected by a digital-based CCF that affects EIMs that perform decay heat removal and containment isolation. Based on this approach, possible partial spurious actuation scenarios are identified in Table 7.1-10. For scenarios 1 and 2, a D3 coping analysis was performed to demonstrate the spurious actuations result in conditions that are bounded by the plant safety analyses, as discussed in Section 7.1.5.2.2.

Each Division of RTS has two RTBs. A partial spurious actuation of RTS within a Division does not result in a reactor trip and, thus, is not evaluated further. This is summarized in Table 7.1-11.

By crediting the diversity attributes between the two Safety Blocks, Scenarios 3 and 4 do not prevent the unaffected Safety Block from initiating protective actions when plant conditions require them. While Scenario 4 would result in conflicting information in the MCR, there are other blocks available to resolve conflicting information.

Figure 7.1-7 identifies the blocks (with green outline) relied upon to automatically initiate safety-related functions when one of the safety blocks has a digital-based CCF (shown in red). Figure 7.1-8 identifies in green outline the available blocks used to resolve information discrepancy and to automatically initiate safety-related functions if a safety block had a CCF (shown in red).

Nonsafety Monitoring and Indication Block

Nonsafety Monitoring and Indication block includes controls for safety and nonsafety equipment. Because Nonsafety Monitoring and Indication is used for normal day-to-day operations, a spurious actuation of a major control function (e.g., rod control, feedwater control) by a digital-based CCF within Nonsafety Monitoring and Indication block is immediately identifiable and, if it exceeds operating limits, is mitigated by Safety Blocks I or II. Figure 7.1-9 identifies the assumed digital-based CCF in red and shows in green outline the available blocks and signals used to resolve information discrepancy.

The actuation priority logic can be used to allow control of safety-related components using nonsafety-related controls; however, this can only be enabled by the operator using a safety-related switch. Without this feature being enabled, the nonsafety-related signals to the actuation priority logic are ignored. Because of the limited period in time in which safety-related components are controlled by nonsafety-related controls, it is not considered credible for a digital based CCF to occur while the enable nonsafety control input is active. The limitations on when the enable nonsafety control switch can be positioned to allow control of safety-related components from nonsafety-related controls are controlled by the plant operating procedures described in Section 13.5.2. As a result, no digital-based CCF within the Nonsafety Monitoring and Indication can directly prevent or spuriously initiate protective actions.

Module Control System

The MCS block is a subset of the actual MCS. The MCS block consists of the control network, controllers, remote I/O network, and remote I/O modules. These components are segmented or explicitly incorporate other functional defensive measures to inhibit the propagation of failures across major control functions. These major control functions are relied on to maintain day-to-day plant operations within operating limits including constraining operational transients. Hazards from MCS digital-based CCF are addressed in Section 7.1.8.

The actuation priority logic can be used to allow control of safety-related components using nonsafety-related controls; however, this can only be enabled by the operator using a safety-related switch. Without this feature being enabled, the nonsafety-related signals to the actuation priority logic are ignored. Because of the limited period in time in which safety-related components are controlled by nonsafety-related controls, it is not considered credible for a digital-based CCF to occur while the enable nonsafety control input is active. The limitations on when the enable nonsafety control switch can be positioned to allow control of safety-related components from nonsafety-related controls are controlled by the plant operating procedures described in Section 13.5.2. As a result, a digital-based CCF within the MCS block cannot directly prevent MPS from initiating protective actions and cannot directly command MPS to spuriously initiate protective actions.

Sensor Block I or II

These blocks have been included in the analysis because safety-related sensors that depend on digital electronics are being used as inputs to the MPS and are subject to a digital-based CCF. Using the function types and the diversity attributes discussed in Section 7.1.5.1.2, Table 7.1-12 through Table 7.1-14 identify how a digital-based CCF affects either one or both sensor blocks. For Table 7.1-12, there is sufficient diversity in the digital-based level measurement between Sensor Block I and II such that a digital-based CCF is limited to one block.

Postulated outputs of a sensor block with a digital based CCF are fail as-is, fail low, or fail high.

Digital-Based CCF of Level Function Type

A digital-based CCF of level function type for Sensor Block I (Figure 7.1-10) causes:

- spurious actuations from MPS
- incorrect information provided to SDIS
- incorrect information provided to MCS

Failed Low Signal

The affected parameter is pressurizer level. Because protective actions are actuated when at least two out of four separation groups demand a reactor trip or ESF actuation, failed low signals result in a spurious reactor trip, containment isolation, decay heat removal actuation, CVCS isolation, demineralized water system isolation, pressurizer heater trip, and secondary system isolation.

Failed low signals received by Safety Block I are provided to MCS to be displayed in the MCR and to be used for nonsafety-related controls. With the spurious actuation of a reactor trip, CNTS isolation, decay heat removal

actuation, CVCS isolation, demineralized water system isolation, pressurizer heater trip, and secondary system isolation, the MCS response to two correct and two incorrect sensor values has no further impact. Pressurizer level is used for nonsafety-related controls; however, with CVCS isolated, the MCS cannot use CVCS makeup and letdown pumps to change pressurizer level.

Failed High Signal

The affected parameter is pressurizer level. Because protective actions are actuated when at least two out of four separation groups demand a reactor trip or ESF actuation, failed high signals result in a spurious reactor trip, CVCS isolation, and demineralized water system isolation.

Failed high signals received by Safety Block I are provided to the MCS to be displayed in the MCR and to be used for nonsafety-related controls. With the spurious actuation of a reactor trip, demineralized water system isolation, and CVCS isolation, the MCS response to two correct and two incorrect sensor values has no further impact. Pressurizer level is used for nonsafety-related controls; however, with the CVCS isolated, the MCS cannot use CVCS makeup and letdown pumps to change pressurizer level. With Sensor Block II still capable of actuating on low-level signals (e.g., containment isolation on low-low pressurizer level), capability to initiate other ESFs is not lost.

Failed As-Is

The affected parameter is pressurizer level. The failed as-is condition for two of the four sensors for each affected parameter does not prevent the initiation of a reactor trip or ESF actuation. Sensor Block II is still capable of identifying plant conditions requiring protective actions.

Failed as-is signals do not lead to spurious initiation of protective actions and may go unnoticed until the valid signal deviates from the failed signals.

Digital-Based Common Cause Failure of Flow Measurement Function Type

A digital-based CCF of flow measurement function type for Sensor Block I (Figure 7.1-11) causes

- spurious actuations from the MPS
- incorrect information provided to the SDIS
- incorrect information provided to the MCS

Failed Low Signal

The affected variable is RCS flow. A failed low signal for the four channels results in a spurious reactor trip and demineralized water system isolation. There is no further impact associated with a failed low signal.

Failed High Signal

The affected variable is RCS flow. A failed high signal for the four channels does not result in spurious actuations; however, the safety blocks would be unable to identify a low RCS flow condition and the operator would have incorrect information.

Failure to identify a low RCS flow condition failure can be considered a Type 3 failure and is discussed in Section 7.1.5.1.10 and Section 7.1.5.1.11.

Failed As-Is

The affected variable is RCS flow. The failed as-is condition for the four channels does not result in spurious actuations. The failed as-is condition can prevent initiation of protective actions based on low flow conditions. The RCS flow is conservatively included in AOO. This failure can be considered a Type 3 failure and is discussed in Section 7.1.5.1.10 and Section 7.1.5.1.11.

7.1.5.1.7 Guideline 7 - Use of Identical Hardware and Software Modules

Only the digital-based flow measurements function type found in Sensor Block I and II are considered to be identical. The other blocks are considered to be independent such that a postulated digital-based CCF is limited to a block. Diversity attributes within and between blocks are discussed in Section 7.1.5.1.2.

7.1.5.1.8 Guideline 8 - Effect of Other Blocks

The blocks are assumed to function correctly in response to inputs that are correct or incorrect.

7.1.5.1.9 Guideline 9 - Output Signals

Figure 7.1-12 identifies in general terms the direction of information or signals between blocks. The following sections describe how the I&C architecture prevents errors from propagating backwards into the output of a previous block.

Safety Blocks I and II

The information from Safety Block I and II to SDIS blocks are through optically isolated transmit-only communication ports as described in Section 7.0.4.1 and Section 7.1.2.3. Signals from the manual control blocks to safety blocks are physical switch contacts that cannot be automatically changed by a digital-based CCF in the safety blocks.

The communication between safety blocks is for

- data sent from Separation Group A and C to Division II of ESFAS and RTS.

- data sent from Separation Group B and D to Division I of ESFAS and RTS.
- data sent from Separation Group A and C to Division II MPS Gateway.
- data sent from Separation Group B and D to Division I MPS Gateway.
- data sent from Division I RTS and ESFAS to Division II MPS Gateway.
- data sent from Division II RTS and ESFAS to Division I MPS Gateway.

The four separation groups are independent and redundant; however, for the purposes of the D3 assessment, the separation groups were grouped into safety blocks according to the FPGA architecture used. Communications from the separation groups to both divisions of RTS and ESFAS are through optically isolated, transmit-only communication ports. Data sent from the separation groups to either division of the MPS gateway are through optically isolated, transmit-only communication ports. Communication from the RTS and ESFAS to the MPS gateways is through optically isolated, transmit-only communication ports as described in Section 7.0.4.1.

Discrete hard-wired inputs from the MCS block to the safety blocks are to the analog portions of ESFAS and RTS that are not vulnerable to a digital-based CCF. Unless the operator enables nonsafety control, these inputs from the MCS block are ignored as described in Section 7.0.4.5 and Section 7.2.3.3.

Division I and II Safety Display and Indication Blocks

Inputs from safety blocks are from optically isolated, transmit-only communication modules. This prevents an error in the SDIS block from automatically propagating backwards to the safety blocks.

Division I and II Manual Control Blocks

Outputs from the Division I and II Manual Controls block are from physical switches in the MCR to the analog portions of ESFAS and RTS that are not vulnerable to a digital-based CCF.

Nonsafety Monitoring and Indication Block

The Nonsafety Monitoring and Indication block is composed of the MCS operator workstations. These workstations send and receive information through redundant domain controllers using redundant network paths.

Module Control System Block

Inputs from safety blocks have been optically isolated and transmitted using one-way communication. Faults within the MCS block cannot propagate backwards into the safety blocks.

Communications between the MCS and Nonsafety Monitoring and Indication blocks are through redundant controllers using redundant network paths. The MCS uses extensive self-checking to detect malfunction of the input/output

equipment, memory parity errors, lost or spurious communication interrupts, program hangups (control and data acquisition), and other feasibility checks that indicate erroneous operation.

7.1.5.1.10 Guideline 10 - Diversity for Anticipated Operational Occurrences

A Type 2 failure within a safety block does not prevent the unaffected safety block from initiating the necessary protective actions. Safety Block I or II alone can initiate necessary protective actions for AOOs. The diversity attributes between Safety Block I and II limit a digital-based CCF to only one safety block.

Safety Block I and II depend on both analog and digital sensors for detecting the need for protective actions. Table 7.1-14 summarizes the safety-related input signals, sensor technology, and their function(s). The digital sensors identified are vulnerable to a Type 3 failure; however, it is not credible to assume a concurrent Type 3 failure of the digital sensors. Instead, a digital-based CCF is assumed to occur with a particular subset of the digital sensors. For example, it is credible for the digital-based flow measurements to have a digital-based CCF concurrent with an AOO. Digital-based CCF of digital-based flow measurements and digital-based level sensors concurrent with an AOO is not considered credible because of the technology diversity.

Although pressurizer level is a digital-based sensor that is a credited signal for some events, there is sufficient diversity between Sensor Block I and II to prevent Type 3 failures from concurrently affecting the pressurizer level sensors in both Sensor Block I and II.

For RCS flow sensors, a D3 coping analysis was performed to demonstrate a Type 3 failure concurrent with an AOO does not result in radiation release exceeding 10 percent of 10 CFR 52.137(a)(2) dose limits or violate the integrity of the primary coolant pressure boundary, as discussed in Section 7.1.5.2.2. The D3 coping analysis considered an AOO concurrent with a digital-based CCF of a credited signal and the sensors of the same type.

7.1.5.1.11 Guideline 11 - Diversity for Accidents

A Type 2 failure within a safety block does not prevent the unaffected safety block from initiating the necessary protective actions. Safety Block I or II alone can initiate necessary protective actions for postulated accidents. The diversity attributes between Safety Block I and II limit a digital-based CCF to one safety block.

Safety Block I and II depend on both analog and digital sensors for detecting the need for protective actions. Table 7.1-14 summarizes the input signal, sensor technology, and its function(s). The digital sensors identified are vulnerable to a Type 3 failure; however, it is not credible to assume a concurrent Type 3 failure of the digital sensors. Instead, a digital-based CCF is assumed to occur with a particular subset of the digital sensors. For example, it is credible for the digital-based flow measurements to have a digital-based

CCF concurrent with a postulated accident. Digital-based CCF of digital-based flow measurements and digital-based level sensors concurrent with a postulated accident is not considered credible because of the technology diversity. A postulated accident may have multiple credited signals, depending on the event sequence. The event and signal credited are obtained from the plant safety analysis.

Although pressurizer level is a digital-based sensor that is a credited signal for some events, there is sufficient diversity between Sensor Block I and II to prevent Type 3 failures from affecting the pressurizer level sensors in both Sensor Block I and II.

A D3 coping analysis was used to demonstrate a Type 3 failure concurrent with a postulated accident does not result in radiation release exceeding 10 CFR 50.34(a)(1) dose limits, violating the integrity of the primary coolant pressure boundary, or violating the integrity of the containment, as described in Section 7.1.5.2.2. The D3 coping analysis considered a postulated accident concurrent with a digital-based CCF of a credited signal and the sensors of the same function type.

7.1.5.1.12

Guideline 12 - Diversity among Echelons of Defense

As shown in Figure 7.1-5, portions of the ESFAS and RTS echelon of defense are combined into the same block. Section 7.1.5.1.2 describes the diversity attributes within blocks and the diversity attributes between blocks.

Although there is diversity among the echelons of defense, a digital-based CCF of digital sensors can adversely impact the four echelons of defense (Section 7.1.5.1.6). For example, if all four RCS flow transmitters are assumed to fail as-is due to a digital-based CCF, then:

- The MCS receives a false signal from RCS flow affecting the makeup control function (failure of control system echelon).
- The RTS does not receive the sensor signal needed to initiate a reactor trip when RCS flow drops below the low-low RCS flow setpoint (failure of RTS echelon).
- The ESFAS does not receive the sensor signal needed to initiate demineralized water system isolation when RCS flow drops below the low RCS flow setpoint (failure of ESFAS echelon).
- The operator is not be able to see an uncontrolled RCS flow decrease in the MCR (failure of monitoring and indication echelon).

Anticipated operational occurrences or postulated accidents concurrent with a digital-based CCF of digital sensors are discussed in Section 7.1.5.1.10 and Section 7.1.5.1.11.

7.1.5.1.13 Guideline 13 - Plant Monitoring

Signals are transmitted from the RTS and ESFAS echelons to the control systems and monitoring and indication echelon. There are no manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions. As a result, none of the monitoring equipment within the monitoring and indication echelon is required to be safety-related.

As discussed in Section 7.1.5.1.6, digital-based CCF of a block within the monitoring and indication echelon does not prevent the operator from being able to resolve conflicting information. By being able to resolve conflicting information, operator-induced transients after a CCF of a block within the monitoring and indication echelon are not credible.

7.1.5.1.14 Guideline 14 - Manual Operator Action

The critical safety functions are accomplishing or maintaining containment integrity, fuel assembly heat removal, and reactivity control; however, there are no Type A accident monitoring variables. Type A variables provide information essential for the direct accomplishment of critical safety functions that require manual action.

Although there are no Type A variables, Division I and II manual controls blocks provide an independent and diverse method of manually actuating the automatic safety-related functions at the Division-level. The actuation priority logic within the EIMs of both safety blocks is implemented in discrete components and downstream of the automatic digital portion of the safety system. The SDIS and manual controls blocks are diverse, so a failure does not prevent the operator from obtaining or resolving conflicting information as described in Section 7.1.5.1.6. As described in Section 7.1.1.2.3 and Section 7.1.5.1.4, the SDIS and manual controls blocks are considered to be independent of the RTS, ESFAS, and control system echelon.

7.1.5.2 Results and Conclusions**7.1.5.2.1 Vulnerabilities to Spurious Actuations Resulting from Digital-Based Common Cause Failures**

After applying the guidelines of NUREG/CR-6303, the following potential vulnerabilities have been identified:

- 1) Potential digital-based CCF within a safety block may lead to spurious initiation of a protective action, as described in Section 7.1.5.1.6:
 - reactor trip
 - DHRS actuation
 - ECCS actuation
 - CNTS isolation

- CVCS isolation
 - pressurizer heater trip
 - demineralized water system isolation (DWSI)
 - low temperature overpressure protection (LTOP)
 - secondary system isolation (SSI)
 - pressurizer line isolation
- 2) Potential digital-based CCF within a safety block may lead to spurious partial initiation of protective actions (Section 7.1.5.1.6). The identified scenarios are provided in Table 7.1-10.
- 3) Potential digital-based CCF of level function type within Sensor Block I or II may result in one of the following (Section 7.1.5.1.6):
- spurious reactor trip, containment isolation, DHRS actuation, CVCS isolation, demineralized water system isolation, pressurizer heater trip, and secondary system isolation
 - spurious reactor trip, CVCS isolation, and demineralized water system isolation
- 4) Potential digital-based CCF of flow function type within Sensor Block I and II may result in one of the following (Section 7.1.5.1.6):
- spurious reactor trip and demineralized water system isolation
 - Type 3 failure of flow function type sensors (Item 6 below)
- 5) Type 3 failures of digital sensors may lead to failure of MPS to initiate protective action(s) during AOOs and postulated accidents. A failure of two of the four MPS separation groups that leads to the spurious initiation of a protection action or combination of protective actions was evaluated by the D3 coping analysis using best-estimate methods. While there are a large number of possible actuation combinations, the analysis of these events can be simplified without addressing each possible combination specifically.

The D3 coping analysis determined the spurious actuation of containment system isolation due to a digital-based CCF is the bounding analysis with regard to the RCPB integrity. Concurrent actuations of a combination of RTS, DHRS, or PZR heater trip have been evaluated to be less limiting because of the additional heatup effects on the delay of reactor trip, DHRS actuation valve opening or PZR heaters being tripped off. Containment system isolation actuation also isolates the CVCS, which increases the heatup effects slightly and negates possible effects of demineralized water system isolation actuation. The consequences of a digital-based CCF that leads to spurious initiation of a combination of MPS protective actions at normal operating pressure and temperature are bounded by the existing inadvertent DHRS analysis.

A postulated digital-based CCF affecting digital-based sensors that lead to a partial spurious initiation of protective actions at normal operating pressure and temperature is bounded by the existing plant safety analyses described in Chapter 15 or have no immediate impact and are non-limiting events.

7.1.5.2.2 Results of Coping Analyses for Postulated Digital-Based Common Cause Failure Vulnerability

As identified in Section 7.1.5.2.1, several postulated digital-based CCF vulnerabilities were identified that required a coping analysis to verify the consequences for the digital-based CCF were acceptable. For the AOOs and postulated accidents, the events were analyzed with postulated digital-based CCFs of the identified sensors that are relied upon and credited for the event in question. The results of the coping analysis concluded the AOO and postulated accident acceptance criteria were met. For the postulated spurious actuations analyzed, none resulted in a plant response or consequence that created conditions that were not bounded by the plant safety analysis described in Chapter 15. As a result, no additional coping strategies have been identified for prevention or mitigation of the postulated spurious actuations analyzed.

The acceptance criteria for the coping analysis is to demonstrate a digital-based CCF of a credited signal and all sensors of the same type, concurrent with a DBE does not violate the integrity of the primary coolant pressure boundary, or result in radiation release for AOOs exceeding 10 percent of 10 CFR 52.137(a)(2) dose limits and for postulated accidents exceeding 100 percent of 10 CFR 52.137(a)(2) dose limits. The analysis summary is provided below for the flow safety-related digital-based sensors.

Low Reactor Coolant System Flow

The RCS flow rate is a function of reactor power in the design, and therefore low RCS flow is only possible during startup conditions. The low-low RCS flow trip is not reached for any Chapter 15 events before another trip signal is reached first. This trip can be credited for actuating RTS in the event of a CVCS or an NPM heatup system malfunction that causes a loss of RCS flow condition during startup. This event is unlikely in combination with a digital-based CCF of the RCS flow sensor because of the limited operating window in which the NPM heatup system is relied upon to generate acceptable RCS flow. Although this event is deterministically postulated and protected for in the safety analysis, it is beyond the scope required by the digital-based CCF coping analysis; therefore no signal diversity is required.

The low RCS flow signal is only used to isolate the demineralized water system; this functionally restricts the scope of postulated boron dilution events, but is not credited as part of the best estimate transient detection or mitigation. The minimum flow is specified in order to generate the appropriate response time as part of the safety analysis evaluation but the change in neutron flux ultimately generates the required mitigating actuation of

demineralized water system isolation for the limiting scenario. In a best estimate analysis, the inadvertent boron dilution would not be postulated concurrent with a failure that reduced the minimum flow. In addition, there is no credible failure that would reduce the RCS flow rate during a boron dilution event.

7.1.5.3 Diversity and Defense-in-Depth Assessment Regulatory Conformance

Conformance with Staff Requirements Memorandum for SECY-93-087

The discussion below provides a summary of how the four-point position is either fully or partially addressed within the I&C system design.

Point 1

A D3 assessment of the MPS was performed. Vulnerabilities to digital-based CCFs are identified in Section 7.1.5.2. Evaluation of vulnerabilities shows plant response to vulnerabilities is either bounded by Chapter 15 analyses or within acceptable limits.

Point 2

The D3 assessment demonstrates there is adequate diversity within the MPS for each event evaluated in the accident analysis (Chapter 15).

A D3 coping analysis was performed to address identified vulnerabilities and demonstrates adequate diversity within the design. The coping analysis described in Section 7.1.5.2 for the postulated vulnerabilities concluded plant response to vulnerabilities is either bounded by Chapter 15 analyses or within acceptable limits.

Point 3

The D3 assessment demonstrates sufficient diversity exists within the MPS to prevent a postulated digital-based CCF from disabling the capability to perform its safety-related functions.

The D3 coping analysis identifies different sensors not vulnerable to the same digital-based CCF that exist to mitigate the associated event conditions without requiring a separate I&C system.

Point 4

Division I and II manual control switches are provided to manually initiate at the division-level the automatic safety-related functions. Manual actuation signals are inputs to the actuation priority logic within an EIM. The actuation priority logic within the EIMs is implemented in discrete components and is downstream of the automatic digital portion of the safety system. The MCS, SDIS, and manual controls are sufficiently diverse that a failure does not prevent the operator from obtaining or resolving conflicting information (Section 7.1.5.1.6).

7.1.6 Common Cause Failure of Nonsafety Related Controls

The two principal factors for the defense against CCFs are quality and diversity. Hardware quality is achieved by following a robust design and development process, and selecting a platform that has extensive operating experience. Software quality is achieved by following a rigorous software development lifecycle. The equipment and architecture used for the MCS and PCS is proven to be reliable based on operating history. In addition, the MPS is diverse from the MCS and PCS. The MPS is from a different vendor and is an FPGA-based design in which the MCS and PCS use microprocessor based controllers.

The guiding principles in SECY-18-0090 state the assessment of the vulnerabilities to a CCF should be commensurate with the safety significance of the system or function. A postulated CCF analysis is performed for the MCS and PPS using realistic assumptions to show the consequences are acceptable. If the postulated failure does not place the plant in a condition that cannot reasonably be mitigated, then further analysis or segmentation requirements are not necessary. A CCF analysis is not performed for low-safety significant systems whose failure would not adversely affect a safety function or place the plant in a condition that cannot be reasonably mitigated.

An analysis was performed to identify the worst-case system failures that may occur as a result of a digital-based CCF in the nonsafety-related process control systems and to identify the preventive, limiting, and mitigative strategies for coping with a digital-based CCF. The systems that could affect the critical safety function were analyzed for multiple failures to determine if that failure scenario was bounded by an existing safety analysis. The analysis showed it is unlikely a CCF would cause the outputs of different system functions to fail in the worst possible way (e.g., rods being withdrawn at maximum speed, and maximum makeup/dilution of the RCS).

The analysis of MCS or PCS concluded a total failure due to a CCF is unlikely because of the redundancy in the power supplies, controllers, signals used for control, server clusters, and the network architecture. The built-in diagnostics and alarming can alert operators of a fault prior to a failure of a function allowing time to fix the issue before a failure occurs. The MCS control networks are independent of each other and the PCS control network. A failure in the PCS control network cannot affect the MCS control networks and a failure in an MCS control network cannot affect the other MCS control networks or the PCS control network.

- The MCS controls MPS safety-related components through a discrete output (not data communications) but requires the MPS Enable Nonsafety switch to enable control requiring operator action. The MPS actuation priority logic circuit also blocks the control request if there is an active manual or automatic actuation signal. No single failure or CCF of the MCS can cause a spurious control signal to an MPS component.
- The PCS controls PPS components through a discrete output from PCS but requires the PPS Enable switch to enable control requiring operator action. The PPS actuation priority logic circuit blocks the control request if there is an active manual or automatic actuation signal. No single failure or CCF of the PCS can cause a spurious control signal to a PPS component.

Segmentation provides an additional defensive and preventive measure against a failure in one controller group from causing an undesirable condition in another controller group. Segmentation is used in the MCS and PCS architecture to provide functional independence between major control functions when susceptibility analysis shows segmentation is needed to address malfunctions and spurious actuations, as set forth in NRC DI&C-ISG-04, Section 3.1, staff position 5.

7.1.7 Simplicity

This section provides a description of the simplicity attributes that have been considered and incorporated into the design of the I&C system architecture. Simplicity is a cross-cutting design element and an evaluation of the simplicity of the I&C architecture was performed across the four fundamental design principles: independence, redundancy, predictability and repeatability, and D3.

Independence

The overall architecture of the MPS is based on the HIPS platform architecture described in TR-1015-18653-P-A. The simplicity of the independent design principle has been incorporated by the following design attributes:

- For each protective function, the associated sensor, signal conditioning, and trip determination are performed by a single, independent SFM. There is one-to-one correspondence for each SFM and its associated protective function. This configuration provides independence within each separation group from other protective safety functions, as well as independence across the separation groups and divisions within the MPS. By adhering to this design attribute, testing and maintenance are enhanced because each protective function can be taken out of service or bypassed for testing, maintenance, or repair without an adverse effect on other protective functions within a separation group or redundant channels across the remaining separation groups.
- Communications are based on simple deterministic protocols and safety data are communicated by redundant communication paths. Communication within the MPS is performed by dedicated logic communication engines; there are no microprocessor based communications as described in Section 4.6 of TR-1015-18653-P-A. Communication is deterministic and does not use interrupts or handshaking. The MPS communications architecture is segmented into five separate and distinct communication domains based on the safety function of the communication:
 - SDB (three redundant SDBs are provided; only trip determination and actuation data is included on these buses)
 - MIB
 - calibration and test bus
- The SDB communication architecture is described in Section 7.5.1 of TR-1015-18653-P-A. The MIB provides monitoring and indication information for the MPS, and does not perform safety functions. The calibration and test bus provides for calibration of tunable parameters and is used during maintenance of the MPS. Communications within the MIB and calibration and test bus are

performed on separate, isolated communication paths that have no interaction with communication on the SDB.

- As described in the HIPS platform topical report, there are no digital communications from the nonsafety-related to the safety-related systems. Nonsafety-related control signals from the MCS to the MPS are non-digital discrete signals routed and isolated through an HWM to the actuation priority logic within the EIM. During normal plant operation, nonsafety-related control is prohibited and blocked by the enable nonsafety control switch, thus providing electrical isolation between nonsafety-related systems and the safety-related MPS.

Redundancy

The HIPS platform design is based on a symmetrical architecture of four separation groups and two divisions. Each of the four separation groups is functionally equivalent to the others and each of the two divisions is functionally equivalent. Two-out-of-four voting is the applied voting strategy.

Through the use of identical redundant channels, testing and maintenance are simplified such that a single SFM can be bypassed for testing or repair without affecting the other remaining redundant separation groups. The MPS voting logic automatically accounts for the separation group bypassed for repair or testing.

Additional aspects of the redundant SDBs are discussed in TR-1015-18653-P-A.

Predictability and Repeatability

The I&C architecture design uses several simplicity design attributes related to the predictability and reliability of the MPS. The logic processing for the reactor trip and engineered safeguards protective functions are very simple. Trip determination is performed by a simple comparator (e.g., bistable) or, at most, by the use of simple arithmetic functions to perform the trip determination function. There is no closed loop control or modulating control functions within the MPS. Protective functions are "actuate only," requiring no process feedback to go to completion. The voting logic is implemented using simple finite-state machines dedicated to a particular safety function or group of safety functions. The use of finite-state machines eliminates the need for a microprocessor system. Therefore, no kernel, operating system, stacks, or heaps are required.

Communication paths are deterministic in design. The MPS work cycle operates on fixed, repeatable cycles. The MPS communications are asynchronous and from input to output, each MPS cycle performs the exact same set of operations in the exact same sequence to complete its safety function.

Diversity and Defense-in-Depth

Section 7.1.5 describes the overall approach to D3. With respect to simplicity, the D3 approach to the I&C design incorporates simplicity by using the same exact building block architecture across redundant separation groups and divisions. For

areas where a digital-based CCF can be introduced, the architecture uses diverse FPGA technologies between separate, redundant divisions.

The voting logic is implemented using simple finite-state machines dedicated to a particular safety function or group of safety functions. The use of finite-state machines eliminates the need for a microprocessor system. Therefore, no kernel, operating system, stacks, or heaps, are required. The I&C architecture comprises a series of building blocks. Each safety block comprises three types of FPGA-based modules: SFMs, communication modules, and EIMs. Because each type of module performs different functions, the logic implementations differ. For example, logic implemented for trip determination on an SFM is different than the logic implemented for two-out-of-four voting on an SVM.

Additionally, with the use of diverse FPGA technologies, inherent diversity attributes of each technology type are automatically introduced, such as different design and analysis tools, different logic programming tools, and diverse, independent verification and validation tools.

7.1.8 Hazards Analysis

This section provides a description of the hazards analysis methodology applied to the design of the I&C systems and how the hazards analysis has been incorporated into the I&C design and architecture. A system hazard analysis was performed for the MPS, NMS, PPS, and SDIS, and considered the hardware, software, organizations, and processes used to develop the system. The hazards analyses is used in conjunction with plant safety analyses, FMEAs, D3 analyses, and multi-discipline design reviews as an additional means of ensuring the correctness and completeness of the requirements for the MPS.

External hazards for the design are addressed in Section 2.2. Internal hazards are addressed in Chapter 3. The electrical power system design conditions are described in Section 8.3.2. The resulting independence requirements for I&C systems are described in Section 7.1.2. The resulting qualification requirements for I&C systems are described in Section 7.2.2.

7.1.8.1 Software-Related Contributory Hazards

Contributory hazards introduced as part of the software development life cycle are addressed as part of the software safety plan that is integrated into the overall software development life cycle described in Section 7.2.1. The software safety plan follows the guidance prescribed in IEEE Std 1228-1994 "IEEE Standard for Software Safety Plans" (Reference 7.1-8). The integration of software safety and hazards analyses performed during the software development life cycle are described below.

Concept Phase

As part of the concept phase in the software life cycle, a preliminary hazards list is prepared on the system that identifies

- hazardous states of the system.
- sequences of actions that can cause the system to enter a hazardous state.
- sequences of actions intended to return the system from a hazardous state to a nonhazardous state.
- actions intended to mitigate the consequences of accidents.

Requirements Phase

During the requirements phase of the software life cycle, a requirements traceability matrix is used in accordance with the Software Requirements Management Plan, as the tracking system to ensure hazards, their responsibility assignment, and their status can be tracked throughout the software life cycle, including retirement.

Design Phase

Software safety design analysis is performed during the design phase of the software life cycle to confirm the safety-critical portion of the software design correctly implements the SIL 3 and 4 software or configurable logic device logic functional requirements identified during the requirements phase and the design introduces no new hazards.

Implementation Phase

Software safety logic analysis is performed during the implementation phase of the software life cycle to confirm the SIL 3 and 4 portions of the logic design are correctly implemented in the logic and the logic introduces no new hazards.

Test Phase

Software safety test analysis is performed during the test phase to confirm the SIL 3 and 4 portions of the software or configurable logic device logic design are correctly implemented in the logic and the logic introduces no new hazards. For example, software stress testing is performed to ensure the safety-critical logic does not cause hazards under abnormal circumstances, such as unexpected input values or overload conditions. Regression testing is performed to ensure changes made to the safety critical logic do not introduce conditions for new hazards.

Throughout each phase, software verification and validation activities are performed, and the results of the software life cycle phase is matched against the system safety requirements and system hazard analysis to ensure

- system safety requirements have been satisfied within the software life cycle phases.
- no additional hazards have been introduced by the work done during the software life cycle activity.

7.1.8.2 Hazards Analysis Methodology

A hazard analysis is a process for examining an I&C system to identify hazards (i.e., factors and causes) and system requirements or constraints to eliminate, prevent, or control them.

The scope of the I&C system hazard analysis encompasses the system design basis described in Section 7.1.1. The analyses performed for the system design examined the associated I&C system, subsystems, and components and their interrelationships and interactions with other systems, subsystems, and components during modes of system operation to identify unintended or unwanted I&C system operation, including the impairment or loss of the ability to perform a safety function.

The I&C system hazard analysis evaluates those conditions and factors associated with the system under analysis and the systems that directly interact with it that can result in unintended or unwanted system operation, including a failure to initiate a protective action. These conditions are designated in the analysis as "Unsafe." Additional analysis is performed to provide guidance for the development process where a control action could affect continuity of operation or create other abnormal operating conditions without causing failure of a required protective action. These conditions are designated in the analysis as "Undesired."

The methodology for the hazard analysis is based on STAMP (Systems-Theoretic Accident Model and Processes) and STPA (Systems-Theoretic Process Analysis) developed at the Massachusetts Institute of Technology "Engineering a Safer World: Systems Thinking Applied to Safety," (Reference 7.1-5). The STPA methodology departs from the standard FMEA and fault-tree analysis by going beyond potential system failure caused by component failures. The STPA includes potential failures caused by interactions between system components, including human operators, which result in inadequate control actions, which can occur without component or logic faults.

Systems-Theoretic Accident Model and Processes

The STAMP model of accident causation is built on three basic concepts: safety constraints, a hierarchical control structure, and process models, along with basic systems theory concepts.

In STAMP, systems are viewed as interrelated components kept in a state of dynamic equilibrium by feedback control loops. Systems are not treated as static,

but as dynamic processes that are continually adapting to achieve their ends and to react to changes in themselves and their environment.

Safety is viewed as an emergent property of the system that is achieved when constraints on the behavior of the system and its components are satisfied. The design of the system must not only satisfy these constraints but must also continue to enforce the constraints as changes and adaptations to the system occur over time.

The STAMP methodology models organizational and process control interactions. The safety of the system under consideration is viewed as a control problem. Safety violations, or accidents, occur when a portion of the control process fails to maintain operation within the limits set by system constraints. Accidents occur when component failures, external disturbances, or unsafe interactions among system components are not adequately handled, or controlled, resulting in unsafe system behavior. In a STAMP-based analysis, after an accident or during the design process, root cause identification is not a goal. The goal is to identify the inadequate control structure, determine what changes need to be made in the system or control structure design, and ensure safety constraints are not violated.

Inadequate, ineffective, or missing control actions necessary to enforce the safety constraints can stem from flaws in the control structure. Figure 7.1-13 shows a basic control loop with examples of the types of flawed control actions that can result in violation of safety constraints.

Systems-Theoretic Process Analysis

The STPA is a process analysis method based on STAMP. In this method, control structures within the system under analysis are identified and diagrammatic representations (models) of those control structures are constructed. The structures defined in this way may or may not reflect the physical structures of the system, but represent the functional controllers, actuators, controlled processes, and sensors and the interactions between these functional components. In many complex systems, the control structures are presented at multiple levels of abstraction in order to capture the levels of component interaction. The control structures can be seen in the high-level control structure diagram in Figure 7.1-14 and Figure 7.1-15, and the lower level functional diagram in Figure 7.1-16.

By evaluating the control structures on a functional level, the design can be guided by the identified hazards and associated safety constraints.

The analysis processes performed in STPA are defined as follows.

- 1) Identify hazardous conditions that could occur for the system under analysis. These can be performance of unwanted actions, failure to perform required actions, or incorrect performance of actions that would result in accidents causing damage to SSC or injuries to operators.
- 2) Identify the potential for inadequate control of the system, unsafe control actions, that could lead to a hazardous state. Hazardous states result from

inadequate control or enforcement of the safety constraints, which can occur because:

- a) A control action required for safety is not provided or not followed.
 - b) An unsafe control action is provided.
 - c) A potentially safe control action is provided too early or too late (i.e., at the wrong time or in the wrong sequence).
 - d) A control action required for safety is stopped too soon or applied too long.
- 3) Determine how each potentially hazardous control action identified in step 1 could occur.
- 4) Design control procedures and mitigation measures, if they do not already exist, or evaluate existing measures if the analysis is being performed on an existing design. For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems.

Following the initial analysis, the next step is to iterate through the process again, repeating until the system development is complete.

7.1.8.3 Hazards Analysis Process

In order to assist in analysis of the functional controls of the system under analysis, a brief system description of the I&C system as described in Section 7.0 is prepared. The system description provides a high-level overview that supports the functional descriptions used later in the analysis without introducing redundancy.

7.1.8.3.1 Identification of Hazard Conditions

The hazards associated with the systems under consideration have been identified in accordance with the procedures that require the performance of this hazard analysis. In accordance with RIL-1101, the hazards of concern are "unintended or unwanted I&C system operation including the impairment or loss of the ability to perform a safety function."

Therefore, the high-level hazards considered were the improper operation of, or a loss of a safety function associated with, the components of the safety systems. Equipment, functions, or operations outside the system under analysis, such as the HSI and the control room, are analyzed to determine if interactions could impair the functions of the analyzed system.

These analyses addressed the hazards from the perspective of an individual signal processing train without the benefit of redundancies or D3 to provide a "worst case" scenario from which the most conservative safety constraints can be identified. The considerations may improve system reliability and availability, but may or may not affect system safety. Other analyses address

the redundant functions to determine if they contribute to system hazards. Examples of high-level hazards are shown in Table 7.1-16. This list is based on the limits for the MPS as provided in Table 7.1-17.

7.1.8.3.2 Identification of High-Level Safety Constraints

The high-level safety constraints are derived from the identification of system hazards. They provide the fundamental limits of system operation. The safety constraint identification numbers shown in Table 7.1-18 indicate the hazard conditions that dictate the requirement for the constraint. The safety functions, based on the DBEs shown in Table 7.1-1 and their setpoints, are detailed in Table 7.1-17. This analysis is based on the safety functions initiated by a setpoint being exceeded and not on the processes that are measured.

High-level safety constraints for nonsafety-related systems or functions could be based on personnel safety, equipment safety, risk significance, or another condition that could affect how the system is designed.

7.1.8.3.3 Expansion of High-Level Safety Constraints

Table 7.1-19 expands the safety constraints shown in Table 7.1-18 to address the individual safety functions of Table 7.1-17 because the algorithms, trip setpoints, and feedback for each of these functions are different. Therefore, the analysis of the associated control functions may be different.

7.1.8.3.4 Control Structures

The control structures are analyzed by identifying the functional controllers and determining the commands or events that are represented by each input and output for each controller. Potentially hazardous conditions for the interactions are identified in a table. The tables are followed by a description of each hazardous condition identified, possible causes for the inadequate control action, and suggested safety constraints to mitigate the unsafe conditions caused by the inadequate control action.

The remainder of this section shows how system decomposition can be performed to capture the operation of the controllers and their interactions. It begins with a brief system overview followed by one or more functional descriptions.

Example System Overview – Module Protection System

The MPS is made up of four separation groups and two divisions. The SFMs in each separation group correspond to the module-level safety functions identified in Table 7.1-17. The SFMs accept inputs from safety-related instrumentation, which are conditioned using filters and other conditioning circuits and converted to digital signals. Each SFM also contains FPGA logic that performs required mathematical functions and a comparison of the digital signals against the safety function setpoint and three communications engines that send the results of the comparison on dedicated, triple redundant

communication buses to the SBMs. The SBM is a communications module that manages the asynchronous data transmission between the SFMs and the SVMs, and provides the capability for maintenance bypass functions.

The basic system configuration showing a single SFM and a single EIM can be seen in Figure 7.1-17.

Example High-Level Control - Module Protection System

The control structure for this analysis consists of the functional interactions between the inputs from the nonsafety-related control system, the MCS; the safety-related protection system, the MPS; operators; outputs to display and indication systems; actuators; the outputs to the safety-related components; and the inputs from the sensors. This structure is shown in Figure 7.1-14.

Beginning at the top, the operator interacts with the control structure using commands through workstation HSIs and the MCS controllers or hard-wired switches to the actuation priority logic portions of the MPS. The commands sent to the MCS allow operators to actuate individual safety system components for maintenance, system alignment following an actuation or other, nonsafety-related operations.

Example Low-Level Logic Structure - Safety Function Module

The SFM logic (Figure 7.1-16) is a non-standard control structure in that there are three controllers (the operator, the signal conditioning, and the trip determination logic) and minimal control feedback. The only feedback provided is loopback input signal verification for the signal conditioning, actuated component position information, and process variable display feedback to the operator.

The control structure diagram shows the configuration of the input signal conditioning and trip determination controllers with output, through the triple redundant communication buses, directed to the associated SBMs. The division level processes are analyzed separately.

The control actions considered in this portion of the analysis begin with the signal conditioning. The signal conditioner is a controller to the extent that it accepts an input from an analog or digital sensor, performs conditioning on the signal, such as filtering and scaling, and then performs an analog-to-digital conversion, if necessary. Signal validation is performed on the signal to reduce the possibility of an inadvertent protective action or the failure to initiate a required protective action. The digital representation of the original analog input signal is sent to the associated trip determination portion of the SFM.

Control Action Analysis

The control actions are analyzed by investigating the control objects in each diagram and the interactions between them. Each interaction, command or event, is evaluated to determine if a hazardous condition results if the

interaction fails to occur, if it occurs in an incorrect manner, if it is late or early in occurring, if it occurs out of sequence, or if it is stopped too soon or continues too long.

For example, looking at the signal conditioning in Figure 7.1-16, an input event that is expected is an analog signal that is received from a sensor. If this does not occur, an unsafe condition could exist with a process variable out of its normal operating range without an appropriate protective action. This unsafe condition results from a failure to execute a correct control action in response to an out-of-normal plant process variable. Similarly, if the analog signal does not accurately reflect plant conditions, it could result in the same type of unsafe control action. Table 7.1-20 reflects this in the first row by showing the control action is unsafe and identifies the hazardous condition as HC-1. The remaining potential hazardous conditions, too early, too late, out of sequence, and stopped too soon, are not indicated as unsafe conditions. This is because the input signal is a continuous stream and is not impacted by timing issues in the MPS. A too-late condition caused by a slow response time of the process sensor is identified by a hazard analysis of the sensing device.

In this hazard analysis, the following conventions are used:

- Hazardous conditions are identified by the designation HC followed by a unique number that is incremented for each identified HC.
- Possible causes are identified by the designation PC followed by a number. Possible causes are not classified according to related hazardous conditions because of their more generic nature.
- Safety constraints are identified by the designation SC followed by a two part number. The first number identifies the hazardous condition the constraint is intended to mitigate. The second number is a unique number incremented for each identified SC.
- Possible causes that refer to "algorithm" errors may be because of requirements, design, or implementation. An FPGA error, after proper design and implementation, could only be the result of physical damage or component failure.
- Board level clock errors may be due to mistiming or loss of clock signals that control the sequencing of FPGA logic. These clock signals are independent for each FPGA board and allow asynchronous operation between FPGA modules.
- Communication errors may be data or signal faults. Data media errors or faults would be the result of physical damage or failure.
- Control actions identified as "Undesired" are actions that do not directly result in an unsafe condition, but may result in an abnormal operation condition or an unnecessary shutdown.

Correlation of Possible Causes to Preliminary Hazard List

Table 7.1-21 shows the basic causes of unsafe control actions identified by the MPS hazard analysis and the system preliminary hazard list (PHL). The hazards identified in the hazard list correlate well with the hazard analysis. The table is not intended to indicate a one-to-one correspondence between the first (Hazards Analysis Identified Cause) and second (PHL Identified Cause) column. For example, the damaged cable from the hazard analysis could be caused by many of the causes from the hazard list. The differences between the lists are that the preliminary hazard list focused on failures due to physical events and focused on the mechanism rather than the effect. The hazard analysis focused on the effect rather than the mechanism. These differences support the use of the STPA methodology for analyzing complex systems such as the MPS.

The I&C system hazard analysis is based on a view of the processes that are performed by the systems described in Section 7.0. The hazards analysis does not explicitly analyze the effects of redundancy and D3; however, the hazard conditions identified in the hazards analysis are mitigated through application of the fundamental design principles of redundancy (Section 7.1.3) and D3 (Section 7.1.5). The hazards analysis methodology described is a living process, performed through the system design life cycle described in Section 7.2.1.1. The cross-referencing of hazard conditions, safety constraints, and functional design requirements ensures potentially hazardous conditions not previously identified by other analysis methods are mitigated by feedback into the design of the system functional requirements.

7.1.9 References

- 7.1-1 NuScale Power, LLC, "Design of the Highly Integrated Protection System Platform," TR-1015-18653-P-A Revision 2.
- 7.1-2 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Standard 603-1991, Piscataway, NJ.
- 7.1-3 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers and Safety Systems of Nuclear Power Generating Stations," IEEE Standard 7-4.3.2-2003, Piscataway, NJ.
- 7.1-4 Institute of Electrical and Electronics Engineers, "IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Standard 379-2000, Piscataway, NJ.
- 7.1-5 Leveson, N.G., *Engineering a Safer World: Systems Thinking Applied to Safety*, Massachusetts Institute of Technology, Cambridge, MA, 2011.
- 7.1-6 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," IEEE Standard 497-2016, Piscataway, NJ.

- 7.1-7 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," IEEE Standard 384-1992, Piscataway, NJ.
- 7.1-8 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Safety Plans," IEEE Standard 1228-1994, Piscataway, NJ.

Table 7.1-1: Module Protection System Design Basis Events

Event	Chapter 15 Analysis
Decrease in Feedwater Temperature	Section 15.1.1
Increase in Feedwater Flow	Section 15.1.2
Increase in Steam Flow	Section 15.1.3.2
Steam System Piping Failures Inside and Outside of Containment	Section 15.1.5
Loss of Containment Vacuum/Containment Flooding	Section 15.1.6
Loss of External Load	Section 15.2.1
Turbine Trip	Section 15.2.2
Loss of Condenser Vacuum	Section 15.2
Closure of Main Steam Isolation Valve(s)	Section 15.2.4
Loss of Nonemergency AC Power to the Station Auxiliaries	Section 15.2.6
Loss of Normal Feedwater Flow	Section 15.2.7
Inadvertent Operation of DHRS	Section 15.2.9
Feedwater System Pipe Breaks Inside and Outside of Containment	Section 15.2.8
Uncontrolled Control Rod Assembly Withdrawal from a Subcritical or Low Power or Startup Condition	Section 15.4.1
Uncontrolled Control Rod Assembly Withdrawal at Power	Section 15.4.2
Control Rod Misoperation	Section 15.4.3
Inadvertent Decrease in Boron Concentration in the Reactor Coolant System	Section 15.4.6
Spectrum of Rod Ejection Accidents	Section 15.4.8
Failure of Small Lines Carrying Primary Coolant Outside Containment	Section 15.6.2
Steam Generator Tube Failure	Section 15.6.3
Loss-of-Coolant Accidents Resulting from Spectrum of Postulated Piping Breaks within the Reactor Coolant Pressure Boundary	Section 15.6.5
Instability Events	Section 15.9
Station Blackout	Section 8.4

Table 7.1-2: Variables Monitored by Module Protection System

Variable	Nominal Range	Nominal (100% RTP)
Pressurizer Level	0 to 100%	50% full scale
Pressurizer Pressure	1100 to 2200 psia	2000 psia
RPV Riser Level	0 to 100%	100%
Wide Range RCS Pressure	0 to 2500 psia	2000 psia
Containment Water Level	0 to 100%	0%
Narrow Range Containment Pressure	0 to 20 psia	0.1 psia
Wide Range Containment Pressure	0 to 1400 psia	0.1 psia
Containment Isolation Valve Position	Open/Closed	Open (Note 1)
ECCS Valve Position	Open/Closed	Closed
Demineralized Water Supply Isolation Valve Position	Open/Closed	Open
DHRS Valve Position	Open/Closed	Closed
Secondary MSIV Position	Open/Closed	Open
Secondary MSIV Bypass Valve Position	Open/Closed	Closed
FWRV Position	Open/Closed	Open
Narrow Range RCS Cold Temperature	40 to 700 °F	482 °F
Narrow Range RCS Hot Temperature	40 to 700 °F	598 °F
NMS-Flood Output Fault	Fault/No Fault	No Fault
Wide Range RCS Hot Temperature	40 to 700 °F	589 °F
Wide Range RCS Cold Temperature	40 to 700 °F	507 °F
Core Exit Temperature	0 to 2300 °F	595 °F
RCS Flow	0 to 110%	100%
Main Steam Pressure (DHRS Inlet Pressure)	0 to 1400 psia	500 psia
Main Steam Temperature (DHRS Inlet Temperature)	100 to 700 °F	575 to 585 °F
Power Range Linear Power	0 to 200% RTP	100% RTP
Intermediate Range Log Power	6 decades: 10^4 to 10^{10} counts per second	100% RTP equivalent
Intermediate Range Doubling Time	-5 to +5 seconds	0 seconds
Source Range Count Rate	5.5 decades: 5 to 10^6 counts per second	-
Source Range Doubling Time	-5 to +5 seconds	0 seconds
Power Range Rate (calculated from Power Range Power)	-20 to +20%/minute	0 %/minute
Source/Intermediate Range Fault	Fault/No Fault	No Fault
Power Range Fault	Fault/No Fault	No Fault
NMS-Flood Supply Fault	Fault/No Fault	No Fault
Inside Bioshield Area Radiation Monitor	1×10^0 to 1×10^7 R/hr	1×10^0 to 1×10^2 R/hr
Reactor Trip Breaker Position Feedback	Open/Closed	Closed
Pressurizer Heater Breaker Position Feedback	Open/Closed	Closed
Narrow Range RCS Cold Temperature	40 to 700 °F	482 °F
ELVS Voltage	0 to 600 VAC	480 VAC
Reactor Safety Valve Position	Open/Closed	Closed
Under-the-Bioshield Temperature	40 to 700 °F	130 °F
NMS-Flood Log Output	4 decades (counts per second)	-
Subcritical Multiplication	0-10	-
Containment Evacuation System Pressure	0 to 14.7 psia	1 psia

Table 7.1-2: Variables Monitored by Module Protection System (Continued)

Variable	Nominal Range	Nominal (100% RTP)
Degrees of Superheat (calculated from MS Temperature and MS Pressure)	-	calculated variable
NMS-Flood Detector Position	Deployed/Retracted	Retracted
RCS Average Temperature (Note 2)	-	calculated variable

Note 1: Normal position for the CIVs for containment flooding and drain, main steam isolation bypass and the RPV high point degasification line are closed; the rest are open.

Note 2: RCS Average Temperature is defined as the numerical average of Narrow Range RCS Hot Temperature and Narrow Range RCS Cold Temperature.

Table 7.1-3: Reactor Trip Functions

Process Variable	Analytical Limit	Number of Channels	Logic
High Power Range Linear Power	High-1 = 25% RTP High-2 = 115% RTP	4	2/4↑
High Intermediate Range Log Power Rate	3 dpm	4	2/4↑
High Power Range Rate	+/- 7.5% RTP/30 seconds	4	2/4↓
High Source Range Count Rate	5x10 ⁵ counts per second	4	2/4↑
High Source Range Log Power Rate	3 dpm	4	2/4↑
High Narrow Range RCS Hot Temperature	620°F	4	2/4↑
High Narrow Range Containment Pressure	9.5 psia	4	2/4↑
High Pressurizer Pressure	2100 psia	4	2/4↑
Low Pressurizer Pressure	1850 psia	4	2/4↓
Low-Low Pressurizer Pressure	1200 psia	4	2/4↓
High Pressurizer Level	80%	4	2/4↑
Low Pressurizer Level	35%	4	2/4↓
High Main Steam Pressure	1200 psia	4	2/4↑
Low Main Steam Pressure	300 psia (≥15% RTP)	4	2/4↓
Low-Low Main Steam Pressure	20 psia	4	2/4↓
High Main Steam Superheat (MS Temperature and Pressure)	150°ΔF	4	2/4↑
Low Main Steam Superheat (MS Temperature and Pressure)	0.0°ΔF	4	2/4↓
Low-Low RCS Flow	0.0 ft ³ /s	4	2/4↓
Low AC Voltage to Battery Chargers	80% of normal ELVS voltage Actuation Delay of 60 seconds (Note 1)	4	2/4↓
High Under-the-Bioshield Temperature	250°F	4	2/4↑
High RCS Average Temperature	555°F	4	2/4↑

Note 1: Normal AC voltage is monitored at the bus(es) supplying the battery chargers for the EDAS.

Table 7.1-4: Engineered Safety Feature Actuation System Functions

ESFAS Function	Process Variable	Analytical Limit	Number of Channels	Logic	Figure Showing the System Automated Function
Emergency Core Cooling System (ECCS)	Low ELVS voltage 24-hour Timer	24 hours	3	2/3	Figure 7.1-1n
	Low RPV Riser Level	540-552 in. (Note 4)	4	2/4↓	
	Low-Low RPV Riser Level	460-472 in. (Note 4)	4	2/4↓	
	ECCS Timer after Reactor Trip	8 hours	3	2/3	
	High-High RCS Average Temperature (Note 3)	620°F	4	2/4↑	
	High-High RCS Pressure (Note 3)	2500 psia	4	2/4↑	
Decay Heat Removal System (DHRS)	High Pressurizer Pressure	2100 psia	4	2/4↑	Figure 7.1-1l
	High Narrow Range RCS Hot Temperature	620°F	4	2/4↑	
	High Main Steam Pressure	1200 psia	4	2/4↑	
	Low AC Voltage to Battery Chargers	80% of normal ELVS voltage Actuation Delay of 60 seconds (Note 1)	4	2/4↓	
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	
	Low Pressurizer Level	35%	4	2/4↓	
	High Under-the-Bioshield Temperature	250° F	4	2/4↑	

Table 7.1-4: Engineered Safety Feature Actuation System Functions (Continued)

ESFAS Function	Process Variable	Analytical Limit	Number of Channels	Logic	Figure Showing the System Automated Function
Secondary System Isolation	High Pressurizer Pressure	2100 psia	4	2/4↑	Figure 7.1-1l
	High Narrow Range RCS Hot Temperature	620°F	4	2/4↑	
	Low Main Steam Pressure	300 psia ($\geq 15\%$ RTP)	4	2/4↓	
	Low-Low Main Steam Pressure	20 psia	4	2/4↓	
	High Main Steam Pressure	1200 psia	4	2/4↑	
	Low Main Steam Superheat (MS Temperature and Pressure)	0.0°ΔF	4	2/4↓	
	High Main Steam Superheat (MS Temperature and Pressure)	150°ΔF	4	2/4↑	
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	
	Low Pressurizer Pressure	1850 psia	4	2/4↓	
	Low Pressurizer Level	35%	4	2/4↓	
	Low AC Voltage to Battery Chargers	80% of normal ELVS voltage Actuation Delay of 60 seconds (Note 1)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	
Containment System Isolation Signal	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	Figure 7.1-1k
	Low-Low Pressurizer Level	15%	4	2/4↓	
	Low AC Voltage to Battery Chargers	80% of normal ELVS voltage Actuation Delay of 60 seconds (Note 1)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	
	Low Pressurizer Level	35%	4	2/4↓	

Table 7.1-4: Engineered Safety Feature Actuation System Functions (Continued)

ESFAS Function	Process Variable	Analytical Limit	Number of Channels	Logic	Figure Showing the System Automated Function
Demineralized Water System Isolation	Reactor Trip	Any Reactor Trip Signal	4	2/4	Figure 7.1-1m
	Low RCS Flow	1.0 ft ³ /s	4	2/4↓	
	High Subcritical Multiplication (SCM)	3.2	4	2/4↑	
Chemical and Volume Control System Isolation	High Pressurizer Level	80%	4	2/4↑	Figure 7.1-1k
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	Figure 7.1-1v
	Low Pressurizer Level	35%	4	2/4↑	Figure 7.1-1w
	Low-Low Pressurizer Level	15%	4	2/4↓	
	Low AC Voltage to Battery Chargers	80% of normal ELVS voltage Actuation Delay of ≤ 60 seconds (Note 1)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	
Pressurizer Heater Trip	Low Pressurizer Level	35%	4	2/4↓	Figure 7.1-1m
	DHR actuation	Any automatic DHR actuation	4	2/4	
Low Temperature Overpressure Protection (LTOP)	Low Temperature Interlock with High Pressure (WR RCS cold temperature and WR RCS Pressure)	Variable based on WR RCS cold temperature and WR RCS Pressure as listed in Table 5.2-5	4	2/4↑	Figure 7.1-1n
Pressurizer Line Isolation	Low Pressurizer Pressure	1850 psia	4	2/4↓	Figure 7.1-1e, Figure 7.1-1h, Figure 7.1-1w

Note 1: Normal AC voltage is monitored at the bus(es) supplying the battery chargers for the EDAS.

Note 2: These signals provide automatic ECCS actuation for beyond-design-basis events.

Note 3: These signals provide automatic ECCS actuation for beyond-design-basis events. The signals have non-safety related function; however, they are implemented using safety-related sensors.

Note 4: Table 15.0-7 identifies how the RPV riser level analytical limits are modeled in the transient and accident analyses of Chapter 15.

Table 7.1-5: Module Protection System Interlocks / Permissives / Overrides

Interlock/ Permissive/ Override	Condition for Interlock/ Permissive/Override	Function
N-1 Permissive	Intermediate Range Log Power Permissive: Permissive established when at least 3 of 4 Intermediate Range Log Power channels > approximately 1 decade above the channel lower range limit.	Allows the operator to manually establish an operating bypass of the following: • Reactor Trip on High Source Range Count Rate • Demineralized water system isolation actuation on High Source Range Count Rate • Reactor Trip on High Source Range Log Power Rate • Demineralized water system isolation actuation on High Source Range Log Power Rate Operating bypasses are automatically removed when permissive condition is no longer satisfied.
N-1 Interlock	Intermediate Range Log Power Interlock: Interlock established when at least 3 of 4 Intermediate Range Log Power channels > approximately 1 decade above the channel lower range limit.	Automatically establishes an operating bypass of the Demineralized Water System Isolation actuation on High Subcritical Multiplication. Operating bypass is automatically removed when Interlock condition is no longer satisfied.
N-2L Permissive	Power Range Linear Power Permissive: Permissive established when at least 3 of 4 Power Range Linear Power Channels > 15% RTP	Allows the operator to manually establish an operating bypass of the following: • Reactor Trip on High-1 Power Range Linear Power. This increases the High Power Range High Linear Power trip to the High-2 trip setpoint) • Demineralized water system isolation actuation on High-1 Power Range Linear Power Operating bypasses are automatically removed when permissive condition is no longer satisfied.
N-2L Interlock	Power Range Linear Power Interlock: Interlock established when at least 3 of 4 Power Range Linear Power Channels > 15% RTP	Automatically establishes an operating bypass of the following: • Reactor Trip on High Intermediate Range Log Power Rate • Demineralized water system isolation actuation on High Intermediate Range Log Power Rate Operating bypasses are automatically removed when interlock condition is no longer satisfied.
N-2H Interlock	Power Range Linear Power Interlock: Interlock established when at least 3 of 4 Power Range Linear Power Channels < 15% RTP	Automatically establishes an operating bypass of the following: • Reactor Trip on High Power Range Positive Rate • Demineralized water system isolation actuation on High Power Range Positive Rate • Reactor Trip on High Power Range Negative Rate • Demineralized water system isolation actuation on High Power Range Negative Rate Operating bypasses are automatically removed when interlock condition is no longer satisfied.

Table 7.1-5: Module Protection System Interlocks / Permissives / Overrides (Continued)

Interlock/ Permissive/ Override	Condition for Interlock/ Permissive/Override	Function
V-1 Interlock	FWIV Closed Interlock: Interlock established when at least one FWIV indicates closed.	Automatically establishes an operating bypass of the following when V-1 interlock is active: - Reactor trip on Low Main Steam Superheat. Automatic establishes operating bypass of the following when the V-1 interlock AND the T-3 interlock are active, OR the containment level interlock, L-1, is active: - Secondary System Isolation actuation on Low-Low Main Steam Pressure. Automatic establishes operating bypass of the following when the V-1 interlock OR the L-1 interlock are active: - Secondary System Isolation actuation on Low Main Steam Superheat. Operating bypasses are automatically removed when interlock condition is no longer satisfied.
RT-1 Interlock	Reactor Tripped Interlock: Interlock established when both divisional reactor trip (RT) breakers indicate open	The RT-1 Interlock is used in conjunction with the T-2, T-3, and L-1 interlocks, and the override function O-1.
T-1 Interlock	Wide Range RCS Cold Temperature Interlock: Interlock established when at least 3 of 4 Wide Range RCS Cold Temperature channels > 290°F	Automatically establishes an operating bypass of the following: Low Temperature Overpressure Protection actuation on High WR RCS Pressure Operating bypass is automatically removed when interlock condition is no longer satisfied.
T-2 Interlock	Wide Range RCS Hot Temperature Interlock: Interlock established when at least 3 of 4 Wide Range RCS Hot Temperature channels < 200°F, AND the RT-1 interlock is active.	Automatically establishes an operating bypass of the following: - Secondary system isolation actuation on Low Pressurizer Level - Chemical and volume control system isolation actuation on Low-Low Pressurizer Level - Containment system isolation actuation on Low-Low Pressurizer Level Operating bypasses are automatically removed when interlock condition is no longer satisfied.

Table 7.1-5: Module Protection System Interlocks / Permissives / Overrides (Continued)

Interlock/ Permissive/ Override	Condition for Interlock/ Permissive/Override	Function
T-3 Interlock	Wide Range RCS Hot Temperature Interlock: Interlock established when at least 3 of 4 Wide Range RCS Hot Temperature channels < 340°F, AND the RT-1 interlock is active.	Automatically establishes an operating bypass of the following: • Secondary system isolation actuation on High Narrow Range Containment Pressure • Containment system isolation actuation on High Narrow Range Containment Pressure • Chemical and volume control system isolation actuation on High Narrow Range Containment Pressure trip • DHRS actuation on High Narrow Range Containment Pressure • Pressurizer heater trip on High Narrow Range Containment Pressure • Pressurizer line isolation on Low Pressurizer Pressure • Reactor trip on Low-Low Pressurizer Pressure • Demineralized Water System Isolation on all Automatic Reactor Trip Signals Operating bypasses are automatically removed when interlock condition is no longer satisfied.
T-4 Interlock	Narrow Range RCS Hot Temperature Interlock: Interlock established when at least 3 of 4 Narrow Range RCS Hot Temperature channels <500°F	Automatically establishes an operating bypass of the following: • Reactor trip on Low Pressurizer Pressure • Demineralized water system isolation actuation on Low Pressurizer Pressure • SSI actuation • Reactor trip on Low Main Steam Pressure • Demineralized water system isolation actuation on Low Main Steam Pressure • SSI actuation. • Low Pressurizer Level Containment System Isolation actuation • Low Pressurizer Level DHRS actuation • Low Pressurizer Level • CVCS isolation actuation Operating bypasses are automatically removed when interlock condition is no longer satisfied.
T-5 Interlock	Wide Range RCS Hot Temperature T-5 interlock: Interlock established when least 3 of 4 Wide Range RCS Hot Temperature channels are less than 440°F	Automatically establishes an operating bypass of the following: • Emergency Core Cooling System actuation on Low RPV Riser Level • Operating bypass is automatically removed when interlock condition is no longer satisfied

Table 7.1-5: Module Protection System Interlocks / Permissives / Overrides (Continued)

Interlock/ Permissive/ Override	Condition for Interlock/ Permissive/Override	Function
L-1 Interlock	Containment Water Level Interlock: Interlock established when at least 3 of 4 Containment Level Channels > 45' AND RT-1 is active	Automatically establishes operating bypass of the following: • Secondary system isolation actuation on Low Pressurizer Level • Secondary system isolation actuation on Low-Low Main Steam Pressure • Secondary system isolation actuation on Low Main Steam Superheat • Containment system isolation actuation on Low-Low Pressurizer Level • Chemical and volume control system isolation actuation on Low-Low Pressurizer Level When the L-1 interlock AND the Wide Range RCS Hot Temperature interlock, T-2, are not active, the operating bypass is automatically removed for the following: • Secondary system isolation actuation Low Pressurizer Level • Containment system isolation actuation on Low-Low Pressurizer Level • Chemical and volume control system isolation actuation Low-Low Pressurizer Level When the L-1 interlock is not active AND either the Wide Range RCS Hot Temperature interlock, T-3, is not active OR the FWIV Closed interlock, V-1, is not active, the operating bypass is automatically removed for the secondary system isolation actuation on Low-Low Main Steam Pressure. When the L-1 interlock AND the FWIV Closed interlock, V-1, are not active, the operating bypass is automatically removed for the secondary system isolation actuation on Low Main Steam Superheat.
O-1 Override	Containment System Isolation Override Function: Override established when manual override switch is active and RT-1 interlock is established	Override allows manual control of the CFDS, CES, RCS injection, and pressurizer spray containment isolation valves if an automatic containment system isolation or a CVCS isolation actuation signal is present with the exception of the High Pressurizer Level CVCS isolation actuation signal. The Override switch must be manually taken out of Override when the Override, O-1, is no longer needed.

Table 7.1-6: Design Basis Event Actuation Delays Assumed in the Plant Safety Analysis

Signal	Sensor	Actuation Delay
High Power Range Linear Power	Power Range Neutron Flux	2.0s
SR and IR Log Power Rate	SR & IR Neutron Flux	Variable
High Power Range Rate	Power Range Neutron Flux	2.0s
High Source Range Count Rate	Source Range Neutron Flux	3.0s
High Subcritical Multiplication	Source Range Neutron Flux	150.0s
High Narrow Range RCS Hot Temperature	Riser Outlet Temperature	8.0s
High Narrow Range Containment Pressure	Containment Pressure	2.0s
High Pressurizer Pressure	Pressurizer Pressure	2.0s
High Pressurizer Level	Pressurizer Level	3.0s
Low Pressurizer Pressure	Pressurizer Pressure	2.0s
Low-Low Pressurizer Pressure	Pressurizer Pressure	2.0s
Low Pressurizer Level	Pressurizer Level	3.0s
Low-Low Pressurizer Level	Pressurizer Level	3.0s
Low Main Steam Pressure	Main Steam Pressure	2.0s
Low-Low Main Steam Pressure	Main Steam Pressure	2.0s
High Main Steam Pressure	Main Steam Pressure	2.0s
Low Main Steam Superheat	Main Steam Pressure & Temperature	8.0s
High Main Steam Superheat	Main Steam Pressure & Temperature	8.0s
Low RCS Flow	RCS Flow	6.0s
Low-Low RCS Flow	RCS Flow	6.0s
Low AC Voltage to the Battery Chargers	AC Voltage	≤ 60.0s
High Under-the-Bioshield Temperature	Under-the-Bioshield Temperature	8.0s
Low RPV Riser Level Range	RPV Riser Level	60.0s
Low-Low RPV Riser Level Range	RPV Riser Level	60.0s

Table 7.1-7: Summary of Post-accident Monitoring Variables

Variable	Range	System	Type A	Type B	Type C	Type D	Type E	Type F
Neutron Flux (Note 1)	0-200% RTP	MPS		X		X		
Core Exit Temperatures	0-2300°F	MPS		X	X	X		
Wide Range RCS Pressure	0-2500 psia	MPS		X	X	X		
Wide Range RCS T _{HOT}	40-700°F	MPS		X				
RPV Riser Level	Top of the RPV riser to the top of the upper core plate	MPS		X	X	X		
Wide Range Containment Pressure	0-1400 psia	MPS		X	X	X		
Containment Isolation Valve Position	Closed	MPS		X	X	X		
Inside Bioshield Area Radiation Monitor	Note 3	MPS		X	X			X
ECCS Valve Position (Note 5)	Open/Closed	MPS				X		
Spent Fuel Pool Water Level	Top of pool to top of spent fuel racks	PPS				X		X
DHRS Valve Position	Open	MPS				X		
Secondary MSIV Position	Closed	MPS				X		
Secondary MSIV Bypass Valve Position	Closed	MPS				X		
FWRV Position	Closed	MPS				X		
RCS Flow	0-120% flow	MPS				X		
Reactor Trip Breaker Position Feedback	Open	MPS				X		
Pressurizer Heater Breaker Position Feedback	Open	MPS				X		
Demineralized Water Supply Isolation Valve Position	Closed	MPS				X		
Under-the-Bioshield Temperature	40-700°F	MPS				X		
NMS Flood Detector Position	Deployed/Retracted	MPS				X		
CRHS Air Supply Isolation Valve Position	Open	PPS				X		
CRHS Pressure Relief Isolation Valve Position	Closed	PPS				X		
CRVS Supply Air Damper Position	Open/Closed	PPS				X		
CRVS General Exhaust Damper Position	Open/Closed	PPS				X		
CRVS Return Air Damper Position	Open/Closed	PPS				X		
RXB Plant Exhaust Stack - Flowrate	0-110% flow rate	RBVS					X	
RXB Plant Exhaust Stack - Noble Gas Activity	Note 2	RBVS					X	
RXB Plant Exhaust Stack - Particulates And Halogens	Note 2	RBVS					X	
RXB Continuous Airborne Monitor - Noble Gas Activity	Note 3	RMS					X	
RXB Continuous Airborne Monitor - Particulates and Halogens	Note 3	RMS					X	
Hot Lab - Area Radioactivity	Note 3	RMS					X	

Table 7.1-7: Summary of Post-accident Monitoring Variables (Continued)

Variable	Range	System	Type A	Type B	Type C	Type D	Type E	Type F
Hot Lab - Particulates	Note 3	RMS					X	
Primary Sampling System Equipment - Area Radioactivity	Note 3	RMS					X	
Containment Sampling System Equipment -Area Radioactivity	Note 3	RMS					X	
EDAS Switchgear Rooms - Area Radioactivity	Note 3	RMS					X	
Safety Instrument Rooms - Area Radioactivity	Note 3	RMS					X	
RXB Refuel Pool - Area Radioactivity	Note 3	RMS					X	
Technical Support Center - Control Support Area Radiation Level	Note 3	RMS					X	
Condenser Air Removal Vacuum Pump Exhaust - Flowrate	0-110% flow rate	CARS					X	
Condenser Air Removal Vacuum Pump Exhaust - Noble Gases	Note 2	CARS					X	
Meteorological And Environmental Monitoring System - Site Specific	N/A	N/A					X	
Plant Environs Radiation and Radioactivity - Site Specific	N/A	N/A					X	
MCR Area Radiation	Note 3	RMS					X	
MCR Noble Gas Activity	Note 3	RMS					X	
MCR Particulates and Halogens	Note 3	RMS					X	

Note 1: The neutron flux PAM variables are provided by the NMS-excore indications; NMS-flood provides the neutron count rate indication during conditions when the containment is flooded.

Note 2: The process and effluent radiation monitoring instrumentation ranges are provided in Table 11.5-1.

Note 3: The fixed area and airborne radiation monitoring instrumentation ranges are provided in Table 12.3-8.

Note 4: Acronyms are defined in Table 1.1-1.

Note 5: ECCS valve position includes the reactor vent valves, reactor recirculation valves, and thier associated trip solenoid valve positions.

Table 7.1-8: Sensor Inputs to Module Protection System

Process Variable	Sensor Type	Output Signal	Safety-Related?	Sensor Block I			Sensor Block II		
				SG A	SG C	DIV. I	SG B	SG D	DIV. II
Pressurizer level (Note 1)	Digital	Analog	Y	X	X	-	X	X	-
RPV riser level	Multiple discrete points (Analog)	Analog	Y	-	X	-	X	-	-
PZR pressure	Analog	Analog	Y	X	X	-	X	X	-
Wide-range RCS pressure	Analog	Analog	Y	X	X	-	X	X	-
Containment water level	Multiple discrete points (Analog)	Analog	Y	X	X	-	X	X	-
Narrow-range containment pressure	Analog	Analog	Y	X	X	-	X	X	-
Wide-range containment pressure	Analog	Analog	N	-	X	-	X	-	-
Containment isolation valve position (except FWIV Valve Position)	Discrete (Analog)	Discrete (Analog)	N	-	-	X	-	-	X
Secondary MSIV position	Discrete (Analog)	Discrete (Analog)	N	-	-	X	-	-	X
Secondary MSIV bypass isolation valve position	Discrete (Analog)	Discrete (Analog)	N	-	-	X	-	-	X
Feedwater regulation valve position	Discrete (Analog)	Discrete (Analog)	N	-	-	X	-	-	X
ECCS valve position	Discrete (Analog)	Discrete (Analog)	N	-	-	X	-	-	X
Narrow-range RCS hot temperature	Analog	Analog	Y	X	X	-	X	X	-
Wide-range RCS hot temperature	Analog	Analog	Y	X	X	-	X	X	-
Narrow Range RCS Cold Temperature	Analog	Analog	Y	X	X	-	X	X	-
Wide-range RCS cold temperature	Analog	Analog	Y	X	X	-	X	X	-
Core exit temperature	Analog	Analog	N	-	X	-	X	-	-
RCS flow (Note 1)	Digital	Analog	Y	X	X	-	X	X	-
Main steam pressure (decay heat removal inlet pressure)	Analog	Analog	Y	X	X	-	X	X	-
Main steam temperature (decay heat removal inlet temperature)	Analog	Analog	Y	X	X	-	X	X	-
Power range linear power	Analog	Analog	Y	X	X	-	X	X	-
Intermediate range log power	Analog	Analog	Y	X	X	-	X	X	-
Source range count rate	Analog	Analog	Y	X	X	-	X	X	-
Source/intermediate range fault	Discrete (Analog)	Discrete (Analog)	Y	X	X	-	X	X	-
Power range fault	Discrete (Analog)	Discrete (Analog)	Y	X	X	-	X	X	-
NMS Supply Fault	Discrete (Analog)	Discrete (Analog)	Y	X	X	-	X	X	-

Table 7.1-8: Sensor Inputs to Module Protection System (Continued)

Process Variable	Sensor Type	Output Signal	Safety-Related?	Sensor Block I			Sensor Block II		
				SG A	SG C	DIV. I	SG B	SG D	DIV. II
Inside bioshield area radiation monitor	Digital	Analog	N	-	X	-	X	-	-
FWIV position	Discrete (Analog)	Discrete (Analog)	Y	-	-	X	-	-	X
Reactor trip breaker position	Discrete (Analog)	Discrete (Analog)	Y	-	-	X	-	-	X
Pressurizer heater breaker position	Discrete (Analog)	Discrete (Analog)	N	-	-	X	-	-	X
DHRS valve position	Discrete (Analog)	Discrete (Analog)	N	-	-	X	-	-	X
Demineralized water system isolation valve position	Discrete (Analog)	Discrete (Analog)	N	-	-	X	-	-	X
ELVS voltage	Analog	Analog	N	X	X	-	X	X	-
Reactor safety valve position	Discrete (Analog)	Discrete (Analog)	N	-	X	-	X	-	-
Under-the-bioshield temperature	Analog	Analog	Y	X	X	-	X	X	-
NMS-Flood	Analog	Analog	N	-	X	-	X	-	-
NMS-Flood Faults	Discrete (Analog)	Discrete (Analog)	N	-	X	-	X	-	-
NMS-Flood Detector Position	Discrete (Analog)	Discrete (Analog)	N	-	X	-	X	-	-
Containment evacuation vacuum pump suction pressure	Analog	Analog	N	X	-	-	-	X	-

Note 1: These sensors are digital-based and perform safety-related functions.

Table 7.1-9: Intentional Differences Between Field Programmable Gate Array Architecture

Software Tool	Safety Block I and Division I SDIS	Safety Block II and Division II SDIS
Design synthesis tool(s)	Suite A	Suite B
Design analysis tool(s)		
Physical design tool(s)		
Design simulation tool(s)		
Physical programming tool(s)		
Independent Verification and Validation design simulation tool(s)	Different than Suite A and Suite B	

**Table 7.1-10: Partial Spurious Actuation Scenarios for Engineered Safety Features
Actuation System within Safety Block I**

Scenario	Protective Action(s) on EIM	Components Actuated
1	Containment isolation, DHRS, and secondary System Isolation	MSIVs MS isolation bypass valves Feedwater isolation valves Secondary MSIVs Secondary MSIV bypass valves Feedwater regulating valves
2	ECCS	ECCS reactor recirculation valve
3	ECCS and LTOP	ECCS reactor vent valves
4	Containment isolation	Containment evacuation CIV Containment flood & drain CIV Reactor component cooling water CIVs
5	CVCS isolation, containment isolation and pressurizer line isolation	CVCS containment isolation valves
6	DWS isolation	DWS isolation valve
7	PZR heater trip	PZR heater breakers
8	DHRS	DHRS Actuation Valves

Table 7.1-11: Consequences of Partial Spurious Reactor Trip

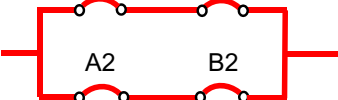
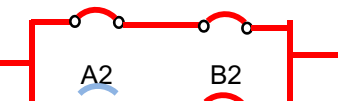
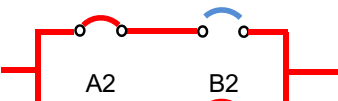
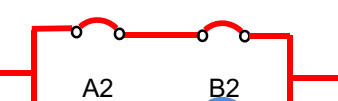
Event		RTS Trip Demand		Reactor Trip Breaker Status	Result	
No.	Description				Reactor Trip	Comments /Notes
1	No trip No failure	A1	B1		No	Normal operation
		N	N			
		A2	B2			
		N	N			
2	Partial spurious Division I trip	A1	B1		No	Only one of the two Division I RTBs trip, which is not enough to cause a reactor trip
		T	N			
		A2	B2			
		N	N			
3	Partial spurious Division I trip	A1	B1		No	Only one of the two Division I RTBs trip, which is not enough to cause a reactor trip
		N	N			
		A2	B2			
		T	N			
4	Partial spurious Division II trip	A1	B1		No	Only one of the two Division II RTBs trip, which is not enough to cause a reactor trip
		N	T			
		A2	B2			
		N	N			
5	Partial spurious Division II trip	A1	B1		No	Only one of the two Division II RTBs trip, which is not enough to cause a reactor trip
		N	N			
		A2	B2			
		N	T			

Table 7.1-12: Effects of Digital-Based Common Cause Failure of Level Function Type on Sensor Block I

Function Type	Process Variable	Sensor Block I	Sensor Block II
Digital-based level measurement	PZR level	Digital-based CCF	OK
Digital-based flow measurement	RCS flow	OK	OK

Table 7.1-13: Effects of Digital-Based Common Cause Failure of Digital-Based Flow Function Type on Sensor Block I and II

Function Type	Process Variable	Sensor Block I	Sensor Block II
Digital-based level measurement	PZR level	OK	OK
Digital-based flow measurement	RCS flow	Digital-based CCF	Digital-based CCF

Table 7.1-14: Safety-Related Digital Sensors Used by Safety Block I and II

Input Signal	Sensor Technology	Function
PZR water level	Digital-based level	Initiate protective action(s)
RCS flow	Digital-based flow	Initiate protective action(s)

Table 7.1-15: Effect of Field Programmable Gate Array Technology Diversity for Postulated Digital-Based Common Cause Failure of Module Protection System Safety Blocks

Event	Event Type	Safety Block I		Safety Block II		Comments
		SG A	SG C	SG B	SG D	
All Design Basis Events	Any Event Type	CCF	CCF	OK	OK	Based on the diversity attributes between Safety Blocks, a digital-based CCF would be limited to either Safety Block I or Safety Block II.
All Design Basis Events	Any Event Type	OK	OK	CCF	CCF	

Table 7.1-16: Example: Hazard Conditions

Hazard ID	Hazard
H-1	Reactor trip does not initiate when required.
H-2	Control room habitability system does not actuate when required.
H-3	Protective action stops before completion.

Table 7.1-17: Example: Safety Functions

Safety Function ID	Safety Function	Initiating Conditions	Setpoint
SF-1a	Reactor trip	High power	25%, 115% RTP
SF-1b		High log power rate	3 decades per minute
SF-1c		High RCS hot temperature	620 °F
SF-2a	DHRS actuation	High pressurizer pressure	2100 psia
SF-2b		High pressurizer level	80%
SF-2c		Low main steam pressure	300 psia

Table 7.1-18: Example: High-level Safety Constraints

Safety Constraint ID	Safety Constraint
SC-1	The safety system shall initiate reactor trip when setpoints listed in the table of safety functions, Table 7.1-3, are exceeded.
SC-2	The safety system shall actuate decay heat removal when required conditions listed in the table of safety functions, Table 7.1-4, are met.
SC-3	All protective actions shall continue to completion in accordance with IEEE Std 603-1991, Clause 5.2.

Table 7.1-19: Example: Safety Constraints Associated with Plant Conditions

Safety Constraint ID	Condition	Constraint
SC-1a	Variable high power	Reactor trip breakers are opened when neutron flux $\geq$ High setpoint
SC-1b	High rate power change	Reactor trip breakers are opened when the rate of change of reactor power $\geq$ High neutron flux rate setpoint
SC-1c	High T_{hot}	Reactor trip breakers are opened when $T_{\text{hot}} \geq$ High T_{hot} setpoint
SC-2a	Low steam pressure	Decay heat removal is actuated when steam pressure $\leq$ Low steam pressure setpoint
SC-2b	High steam pressure	Decay heat removal is actuated when steam pressure $\geq$ High steam pressure setpoint
SC-2c	Containment isolation	Decay heat removal is actuated when containment isolation is actuated

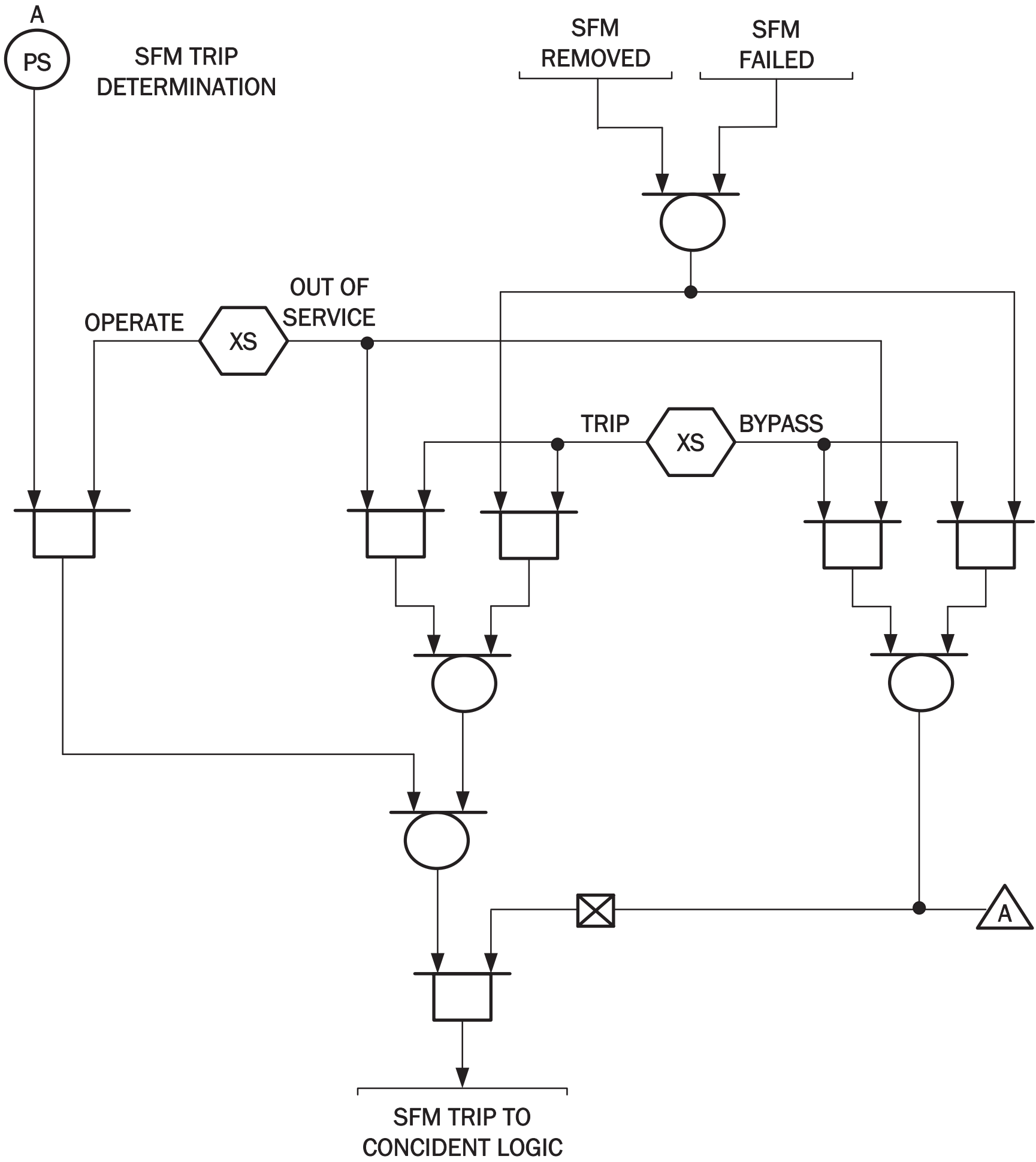
Table 7.1-20: Example: Control Action Analysis

Control Object	Command or event	Not Provided	Incorrect Provided	Too Early	Too Late	Out of Sequence	Stopped Too Soon
Signal conditioning	Receives analog input	Unsafe - [HC-1]	Unsafe - [HC-1]	N/A	N/A	N/A	N/A
Signal conditioning	Digital output	Unsafe - [HC-2]	Unsafe - [HC-2]	N/A	Unsafe - [HC-3]	N/A	N/A

Table 7.1-21: Example: Identified Hazard Causes

Hazard Analysis Identified Cause	PHL Identified Cause
Analog to digital conversion incorrect	Failure due to seismic disturbance/impact
Board level clock error	Damaged by high/low pressure or rapid change of pressure
Common cause failure of triple redundant communication transmitters	Damaged due to falling objects
Communication media open or short	Damaged due to impacts
Damaged cable	Damaged due to inadvertent motion
Electrical fault	Damaged due to loose object translation
Feedback processing error	Fails to operate
Hardware (actuator) fault	Grounding failure
Hardware (circuit board) fault	Insufficient physical space for operation of isolation device
Hardware (switch or wiring) open or short	Leaking
Loss of power	Loss of power
Module hardware fault	Operates at incorrect time
Operator error	Operates inadvertently
Power supply voltage too high/low	Operates incorrectly/erroneously
Procedural error	Receives erroneous data
Reactor trip breaker fault	Sends erroneous data
Safety-related isolator fault	Failure due to corrosion
Sensing line damaged	Failure due to faulty calibration
Sensor does not provide an output	Failure due to overvoltage or overcurrent
Setpoint error	Failure due to dust/dirt
Software/algorithm error	Failure due to EMI/RFI interference
	Failure due to fire
	Failure due to flooding
	Failure due to maintenance error
	Failure due to maintenance/installation error
	Failure due to moisture/humidity
	Failure due to radiation
	Failure due to temperature extremes
	Failure due to vibration
	Structural failure

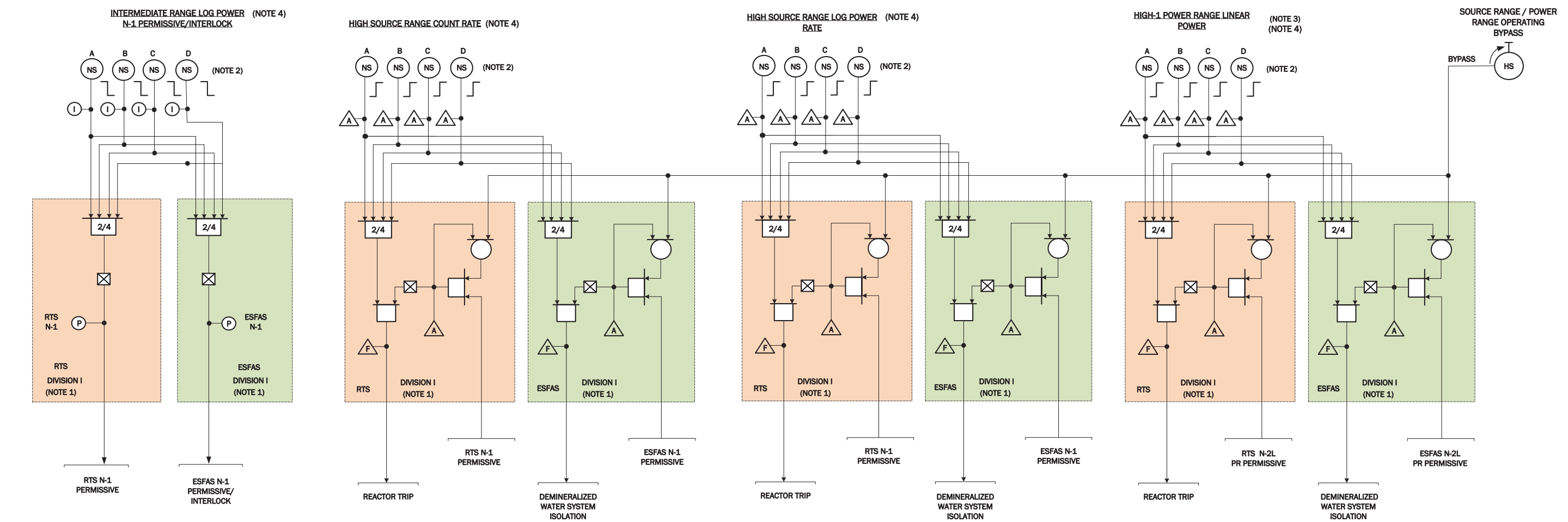
Figure 7.1-1a: Module Protection System And Plant Protection System Trip or Bypass Switch Logic



There is a trip/bypass switch for each SFM that has a safety function to allow removing the SFM from service.

- If the out of service switch on the SFM is in the operate position, the trip determination result of the safety function algorithm is sent to the RTS and ESFAS for that safety function.
- If the out of service switch is in the out of service position, the position of the trip/bypass switch determines what is sent to the RTS and ESFAS. If the trip/bypass switch is in bypass, safety functions for that SFM are forced to not trip or not actuate. If the trip/bypass switch is in the trip position, then safety functions for that SFM are forced to trip or actuate.
- If the SFM fails to communicate correctly to SBM or is removed, the position of the trip/bypass switch will determine the commands sent to the RTS and ESFAS for the safety function on that SFM.

Figure 7.1-1b: Source Range and Power Range Trips



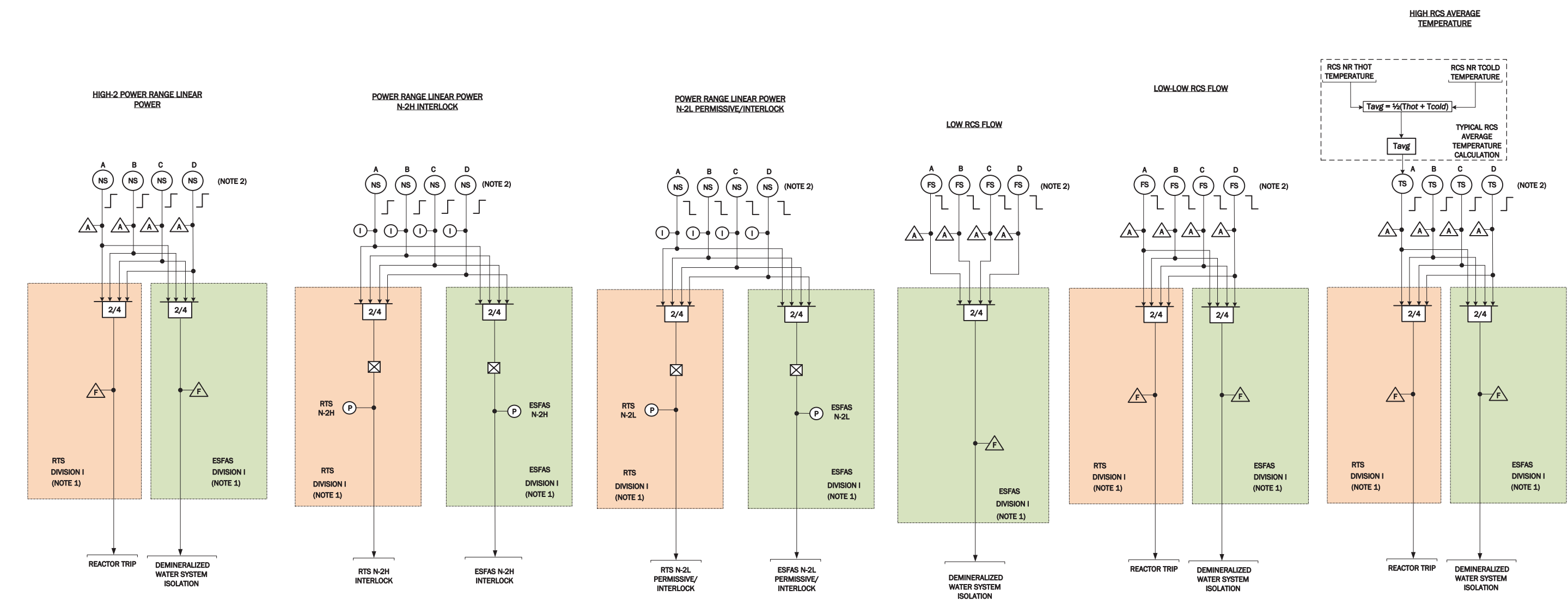
NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: THERE IS A TRIP/BYPASS SWITCH FOR EACH SFM THAT HAS A SAFETY FUNCTION THAT SUPPORTS REMOVING THE SFM FROM SERVICE.

NOTE 3: THE REACTOR STARTUP SEQUENCE WILL BE PHASED WITH A STARTUP/HEATUP HOLD POINT. ONCE THIS POWER LEVEL HAS BEEN ESTABLISHED, THE HIGH-1 POWER TRIP WILL BE BYPASSED SO THAT POWER CAN BE INCREASED TO FULL POWER. THE HIGH-2 POWER TRIP IS IN PLACE WHEN THE HIGH-1 TRIP IS BYPASSED.

NOTE 4: SEE FIGURE 7.1-5 FOR MODULE PROTECTION SYSTEM INTERLOCKS / PERMISSIVES / OVERRIDES

Figure 7.1-1c: Power Range High-2 Power Trip and N-2 Interlocks, Low and Low Low RCS Flow Trips

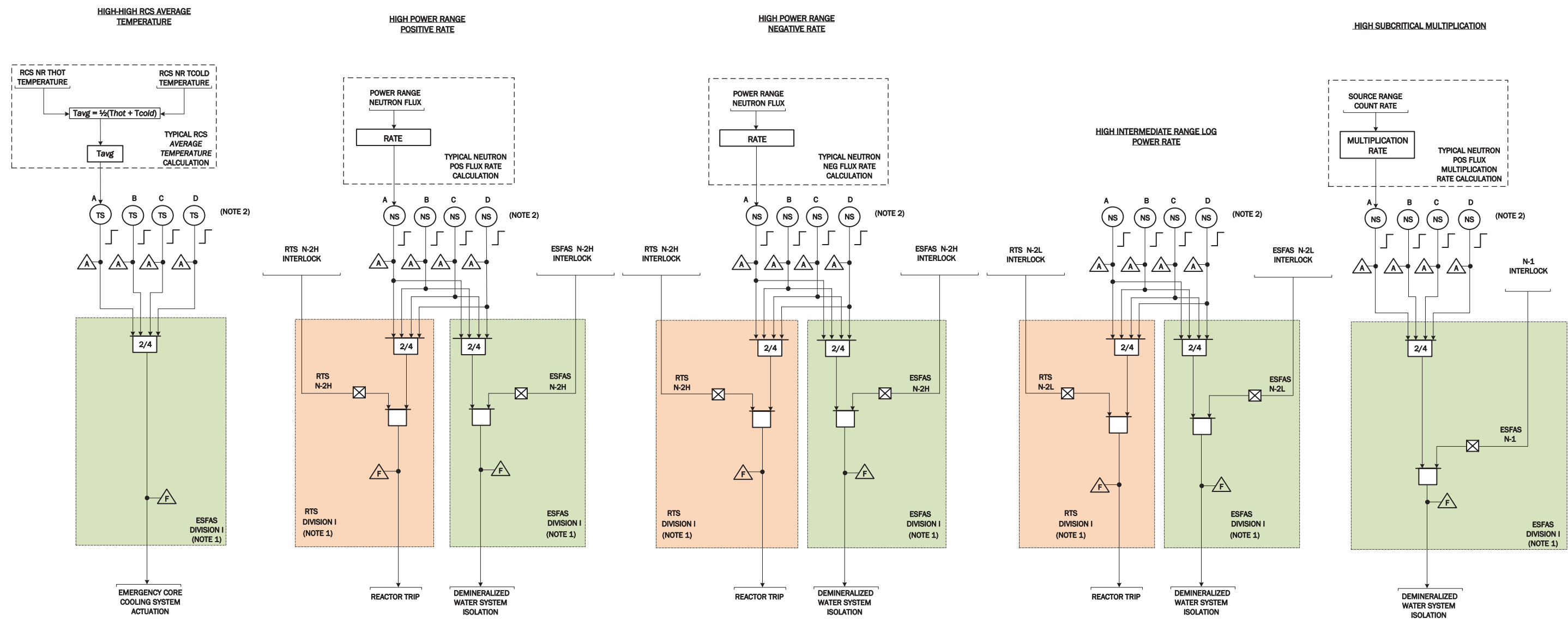


NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: THERE IS A TRIP/BYPASS SWITCH FOR EACH SFM THAT HAS A SAFETY FUNCTION THAT SUPPORTS REMOVING THE SFM FROM SERVICE.

NOTE 3: SEE FIGURE 7.1-5 FOR MODULE PROTECTION SYSTEM INTERLOCKS / PERMISSIVES / OVERRIDES

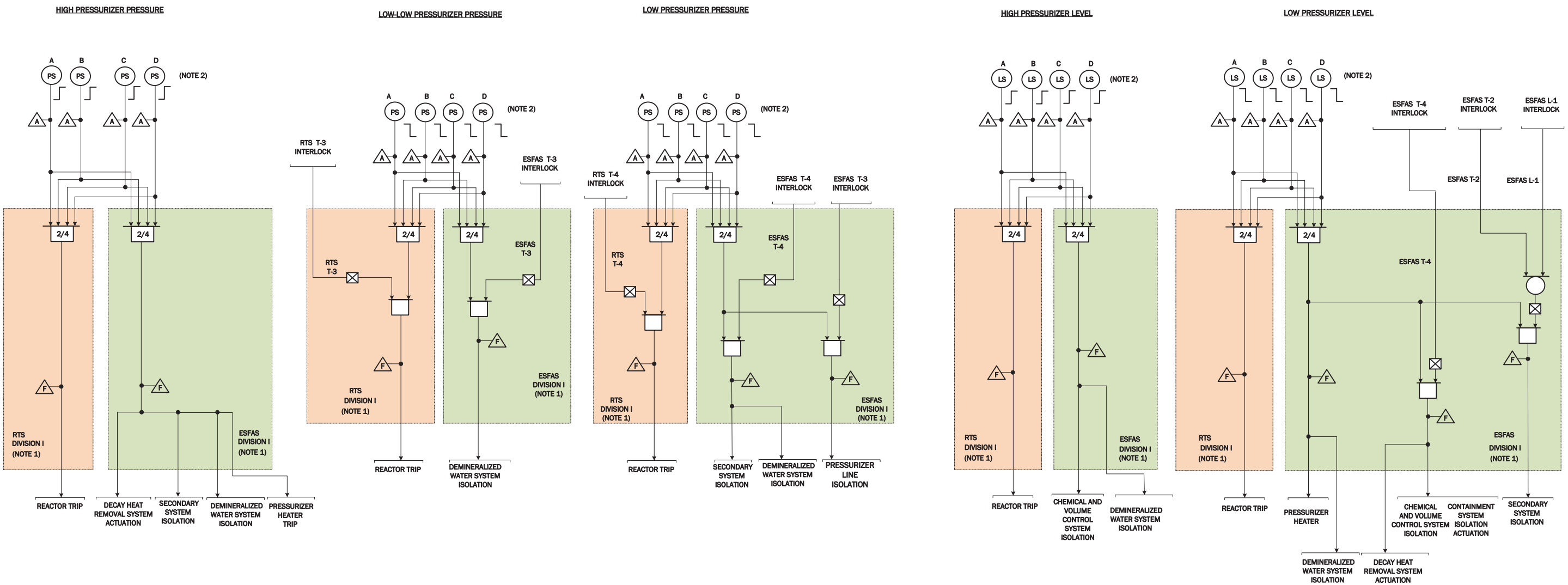
Figure 7.1-1d: Power Range and Intermediate Range Rate Trips



NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: THERE IS A TRIP/BYPASS SWITCH FOR EACH SFM THAT HAS A SAFETY FUNCTION THAT SUPPORTS REMOVING THE SFM FROM SERVICE.

Figure 7.1-1e: Pressurizer Pressure and Level Trips



NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: THERE IS A TRIP/BYPASS SWITCH FOR EACH SFM THAT HAS A SAFETY FUNCTION THAT SUPPORTS REMOVING THE SFM FROM SERVICE.

Figure 7.1-1f: Reactor Coolant System Hot Temperature Trip, Temperature Interlocks

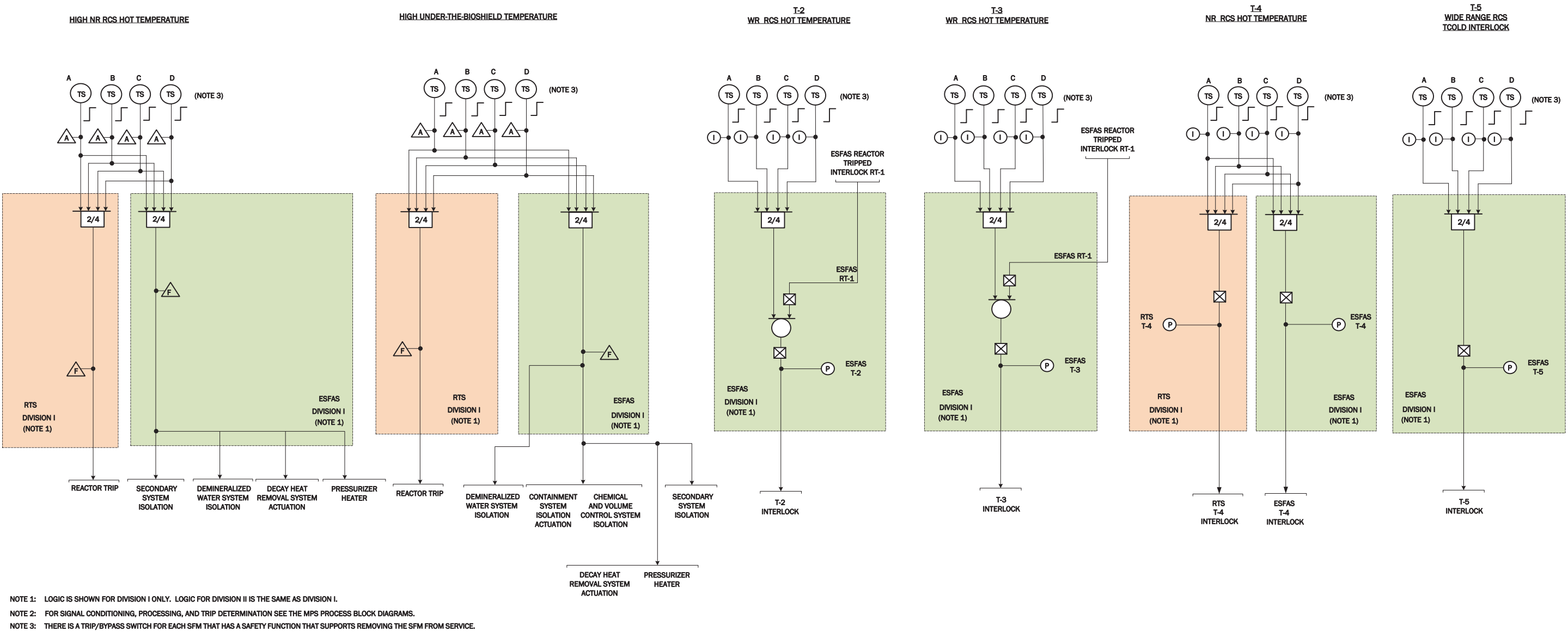
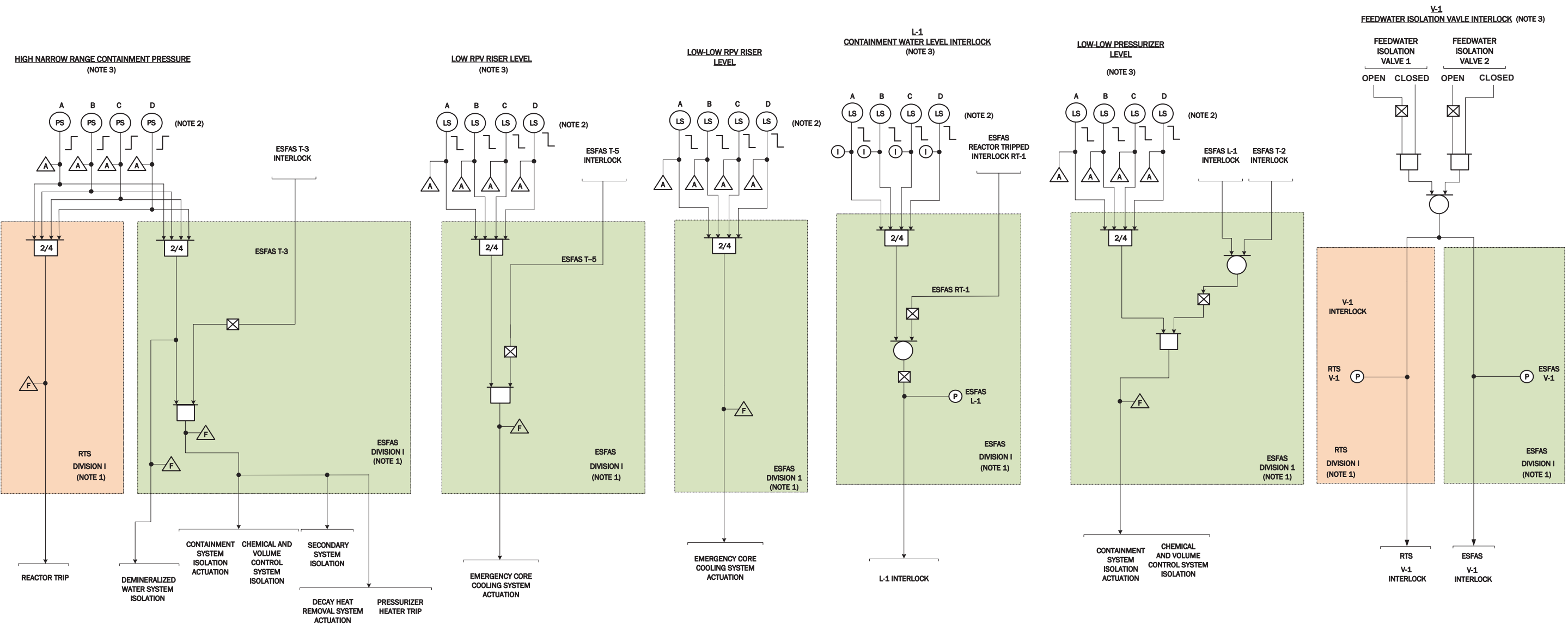


Figure 7.1-1g: Pressurizer Level Interlock and Trip, High Containment Pressure, and High Containment Level Trips

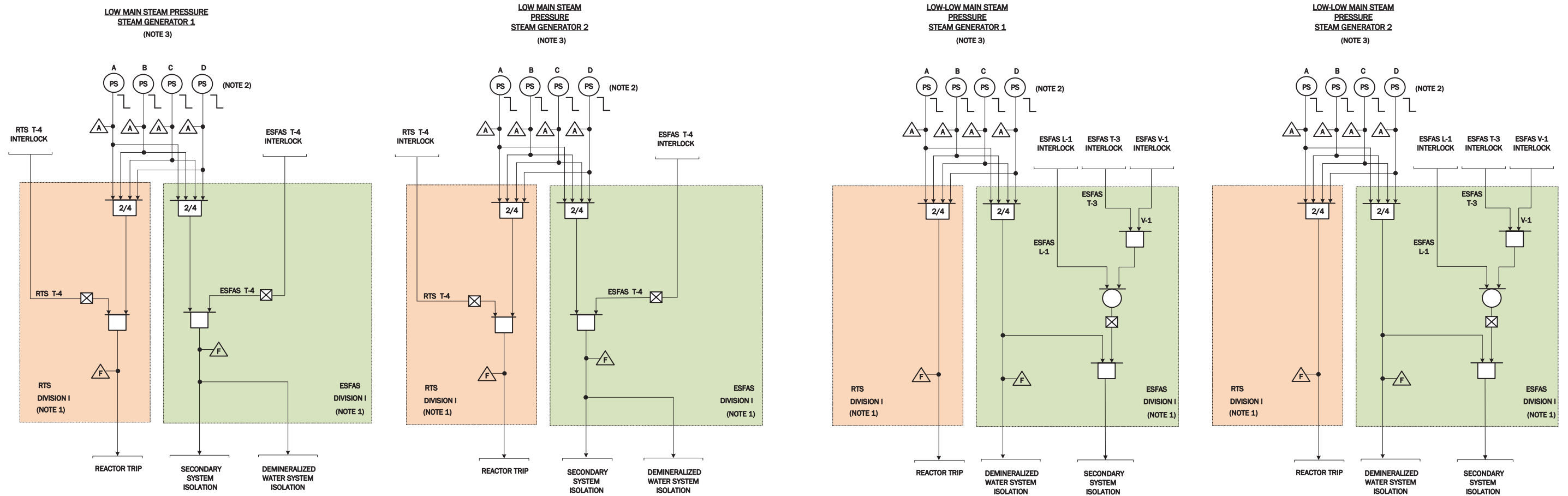


NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: THERE IS A TRIP/BYPASS SWITCH FOR EACH SFM THAT HAS A SAFETY FUNCTION THAT SUPPORTS REMOVING THE SFM FROM SERVICE.

NOTE 3: SEE FIGURE 7.1-5 FOR MODULE PROTECTION SYSTEM INTERLOCKS / PERMISSIVES / OVERRIDES

Figure 7.1-1h: Steam Generator Low and Low Low Main Steam Pressure Trips

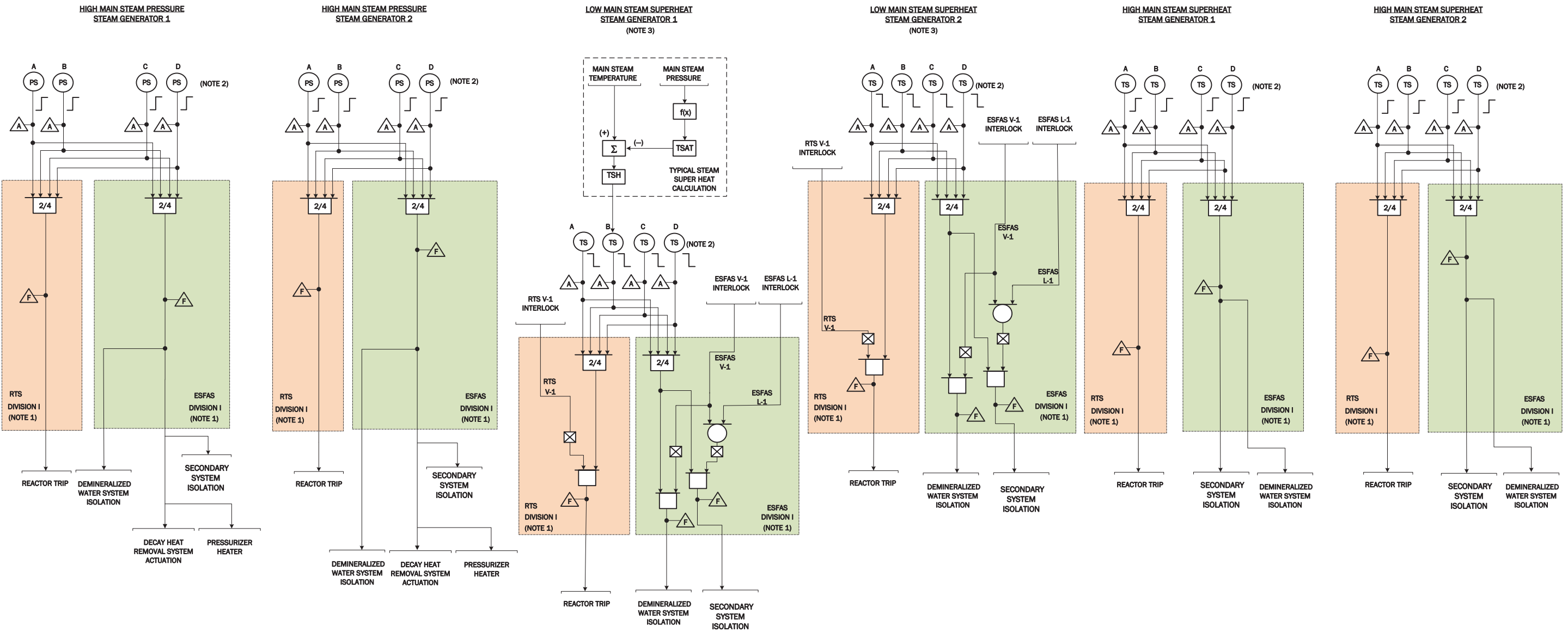


NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: THERE IS A TRIP/BYPASS SWITCH FOR EACH SFM THAT HAS A SAFETY FUNCTION THAT SUPPORTS REMOVING THE SFM FROM SERVICE.

NOTE 3: SEE FIGURE 7.1-5 FOR MODULE PROTECTION SYSTEM INTERLOCKS / PERMISSIVES / OVERRIDES

Figure 7.1-1i: High Main Steam Pressure and Steam Generator Low and High Steam Superheat Trips

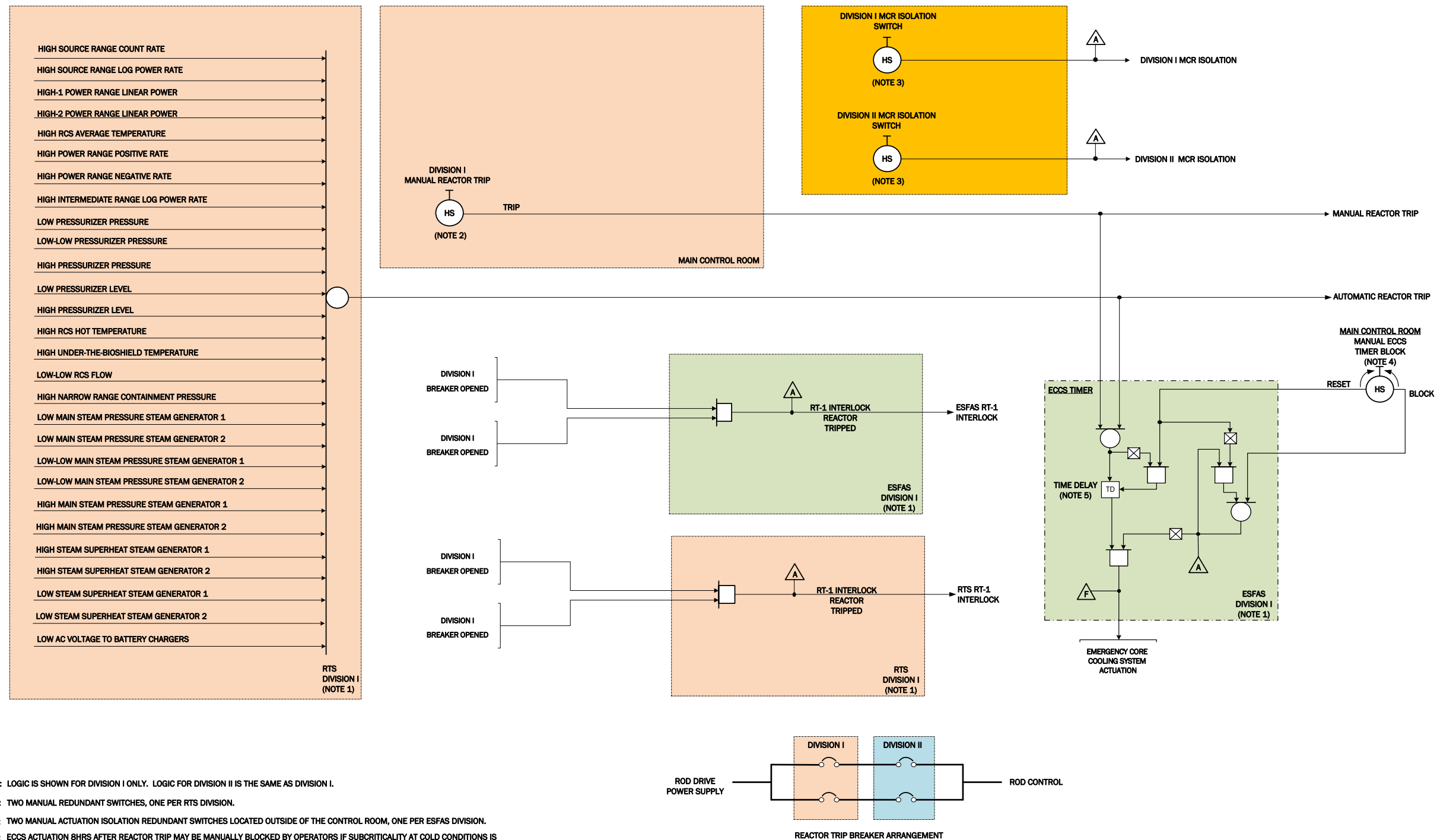


NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: THERE IS A TRIP/BYPASS SWITCH FOR EACH SFM THAT HAS A SAFETY FUNCTION THAT SUPPORTS REMOVING THE SFM FROM SERVICE.

NOTE 3: SEE FIGURE 7.1-5 FOR MODULE PROTECTION SYSTEM INTERLOCKS / PERMISSIVES / OVERRIDES

Figure 7.1-1j: Reactor Trip and Reactor Tripped Interlock RT-1



NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

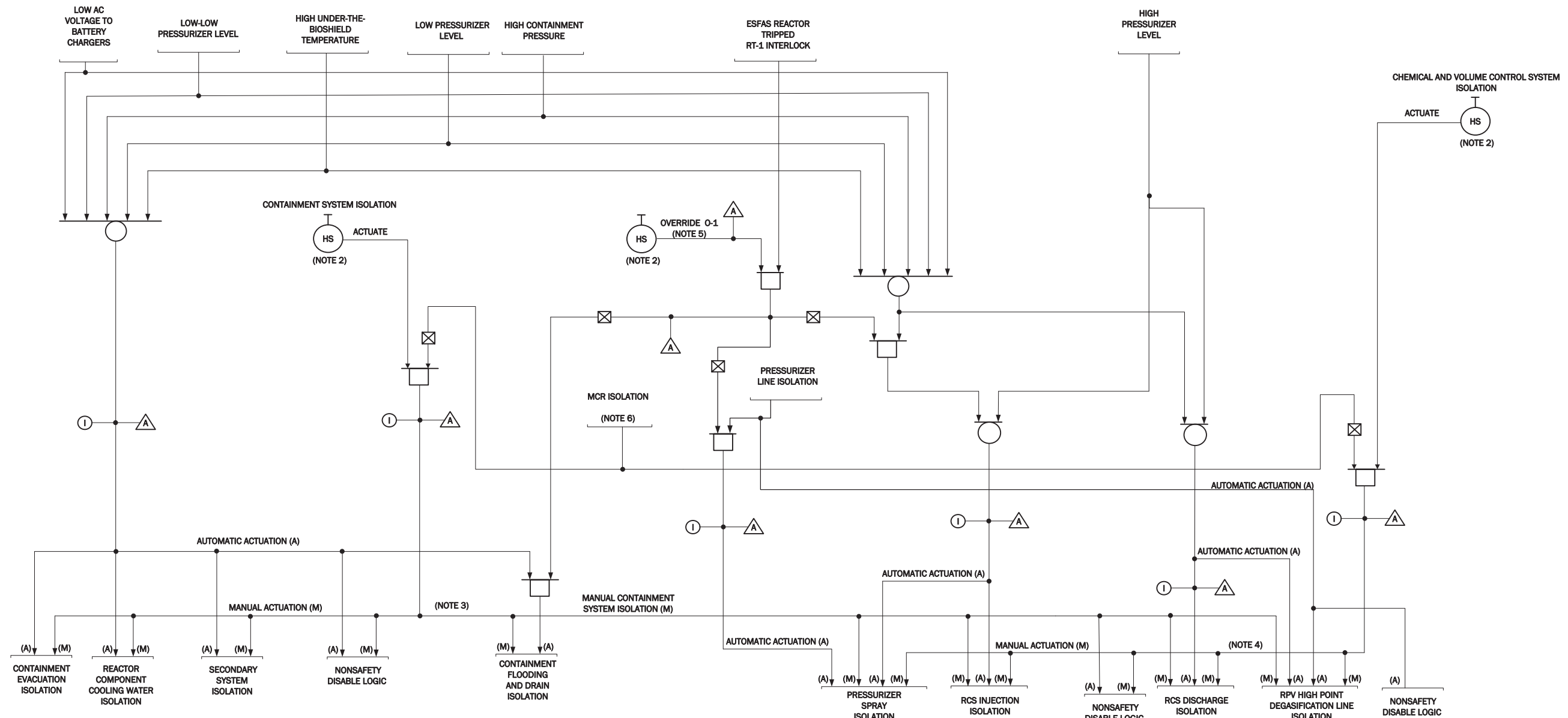
NOTE 2: TWO MANUAL REDUNDANT SWITCHES, ONE PER RTS DIVISION.

NOTE 3: TWO MANUAL ACTUATION ISOLATION REDUNDANT SWITCHES LOCATED OUTSIDE OF THE CONTROL ROOM, ONE PER ESFAS DIVISION.

NOTE 4: ECCS ACTUATION 8HRS AFTER REACTOR TRIP MAY BE MANUALLY BLOCKED BY OPERATORS IF SUBCRITICALITY AT COLD CONDITIONS IS CONFIRMED AND IF IT IS CONFIRMED THAT THE RPV CONTAINS SUFFICIENT HYDROGEN TO MAINTAIN A CRITICAL HYDROGEN CONCENTRATION IN THE RCS THROUGHOUT DHRS COOLDOWN.

NOTE 5: A CHANGE IN LOGIC STATE (FROM TRUE TO FALSE) RESETS THE TIMER. TIMER IS INSTANTIATED IN THE ESFAS SVM(S).

Figure 7.1-1k: ESFAS - Containment System Isolation and Chemical and Volume Control System Isolation Interlocks



NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: TWO SWITCHES, ONE PER ESFAS DIVISION.

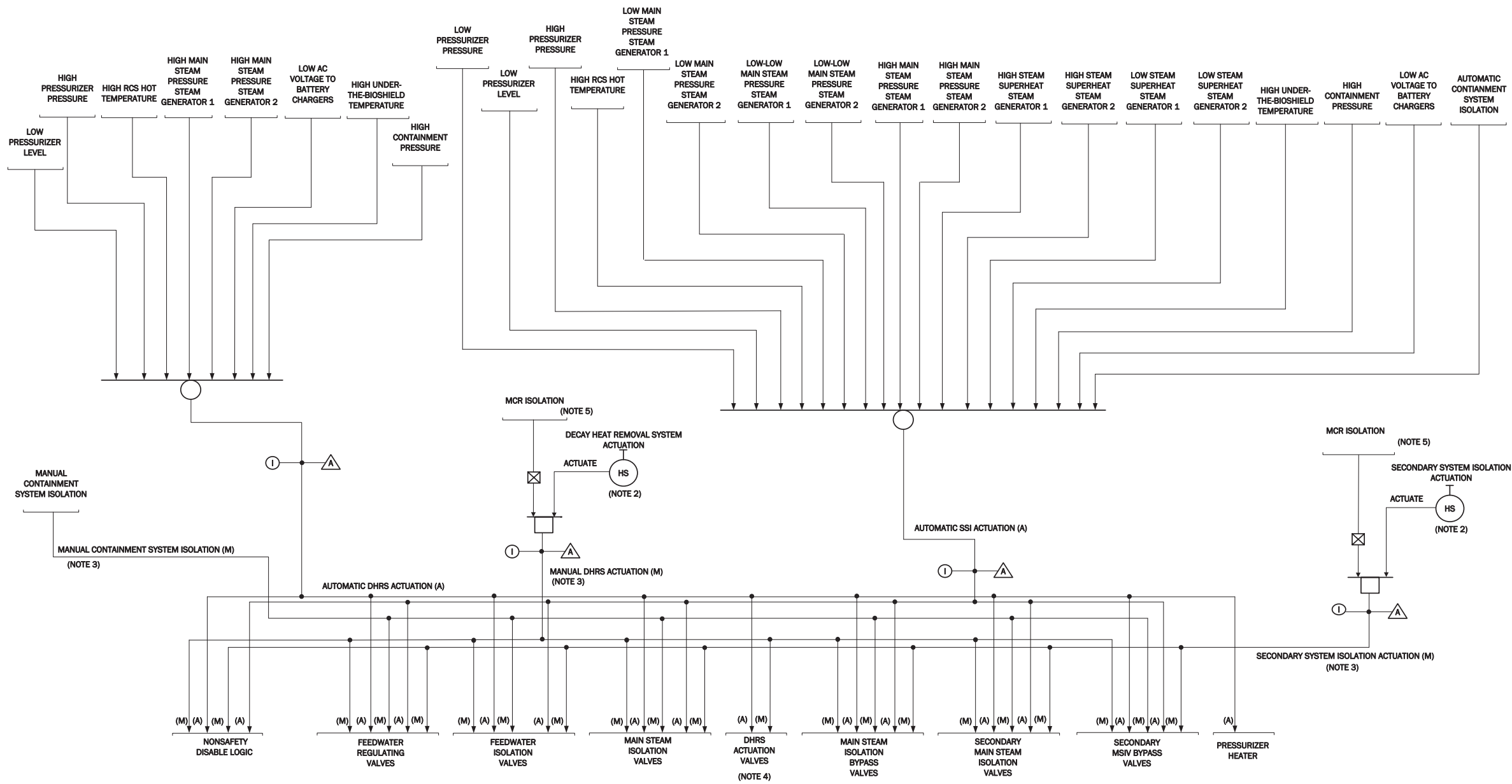
NOTE 3: MANUAL ACTUATION INITIATES CONTAINMENT SYSTEM ISOLATION AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.

NOTE 4: MANUAL ACTUATION INITIATES CHEMICAL AND VOLUME CONTROL SYSTEM ISOLATION AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.

NOTE 5: OVERRIDE TO ALLOW OPERATORS TO ADD WATER VIA CFDS OR CVCS.

NOTE 6: TWO MANUAL ACTUATION ISOLATION SIGNALS, ONE PER ESFAS DIVISION.

Figure 7.1-1I: ESFAS - Decay Heat Removal System and Secondary System Isolation Actuation, FWIV Interlock



NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.
NOTE 2: TWO SWITCHES, ONE PER ESFAS DIVISION.
NOTE 3: MANUAL ACTUATE INITIATES ACTUATION AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.
NOTE 4: DECAY HEAT REMOVAL SYSTEM ACTUATION IS DEFINED AS THE SIMULTANEOUS CLOSURE OF THE FWIV, FWRV, MSIV, SECONDARY MSIV AND THE OPENING OF THE DHRS ACTUATION VALVES FOR A GIVEN TRAIN OF DHRS.
NOTE 5: TWO MANUAL ACTUATION ISOLATION SIGNALS, ONE PER ESFAS DIVISION.

Figure 7.1-1m: ESFAS - Demineralized Water System Isolation, Pressurizer Heater Trip

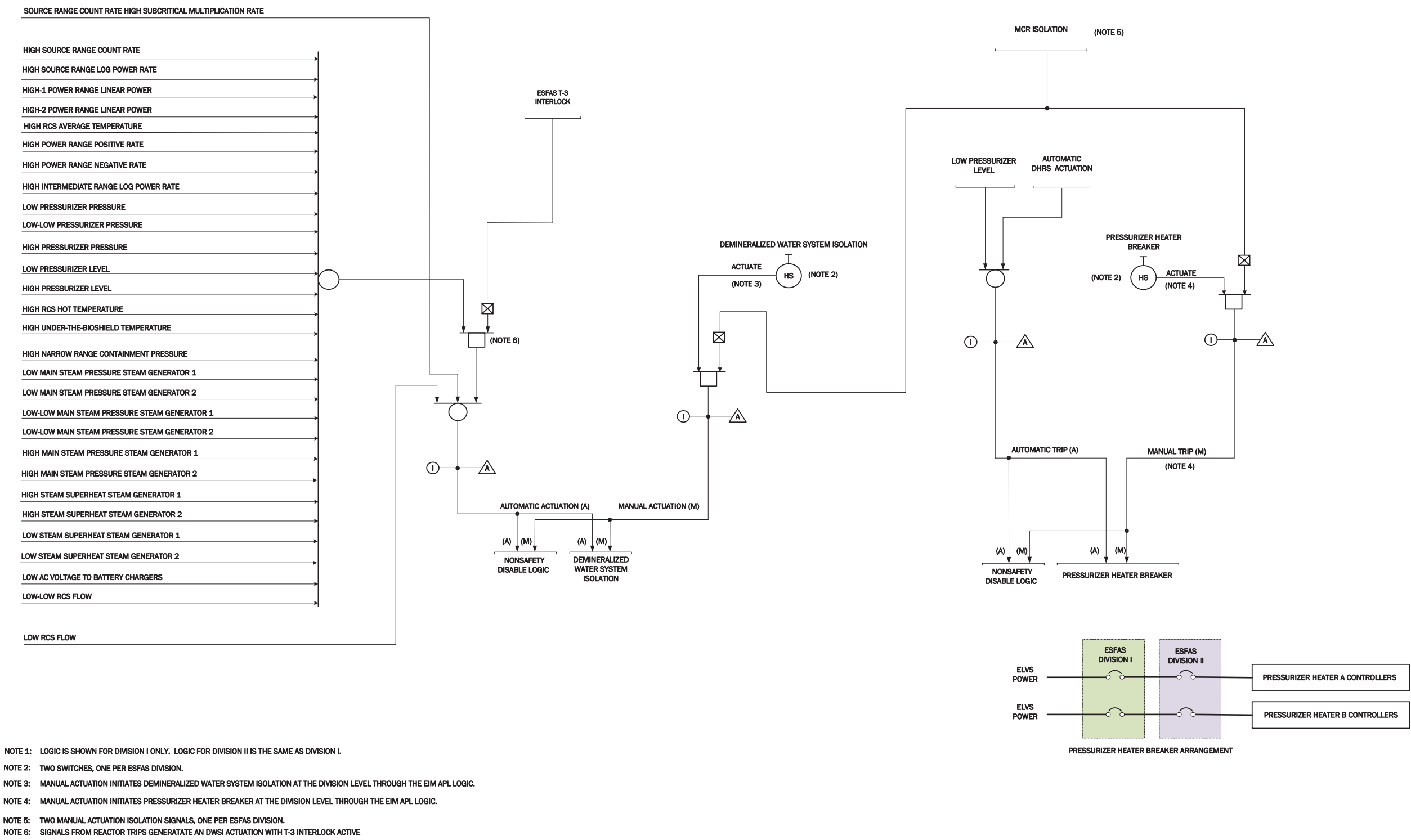
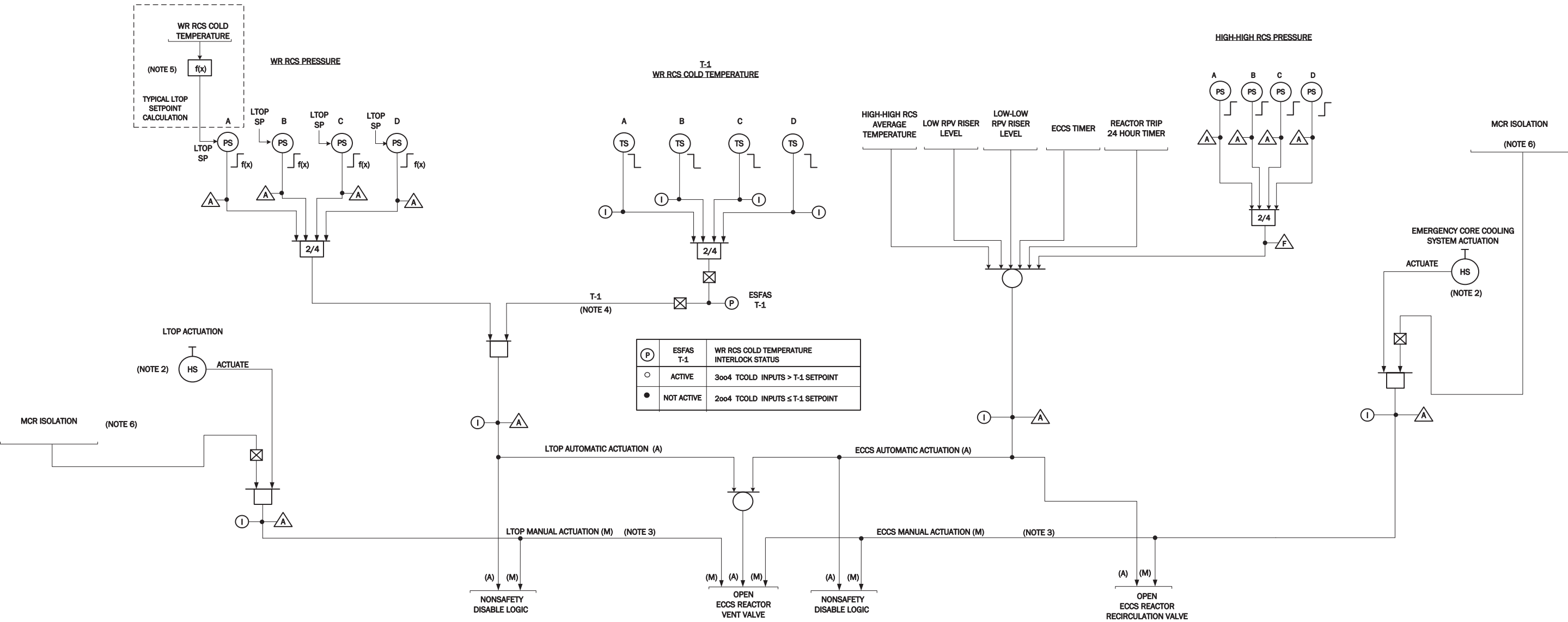


Figure 7.1-1n: ESFAS Emergency Core Cooling System Actuation, Low Temperature Overpressure Protection Actuation



- NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.
- NOTE 2: TWO SWITCHES, ONE PER ESFAS DIVISION.
- NOTE 3: MANUAL ACTUATE INITIATES LTOP ACTUATION AND EMERGENCY CORE COOLING SYSTEM ACTUATION AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.
- NOTE 4: LOW TEMPERATURE INTERLOCK T-1: AUTOMATIC BLOCK ABOVE T-1; AUTOMATIC LTOP ENABLE BELOW T-1.
- NOTE 5: LTOP SETPOINT (SP) IS CALCULATED BASED ON WR RCS COLD TEMPERATURE. LTOP ACTUATION OCCURS WHEN 2/4 WR RCS PRESSURE INPUTS INCREASE ABOVE THE LTOP SP.
- NOTE 6: TWO MANUAL ACTUATION ISOLATION SIGNALS, ONE PER ESFAS DIVISION.

Figure 7.1-1o: Decay Heat Removal System Valve Actuation

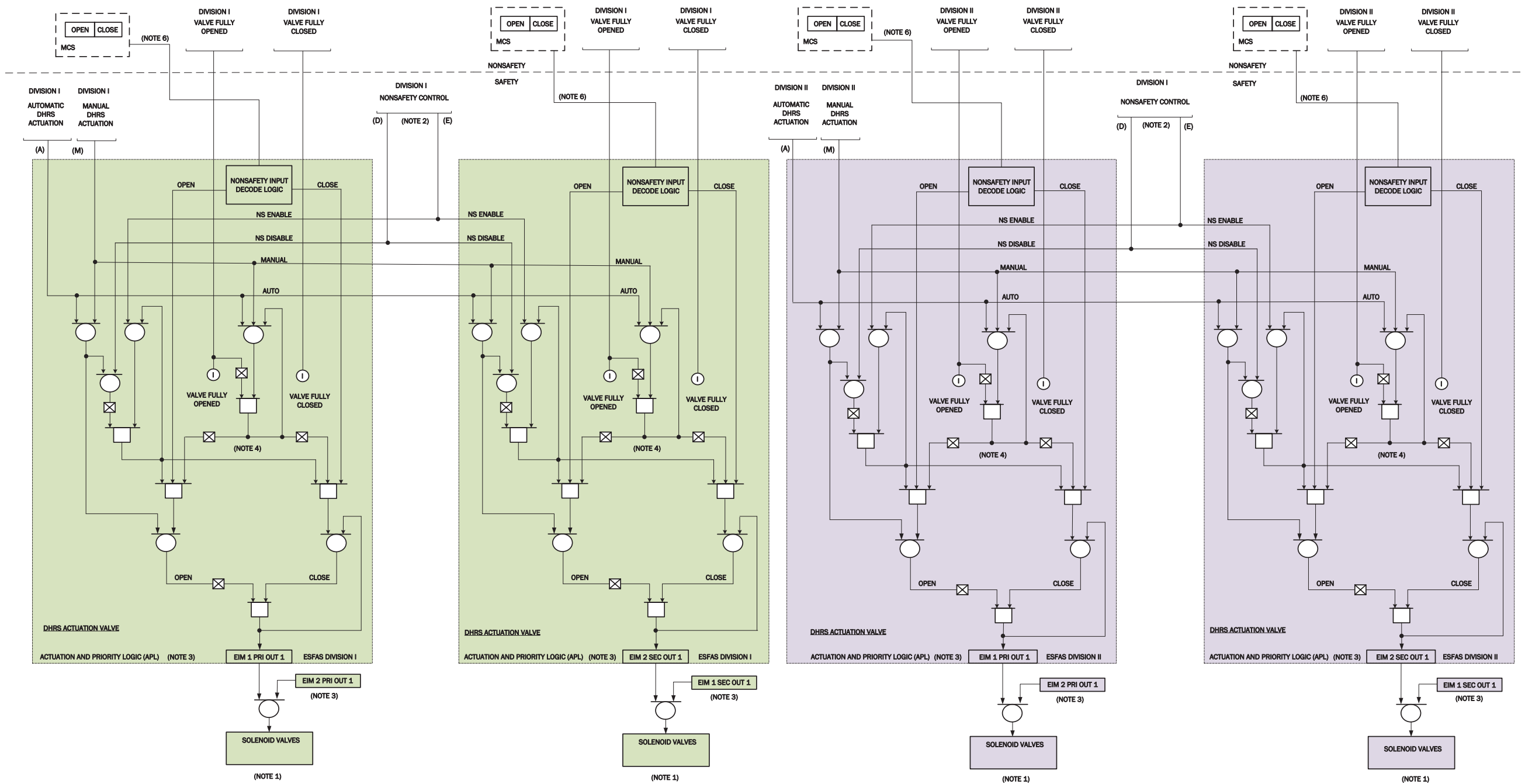
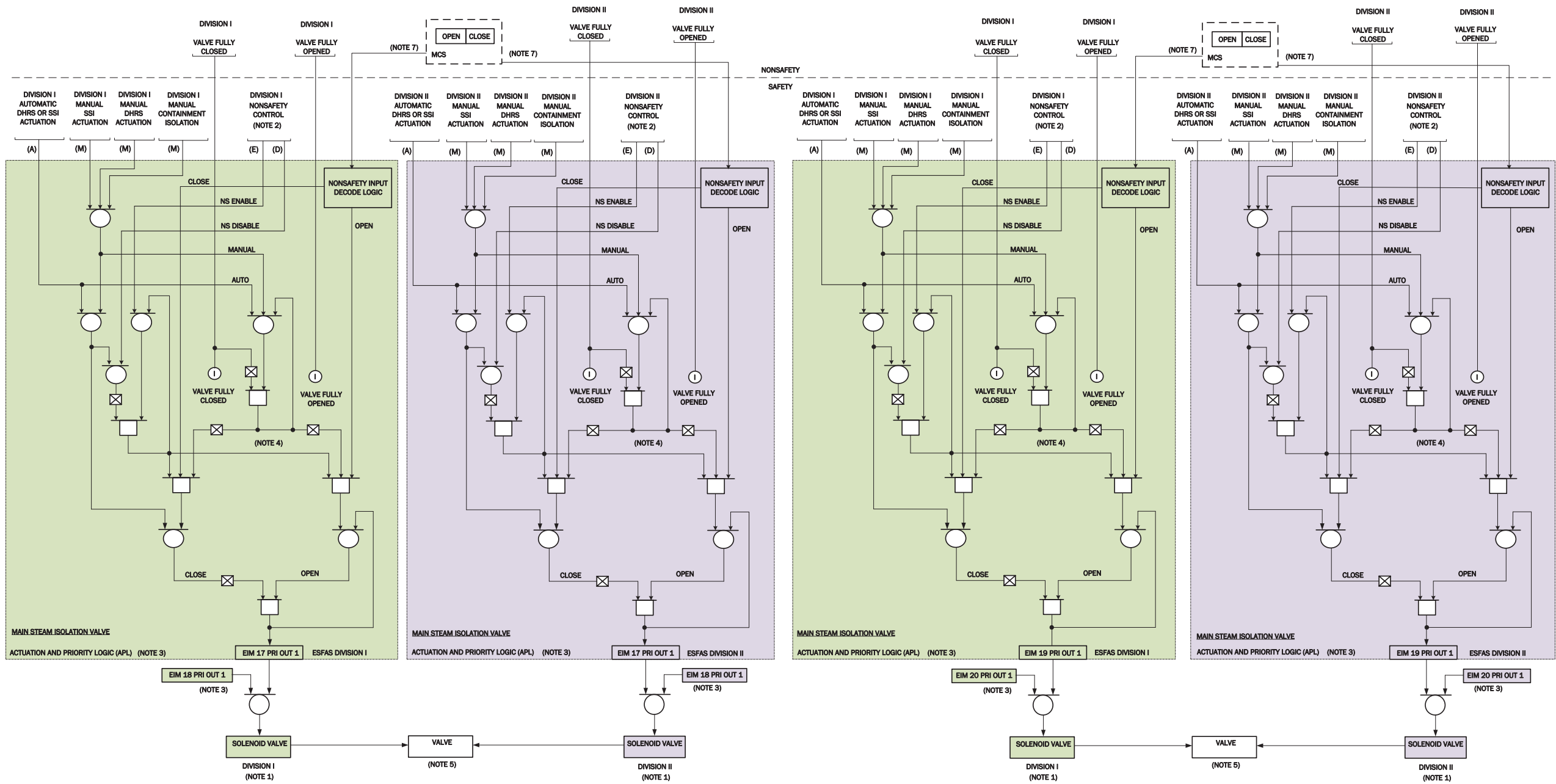


Figure 7.1-1p: Main Steam Isolation Valve Actuation



NOTE 1: SOLENOID IS ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOID IS DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

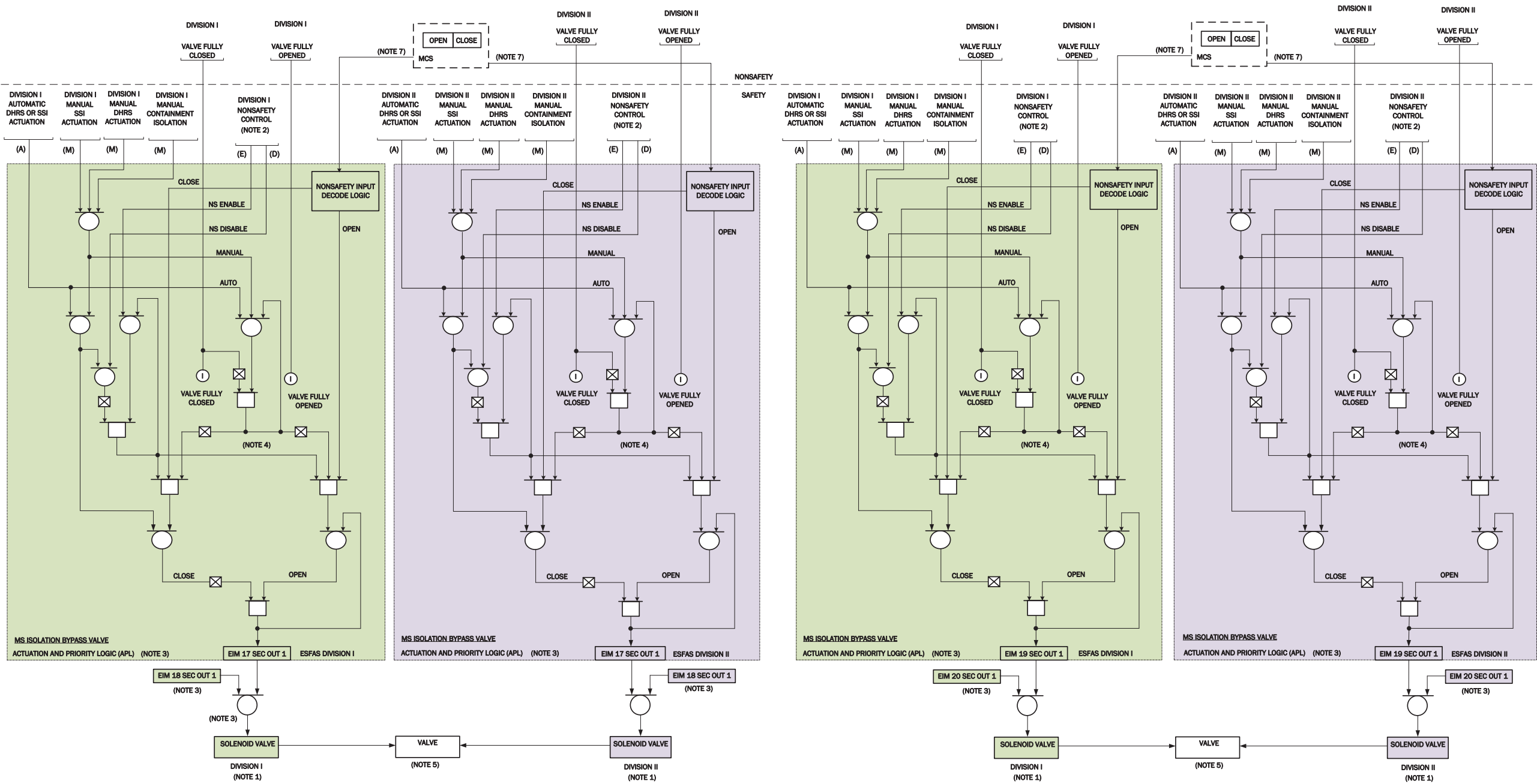
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS, ONE FROM EACH DIVISION. THE VALVE CLOSURES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOIDS IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1q: Main Steam Isolation Bypass Valve Actuation



NOTE 1: SOLENOID IS ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOID IS DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.
NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSURES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOID IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.
NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1r: Secondary Main Steam Isolation Valve Actuation

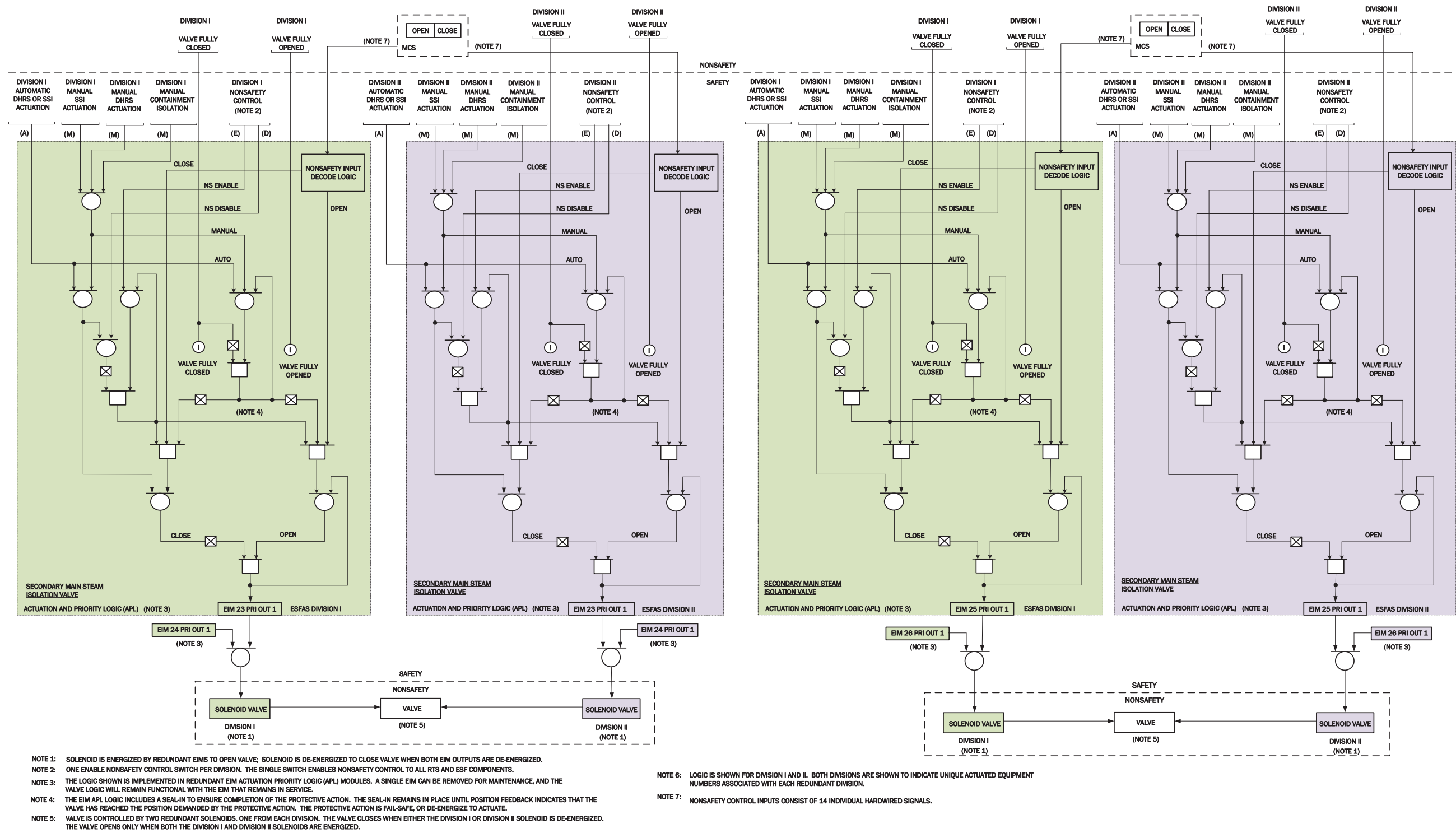


Figure 7.1-1s: Secondary MSIV Bypass Valve Actuation

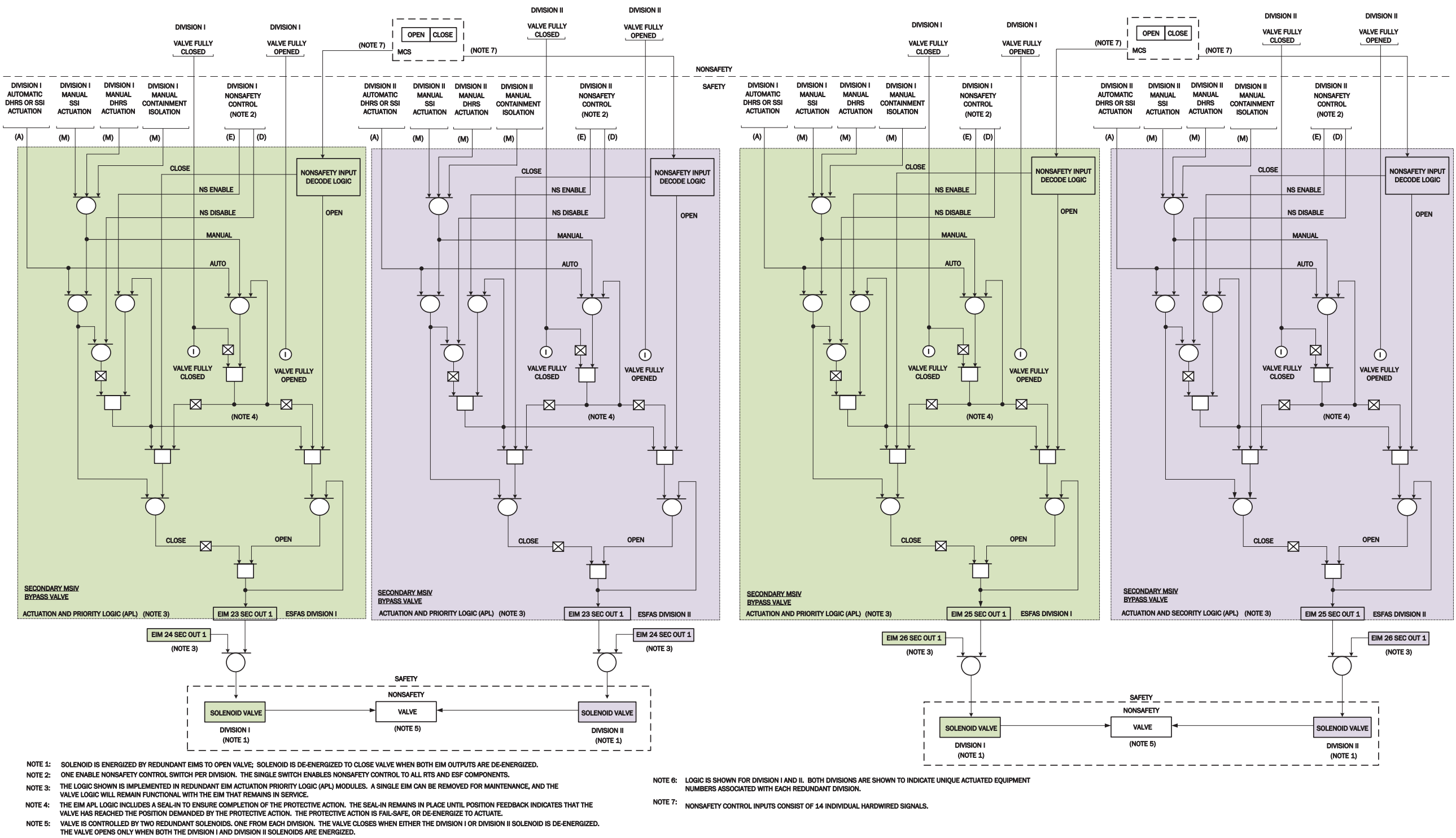
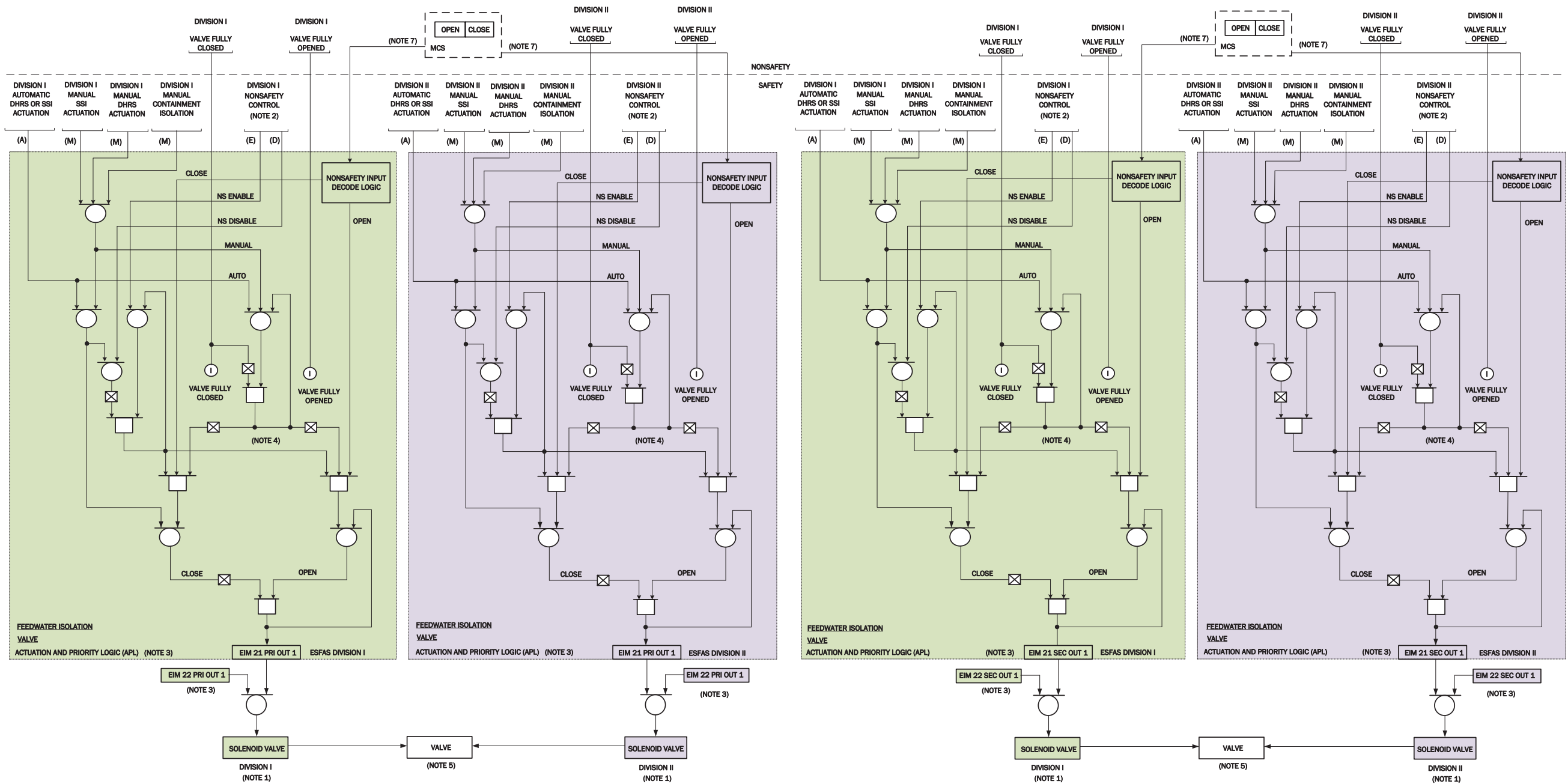


Figure 7.1-1t: Feedwater Isolation Valve Actuation



NOTE 1: SOLENOID IS ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOID IS DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMAND BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.
NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSURES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOID IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.
NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1u: Feedwater Regulating Valve Isolation

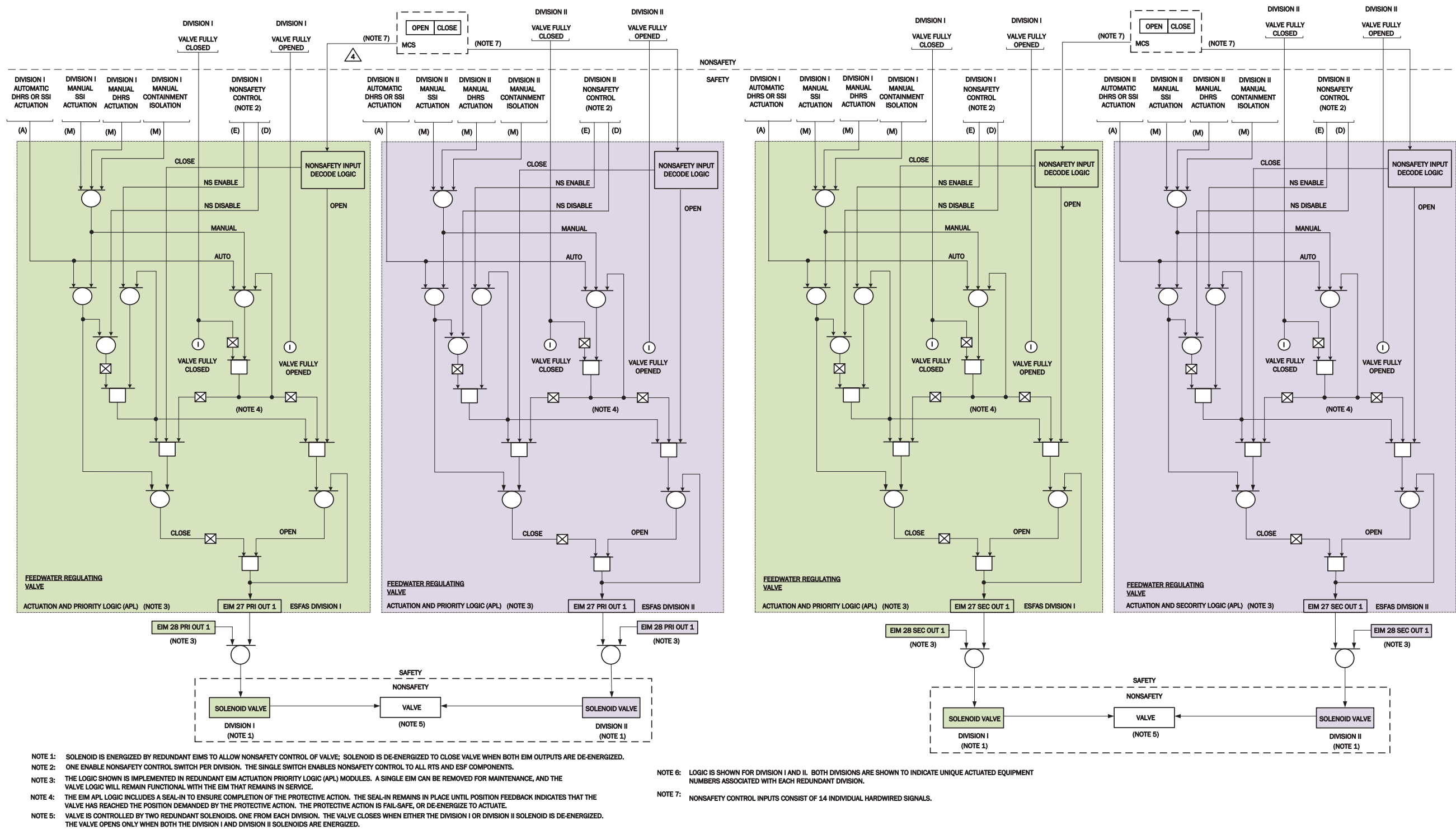
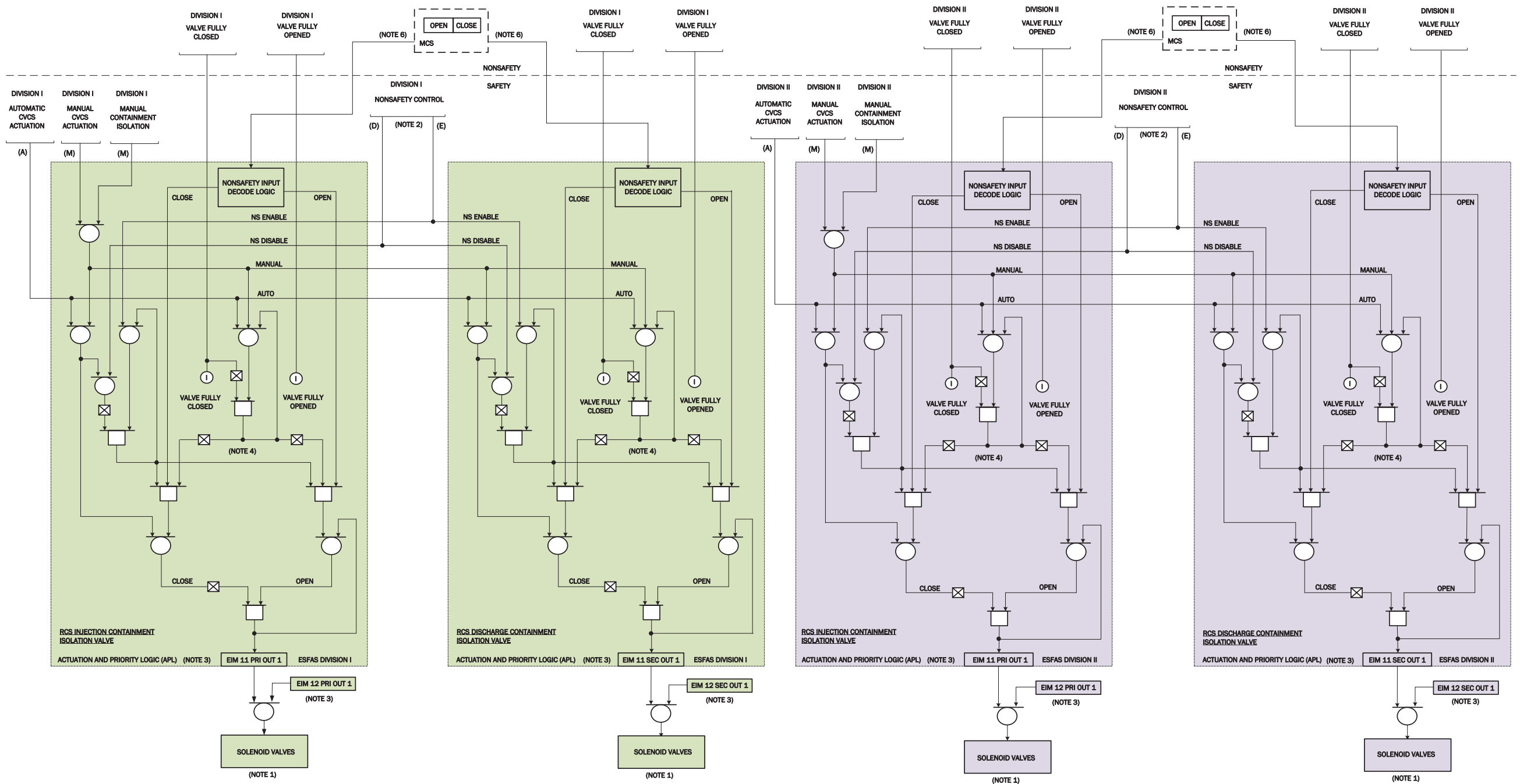


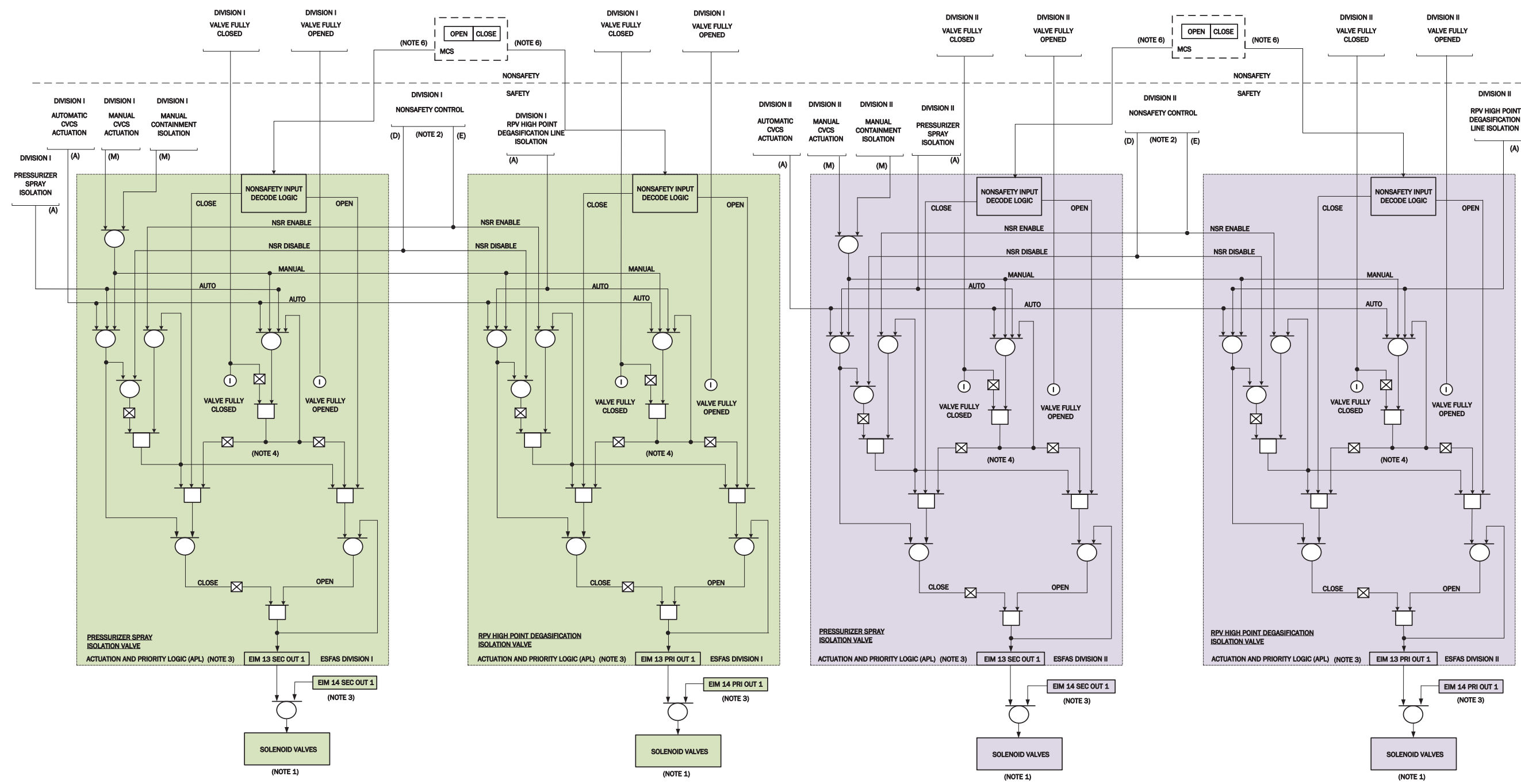
Figure 7.1-1v: Chemical and Volume Control System RCS Injection and Discharge Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.
NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

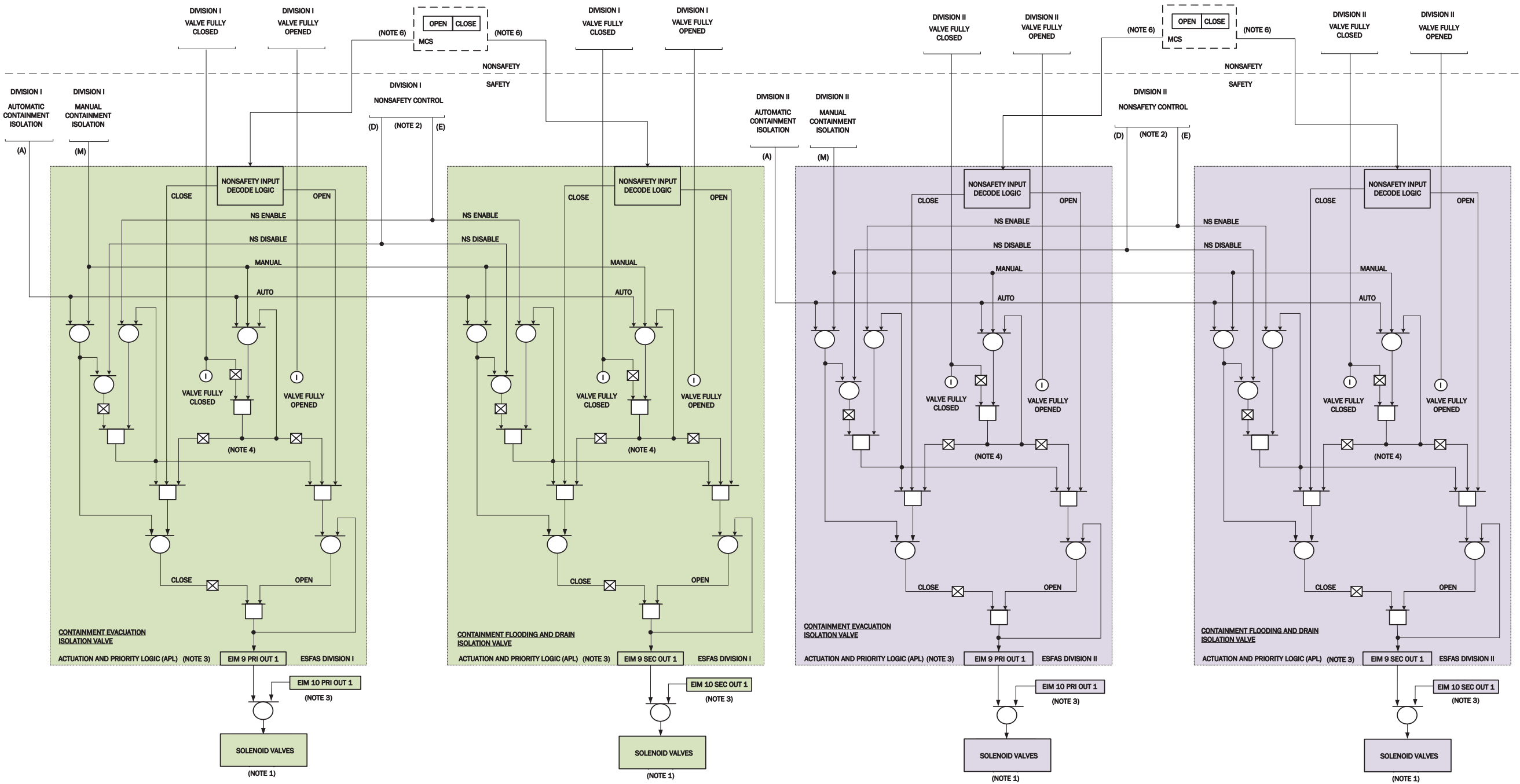
Figure 7.1-1w: Chemical and Volume Control System Pressurizer Spray and High Point Degasification Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.
NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

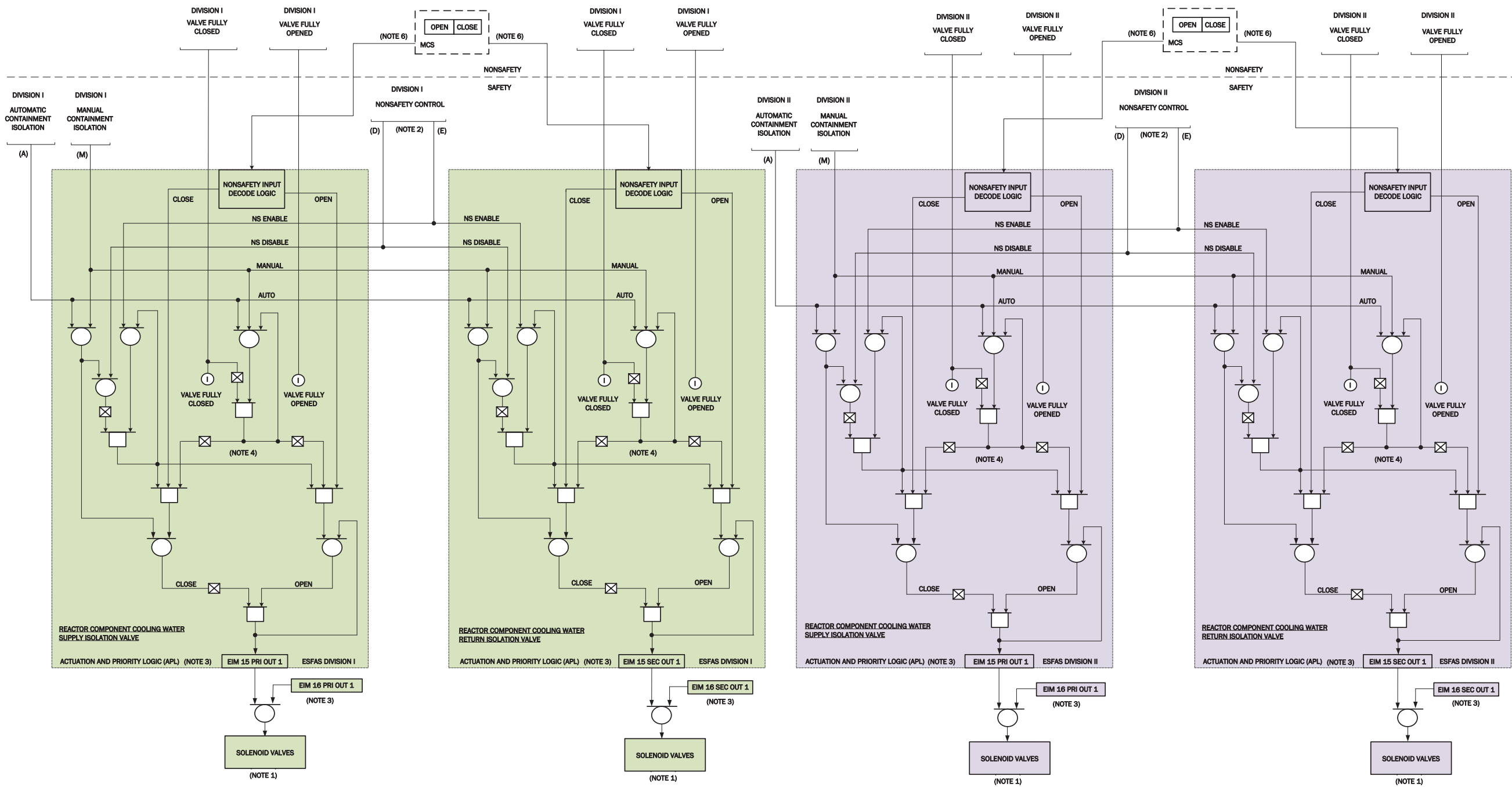
Figure 7.1-1x: Containment Flooding and Drain and Containment Evacuation Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.
NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1y: Reactor Component Cooling Water System Valve Actuation



- NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.
- NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1z: Demineralized Water Supply Valve Actuation

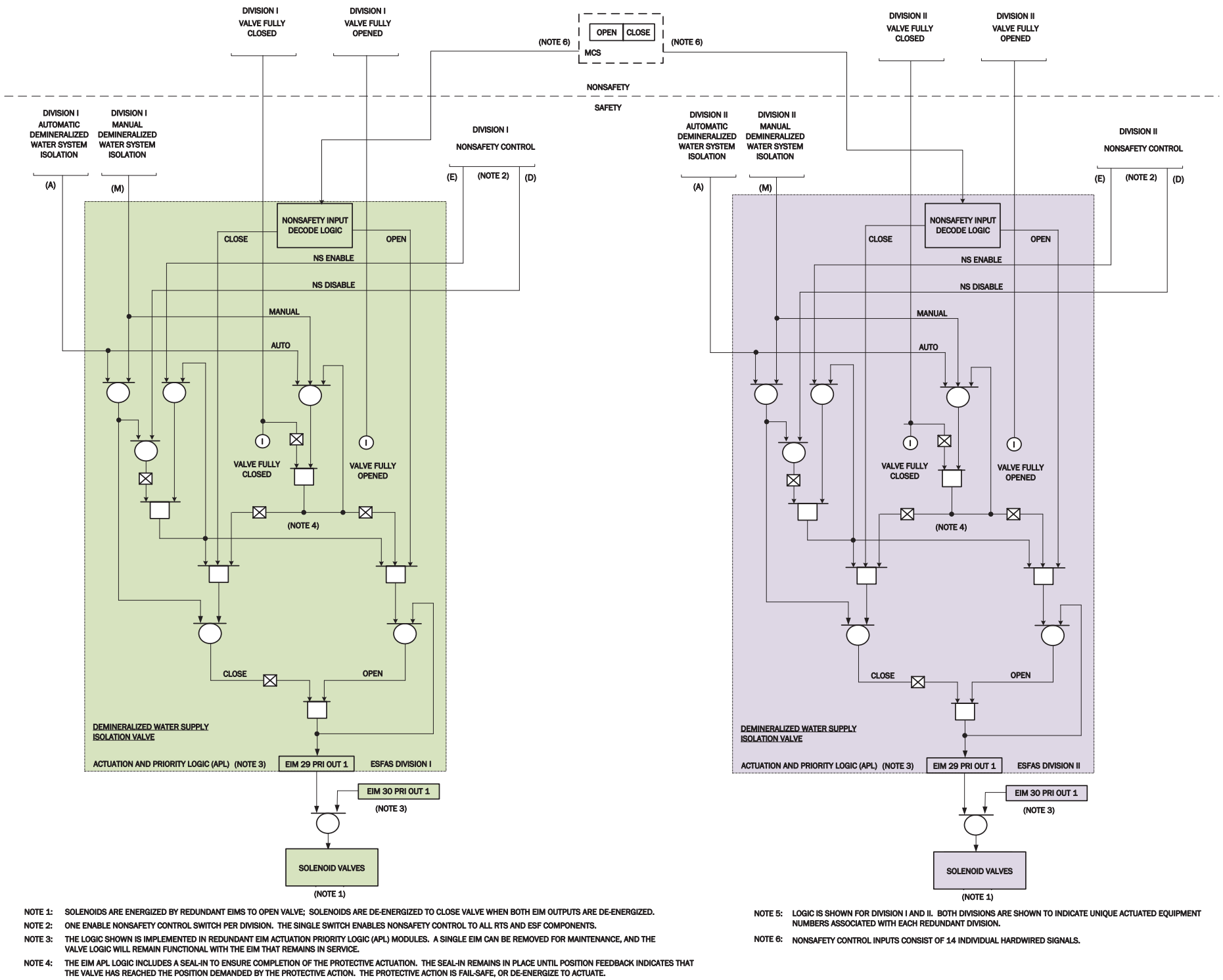


Figure 7.1-1aa: Emergency Core Cooling System Reactor Vent Valve 1 & 2 Actuation

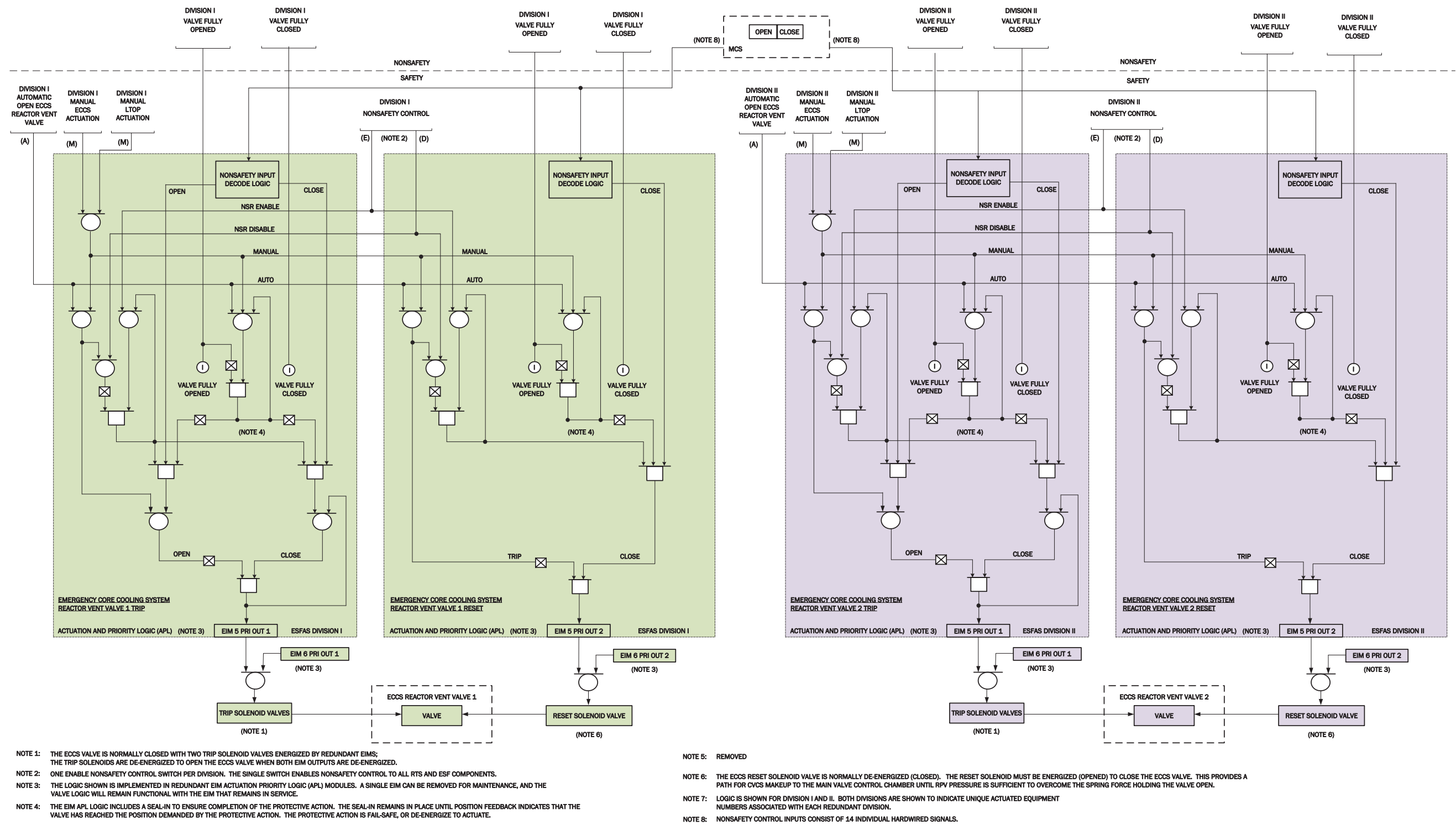


Figure 7.1-1ab: Emergency Core Cooling System Reactor Recirculation Valve Actuation

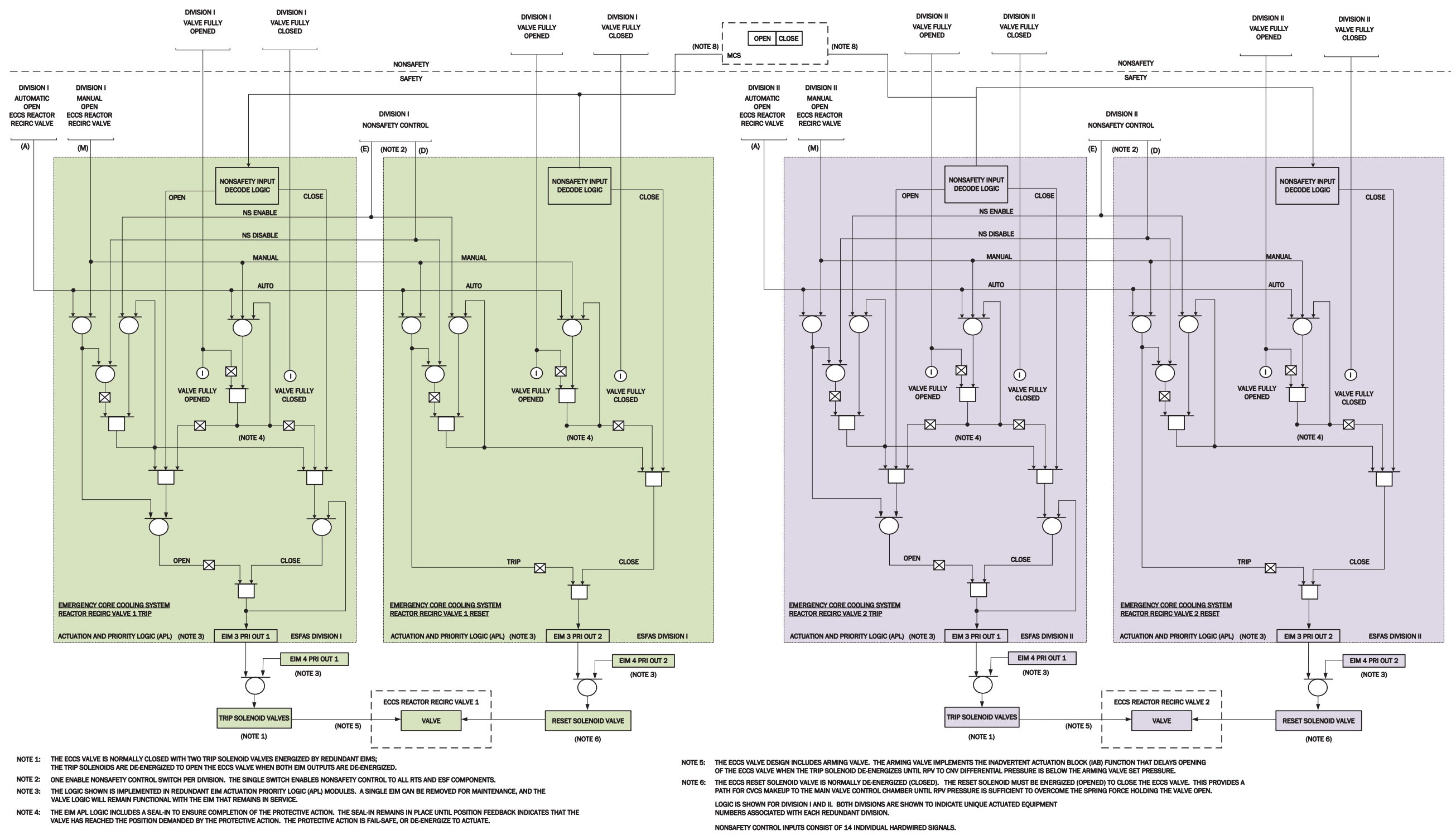
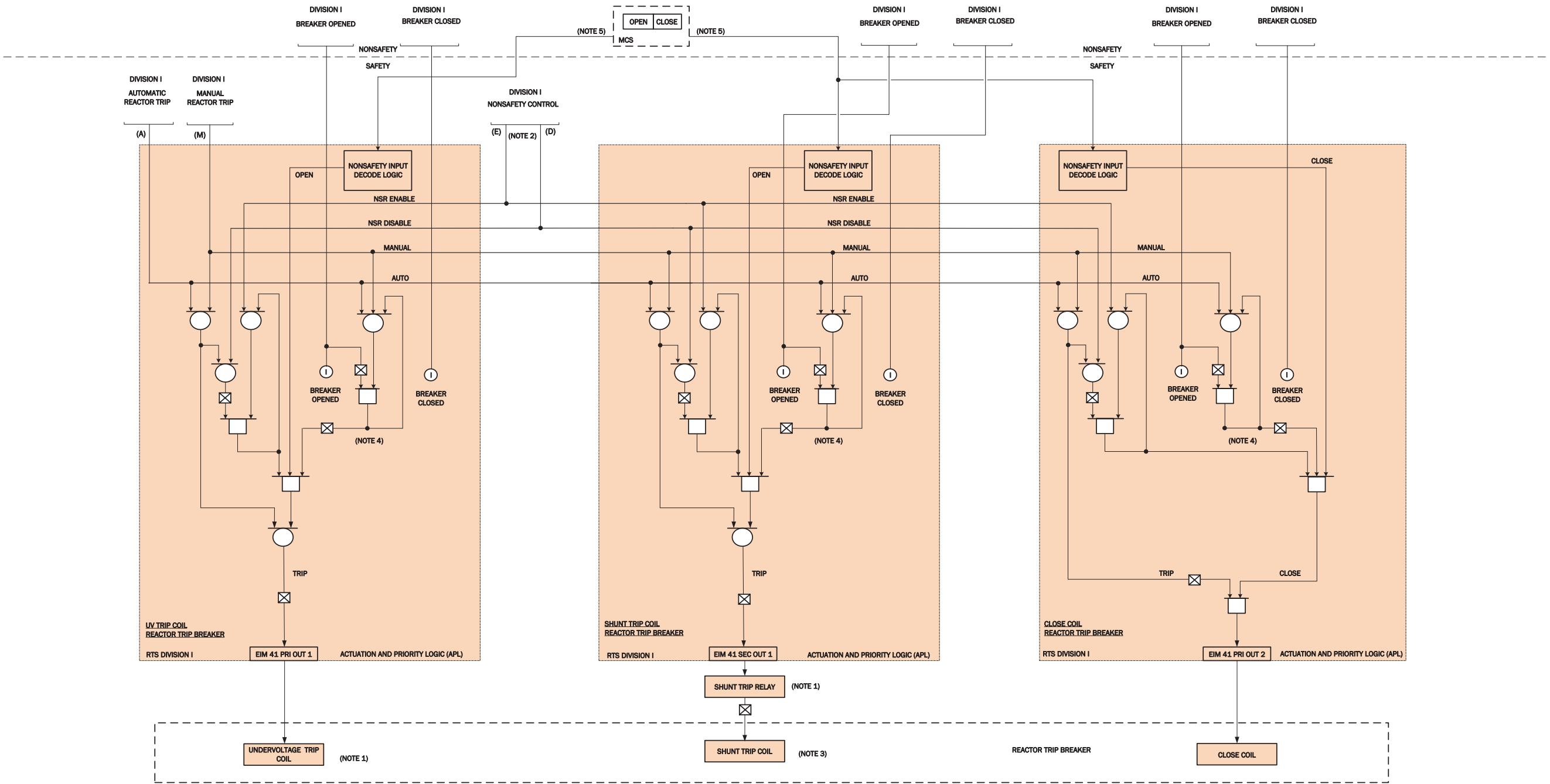


Figure 7.1-1ac: Reactor Trip Breaker Division I A



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUTS ARE DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

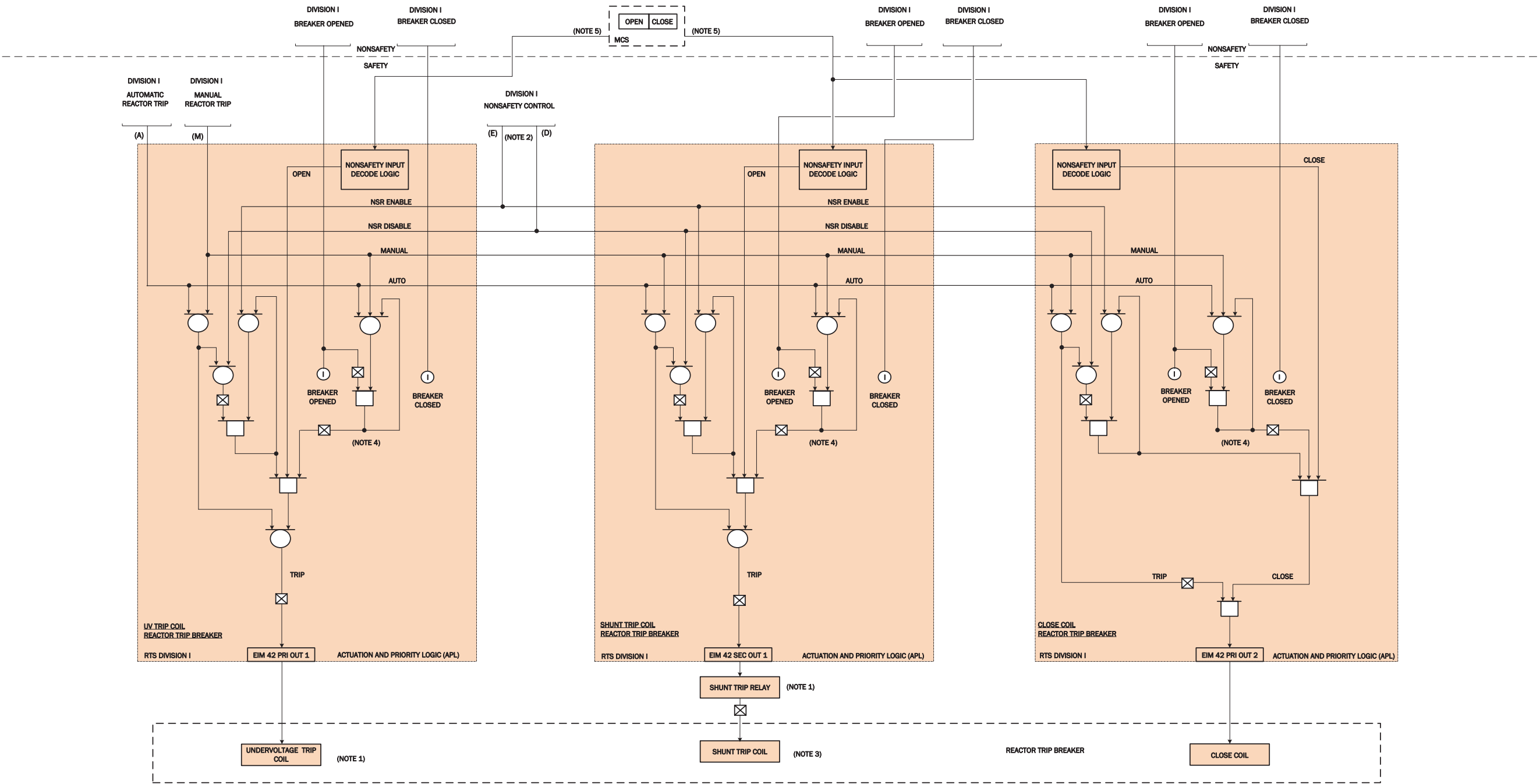
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMAND BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ad: Reactor Trip Breaker Division I B



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUTS ARE DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

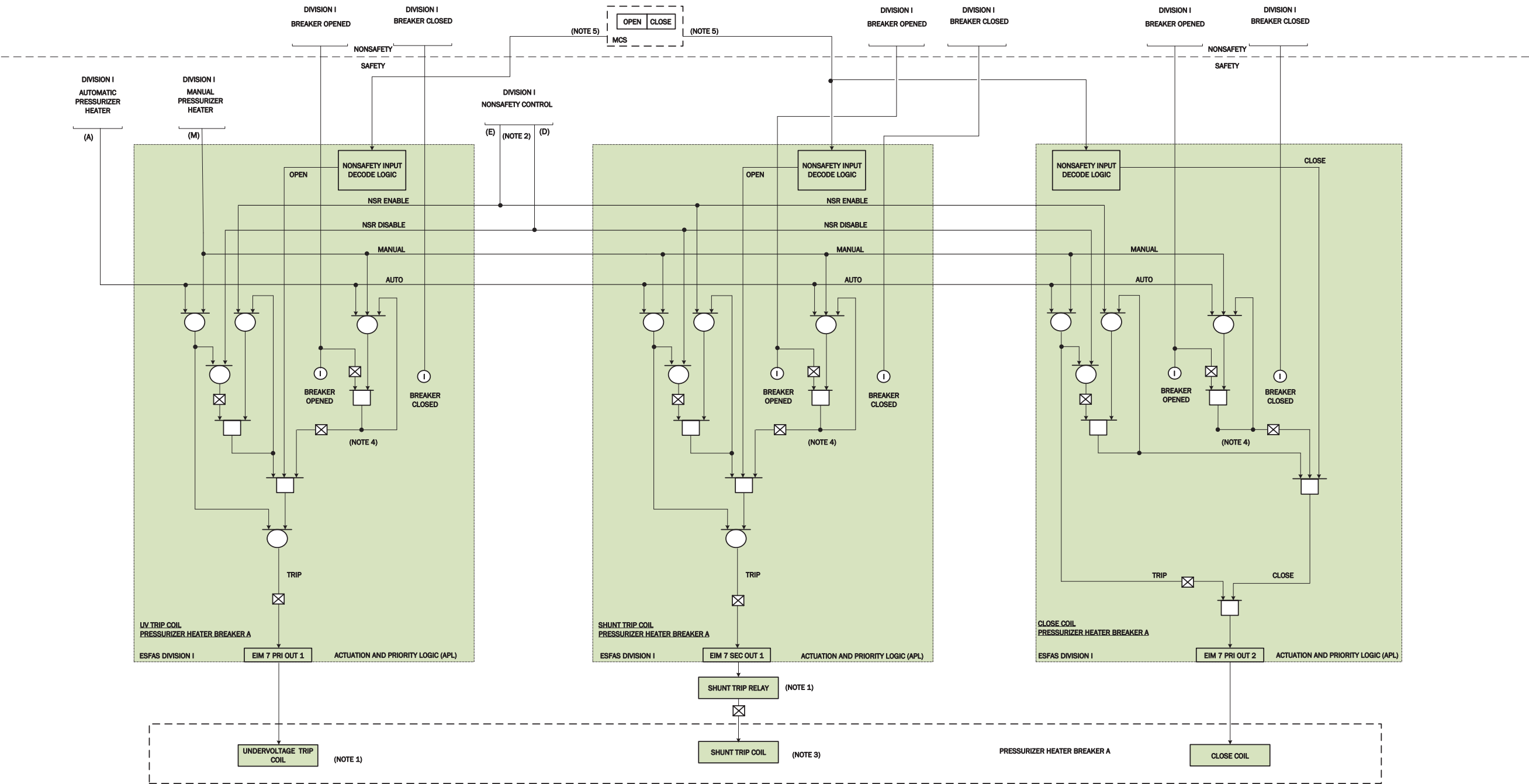
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMAND BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ae: Pressurizer Heater Breaker Proportional Heater A



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUT IS DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1af: Pressurizer Heater Breaker Proportional Heater B

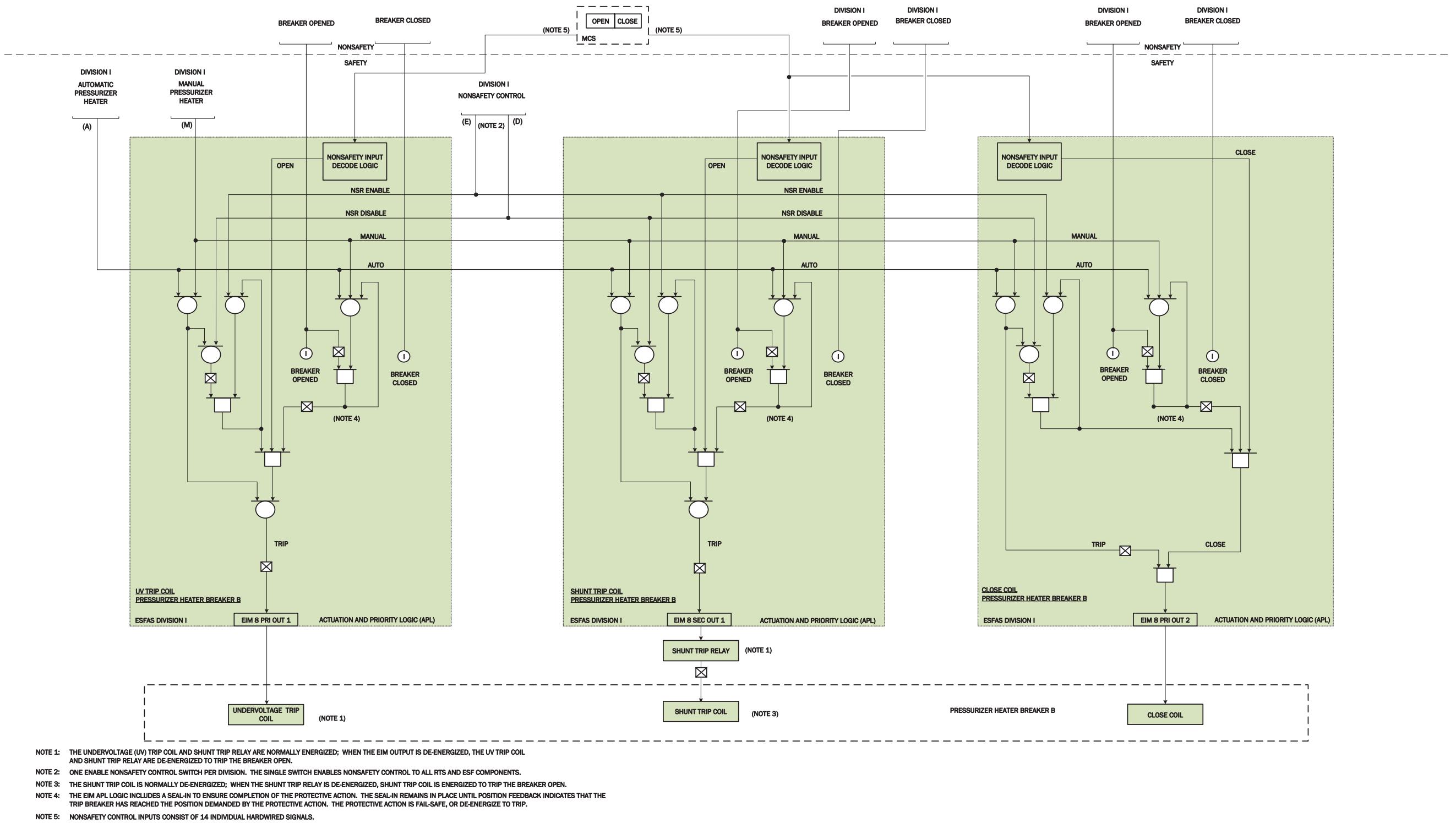


Figure 7.1-1ag: Loss of AC Power to ELVS Battery Chargers

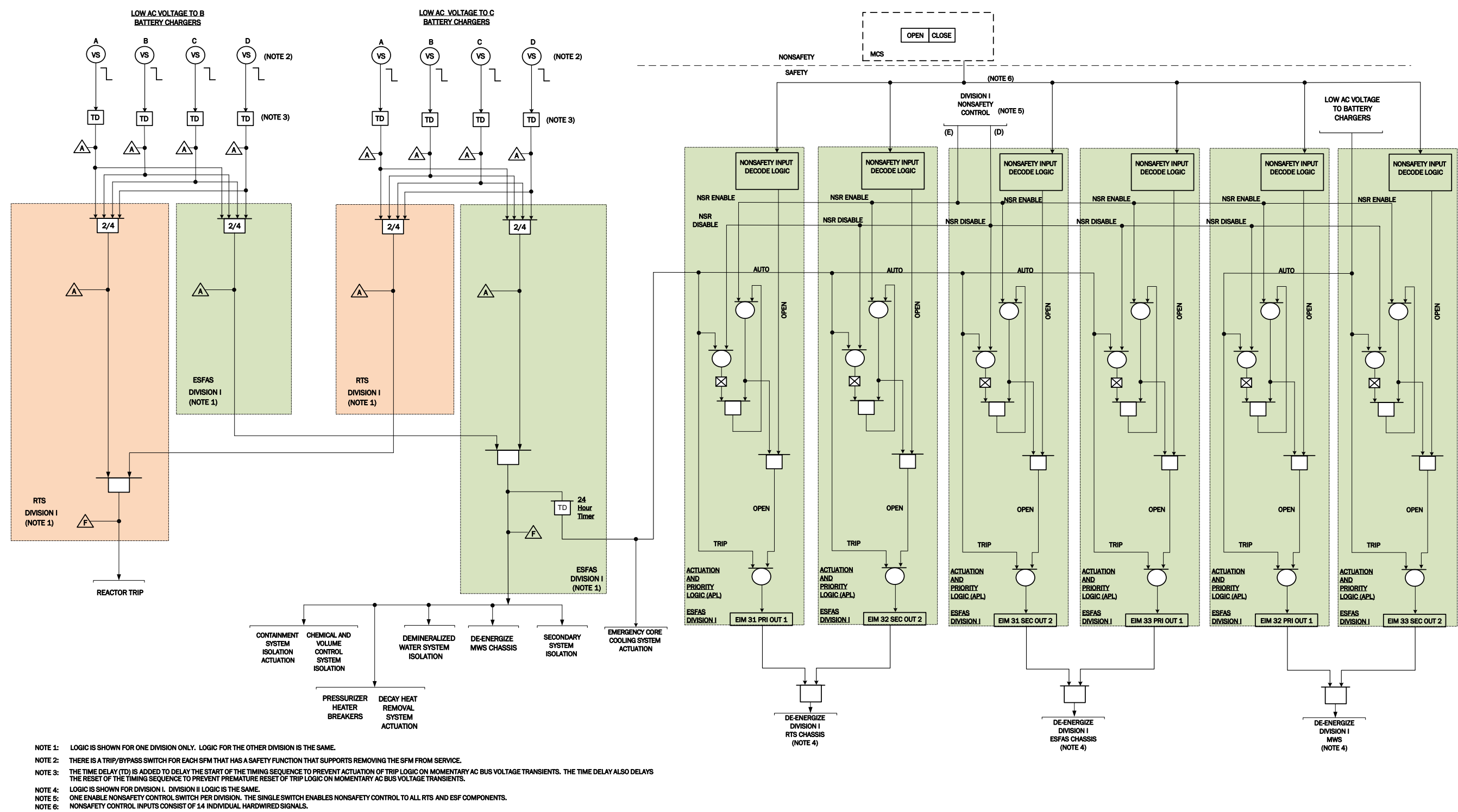
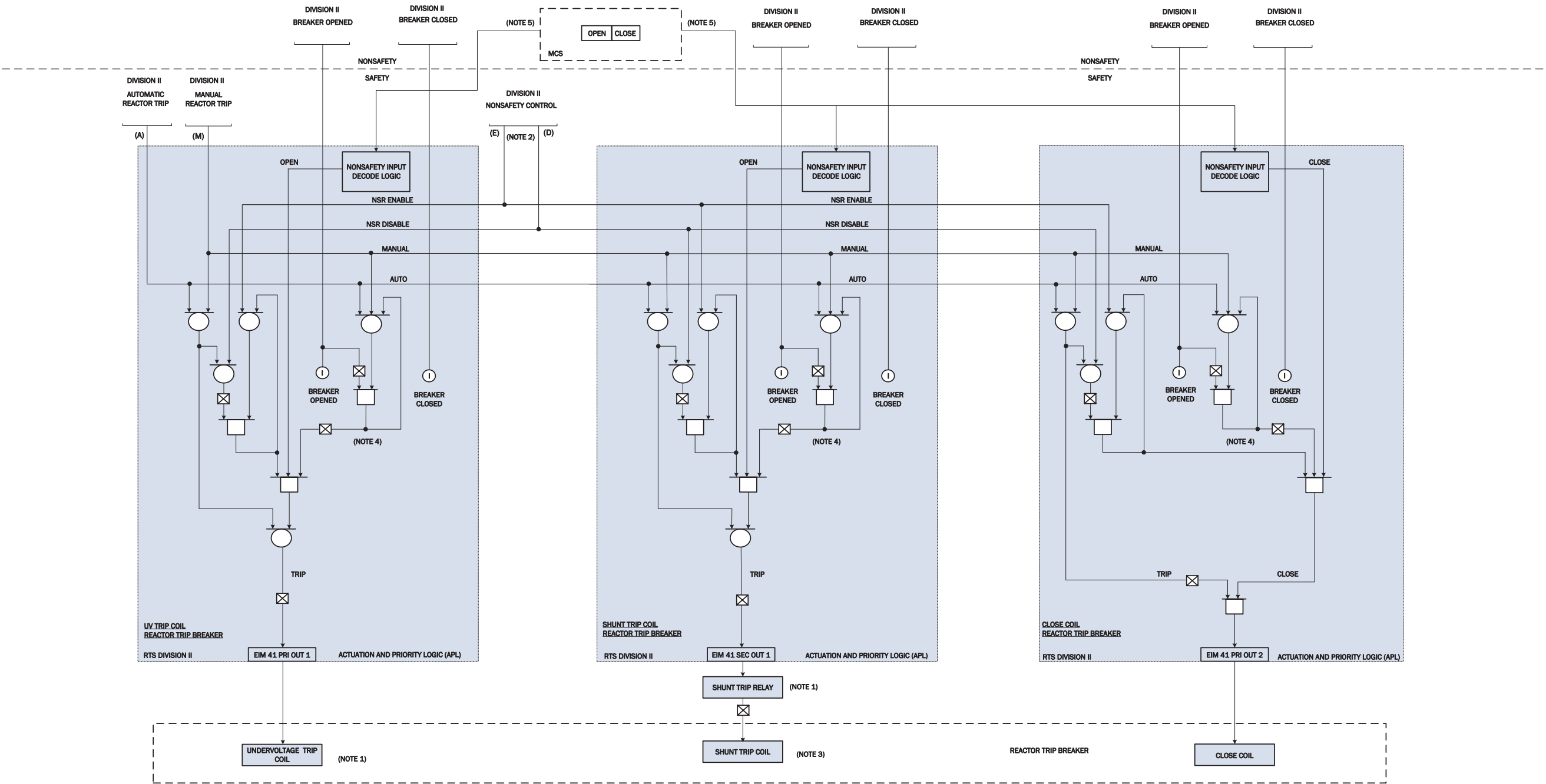


Figure 7.1-1ah: Reactor Trip Breaker Division II A



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUTS ARE DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

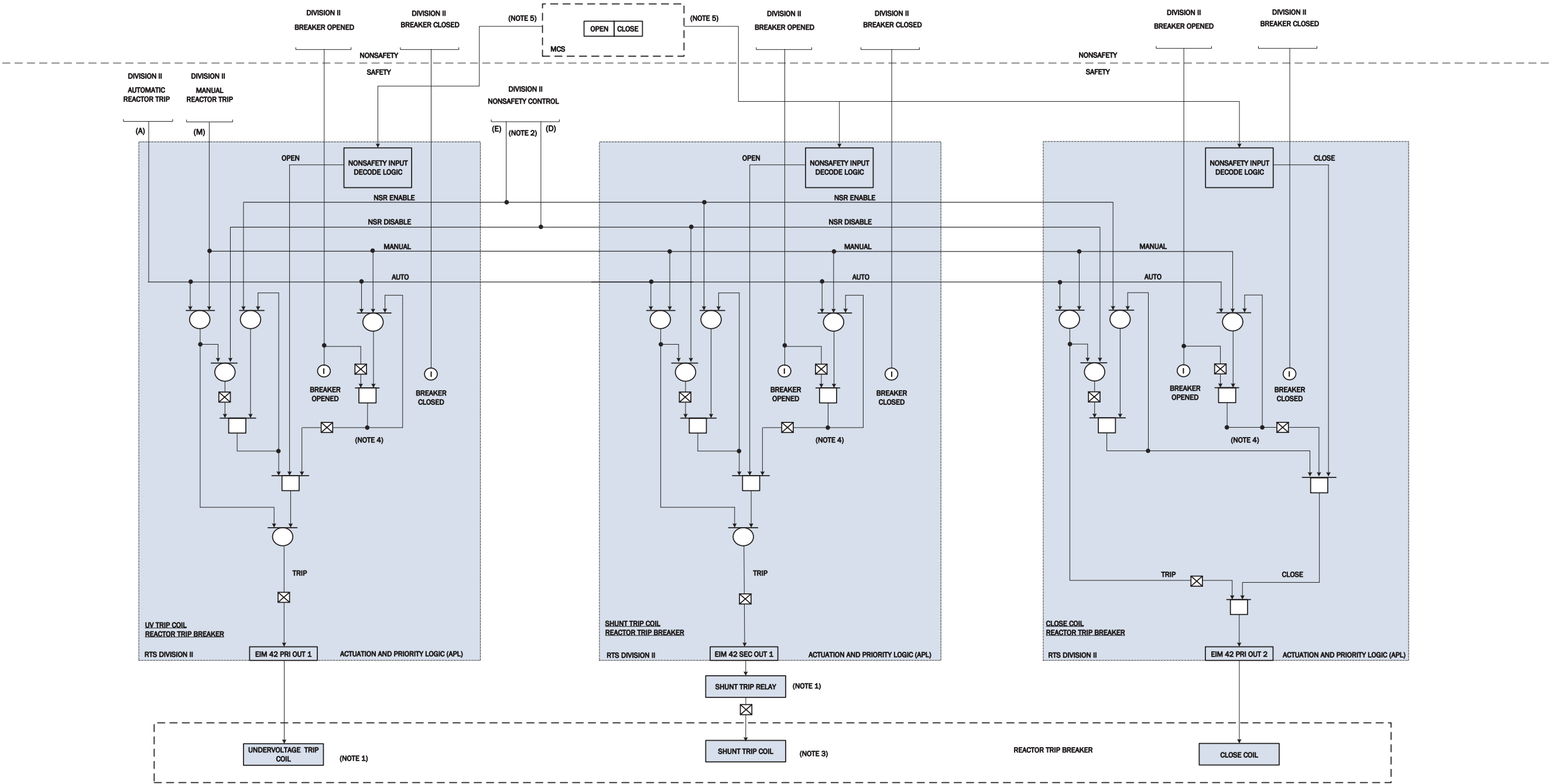
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ai: Reactor Trip Breaker Division II B



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUTS ARE DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

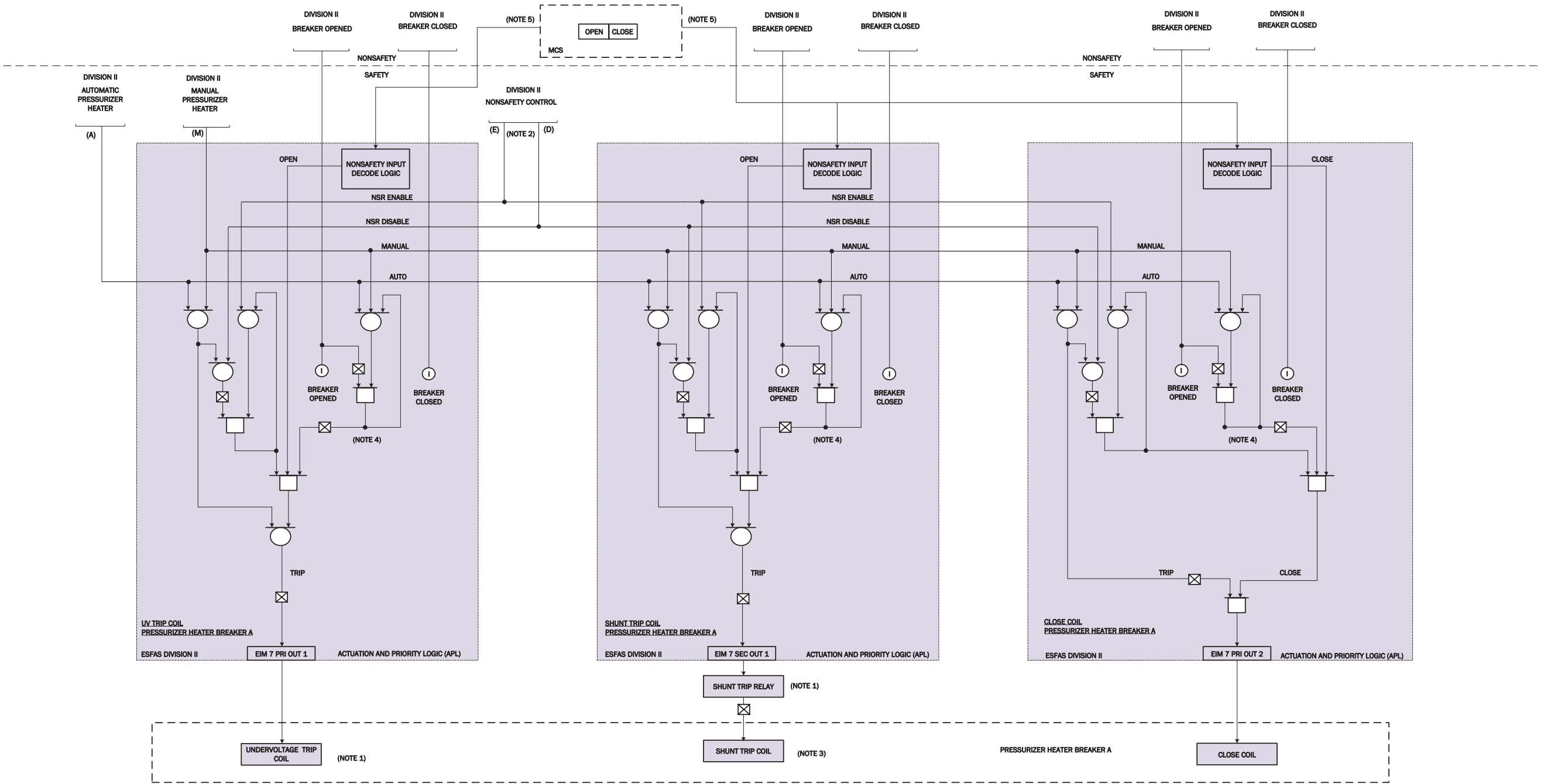
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1aj: Pressurizer Heater Trip Breaker Backup Heater A



- NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUT IS DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.
- NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL RTS AND ESF COMPONENTS.
- NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.
- NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.
- NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ak: Pressurizer Heater Trip Breaker Backup Heater B

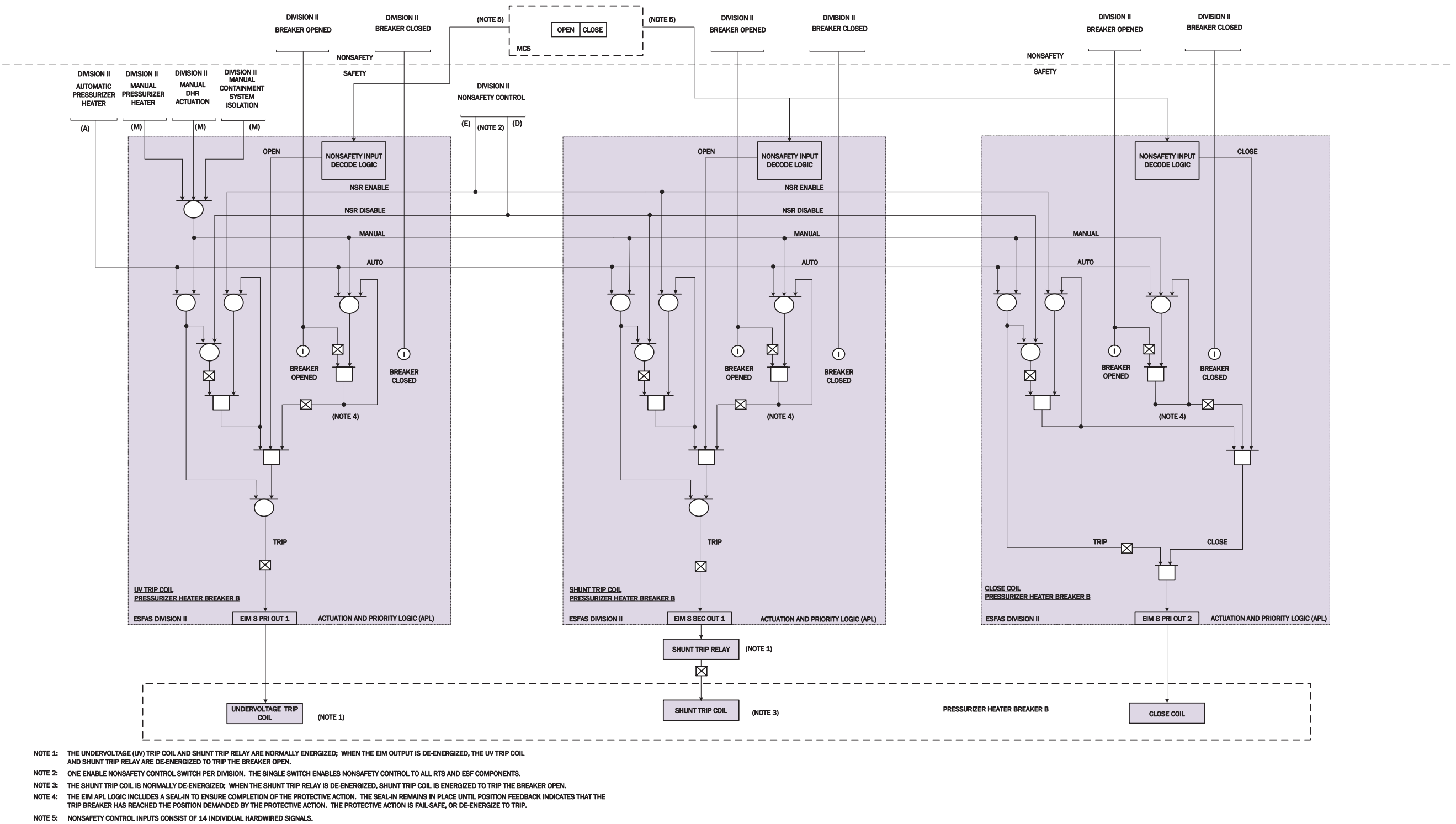
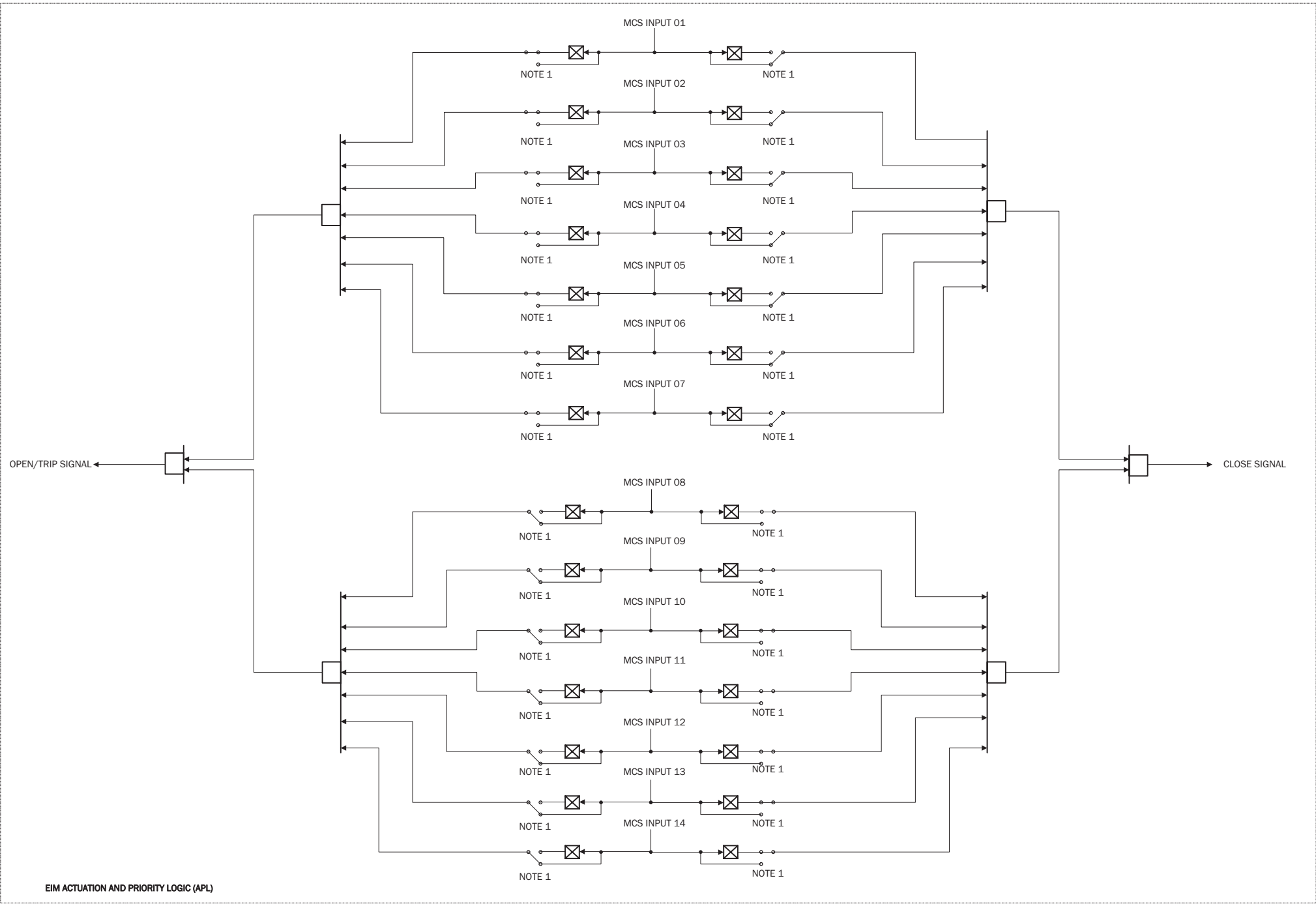
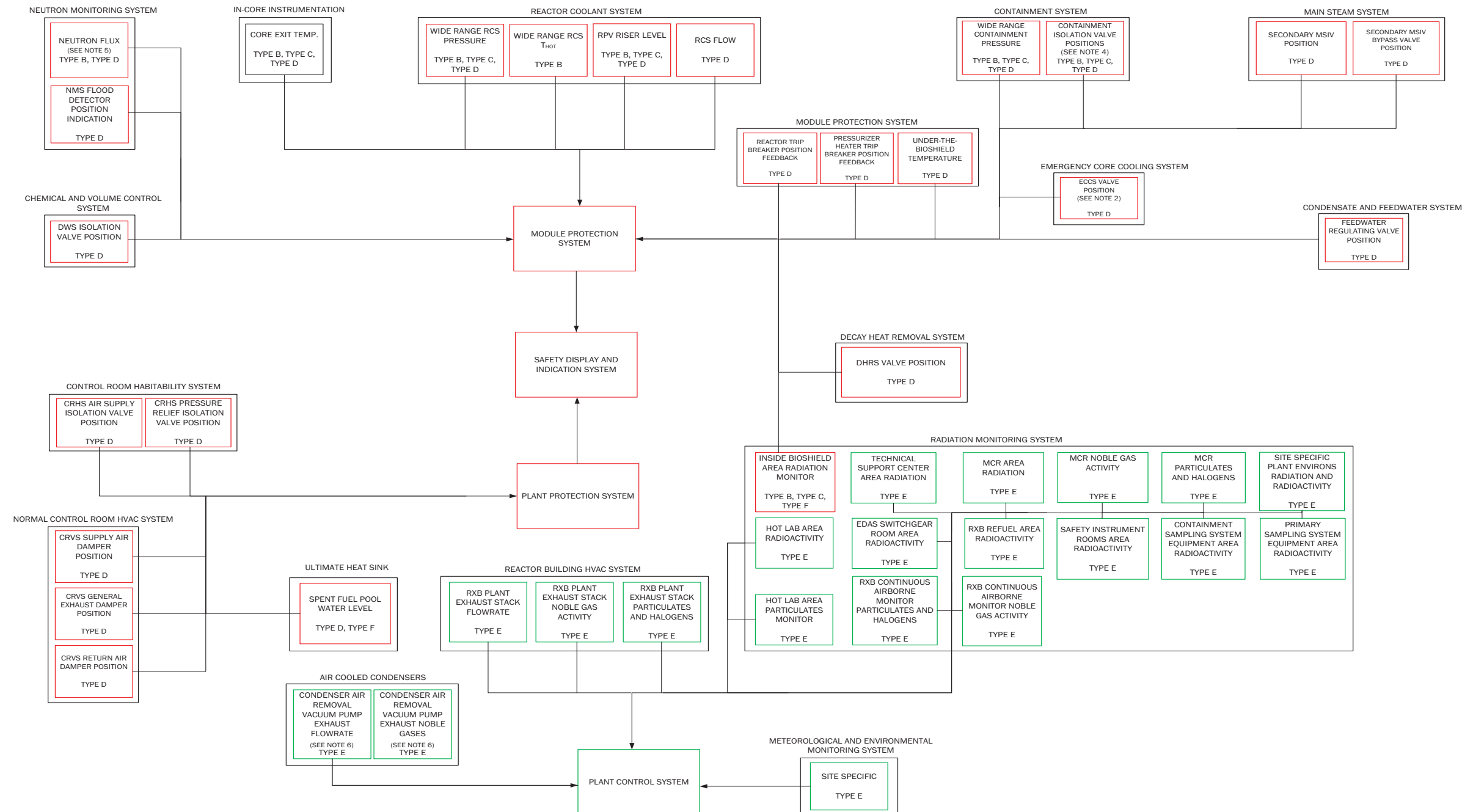


Figure 7.1-1aI: Actuation Priority Logic Nonsafety Input Control Logic



NOTE 1: CONNECTIONS TO BE CONFIGURED WITH SWITCHES OR JUMPERS FOR EACH SPECIFIC EIM APPLICATION.

Figure 7.1-2: Post-Accident Monitoring General Arrangement Drawing



NOTES:

1. SAFETY-RELATED SSOs DEPICTED ARE SAFETY-RELATED FOR A FUNCTION OTHER THAN POST ACCIDENT MONITORING. POST ACCIDENT MONITORING IS NOT A SAFETY-RELATED FUNCTION (NO TYPE A VARIABLES)
2. THE VALVE POSITIONS FOR THIS VARIABLE ARE FOR RRVs, RVVs, AND THEIR ASSOCIATED TRIP SOLENOID VALVES.
3. COLOR CODES IDENTIFY THE DIRECT OR INDIRECT SUPPORTING ELECTRICAL SYSTEM FOR A GIVEN VARIABLE

	= AUGMENTED DC POWER SYSTEM (EDAS)
	= NORMAL DC POWER SYSTEM (EDNS)
	= NOT APPLICABLE (e.g., SELF-POWERED, POWERED FROM PROCESS)
4. CONTAINMENT ISOLATION VALVES:
PZR SPRAY
RCS INJECTION
RCS DISCHARGE
RPV HIGH POINT DEGASSIFICATION
CES
CFDS
RCOWS INLET
RCOWS OUTLET
MSIV
MS ISOLATION BYPASS
FWIV
5. POST ACCIDENT MONITORING NEUTRON FLUX SIGNALS:
POWER RANGE LINEAR POWER
INTERMEDIATE RANGE LOG POWER
SOURCE RANGE COUNT RATE
NMS-FLOOD - NEUTRON MONITORING DURING FLOODED CONTAINMENT CONDITIONS.
6. INTEGRATED SAMPLING SKID WITH "PING" MONITOR TO DETECT PARTICULATE/IODINE/O NOBLE GAS/AR-41 GAMMA AND PROVISIONS FOR REPRESENTATIVE GRAB SAMPLING VIA TAKEOFF AND RETURN PATH FOR MONITORING PROCESS FLOW.

Figure 7.1-3: Blocks Selected for Defense-in-Depth Analysis

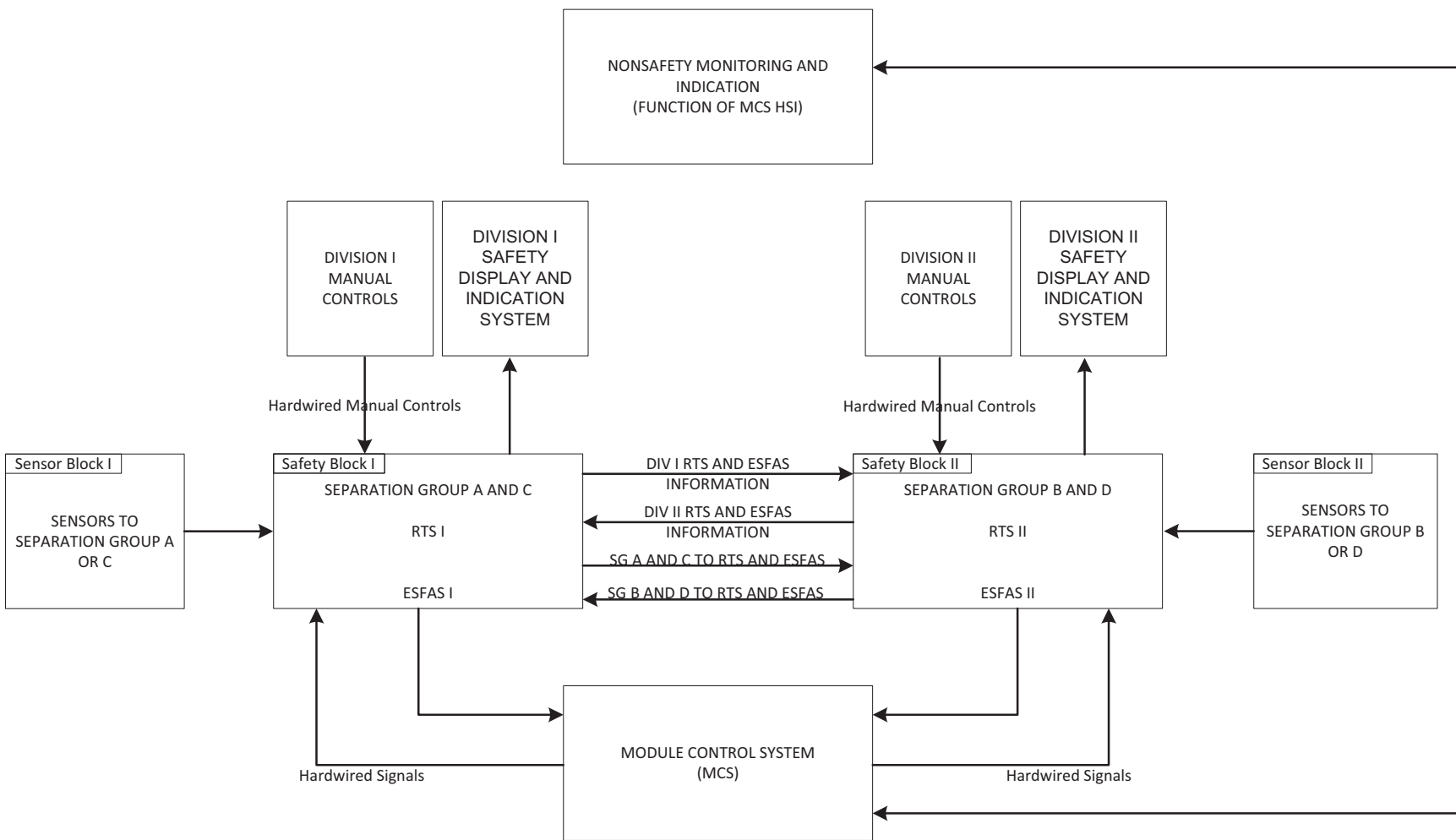


Figure 7.1-4: Blocks Selected for Defense-in-Depth Analysis

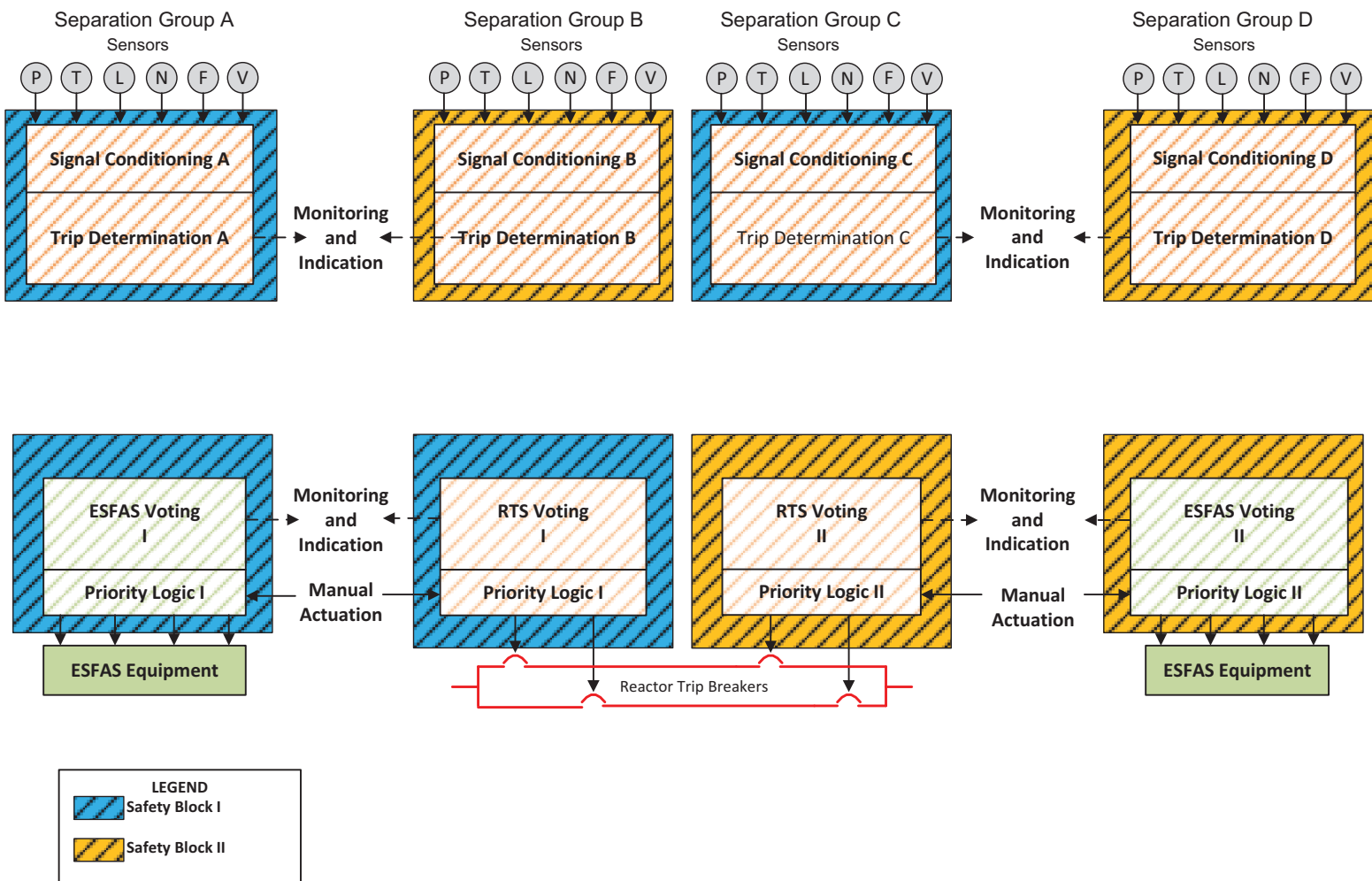


Figure 7.1-5: Four Echelons of Defense within Chosen Blocks

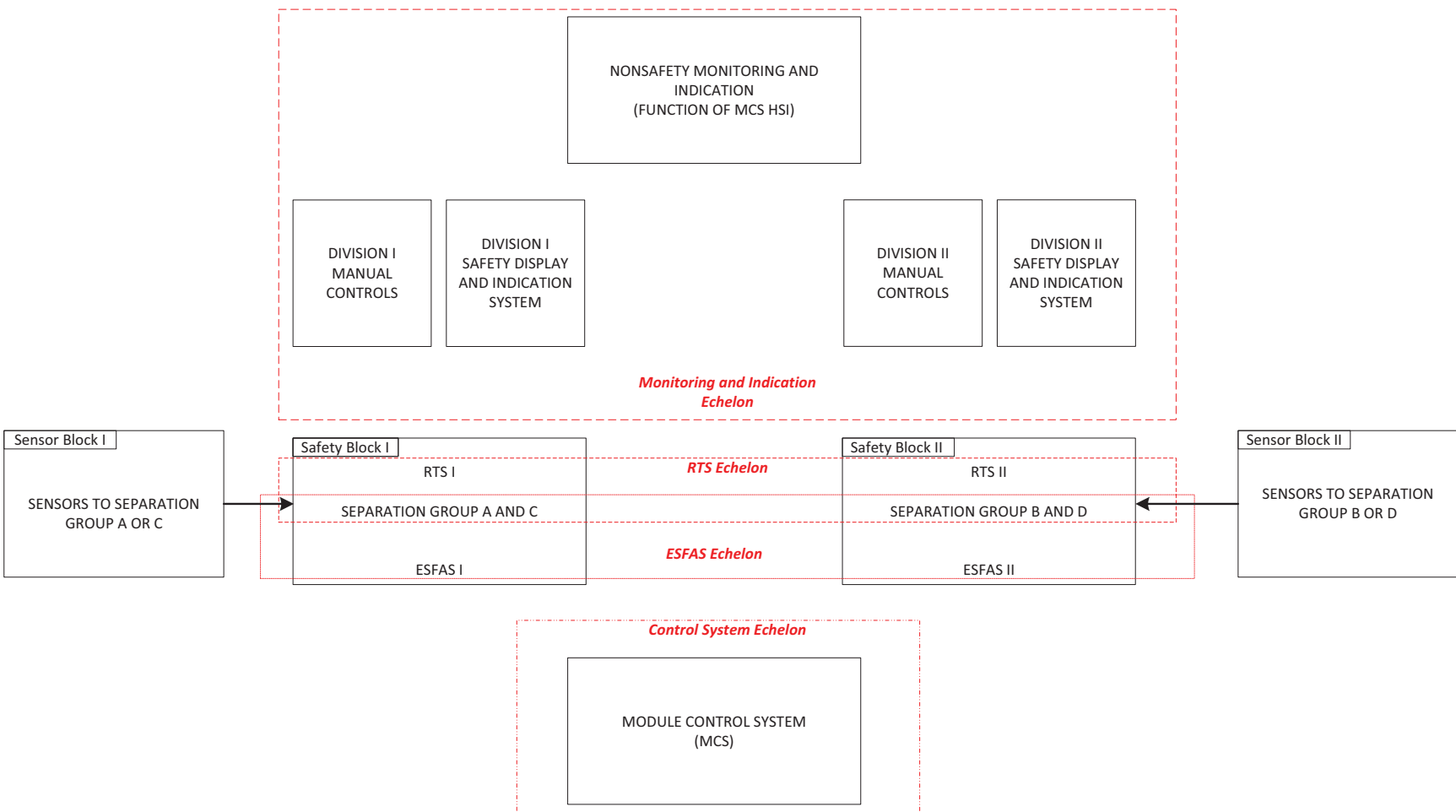


Figure 7.1-6: Common Cause Failure of Division I Safety Display and Indication System

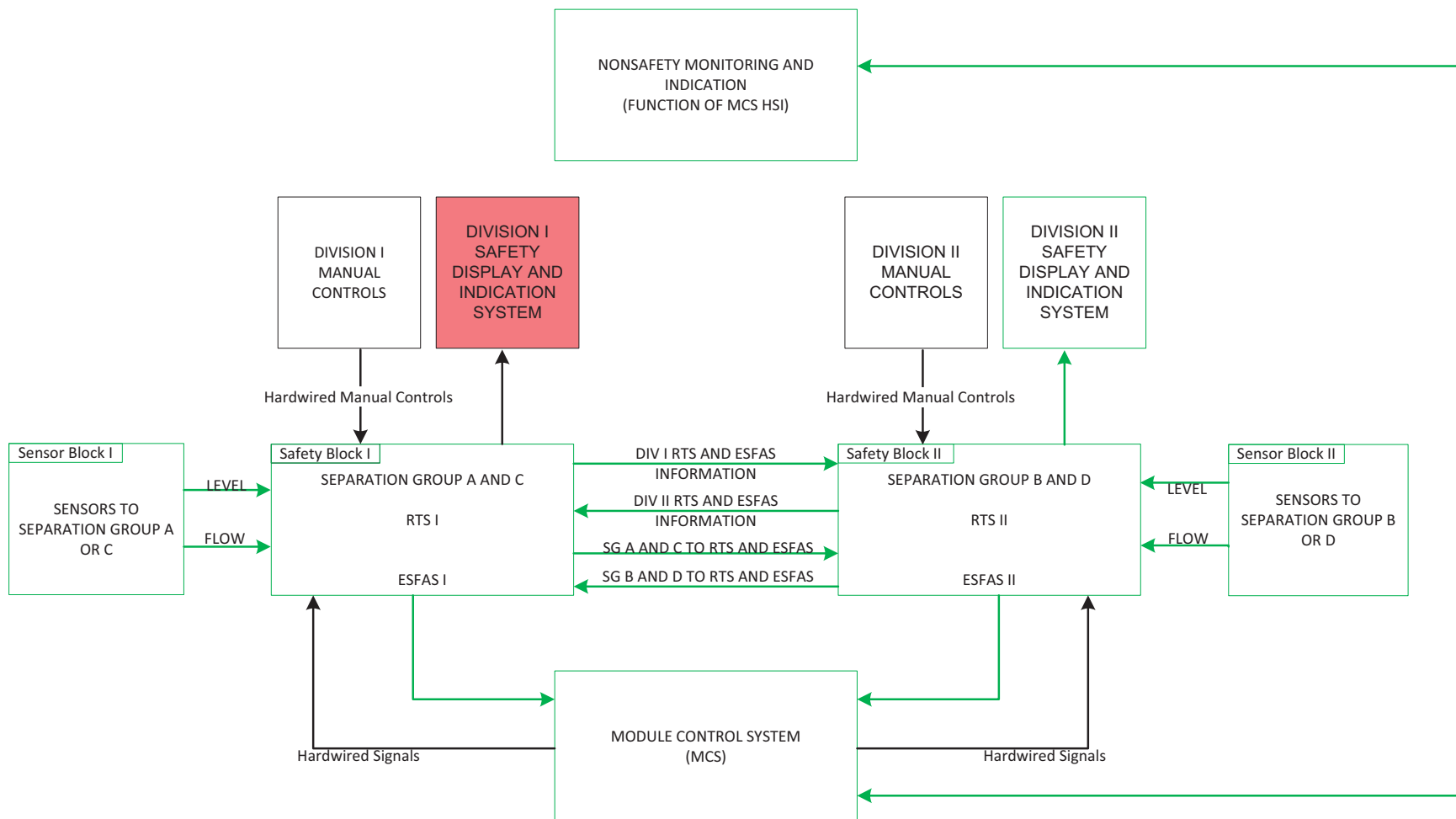


Figure 7.1-7: Common Cause Failure of Safety Block I with Correct Indication

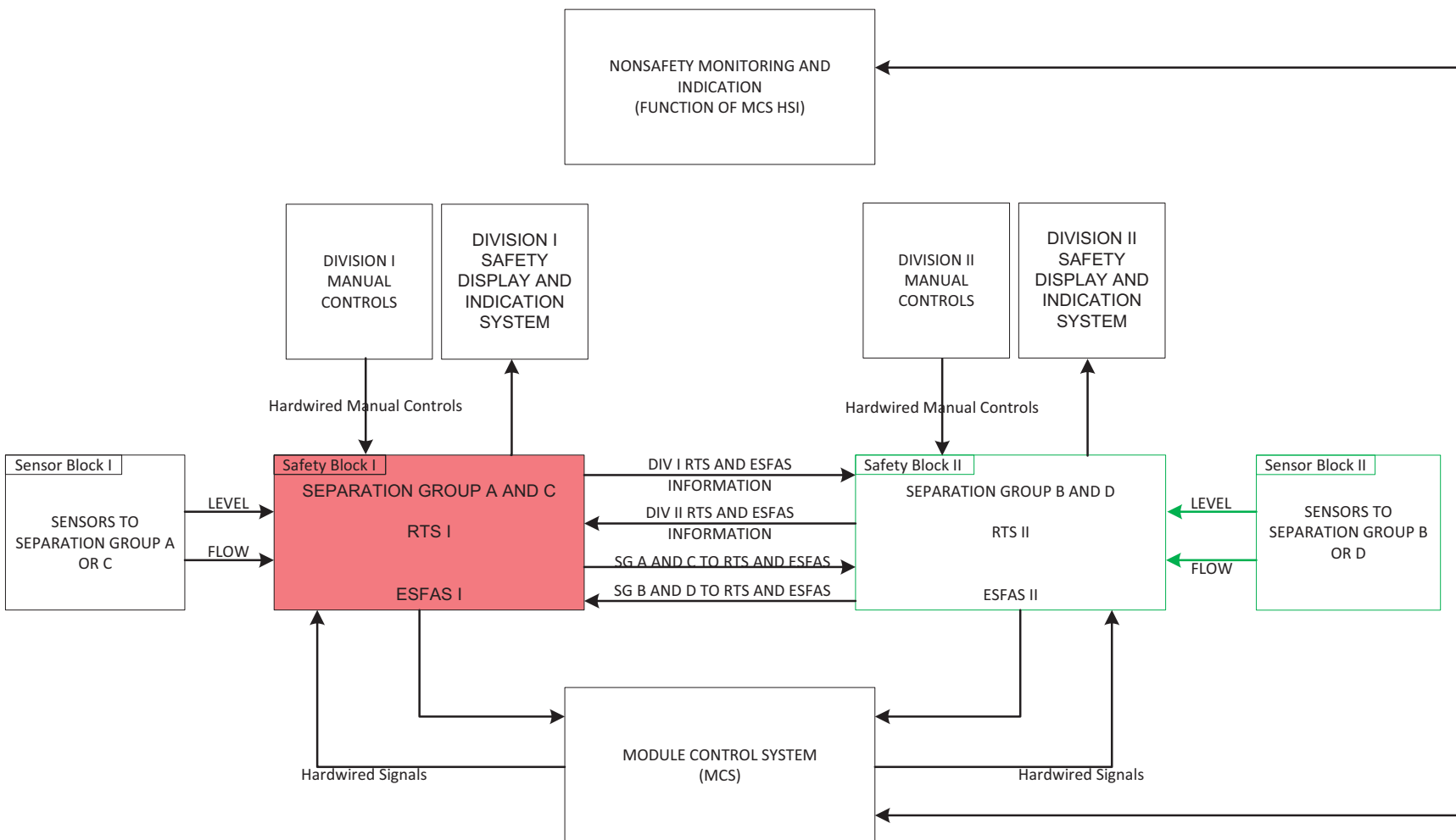


Figure 7.1-8: Common Cause Failure of Safety Block I with False Indication

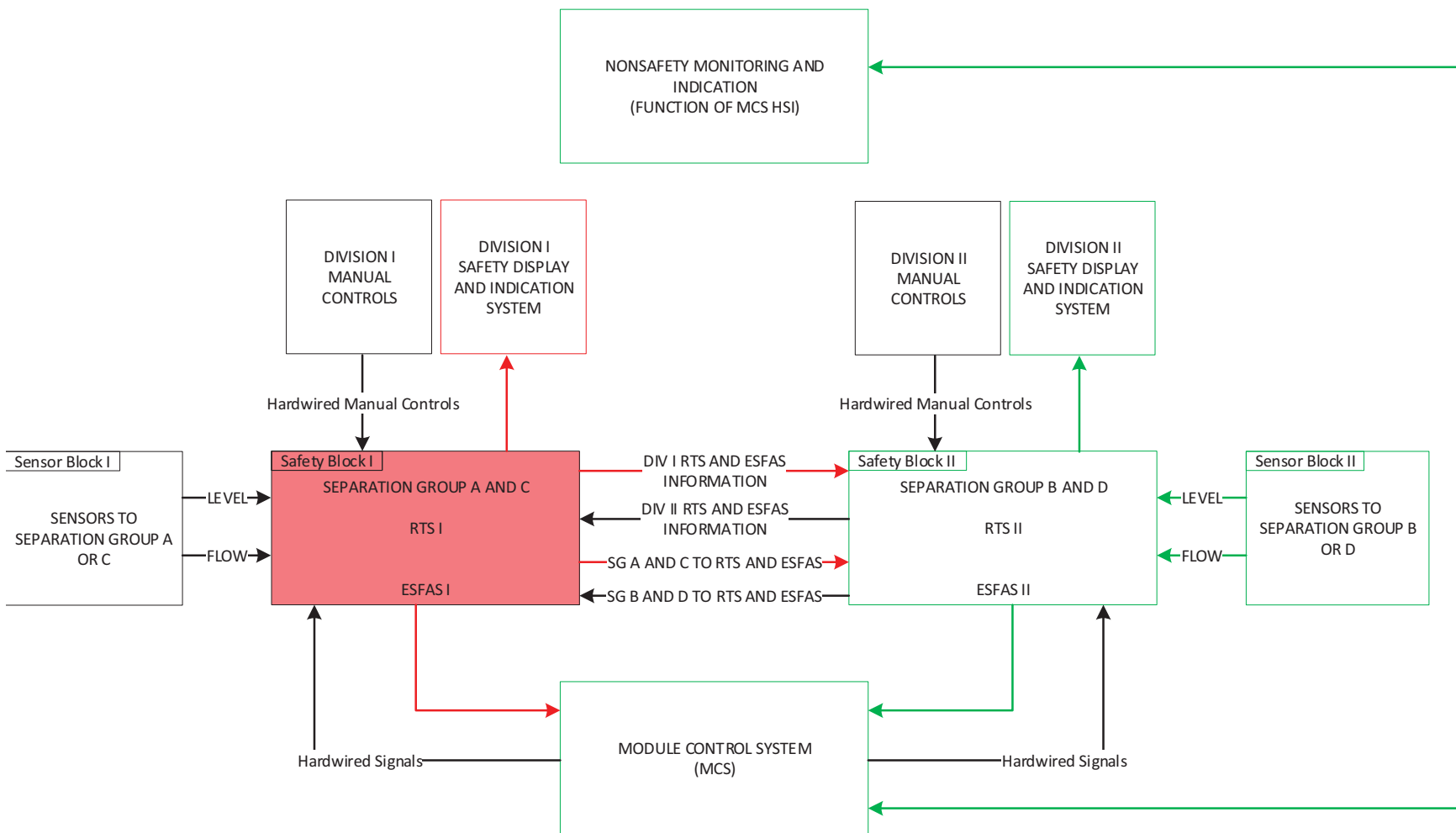


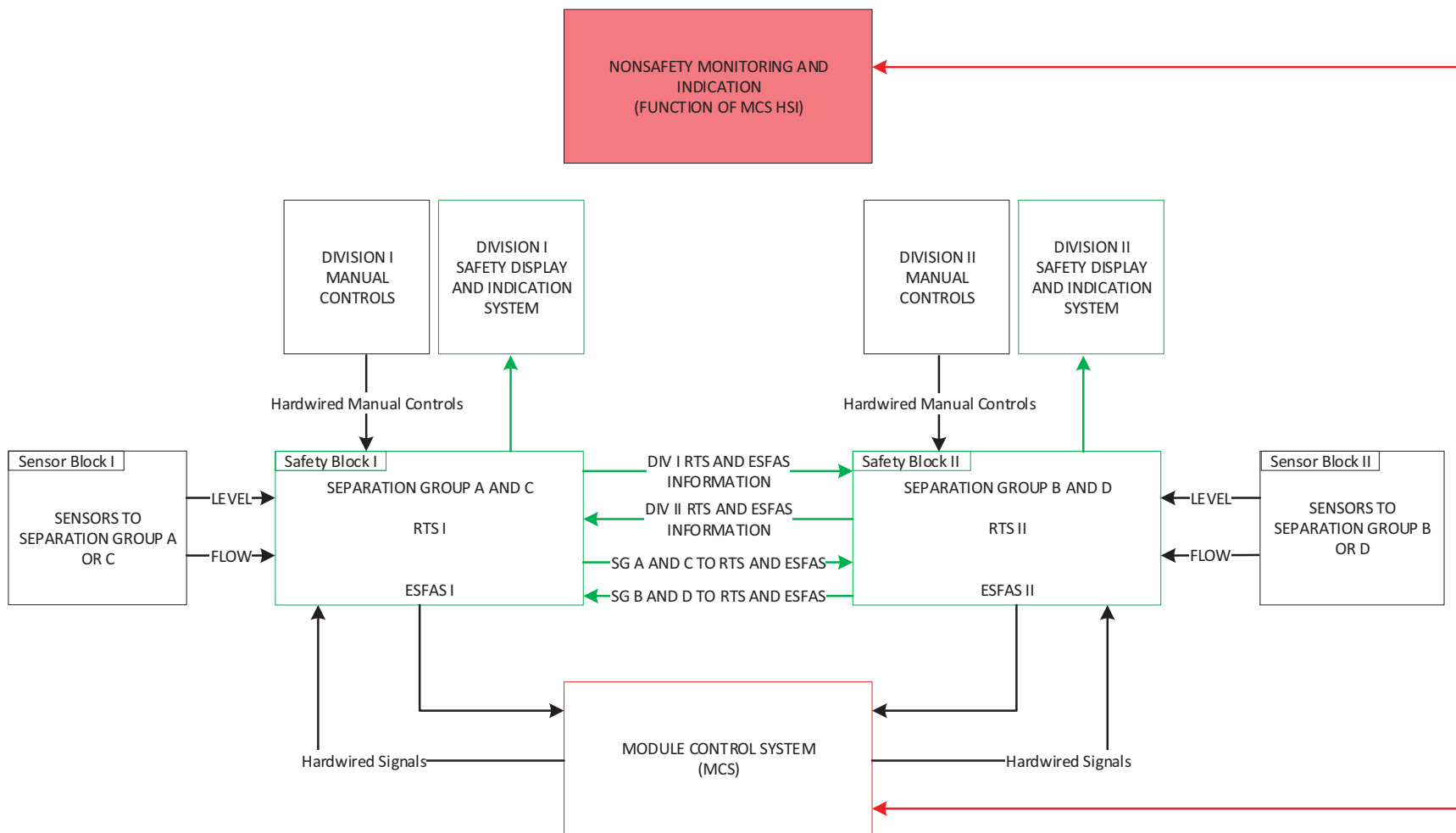
Figure 7.1-9: Common Cause Failure of Nonsafety Monitoring and Indication

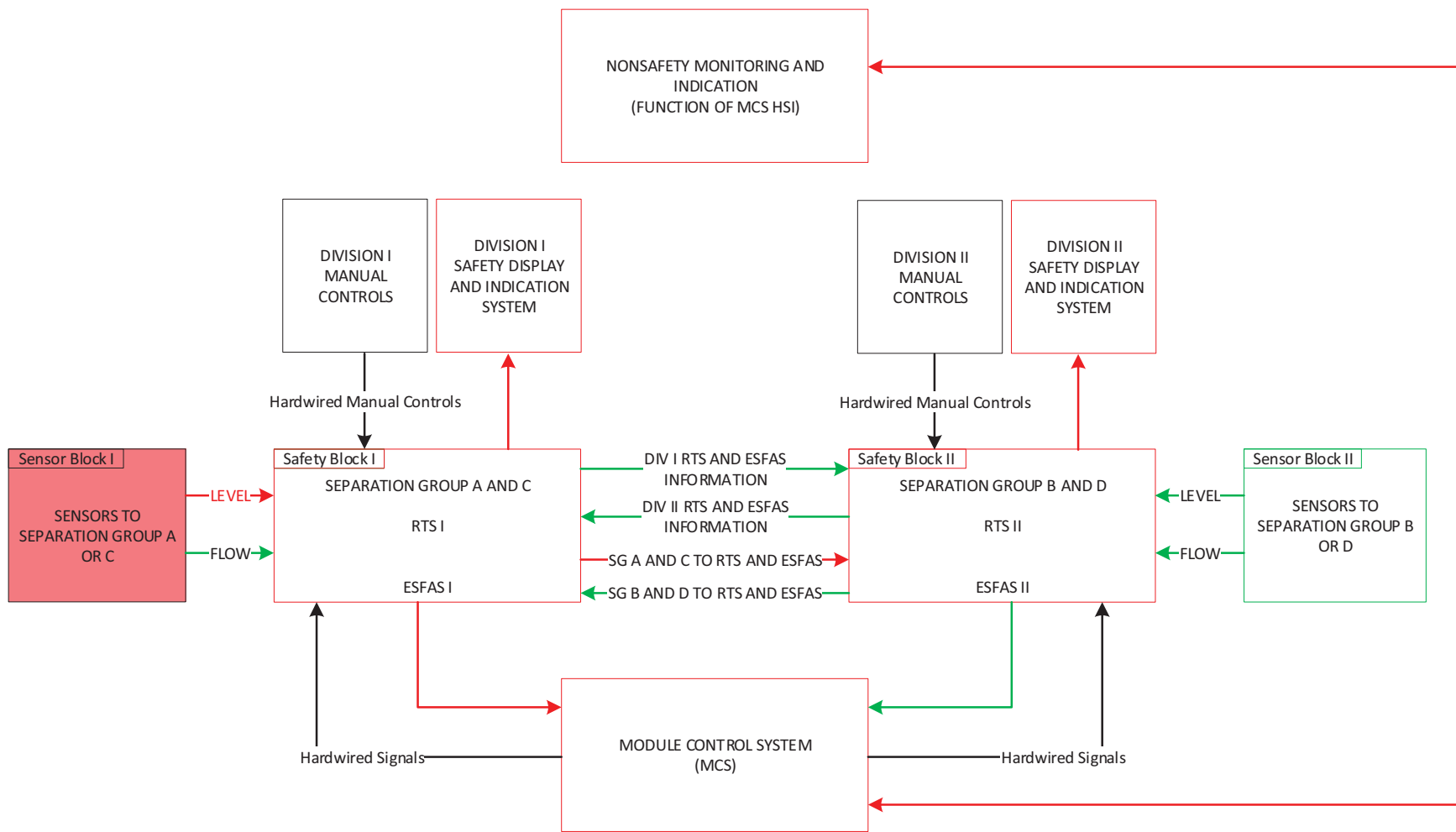
Figure 7.1-10: Digital-Based Common Cause Failure of Level Function Type in Sensor Block I

Figure 7.1-11: Digital-Based Common Cause Failure of Flow Function Type in Sensor Block I and II

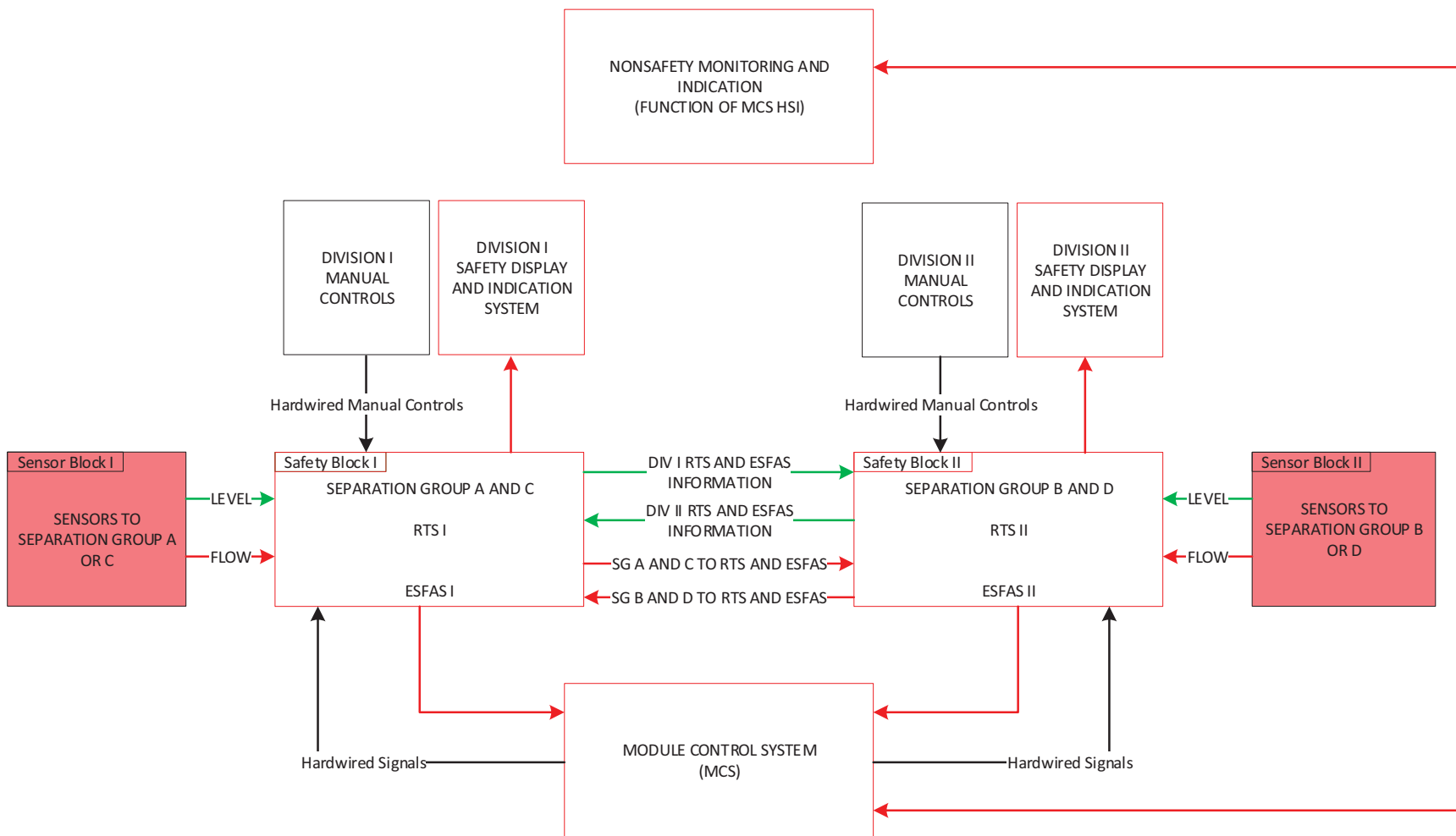


Figure 7.1-12: Direction of Information and Signals between Analysis Blocks

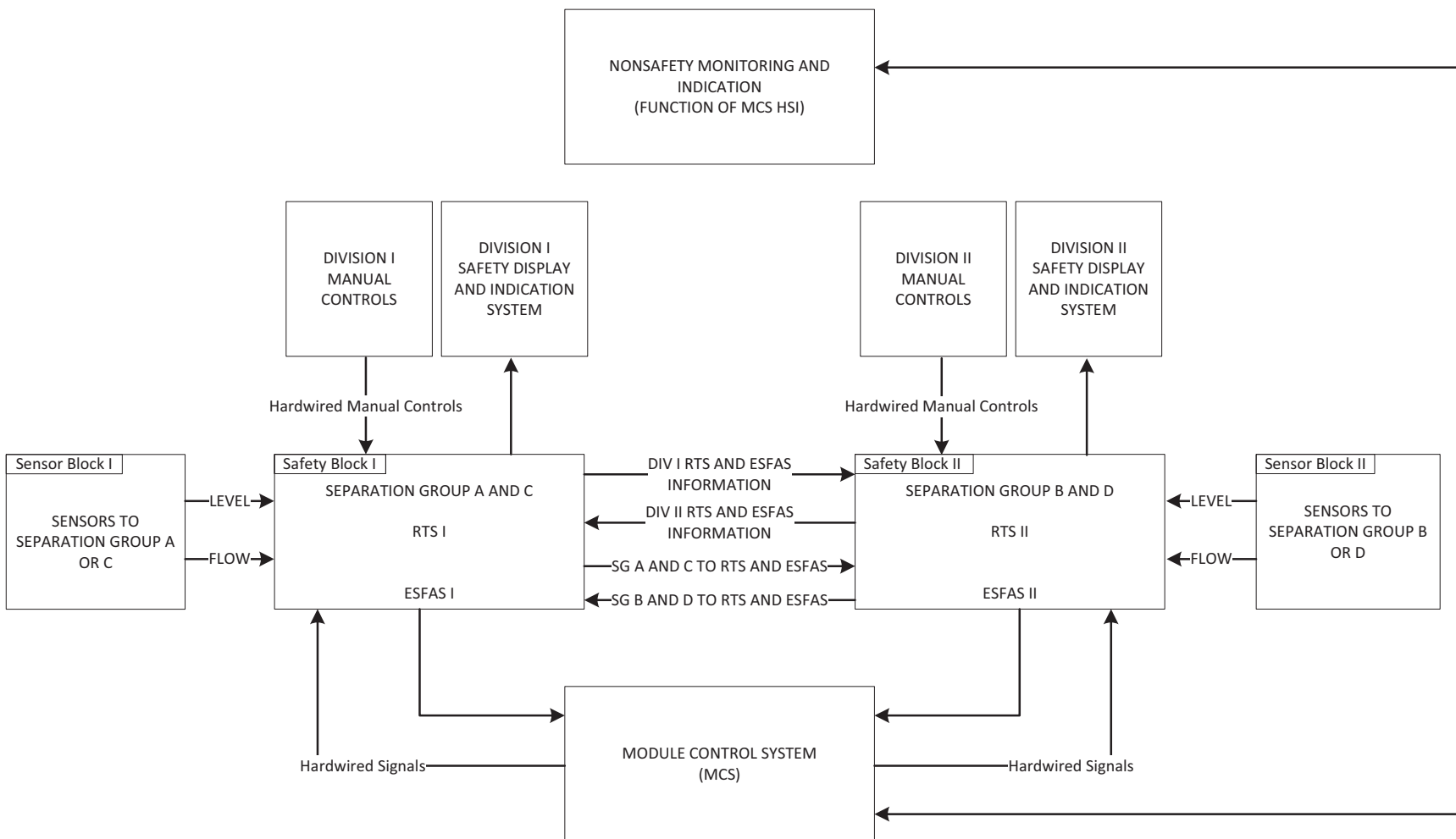


Figure 7.1-13: Basic Control Loop with Example Flawed Control Actions

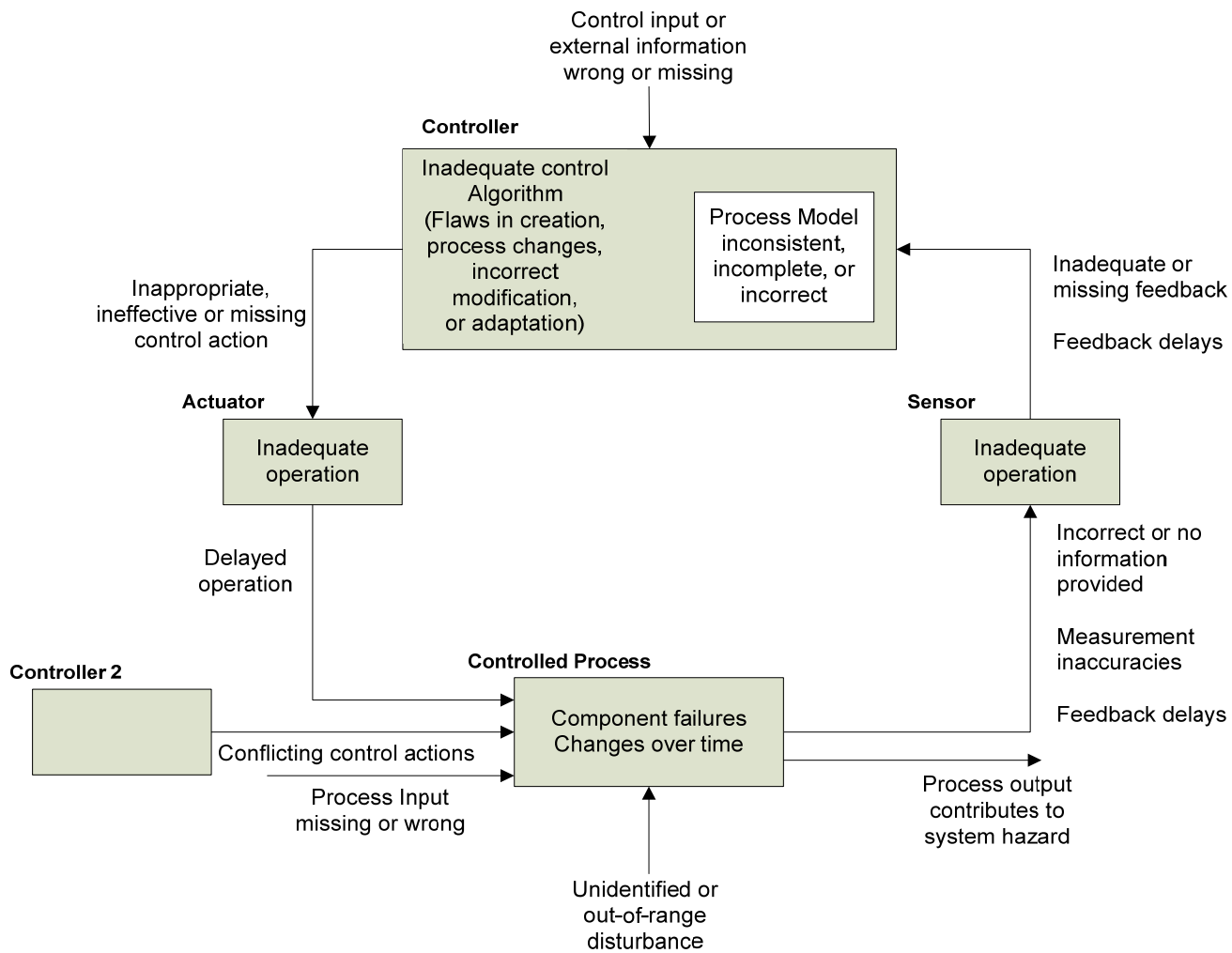


Figure 7.1-14: Example Module Protection System High Level Control Structure

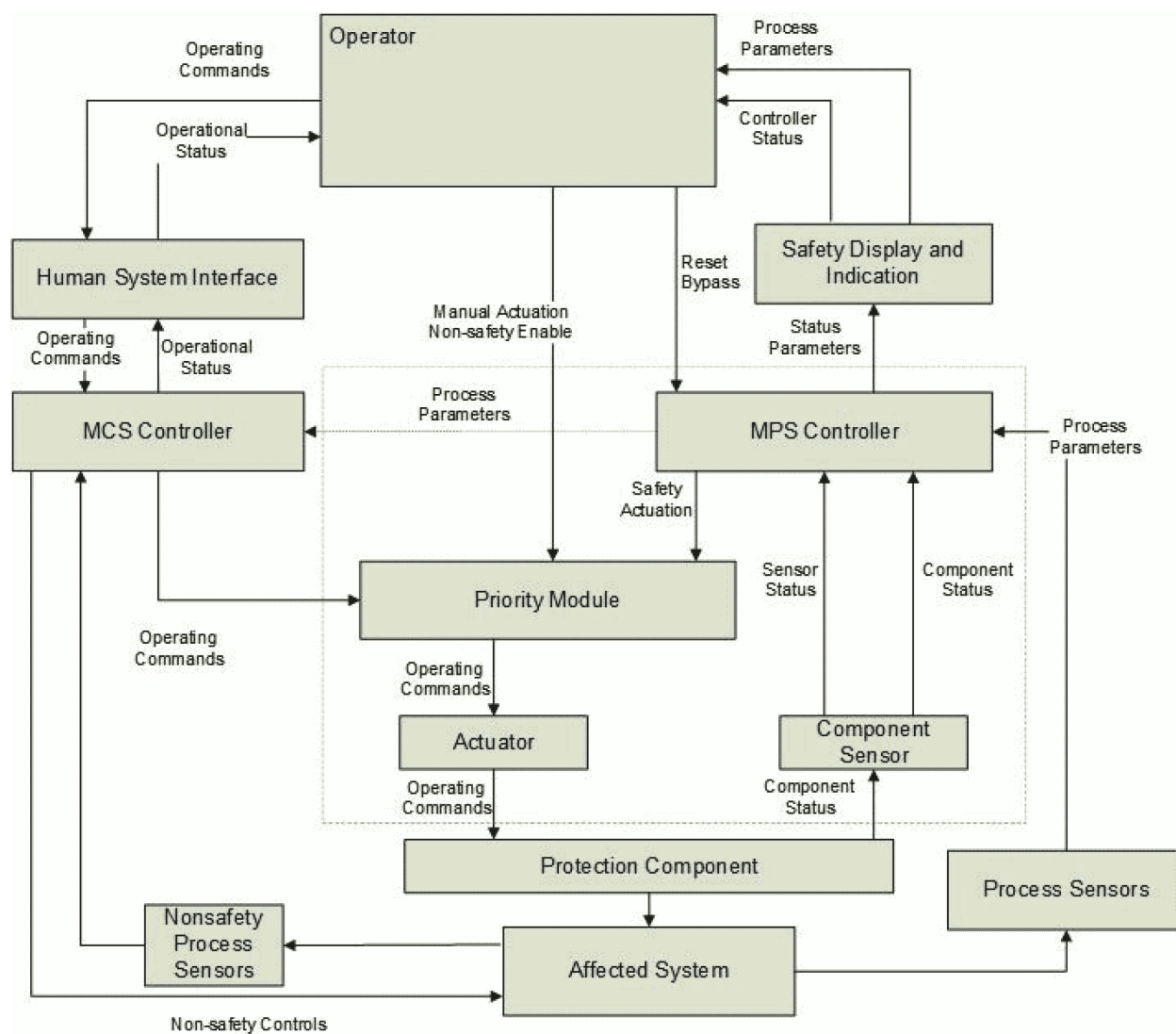


Figure 7.1-15: Example Neutron Monitoring System High Level Control Structure

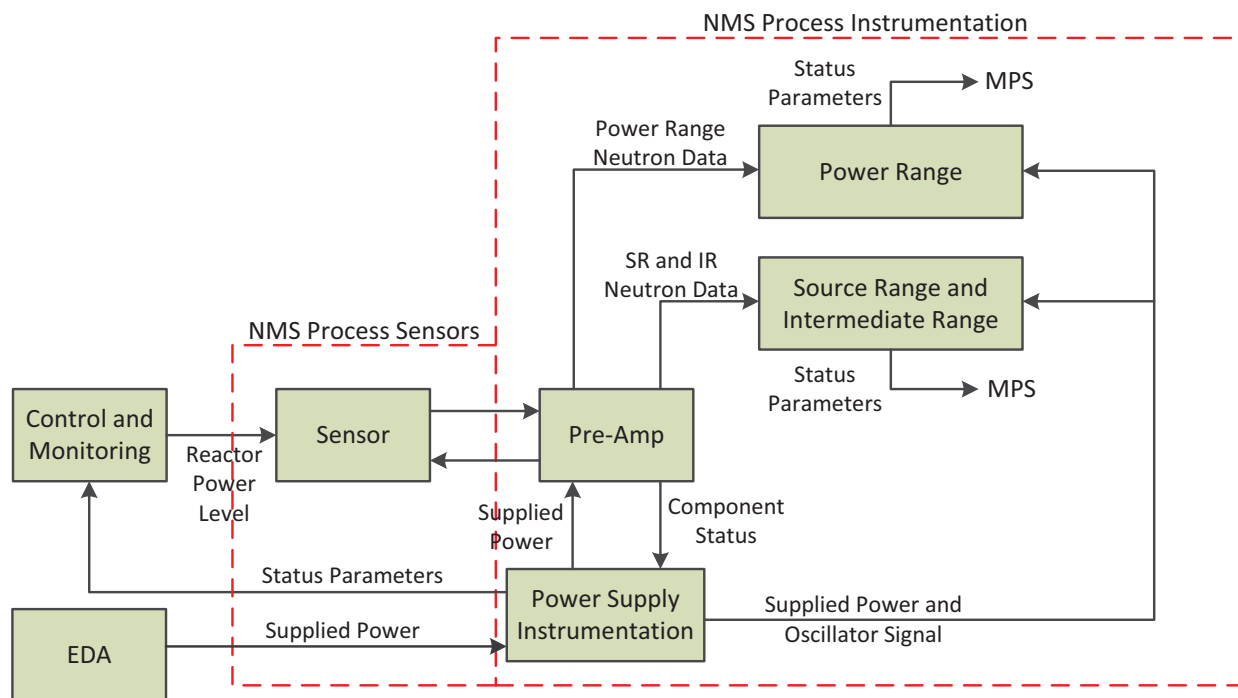


Figure 7.1-16: Safety Function Module Low-Level Logic Structure

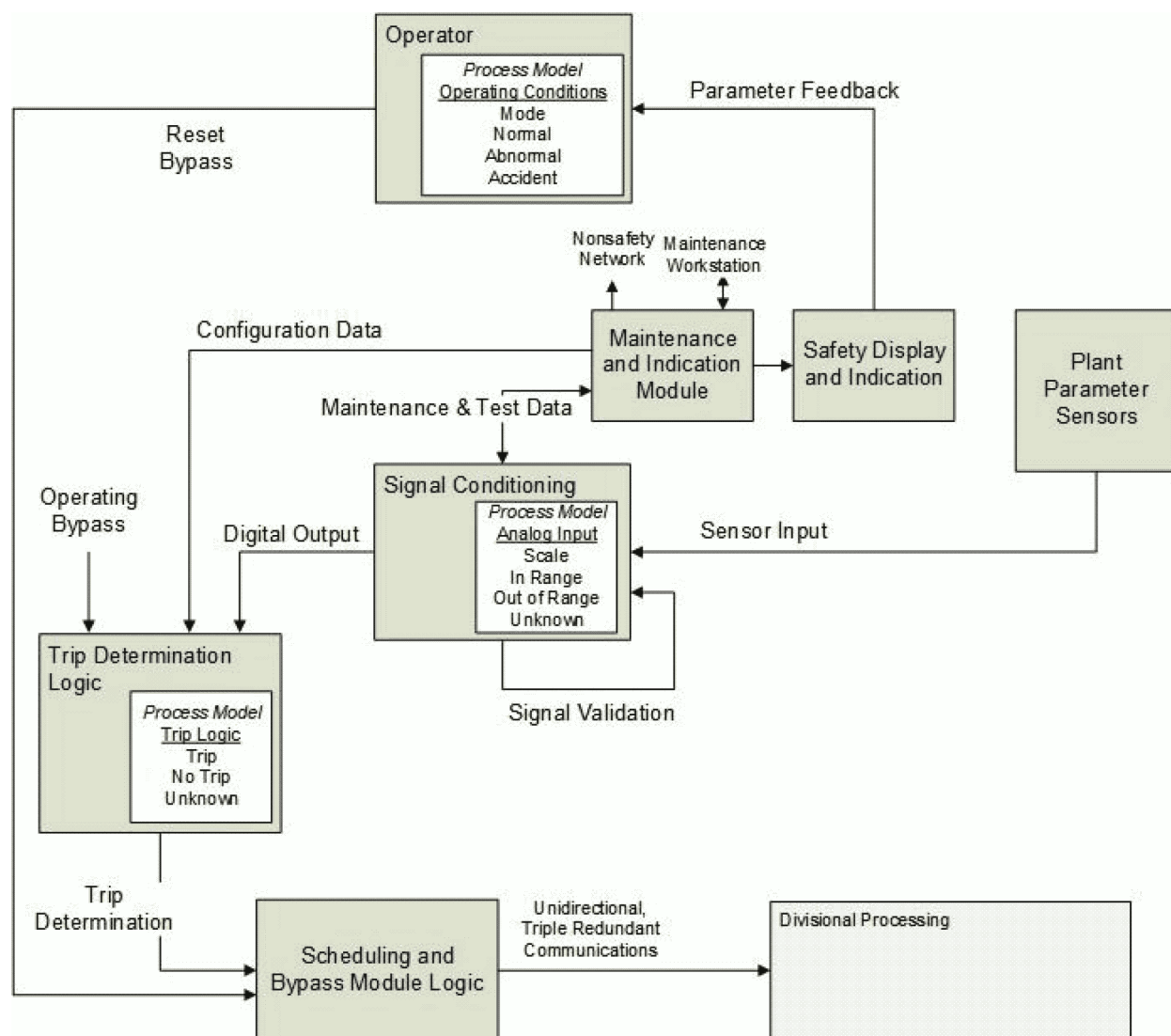
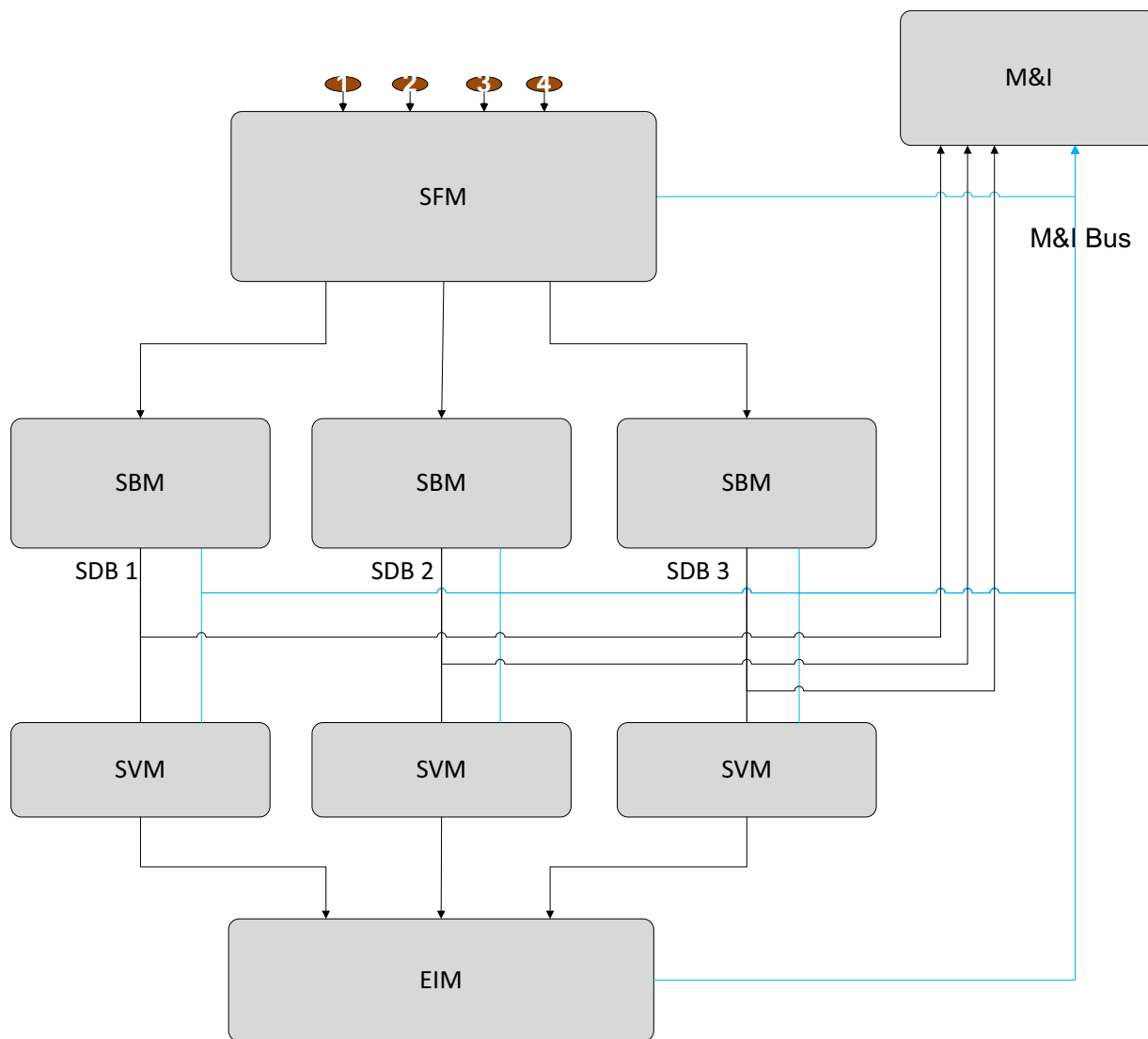


Figure 7.1-17: Basic Module Protection System Configuration



7.2 System Features

The safety-related digital instrumentation and controls (I&C) safety systems include features that complement the fundamental design principles described in Section 7.1, and address specific functional and design requirements contained in IEEE Std 603-1991 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," (Reference 7.2-10) Section 5 (Safety System Criteria), Section 6 (Sense and Command Features-Functional and Design Requirements), and Section 7 (Executive Features-Functional and Design Requirements), and the corresponding guidance provided in IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 7.2-12).

Specific features that are incorporated in the safety-related I&C system designs are described in Section 7.2.1 through Section 7.2.15 below and include the following:

- quality
- equipment qualification
- reliability, integrity, and completion of protective action
- operating and maintenance bypasses
- interlocks
- derivation of system inputs
- setpoints
- auxiliary features
- control of access, identification, and repair
- interaction among sense and command features and other systems
- multi-module stations
- automatic and manual control
- displays and monitoring
- human factors considerations
- capability for test and calibration

7.2.1 Quality

The overall Quality Assurance Program (QAP) applied to the design of the safety-related and nonsafety-related I&C systems is described in the Quality Assurance Program Description, discussed in Section 17.5. The QAP complies with ASME NQA-1-2008 (Reference 7.2-2) and ASME NQA-1a-2009 Addenda (Reference 7.2-3).

The information in this section satisfies the application specific information requirements in NuScale topical report "Design of the Highly Integrated Protection System Platform" (Reference 7.2-24) listed in Table 7.0-2 for application specific action item (ASAI) numbers 4, 16, 47, 49, 50, and 51.

The design of I&C systems meets the QAP. The QAP satisfies the requirements of 10 CFR Part 50 Appendix B and guidance of RG 1.28 (Table 1.9-2).

The overall QAP is supplemented by four process plans:

- Digital Safety Systems Project Plan
- Digital I&C Software Development Plan
- Digital I&C Software Verification and Validation Plan
- Digital I&C Software Quality Assurance Plan

The Digital Safety Systems Project Plan provides the foundation for the digital I&C development effort. It defines the purpose, scope, objectives, high-level schedule, and project team. This plan provides a description of the framework for the I&C design and development process. This framework supplements the overall development process plans (i.e., the Quality Management Plan and the Digital I&C Software Development Plan) with specific system, hardware, and software development activities and includes a description of the proposed development life cycles as well as the management activities that are implemented in the design and development of safety and other applicable nonsafety-related I&C systems.

The Digital I&C Software Quality Assurance Plan and the Digital I&C Software Development Plan define the following:

- the standards, methods, tools, and procedures for the software design and development process
- the activities performed for the phases of the software development
- requirements traceability from the software concept phase to installation and checkout phase
- safety-related requirements documentation, evaluation, review, verification, and testing during the software design process to minimize unknown, unreliable, and abnormal conditions
- the organization and responsibilities of individuals or groups involved in the various software verification and validation (V&V) and review activities
- the structure for test and review guidance for software functional testing
- the requirements and guidelines necessary to prepare, execute, and document software tests
- the requirements for software test documentation
- the requirements for metrics that include error tracking and resolution

The Digital I&C Software Quality Assurance Plan describes the approach, management, organization, responsibilities, and methodologies used for development of software products and configurable logic devices for safety-related and risk-significant I&C systems. This plan describes the following software development activities:

- regulatory requirements applicable to safety-related I&C software products

- processes for developing safety-related I&C software
- required software life cycle processes
- quality assurance (QA) activities performed during the phases of the software life cycle
- responsibilities and authorities for accomplishing software activities
- identification of tools and the resources required for plan execution
- applicable processes for certifying commercial grade software for use in safety-related I&C systems

The Digital I&C Software Quality Assurance Plan defines requirements to ensure compliance with applicable portions of IEEE Std 7-4.3.2-2003 for meeting the unique quality aspects of safety-related software, as specified by Regulatory Guide 1.152. The plan follows the guidelines of IEEE Std 730-2002, "IEEE Standard for Software Quality Assurance Plans" (Reference 7.2-13).

Software development and QA controls are applied to the following I&C systems:

- module protection system (MPS)
- safety display and indication system (SDIS)
- in-core instrumentation system (ICIS)
- plant protection system (PPS)
- module control system (MCS)
- plant control system (PCS)
- radiation monitoring system (RMS)
- Structures, systems, and components (SSC) that contain embedded digital devices

The following items are excluded from these software development and QA controls:

- plant simulator software, which is subject to ANSI/ANS 3.5-2009, "Nuclear Power Plant Simulators for Use in Operator Training and Examination," (Reference 7.2-1) and RG 1.149
- software or complex logic for physical security protection, as delineated within 10 CFR 73.55

The following regulations, regulatory guide, and industry standard apply to the QAP for digital I&C safety systems.

- 10 CFR 50.55a(h)
- 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 1
- Appendix B to 10 CFR Part 50
- Regulatory Guide 1.152
- IEEE Std 7-4.3.2-2003 Section 5.3

The life cycle process defined in the Digital Safety Systems Project Plan satisfies the software development requirements of IEEE Std 7-4.3.2-2003 Section 5.3. The combination of the QAP and Digital I&C Software Quality Assurance Plan satisfy the software QA requirements of IEEE Std 7-4.3.2-2003 Section 5.3.1. The Digital I&C Software Quality Assurance Plan requires that the Digital I&C Software Management Plan address quality metrics, as required by IEEE Std 7-4.3.2-2003 Section 5.3.1.1.

The Digital I&C Software Quality Assurance Plan incorporates tool requirements from IEEE Std 7-4.3.2-2003. The Digital I&C Software Quality Assurance Plan satisfies the software tool use requirements of IEEE Std 7-4.3.2-2003 Section 5.3.2.

The Digital I&C Software Verification and Validation Plan is based on IEEE Std 1012-2004 (Reference 7.2-18), as endorsed by RG 1.168. The V&V program for safety-related software (i.e., SIL 4) is implemented by a V&V team that is technically, financially, and managerially independent from the design development team. The Digital I&C Software Verification and Validation Plan conforms to IEEE Std 1012-2004 with adaptations, as allowed by the standard, and exceptions:

Adaptations

- Verification and validation activities are adapted to life cycle and complex logic device technology (e.g., FPGA). In the application of different FPGA technologies within the MPS, the V&V activities are the same; they do not differentiate among different FPGA technologies.

Exceptions

- Exception is taken to documentation requirement details in Sections 6 and 7 of IEEE Std. 1012-2004 that conflict with standard documentation practices, quality assurance requirements and processes, or are inconsistent with the platform neutral strategy.

The Digital I&C Software Verification and Validation Plan, with the noted exception, satisfies the requirements of IEEE Std 7-4.3.2-2003 Sections 5.3.3 and 5.3.4.

The Digital I&C Software Configuration Management Plan conforms to IEEE Std 828-2005 "IEEE Standard for Software Configuration Management Plans," (Reference 7.2-14) as endorsed by RG 1.169. The Digital I&C Software Configuration Management Plan satisfies the configuration management requirements of IEEE Std 7-4.3.2-2003 Section 5.3.5.

Three process plans (the Digital I&C Software Development Plan, the Digital I&C Software Management Plan, and the Digital I&C Software Quality Assurance Plan) define expectations for risk management during the development of digital I&C systems, based on the guidance in IEEE Std 7-4.3.2-2003. The implementation of the risk management tasks is linked to the NuScale project management process, which has risk management elements. The Digital I&C Software Development Plan and the Digital I&C Software Quality Assurance Plan satisfy the risk management requirements of IEEE Std 7-4.3.2-2003 Section 5.3.6.

The Digital I&C Quality Assurance Plan provides a framework for commercial grade dedication. The Digital I&C Software Quality Assurance Plan requires use of EPRI TR-106439, "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," (Reference 7.2-4) for the commercial grade dedication of digital I&C equipment. RG 1.152 and RG 1.168 note that EPRI TR-106439 contains adequate guidance that the NRC has endorsed. The programmatic requirements applied to the commercial grade dedication of digital I&C equipment satisfy the requirements of IEEE Std 7-4.3.2-2003 Section 5.4.2.

Regulatory Guide 1.152 also addresses expectations for a secure development and operational environment (SDOE) for protection of digital safety systems. The Digital Safety System SDOE Plan is a process plan that defines security controls for the phases of the digital safety system development life cycle. An SDOE Vulnerability Assessment is performed during the basic design stage to identify and mitigate potential weaknesses or vulnerabilities in the phases of the digital safety system life cycle that may degrade the SDOE or degrade the reliability of the system. This assessment also identifies design requirements that are verified or added to the requirements specification for the system. The Digital Safety System SDOE Plan and SDOE Vulnerability Assessment satisfy the risk management SDOE requirements of RG 1.152.

The following describes approach to application of RGs and IEEE standards to software development:

- adapt to complex logic device technology. In the application of different FPGA technologies within the MPS, the V&V activities are the same; they do not differentiate among different FPGA technologies.
- capturing key aspects (i.e., those with a clear nexus to safety) while not committing to other less important or administrative requirements (i.e., those without a clear nexus to safety)
- maintain flexibility where warranted to support implementation of a platform neutral strategy for the safety-related I&C systems
- specifying universally important aspects of software quality that are applicable to safety-critical vendor processes and avoid over-specification that limits choices or complicates implementation of the platform neutral strategy
- Regulatory Guide 1.173 endorses IEEE Std 1074-2006 "IEEE Standard for Developing a Software Project Life Cycle Process" (Reference 7.2-21). The digital I&C safety system development life cycle is implemented in the following process plans:
 - Digital Safety Systems Project Plan
 - Digital I&C Software Management Plan
 - Digital I&C Software Development Plan
 - Digital I&C Software Quality Assurance Plan
 - Digital I&C Software Verification and Validation Plan
 - Digital I&C Software Master Test Plan

- Digital I&C Software Requirements Management Plan
- Digital I&C Software Configuration Management Plan
- Digital I&C Software Integration Plan
- Digital I&C Software Safety Plan
- Digital I&C Software Installation Plan
- Digital I&C Software Training Plan

These documents define the digital I&C safety system development life cycle, key development activities and sequences, management responsibilities, and necessary support activities. In addition to meeting the requirements of IEEE Std 1012-2004, the digital I&C safety system development life cycle described in these key planning documents conforms to the requirements in IEEE Std 1074-2006, as endorsed by RG 1.173.

- Regulatory Guide 1.172 endorses IEEE Std 830-1998, “IEEE Recommended Practice for Software Requirements Specifications,” (Reference 7.2-16) as an acceptable approach for the preparation of software requirements specifications. The Digital I&C Software Development Plan specifies the requirements for the development of software requirements specifications for the safety-related digital I&C systems, consistent with the technical guidance in RG 1.172 and IEEE Std 830-1998. For RG 1.170, the requirements of IEEE Std 829-2008 “IEEE Standard for Software and System Test Documentation,” (Reference 7.2-15) are tailored to the NuScale I&C development life cycle, which is different than that of the conceptual waterfall life cycle listed in RG 1.152. NuScale maps the applicable tasks from IEEE Std 829-2008 to the NuScale I&C development life cycle. NuScale also takes exception to some of the administrative requirements in the standard that conflict with established engineering or QA documentation requirements.
- Regulatory Guide 1.171 endorses IEEE Std 1008-1987, “IEEE Standard for Software Unit Testing,” (Reference 7.2-17) as an acceptable approach for performing unit testing of safety system software. The Digital I&C Software Master Test Plan specifies the requirements for performing software component or unit testing for the safety-related digital I&C systems, consistent with the technical guidance in RG 1.171, and IEEE Std 1008-1987 with the following exceptions:
 - adjustment of testing methods to reflect the use of complex logic device testing tools
 - adjustment of specification documents to reflect the use of complex logic device testing tools (i.e., to produce test documents)
 - exceptions to IEEE Std 829-2008 for software test documentation, as discussed below
- Regulatory Guide 1.170 endorses IEEE Std 829-2008 as an acceptable approach for safety system software test documentation. The Digital I&C Software Master Test Plan specifies the requirements for software test documentation, consistent with the technical guidance in RG 1.170, and IEEE Std 829-2008 with the exception of documentation requirement details of the standard that conflict with

standard engineering documentation practices or quality assurance requirements and procedures.

- Regulatory Guide 1.169 endorses IEEE Std 828-2005 as an acceptable approach for safety system software configuration management. The Digital I&C Software Configuration Management Plan specifies the requirements for software configuration management, consistent with the guidance in RG 1.169, and IEEE Std 828-2005. The Digital I&C Software Configuration Management Plan conforms to the requirements in IEEE Std 828-2005, as endorsed by RG 1.169.
- Regulatory Guide 1.168 endorses IEEE Std 1012-2004 as an acceptable approach for V&V of safety system software. The RG also endorses IEEE Std 1028-2008 “IEEE Standard for Software Reviews and Audits,” (Reference 7.2-19) as an acceptable approach for carrying out software reviews, inspections, walkthroughs, and audits typically used in association with software QA activities. The Digital I&C Software Verification and Validation Plan conforms to RG 1.168, and IEEE Std 1012-2004 with adaptations and exceptions as follows:

Adaptations

- Verification and validation activities are adapted to NuScale life cycle and complex logic device technology. In the application of different FPGA technologies within the MPS, the V&V activities are the same; they do not differentiate among different FPGA technologies.

Exceptions

- Consistent with the guidance in RG 1.170, exceptions are taken to documentation requirement details in Sections 6 and 7 of IEEE Std 1012-2004 that conflict with standard documentation practices or are inconsistent with the platform neutral strategy (where flexibility is retained to adopt established vendor documentation formats). The approved QAP (Section 17.5) takes precedence.

Software reviews, inspections, walkthroughs, and audits are performed as part of software design, V&V, and quality assurance activities during development phase. These activities are performed and documented QA program requirements. Exception is to the methods and documentation requirement specified in IEEE Std 1028-2008, because these details conflict with standard documentation practices or quality assurance requirements and processes, or are inconsistent with the platform neutral strategy (where flexibility is retained to adopt established vendor methods and documentation formats for these activities).

7.2.1.1 Instrumentation and Controls Safety System Development Process

Figure 7.2-1 provides a graphical representation of the overall system and software life cycle processes. The system and software life cycles for development of the I&C safety systems consist of five major elements:

- project management and organizational processes
- safety analyses

- system and software technical development
- independent verification and validation
- configuration management

The project management and organizational processes are used to establish the infrastructure for I&C safety system development. The system and software safety analyses are performed throughout the system and software life cycle phases in order to identify hazards associated with I&C system design and operation. The system and software technical development processes establish the methodology for the system and software design development life cycle of the I&C safety systems. Independent V&V processes establish V&V methods, activities, and oversight for development of the I&C safety systems, which are technically, financially, and managerially independent from the development organization.

As indicated in Figure 7.2-1, technical development is split into three distinct elements:

- basic design
- detailed design
- system integration, installation, and testing

Basic design activities are the overall design requirements for the I&C systems. Lower level digital component and software design activities are performed in accordance with the basic design requirements and are considered to be a part of detailed design. Figure 7.2-2 provides a detailed representation of the system and software design technical development activities. A description of the life cycle phases associated with system and software technical development is provided in Section 7.2.1.1.1. The software development life cycle is the same for the two types of FPGAs used in the highly integrated protection system (HIPS) platform.

The digital I&C system and software development life cycle is correlated to other life cycles presented in various regulatory documents in Figure 7.2-3.

7.2.1.1.1 Basic Design Overview

The set of technical development activities considered to be a part of the system basic design is shown in Figure 7.2-2. Basic design activities coincide with what is typically considered the concept phase with regard to a software development life cycle. For this reason, specific exit criteria are specified only for the equipment requirements specification phase of basic design to meet safety software development QA requirements. System basic design activities are highly iterative in nature, beginning with system requirements documentation development, and ending with detailed equipment requirements specification (ERS) development.

Basic design activities are performed in accordance with the design control process, which is a sequential approach to system design consisting of preliminary and final design documents. Preliminary design documents are

those issued for conceptual design or those that reference draft, preliminary, or conceptual information. Final design documents are those issued for procurement, fabrication, construction, or detailed design.

During the system development life cycle process, multiple iterations between the system functional requirements specification phase and the system design phase are performed. For this reason, the final activities of a successive system development life cycle phase cannot be performed until the final design, safety analyses, V&V, and QA activities are completed for the previous life cycle phase.

Life cycle phase entry and exit criteria are defined in the Digital I&C Software Quality Assurance Plan.

7.2.1.1.1.1 System Concept Phase

System Functional Requirements

During this system development phase, system functional requirements documentation is prepared following the design control process and procedures. The output of this phase is the approved and configuration-controlled system requirements documentation. The Digital I&C Software Quality Assurance Plan, Digital I&C Software Verification and Validation Plan, Digital Safety Systems Safety Plan, Digital Safety Systems SDOE Plan, and preliminary hazard analyses are final products of this phase.

The Digital I&C Software Quality Assurance Plan is a process plan that identifies the QA procedures applicable to specific system and software development processes, as well as identifying particular methods chosen to implement QA procedures.

The Digital I&C Software Verification and Validation Plan is a process plan that documents the V&V activities necessary for the system development life cycle.

The Digital Safety Systems Safety Plan is a process plan that documents the process for examining the system throughout its system and software development life cycles to identify hazards (i.e., factors and causes), I&C requirements, and constraints to eliminate, prevent, or control. The hazard analyses covered in the Digital Safety System Safeties Plan examine safety-related I&C systems, subsystems, and components, interrelationships and interactions with other systems, subsystems, and components to identify unintended or unwanted I&C system operation including the impairment or loss of the ability to perform a safety function.

The Digital Safety Systems SDOE Plan is a process plan that documents the process for ensuring that the development processes and documentation are secure such that the system does not contain undocumented logic, unwanted functions or applications, and other logic

that could adversely impact the integrity or reliability of the digital safety system. The Digital Safety Systems SDOE Plan also addresses physical security requirements and access control features.

A requirements traceability matrix (RTM) is developed in this phase. The RTM is documented, tracked, and maintained throughout the following system and software development phases and facilitates bidirectional traceability of the system requirements.

Conceptual System Design

In the conceptual system design phase, the system design team prepares the conceptual system design documentation following the design control process and procedures. These documents provide the system architecture and design details and is developed based on the system requirements documentation and safety analysis requirements as inputs.

The system design documentation is analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management. Bi-directional traceability is established between the system design documentation and the system requirements documentation. The system design documentation is also used as input to the ongoing system safety analyses. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the conceptual system design phase.

System Prototype Development

In the system prototype development phase, the system design team develops a system prototype as an integrated part of the system basic design process in order to reduce the overall project risk. The prototype development activities are not required to be performed under a 10 CFR Part 50 Appendix B program. The prototyping is used to put together a working model in order to test various aspects of a design, illustrate ideas, investigate new features, and provide guidance in the development of the detailed ERS. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the system prototype development phase.

The primary purpose of a prototype development effort is to:

- provide early proof of concept demonstration
- acquire experience with the system behavior, including understanding
 - system dynamics
 - bus communications
 - system integrity monitoring
 - input and output limitations
 - software development process
- support identification of problems with the efficacy of a new design
- support refinement of potential risks associated with system development, implementation, operation, and maintenance

System Equipment Requirements

In the equipment requirements specification phase, an ERS or equivalent is prepared for the applicable system products. The ERS is developed based on the system requirements documentation, the system design documentation, and prototype lessons learned as inputs. The primary output of this phase is the approved ERS. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the equipment requirements specification phase.

The Digital I&C Software Integration Plan, Digital I&C Software Configuration Management Plan, Digital I&C Software Master Test Plan and Digital I&C Software Installation Plan are also products of this phase.

The Digital I&C Software Integration Plan documents the integration and testing of software items, hardware, manual processes, and other system interfaces that constitute the I&C system, consistent with the architectural design.

The Digital I&C Software Configuration Management Plan documents the process for providing the identification and configuration baselines for system and software items.

The Digital I&C Software Master Test Plan provides guidance for test planning and management for system and software testing for digital safety systems.

The Digital I&C Software Integration and Installation Plans together describe the general procedures for installing the finished system in the production environment.

7.2.1.1.2 Detailed Design Overview

A set of technical development activities are performed after completion of the detailed ERSs and are considered to be a part of the system detailed design as shown in Figure 7.2-2. The detailed design activities are performed by a vendor under a 10 CFR Part 50 Appendix B QAP, which meets the requirements of the Quality Assurance Plan.

Detailed system design includes hardware development and an iterative software development process that are described in the Digital I&C Software Development Plan.

The life cycle phase entry and exit criteria are defined in the Digital I&C Software Quality Assurance Plan.

7.2.1.1.2.1 System Requirements Phase

Hardware Planning

The hardware planning phase is used to define the system hardware development framework and organize the hardware development project. This phase ends with a completed Hardware Development Plan. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the hardware planning phase.

The Hardware Development Plan identifies the activities and associated tasks included in each hardware development life cycle phase, the task inputs and outputs, and establishes the review, verification, and validation of those outputs.

Software Planning

The software planning phase is used to define the software development framework and organize the software development project. This phase ends with a completed Digital I&C Software Development Plan, Digital I&C Software Verification and Validation Plan, Digital I&C Software Master Test Plan, and Digital I&C Software Training Plan. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to

the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the software planning phase.

This phase includes the following tasks:

- organizing the software development team
- identifying the tasks to be performed by the sub-vendor and by NuScale
- determining the software integrity level
- establishing the exact requirements in the Digital I&C Software Development Plan for the following:
 - interfaces with the system design process
 - software development cycle
 - SIL determination
 - end-of-phase reviews (scope, participants)
 - list of software development products (e.g., documentation, hardware description language listing, and so on)
- defining and arranging support activities for software development, such as configuration management, software QA, and software project management

The Digital I&C Software Development Plan defines which activities and associated tasks are part of the software development life cycle phase, states the task inputs and outputs, and requires the review, verification, and validation of those outputs. The Digital I&C Software Development Plan describes the process for the translation of the detailed design into hardware description language.

The Digital I&C Software Verification and Validation Plan defines the activities, expectations, processes, and base level of rigor for V&V that is to be performed for SIL 1 through 4 software systems.

The Digital I&C Software Master Test Plan defines criteria for the test organization, test schedule, test resources, responsibilities, tools, techniques, and methods necessary for software testing.

The Digital I&C Software Training Plan documents the training management, implementation, and resource characteristics necessary for the software development project.

Hardware Requirements

During the hardware requirements phase, the requirements provided in the ERS are analyzed, decomposed and allocated to a level that is

implementable in hardware according to the Hardware Development Plan. The primary output of this phase is the hardware requirements specification. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the hardware requirements phase.

Software Requirements

During the software requirements phase, the requirements provided in the system requirements documentation, system design documentation, and ERS are analyzed and decomposed. The requirements are allocated to a level that is implementable in software according to the Digital I&C Software Development Plan. The outcome of the requirements analysis and functional decomposition is captured in the RTM where requirements are maintained and traced for system verification. The primary output of this phase is the Digital I&C Software Requirements Specification with the Interface Requirements Specification.

The independent V&V team develops the Acceptance and System Test Plans for SIL 4 software systems during this phase.

The Digital I&C Software Requirements Specification is analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management according to the Digital I&C Software Configuration Management Plan. The Digital I&C Software Requirements Specification is also used as input to the ongoing I&C system safety analyses. Additional outputs of this phase include an SDOE assessment, criticality assessment update, RTM update, interface requirements specification, and a software safety analysis. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the software requirements phase.

7.2.1.1.2.2

System Design Phase

Hardware Design

During the hardware design phase, the hardware is designed, documented, and verified to meet the hardware requirements specification in accordance with the Hardware Development Plan. The system hazard analysis is reviewed when final system design information or inputs are

revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the hardware design phase.

Software Design

In the software design phase, a Software Design Description for the applicable software products is prepared according to the Digital I&C Software Quality Assurance Plan. The Software Design Description is developed based on the Software Requirements Specification and the system architecture described in the ERS as inputs. The Software Design Description demonstrates adequate coverage of the software requirements and the absence of unnecessary functions.

The primary outputs of this phase are the approved Software Design Description and the necessary interface design descriptions, and the acceptance, system, integration, and test design documents. The Software Design Description and Interface Design Description are analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management according to the Digital I&C Software Configuration Management Plan. The Software Design Description is also used as input to the ongoing I&C system safety analyses. Additional outputs of this phase include an SDOE assessment, criticality assessment update, RTM update, and a software safety analysis. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the software design phase.

The principles applied in the software integration tests are also defined during this phase to evaluate software performance. Software component and integration test plans are developed according to the Digital I&C Software Master Test Plan.

7.2.1.1.2.3

System Implementation Phase

Software Implementation

The Digital I&C Software Integration Plan governs both software implementation and integration tasks performed during the software implementation phase. During the software implementation phase, the implementation process transforms the detailed logic design into hardware description language. The functions described in the Software Design

Description are developed in the software development environment using applicable coding standards (e.g., Hardware Description Language Specifications and Conventions Guideline). Analysis is performed on the software to identify potential hazards.

This phase includes the generation, testing, and assessment of the developed software including development of test procedures and test cases. The purpose of the testing and assessments is to support development and evaluation of the individual logic components or units defined during the logic design phase.

The correct implementation of the Software Requirements Specification is validated during software component tests with the software development and simulation tools, and during testing on the test and development system.

Responsibilities for acceptance, system, component, and integration testing are provided in the Digital I&C Software V&V Plan, and the Digital I&C Software Master Test Plan.

Additional outputs of this phase include an SDOE assessment, criticality assessment update, RTM update, and a software safety analysis update. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the software implementation phase.

The software is implemented on system hardware and tested in accordance with the Digital I&C Software Verification and Validation Plan and the Digital I&C Software Master Test Plan. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the software configuration phase.

7.2.1.1.3 System Testing, Installation, Operations, and Maintenance

7.2.1.1.3.1 System Testing Phase

Final system and factory acceptance testing is performed based on the approved System Test Plan that is specific to the system under test. The acceptance test procedures are developed in this phase by the independent V&V team for SIL 4 software systems.

During this phase, the software is integrated with software from previous iterations and logic integration testing is performed in accordance with the test procedures. Integration test execution results are analyzed to determine if the system implements the requirements and design and that the software components function correctly. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the system testing phase.

7.2.1.1.3.2 System Installation Phase

Installation and checkout activities are performed when the developed system is installed in the target environment and location and site acceptance testing (SAT) is conducted. The installation and checkout V&V activities address system installation and acceptance and are described in the Digital I&C Software Development Plan.

System tests are performed in accordance with the SAT test procedures. Tests are analyzed to determine if the system implements the system design requirements and that the software components function correctly together. Test results are analyzed to determine if the software satisfies system objectives. Tests pass or fail based on the acceptance criteria stipulated in the test plans and based on specific requirements found in the system requirements documentation. The system hazard analysis is reviewed when final system design information or inputs are revised or changed to determine whether the changes impact the inputs or results of the hazard analysis. The hazard analysis is updated according to the process described in Section 7.1.8.3 if the design changes are determined to impact the existing hazard analysis or if new hazards are identified according to the Digital I&C Software Quality Assurance Plan with the results documented in the system installation phase.

7.2.1.1.3.3 Operation Phase

The operation phase covers the operation of the developed and installed system in the target environment and location. The objectives of operation V&V tasks are to evaluate new constraints in the system, assess proposed changes and the impact on the software, and evaluate operating procedures for correctness and usability.

7.2.1.1.3.4 Maintenance Phase

The maintenance phase is activated when the software product undergoes modifications caused by a problem or a need for improvement or adaptation. The maintenance V&V activity addresses modifications (e.g.,

enhancements, additions, and deletions), migration, or retirement of the system during the operation process.

Modifications to the software are treated as development processes and are verified and validated in accordance with the development process described in Section 7.2.1.1.1.1 through Section 7.2.1.1.2.3.

7.2.1.2 Software Development Activities

The Digital I&C Software Development Plan describes the activities employed in the development of I&C system software. The development activities are adjusted based on the software classification that is based on the SIL scheme defined in the software classification procedure. This procedure governs the criticality analysis performed to determine the SIL level of the software necessary to accomplish the safety functions and requires that functions of lower SIL levels that support a system safety function are reclassified to the highest SIL level appropriate for the supported system safety function. In the application of different FPGA technologies within the MPS, the software development activities are the same; they do not differentiate among different FPGA technologies.

7.2.1.2.1 Instrumentation and Controls Software Safety Analyses

A software safety analysis is conducted and is documented in a Software Safety Analysis Report, which is initiated in the concept phase with the Preliminary Hazard Analysis and updated throughout subsequent life cycle phases. When a report is first initiated or subsequently updated, an independent V&V team performs V&V. Anomalies identified during the V&V process are documented in a V&V anomaly report and reported to the software development team. Anomalies must be satisfactorily resolved before issuing a V&V task report.

The Software Safety Analysis Report constitutes a configuration item and is placed under configuration management, for which change control is documented pursuant.

7.2.1.2.2 Instrumentation and Controls System Requirements

A Digital I&C System Requirements Specification is developed describing the identification, development, documentation, review, approval, and maintenance of I&C system requirements. The system requirements documentation together with the system design documentation developed during the I&C basic design process (Section 7.2.1.1.1) may be used as a System Requirements Specification. The Digital I&C System Requirements Specification includes the following:

- the need for system and software safety analyses throughout the life cycle
- functions and capabilities of the I&C system during operations
- system boundaries
- safety classification

- safety functional properties and additional features not performing a safety function
- licensee requested features
- safety, security, and human machine interfaces
- operations and maintenance measures, including intended fault identification, test, calibration and repair
- design constraints
- qualification requirements
- results from hazard analyses
- restrictions and constraints placed on the system to ensure compatibility with other plant systems

The Digital I&C Software Requirements Management Plan governs the development, management and control of software requirements during the software development process. An RTM is initially populated from the system requirements and system design specifications to facilitate bidirectional traceability (from requirements to system validation testing) of system requirements.

Where appropriate, the RTM identifies references to analyses and supporting documentation that establish the bases for system requirements.

Inconsistencies between system requirements documentation and other system-related elements, such as hardware and software, are identified and evaluated. The completed Digital I&C System Requirements Specification is used as input to the ongoing I&C system safety analysis activity.

For SIL 4, an independent V&V team performs V&V of the Digital I&C System Requirements Specification. For SIL 1, 2, and 3, an independent verifier within the engineering or V&V team performs this function. Anomalies identified during the V&V process are documented in a V&V anomaly report and reported to the software development team. Anomalies must be satisfactorily resolved before issuing a V&V task report.

The Digital I&C System Requirements Specification is baselined, updated as necessary, and placed under configuration management.

7.2.1.2.3 Instrumentation and Controls System Architecture

The system design documentation documents the system architecture and design details and uses the system requirements documentation and safety analysis requirements as inputs. The system design documentation is analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management. Bi-directional traceability is established between the system design documentation and the system requirements

documentation. The system design documentation is also used as input to the ongoing system safety analyses.

7.2.1.2.4 Instrumentation and Controls System Design

A system prototype is used to test various aspects of a design, illustrate ideas, investigate new features, and provide guidance in the development of the detailed ERS. The system design effort addresses

- system dynamics
- bus communications
- system integrity monitoring
- input and output limitations

The ERS is based on the system requirements documentation, the system design documentation, and prototype lessons learned as inputs.

The ERS is analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management. Bidirectional traceability is established between the ERS and the system design documentation. The ERS is used as input to the ongoing system safety analyses.

7.2.1.2.5 Software Requirements

A Software Requirements Specification along with an interface requirements specification is developed for the software product to document the basis for the design and implementation of software or complex logic within the digital I&C system. In this development process, a software or complex logic product is the highest element in the software hierarchy. Software or complex logic products are comprised hierarchically of software components and software modules.

The Software Requirements Specification is derived from and traceability is ensured with the system design, I&C system architecture, system design documentation, and Digital I&C System Requirements Specification. Where appropriate, the RTM identifies references to analyses and or supporting documentation that establish the basis for software requirements.

The completed Software Requirements Specification is used as input to the ongoing I&C software safety analysis activity for SIL 3 and 4 software or complex logic.

For SIL 4 software, an independent V&V team performs V&V of the Software Requirements Specification. For SIL 1, 2, and 3 software, an independent verifier within the engineering or V&V team performs this function. Anomalies identified during the V&V process are documented in a V&V anomaly report and reported to the software development team. Anomalies must be satisfactorily resolved before issuing a V&V task report.

The Software Requirements Specification is baselined, updated as necessary, and placed under configuration management.

7.2.1.2.6 Software Design

A Software Design Description is developed for the software product to document the detailed design for the software or complex logic elements of the software system and how the software units are to be constructed. It addresses the methods by which software units are refined into lower levels including software modules to allow coding programming, compiling (not applicable for complex logic), and testing. The software or complex logic is also divided into a set of interacting units, including the description of those units, the interfaces, and dependencies in a structured fashion. The interface design description supplements the Software Design Description as described in Section 7.2.1.

The design of the software module is restricted to one clearly identified function that involves minimum interaction with other functions to minimize the impact of changes. The interfaces among the various units are simple, completely identified, and documented.

The applicable software design is incorporated from the Software Requirements Phase into the software design and implementation and traceability is established between software unit(s) and software module(s).

An assessment of the software design is performed to ensure the software design adequately covers the requirements in the Software Requirements Specification and does not contain unnecessary software, complex programmable logic, or functions. The software design is assessed to:

- identify unused capabilities
- evaluate the safety benefit of the intended function and whether those functions adversely impact performance of the safety function
- identify compensatory measures taken

Security analysis verification is performed as part of the verification and validation activities to ensure the secure development environment requirements are met and the developer has removed hidden functions or code that may have been used in development or unit testing and is not required to meet the system design requirements.

Vulnerability assessments is performed on software and complex programmable logic that is developed and classified as SIL 4. The vulnerability assessments evaluate that the design configuration items of the secure development environment are reviewed to ensure they are correctly translated from the system design specification and are correct, accurate, and complete. Details of the Secure Development Environment are described in Section 7.2.9.1.

In cases where previously developed software or commercial off-the-shelf software is used, the Digital Safety Systems SDOE and Digital I&C Software Development Plans contain requirements during the implementation phase of software development for evaluating and assessing that both developed code and previously developed or commercial off-the-shelf software meets the specified design requirements for system reliability and secure development and operational environment.

For commercial off-the-shelf software, previously developed software or complex programmable logic classified as SIL 4, the Digital I&C Quality Assurance Plan requires an evaluation of vendors and suppliers of digital I&C systems to verify that the software or complex programmable logic adheres to the SDOE design requirements and does not adversely affect system reliability.

The Digital I&C Software Quality Assurance Plan and the Digital I&C Software Verification and Validation Plan govern the use of support software and tools (e.g., software and hardware description language code generating tools, software compilers, software assemblers, software operating systems, software or logic coverage analyzers). The Digital I&C Software Configuration Management Plan governs the process for controlling code change requests and modifications.

The completed Software Design Description is used as input to the ongoing software safety analysis activity for SIL 3 and 4 software or complex logic.

For SIL 4 software, an independent V&V team performs a V&V of the Digital I&C Software Design Description. For SIL 1, 2, and 3 software, an independent verifier performs this function. Anomalies identified during the V&V process are documented in a V&V anomaly report and reported to the software development team. Anomalies must be satisfactorily resolved before issuing a V&V task report.

The Software Design Description is baselined, updated as necessary, and placed under configuration management.

7.2.1.2.7 Software Implementation

The Digital I&C Software Integration Plan governs both software implementation and integration tasks performed during the software development life cycle. The detailed design within the Software Design Description is translated into computer code in the selected programming language, whether a standard software language for typical source code or hardware description language for a complex logic device. The code capability of executing the safety design features and methods developed during the software design process is confirmed and is documented within the Software Design Description and Software Safety Analysis Report.

The code is confirmed using the coding rules, methods, standards, and other applicable criteria of the Software Coding and Hardware Description

Language Coding Guidelines may be provided by the vendor. Alternatively, a Software Coding Conventions and Guidelines Document developed specifically for the product being coded may be used so long as the following top level attributes of software safety are satisfied for SIL 3 and 4 software or complex logic:

- reliability
- robustness
- traceability
- maintainability

The software code or complex logic is designed to facilitate analysis, testing and readability.

For SIL 4 software, an independent V&V team performs a V&V of the software or complex logic. For SIL 1, 2, and 3 software, an independent verifier performs this function. Anomalies identified during the V&V process are documented in a V&V anomaly report and reported to the software development team. Anomalies must be satisfactorily resolved prior to issuing a V&V task report.

The software or complex logic is baselined, updated as necessary, and placed under configuration management.

The Digital I&C Software Master Test Plan governs the generation of the following test documents in the implementation phase of the software life cycle:

- component test case
- integration test case
- system test case
- factory acceptance test and SAT cases
- component test procedure
- integration test procedure
- system test procedure
- component test report

An independent V&V test engineer performs component level testing for SIL 4 software or complex logic. A test engineer from the engineering or V&V team performs the testing for the SIL 1, 2, and 3 software or complex Logic.

Complex logic component testing includes but is not limited to the following:

- function simulation
- static analyses
- gate-level simulation

- timing simulation
- static timing analysis

Software component testing includes but is not limited to the following:

- white box testing
 - statement testing
 - path testing
 - branch testing
 - negative testing
 - failure testing
- black box testing
 - functional testing
 - interface testing
 - stress testing
 - regression testing
 - performance testing
 - negative testing
 - failure testing

The test documents are baselined, updated as necessary, and placed under configuration management.

7.2.1.2.8 Software Integration and Testing

The Digital I&C Software Master Test Plan governs the generation of the following test documents in the test phase of the Software Life Cycle:

- factory acceptance test and SAT procedures
- integration test report
- system test report
- factory acceptance test report

For SIL 4 software or complex logic, a test engineer from an independent V&V team:

- develops the test documentation listed above
- conducts software integration testing to verify that software requirements have been adequately implemented for this phase of the software life cycle
- compares integration test results to the requirements in the Digital I&C Software Requirements Specification and Interface Requirements Specification to ensure satisfaction of requirements.

- identifies and resolves discrepancies between actual and expected results in integration testing.
- ensures that the integrated software or complex logic modules have successfully passed integration testing and that the software system is integrated with applicable hardware systems.
- conducts system testing on a complete, integrated system to evaluate system performance based on the I&C system requirements from the System Requirements Specification and system design documentation.
- ensures the detection of inconsistencies between the software or complex logic and the hardware.
- documents system test results and analyzes test results to verify that digital I&C system requirements have been satisfied.
- demonstrates that hazards identified in the Software Safety Analysis Report have been eliminated or controlled to an acceptable level of risk and ensures that additional hazardous states identified during testing undergo analysis prior to software delivery or use
- evaluates and ensures the correction of test discrepancies identified and makes provisions available for appropriate regression testing following changes made to resolve discrepancies.
- provides the completed system test results in the System Test Report to the engineering team as an input to the ongoing digital I&C system safety analysis activity.

For SIL 4 software or complex logic, an independent engineer performs V&V of the test documents developed by the V&V team and documents the results on corresponding V&V task reports. For SIL 1, 2, and 3 software or complex logic, an independent verifier within the engineering or V&V team performs the V&V of the test documents developed by the test engineer from the engineering team and documents the results.

The test documents are baselined, updated as necessary, and placed under configuration management.

7.2.1.2.9 Instrumentation and Controls System Installation

A digital I&C system installation and site test plan is used that documents the methods by which the I&C safety system is installed and connected to other plant systems. The engineering team ensures that the system installation plan describes the following:

- procedures
 - software installation
 - combined hardware and software installation
 - systems installation

- confirmation measures
 - computer system is functional
 - sensors and actuators are functional and the required cards are present and installed in the correct slots (when applicable)
 - communication system is correctly installed
 - correct software versions (i.e., consistent with the versions used for final system testing) are installed on the correct digital I&C system

For SIL 4 software or complex logic, a team performs V&V of the installation package and documents the results on corresponding V&V task reports. For SIL 1, 2, and 3 software or complex logic, an independent verifier within the engineering or V&V team does the V&V and documents the results.

The installation package is baselined, updated as necessary, and placed under configuration management.

The completed system installation results are documented and used as input to the ongoing I&C system safety analysis activity.

The SAT demonstrates that the installed system performs in accordance with the system design basis. The Digital I&C Software Master Test Plan governs the generation of the Site Acceptance Test Report.

For SIL 4 software or complex logic, the independent V&V team works with the licensee to ensure that SAT demonstrates that the installed system performs the safety function described in the system design basis. For SIL 2 and 3 software or complex logic, an independent verifier from the engineering or V&V team works with the licensee to ensure that SAT demonstrates that the installed system performs the intended function described in the system design basis.

The SAT report is baselined, updated as necessary, and placed under configuration management. The final V&V report is prepared prior to turning the system over to the plant licensee.

7.2.1.2.10 Instrumentation and Controls System Operations

COL Item 7.2-1: An applicant that references the NuScale Power Plant US460 standard design will implement the life cycle processes for the operation phase for the instrumentation and controls systems, as defined in IEEE Std 1074-2006 and IEEE Std 1012-2004.

7.2.1.2.11 Instrumentation System Maintenance

COL Item 7.2-2: An applicant that references the NuScale Power Plant US460 standard design will implement the life cycle processes for the maintenance phase for the instrumentation and controls systems, as defined in IEEE Std 1074-2006 and IEEE Std 1012-2004.

7.2.1.2.12 Instrumentation System Retirement

COL Item 7.2-3: An applicant that references the NuScale Power Plant US460 standard design will implement the life cycle processes for the retirement phase for the instrumentation and controls systems, as defined in IEEE Std 1074-2006 and IEEE Std 1012-2004. The Digital I&C Software Configuration Management Plan provides guidance for the retirement and removal of a software product from use.

7.2.1.3 Project Management and Organizational Processes

The digital I&C safety system development life cycle is implemented using the following key documents:

- Digital Safety Systems Project Plan
- Digital Safety Systems Safety Plan
- Digital I&C Software Management Plan
- Digital I&C Software Development Plan
- Digital I&C Software Quality Assurance Plan
- Digital I&C Software Verification and Validation Plan
- Digital I&C Software Master Test Plan
- Digital I&C Software Configuration Management Plan
- Digital I&C Software Requirements Management Plan
- Digital I&C Software Integration Plan
- Digital I&C Software Installation Plan
- Digital I&C Software Training Plan

These documents define the key development activities and sequences, management responsibilities, and necessary support activities.

The Digital I&C Software Management Plan, in conjunction with the overall Project Management Plan provides the framework for development of the project schedule, including major milestones and baseline reviews at each phase of the software life cycle, work products and project deliverables at each phase of the software life cycle. The Digital I&C Software Quality Assurance Plan and Software Management Plan address the aspects of risk management and development tools.

The Digital I&C Software Management Plan implements the requirements for overall management of the I&C system design and development project life cycle. The major project functions in the Software Management Plan include:

- Overall I&C project management
- Development of the Digital I&C software planning documents

- Development of System and Software Requirements Specifications and Design
- Descriptions by the design engineering team
- Performance of hazard analysis and SDOE vulnerability assessments by the Independent V&V and design engineering teams, respectively
- Coordination of risk analysis by the independent IV&V engineer with generation or update of the project risk register by the project manager
- Development of software and complex logic by the design engineering team
- Development of test documentation and performance of testing by independent V&V test engineers for SIL 4 software and complex logic.
- Management of the configuration of software and complex logic device logic and its documentation by Configuration Management
- Independent Verification and Validation of configuration of SIL 4 software and complex logic device logic Quality reviews and audits by the Quality Assurance organization

The Digital I&C Software Verification and Validation Plan addresses the aspects of quality metrics. RG 1.28, RG 1.152, and IEEE Std 7-4.3.2-2003 contain additional details regarding risk management, quality metrics, and the control of software tools (Section 7.2.1).

7.2.1.4 Software Quality Assurance Processes

RG 1.28, RG 1.152 and IEEE Std 7-4.3.2-2003 discuss software QA (Section 7.2.1).

7.2.1.5 Software Verification and Validation Processes

RG 1.152, and IEEE Std 7-4.3.2-2003 discuss software V&V (Section 7.2.1).

RG 1.168, IEEE Std 1012-2004, and IEEE Std 1028-2008 discuss software audits (Section 7.2.1).

7.2.1.6 Software Configuration Management Processes

RG 1.152, and IEEE Std 7-4.3.2-2003 in Section 7.2.1, as well as the discussion of RG 1.169, and IEEE Std 828-2005 discuss software configuration management process (Section 7.2.1).

7.2.2 Equipment Qualification

The I&C structures, systems, and components are designed to perform their safety-related functional requirements over the range of environmental conditions postulated for the area that the components are located and during the time period when this performance is required.

The I&C systems equipment qualification meets the criteria contained in Section 5.4 of IEEE Std 7-4.3.2-2003, and the requirements of Section 5.4 of IEEE Std 603-1991. The equipment qualification meets the guidance contained in RG 1.209 and RG 1.151.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI numbers 17, 18, and 23.

7.2.2.1 Instrumentation and Controls Qualification

Module Protection System and Neutron Monitoring System-Excore Equipment Operating Environment

Module protection system and neutron monitoring system (NMS)-excore rack-mounted equipment is installed in a mild environment and is designed to meet the environmental conditions described in Section 3.11 and Appendix 3C. The MPS and NMS rack-mounted equipment do not require environmental controls to perform their safety functions. The NMS-excore detectors are located in support mechanisms submerged in the reactor pool next to the NuScale Power Module (NPM), which is a harsh environment. The I&C equipment rooms where MPS and NMS cabinets are located provide an environment that would at no time be more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences.

The MPS and NMS-excore components are environmentally qualified in accordance with IEEE Std 323-2003, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations," (Reference 7.2-6) as endorsed by RG 1.209 for mild environments as described in Section 3.11 and in accordance with IEEE Std 323-1974 "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations," (Reference 7.2-7) as endorsed by RG 1.89 for harsh environments.

Protection from natural phenomena for the MPS and NMS-excore processing electronics is provided by the location of the MPS and NMS-excore cabinets in the reactor building (Section 1.2). This location is remote from the NMS-excore detectors and in a mild environment which provides protection for the processing electronics portion of the NMS-excore instrumentation.

MPS separation groups A, C, and Division I of the reactor trip system (RTS), engineered safety features actuation system (ESFAS), and separation groups A and C NMS-excore signal processing equipment are in one room; and MPS separation groups B, D, and Division II of the RTS, ESFAS, and separation groups B and D NMS-excore equipment are located in a different room.

The Reactor Building and Control Building arrangement and design enable systems and components required for safe plant operation and shutdown to withstand or to be protected from the effects of sabotage, environmental conditions, natural phenomena, postulated design basis accidents, and

design-basis threats. Chapter 3 provides details on the design of the reactor and control buildings.

The MPS is an FPGA-based system, which does not use software in a traditional manner; therefore, there is no software which executes while the system is in operation. However, FPGAs are programmed, and qualification testing is performed in accordance with IEEE Std 7-4.3.2-2003 (Section 7.2.1).

The NMS-excore contains sensors and analog signal processing equipment and is not a digital computer system; therefore, the requirements of IEEE Std 7-4.3.2-2003 do not apply.

Fire Protection Considerations

The MPS equipment and cabling are designed in accordance with the NuScale fire protection design criteria described in Section 9.5.1. MPS separation groups A, C, and Division I of the RTS and ESFAS and separation groups A and C NMS-excore signal processing equipment are located in one room; and separation groups B, D, and Division II of the RTS, ESFAS, and separation groups B and D NMS-excore equipment are located in a different room; the rooms are located in two different fire zones. Module protection system and NMS-excore cables are required to pass the flame test as required in IEEE Std 1202-2006 (Reference 7.2-26) as endorsed by RG 1.189.

The MPS equipment and cable routing is designed to meet the separation requirements of IEEE Std 384-1992 "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," (Reference 7.2-9) as endorsed by RG 1.75. These design attributes also provide separate rooms and cable runs to prevent a fire or explosion from affecting more than one division of MPS and NMS-excore equipment (Section 9.5.1.2).

To reduce the MPS and NMS-excore susceptibility to smoke exposure as discussed in RG 1.209, fire protection methods are employed such as isolation and detection practices and minimization of combustible materials in the I&C equipment rooms and MPS cabinets. Section 9.5.1 provides more detail on the fire protection methods employed in the NuScale Power Plant (NPP) design. The MPS and NMS-excore equipment do not use chassis fans, which can distribute smoke, soot, and dust on the electronic circuitry and can cause degradation of the equipment. There is no forced cooling of internal MPS or NMS-excore hardware equipment.

The MPS manual trip/actuate, operating bypass, and enable nonsafety control switches are located in the main control room (MCR).

The reactor trip breakers (RTBs) and the pressurizer heater breakers are located in the associated MPS division room.

In the event of a fire in the MCR, the operators trip the reactors, initiate decay heat removal and initiate containment isolation prior to evacuating the MCR. These actions result in passive cooling that achieves and maintains the modules in a

safe shutdown condition. Operators can also place the reactors in safe shutdown from outside the MCR in the I&C equipment rooms within the reactor building. Following shutdown and initiation of passive cooling, the design does not rely on operator action, instrumentation, or controls outside of the MCR to maintain a safe stable shutdown condition. There are two MCR isolation switches for each NPM located outside the control room that when repositioned isolate the MPS manual actuation switches, override switches and enable nonsafety control switches for each NPMs module protection system in the MCR to prevent spurious actuation of equipment due to fire damage.

Module Protection System and Neutron Monitoring System Equipment Electromagnetic Interference and Radio Frequency Interference Qualification

The MPS and NMS-excore equipment is designed and qualified in accordance with the guidance provided in RG 1.180 for compliance with NRC regulations regarding electromagnetic interference and radio frequency interference and power surges on safety-related I&C systems. Regulatory Guide 1.180 provides several acceptable methods for addressing electromagnetic compatibility consideration for qualifying safety-related I&C systems for the expected electromagnetic environment in nuclear power plants. The electromagnetic interference and radio frequency interference, surge withstand capabilities, and operating envelopes are elements of the total package that is needed to ensure electromagnetic compatibility within an NPP.

For compliance to RG 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants," NuScale applies the guidance for electromagnetic interference and radio frequency interference protection from IEEE Std 1050-1996 "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations," (Reference 7.2-20) to the design of I&C systems. IEEE Std 665-1995, "IEEE Guide for Generating Station Grounding," (Reference 7.2-11) and IEEE Std C62.23-1995 "IEEE Application Guide for Surge Protection of Electric Generating Plants," (Reference 7.2-5) provide guidance and do not contain specific mandatory design requirements.

7.2.3 Reliability, Integrity, and Completion of Protective Action

This section discusses the reliability and integrity of the I&C systems, and the ability to complete a protective action once initiated to accomplish the safety functions. The design of the I&C systems meets the reliability, system integrity, and completion of protective action criteria contained in Sections 5.5 and 5.15 of IEEE Std 7-4.3.2-2003, and the requirements of Sections 5.2, 5.5, 5.15 and 7.3 of IEEE Std 603-1991.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI numbers 15, 18, 19, and 37.

7.2.3.1 Reliability Characteristics

The majority of the MPS hardware is developed and constructed using FPGA logic that does not require the use of a central processing unit or an operating

system as found in most other digital instrumentation. The remaining hardware for the MPS is developed and constructed using discrete logic or analog components. The FPGA logic elements are arranged in an array of open connections that can be compared to a series of similar but unconnected discrete logic elements on a breadboard, where the functionality of the overall circuit is undetermined until the connections are made. The FPGA also contains a series of reconfigurable interconnects that allow the logic elements to be “wired together.”

The Software QAP described in Section 7.2.1 establishes the QA requirements applied to development of the hardware description language that is used to configure and implement the FPGA logic within the MPS. Because of the potential for programming errors for both hardware description language programming and traditional programming, a well-defined, high-quality design process, and the rigorous V&V effort described in Section 7.2.1 provide reasonable assurance that the resulting system performs the associated safety function in a predictable and reliable manner.

Qualitative reliability goals have been established for the MPS to meet the single failure criterion. The MPS meets the qualitative reliability goals and the requirements of IEEE Std 379-2000 "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," (Reference 7.2-8) to satisfy the single failure criterion through the addition of redundancy (Section 7.1.3), diversity (Section 7.1.5) and testability (Section 7.2.15). The MPS remains functional in the presence of a single failure. An MPS hazard analysis is performed using the methodology described in Section 7.1.8 to evaluate potential hazards from connected systems and establish safety constraints to meet the qualitative reliability goals established for the system. There are no failure modes that are undetectable or prevent the MPS from performing its RTS, ESFAS, and post-accident monitoring (PAM) functions.

The NMS is an analog system, there is no software used. Qualitative reliability goals have been established for the NMS to meet the single failure criterion. The NMS meets the qualitative reliability goals and the requirements of IEEE Std 379-2000 to satisfy the single failure criterion and the NMS remains functional in the presence of a single failure. The NMS hazard analysis (Section 7.1.8) is also performed to evaluate potential hazards from connected systems and establish safety constraints to meet the qualitative reliability goals established for the system. Failures resulting in a loss of neutron flux information can be identified through anomalous indication, alarms in the MCR, or periodic testing. There are no failure modes in the NMS that are undetectable or prevent the NMS from performing its required safety functions.

7.2.3.2 System Integrity Characteristics

The MPS maintains the capability to initiate protective functions during and following anticipated operational occurrences (AOOs), postulated accidents, and design-basis events (DBEs) resulting from natural external phenomena such as earthquakes, tornadoes, hurricanes, floods and winds. The functional capability of the system is maintained during internal events such as fires, flooding, explosions, missiles, electrical faults, and pipe whip. The equipment is environmentally and

seismically qualified in accordance with RG1.209 and IEEE Std 323-1974 as described in Section 7.2.2.

Rack-mounted MPS and NMS equipment is located in an environmentally controlled area. However, the MPS and NMS rack-mounted equipment do not require environmental controls to perform their safety functions and are designed to accommodate abnormal conditions due to the loss of normal heating, ventilation, and air conditioning (HVAC) in the area for a minimum of 72 hours, coincident with AOOs and postulated accidents. The MPS equipment is designed to meet the normal and abnormal environmental conditions as described in Section 3.11 and Appendix 3C.

The design of the MPS is based on FPGA technology. The MPS platform is designed with redundancy and embedded self-test capability to ensure system integrity by detecting and alarming faults in the MCR. Diagnostics and testing capabilities are designed into the MPS platform to ensure there is a systematic approach to maintaining and testing the system (Section 7.2.15).

The MPS platform implements advanced failure detection and mitigation to ensure system or component failures do not remain undetected. The operation of the system is deterministic in nature and allows the system to monitor in order to validate functional performance. The MPS is designed such that it can be tested and calibrated while retaining the capability to accomplish the required safety functions. Testing from the sensor inputs to the MPS through the actuated equipment is accomplished through a series of overlapping sequential tests with the majority of the tests capable of being performed with the plant at full power. Where testing final equipment at power has the potential to upset plant operation or damage equipment, provisions are made to test the equipment at reduced power or when the reactor is shut down. Periodic surveillance testing capability is incorporated to ensure that functional tests and checks, calibration verification, and time response measurements are validated. Periodic surveillance testing of sensors that are part of the MPS is performed in accord with the plant technical specifications.

Diagnostics data for the separation group and division of the MPS are provided to the maintenance workstation (MWS). There is an MWS in each I&C equipment room that supports the MPS separation groups and division in that room. The interface between the MPS and the MWS is an optically isolated, one-way diagnostic interface connected to the calibration and test bus that is used to update tunable parameters. The calibration and test bus is configured as a one-way, receive-only interface. Diagnostics data are communicated through the monitoring and indication bus (MIB), which is a physically separate, isolated communications path from the safety data communication paths associated with the MPS safety functions (e.g., the safety data bus), thereby ensuring the diagnostics functionality is independent of the safety functionality. The diagnostic data comes across the MIB communications module through a one-way transmit-only connection through the MPS gateway to the MWS.

The MPS is designed such that in the event of a condition such as a system disconnection or loss of power, it fails into a safe state. The EIM outputs are

designed to remove power to the final actuation devices causing them to go to a safe-state (e.g., RTBs open, emergency core cooling system (ECCS) valves open) to ensure that a loss of power or other detected fault that causes the EIM to go into a faulted state also causes the interface to remove power to the final actuated device.

The NMS operates throughout normal reactor operation and provides PAM data to the MPS during and after a DBE. Failures of the NMS equipment are identified through system health monitoring of the NMS detectors and signal processing equipment. Periodic surveillance testing is performed on the NMS in accordance with the plant technical specifications. Failure of NMS-excore components generate a fault signal and an actuate/trip signal for that particular NMS-excore channel. The fault signal is transmitted to the MPS for display to the control room operators.

The NMS incorporates four redundant sets of detectors that are completely independent so that a failure in one redundant channel does not affect the other three.

7.2.3.3 Completion of Protective Action

The MPS is designed such that once a protective action is initiated, either automatically or manually, the sequence of protective actions continues until it has reached completion.

Seal-in of ESFAS actuation logic is provided at the EIM to account for transient process conditions that may change during a DBE (e.g., containment pressure). This seal-in prevents logic and final actuated devices from returning to the non-trip or non-actuated state due to changing process conditions. Seal-in is also provided at the EIM for the RTS actuation logic functions. The reactor trip function is inherently latched by removing electrical power from the control rod drive mechanisms causing the control rods to fall into the reactor core by gravity.

After the initiation of a protective action that requires components to go to an actuated position or safe-state, the MPS continues to hold the requested state after the initiating signal goes away. The EIM in the MPS functions as a state machine in that it accepts a request for a particular position of a final actuation device and retains that position until a new position has been requested.

Deliberate operator action is required to change the state of actuated equipment and return the MPS to a normal configuration. The operator uses the enable nonsafety control switch and the MCS to place components in their normal configuration. The actuation and priority logic (APL) circuit controls the manual control of components using the MCS as described below.

The APL circuit is designed to give priority to safety-related RTS and ESF signals over nonsafety-related signals in all modes of operation. The APL circuit does not contain digital technology; it is constructed of discrete logic components and functions separately from the FPGA logic within the EIM.

The APL circuit accepts inputs from three sources:

- 1) Automatic reactor trip or ESF actuation signals from its own safety division.
- 2) Manual reactor trip or ESF actuation signals from its own divisional manual actuation switches in the MCR.
- 3) Enable nonsafety control switch and nonsafety-related control input signals from the module control system. If the enable nonsafety control switch is not active (i.e., nonsafety-related inputs are disabled), the nonsafety-related control signal is ignored.

The actuation priority logic evaluates these signals, and generates and provides output signals to the EIM to actuate or trip the final actuation devices based on the logic described in this section.

The highest priority is given to the automatic and manual RTS and ESFAS actuation signals. As shown in Figure 7.1-1k through Figure 7.1-1ak, these actuation signals have equal, highest priority; they are differentiated by the sequence by which they are received by the APL circuit, such that the first active signal received is used to generate the output.

If an automatic or manual RTS or ESF actuation signal is active, these signals have the highest logic priority; the RTS and ESF signals are processed and an actuation command is sent directly to the EIM output to actuate or trip the final actuation device. The position of the enable nonsafety control switch does not matter. The enable nonsafety control switch does not impede the handling and evaluation of active automatic or manual RTS or ESF actuation signals as these are processed at the highest logic priority.

If the nonsafety control inputs are disabled by the enable nonsafety control switch, then nonsafety control inputs are rejected and not processed by the APL circuit.

For cases when the enable nonsafety control switch is enabled to allow nonsafety control inputs, there must be no active RTS or ESF manual or automatic signal present. If the enable nonsafety control switch is enabled, and there is no RTS or ESF signal, then the nonsafety manual control inputs from the MCS are used by the APL circuit to control the final component (e.g., containment isolation valve).

During the time the nonsafety control inputs are enabled, if an automatic or manual RTS or ESF signal is generated and received by the APL circuit, the actuation priority logic immediately disables the enable nonsafety control logic input and rejects nonsafety control inputs. The actuation priority logic circuit processes the RTS or ESF command to position the final actuation device to its safe state.

Re-initiation of manual controls from nonsafety equipment is possible only if the protective action has gone to completion and the operator deliberately blocks the safety signal using the override function via the manual override switches provided or the initiating signal is no longer present. The enable nonsafety control

switch is a momentary contact switch; therefore, the operator must deliberately manipulate the enable nonsafety control switch to re-enable nonsafety control inputs.

The actuation priority logic is based on discrete logic that allows for testing of possible combinations of inputs and the evaluation of the associated outputs.

7.2.4 Operating and Maintenance Bypasses

An operating bypass is provided for certain protective actions when they are not necessary in a particular mode of plant operation. Different modes of plant operation may necessitate an automatic or manual bypass of a safety function. Operating bypasses are used to permit mode changes. A maintenance bypass is provided to bypass safety system equipment during maintenance, testing, or repair. A maintenance bypass may reduce the degree of redundancy of equipment, but it does not result in the loss of a safety function. Operating and maintenance bypasses are described in the following sections.

The MPS operating and maintenance bypasses conforms to Sections 5.8, 6.6, 6.7, 7.4 and 7.5 of IEEE Std 603-1991 and the guidance contained in RG 1.47. The display of bypassed and inoperable status information is described in Section 7.2.13, which conforms to 10 CFR 50.34(f)(2)(v).

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI numbers 7, 42, 43, and 45.

7.2.4.1 Operating Bypasses

The MPS includes interlocks, permissives, and operational and maintenance bypasses that prohibit or permit certain protective actions either automatically or through a combination of automatic and manual actions to allow plant mode changes.

The MPS logic automatically prevents the activation of an operating bypass or initiates the appropriate safety function(s) when permissive or interlock conditions for the operating bypass are not met. The operating bypass circuits contain both permissive features that allow a protective function to be bypassed when the function is not required and interlock features that automatically activate an operating bypass when conditions are met. When permissive and interlock conditions are no longer met, operating bypasses are automatically deactivated.

Operating bypasses are required to allow changing plant modes and provide operator control of certain functions based on safety analysis or plant operations. The operating bypasses for MPS functions, interlocks, and permissives are shown in Table 7.1-5. These bypasses block certain protective actions that otherwise prevent mode changes during plant operation (e.g., plant start-up). The operating bypasses are automatically removed when the plant moves to an operating condition where the protective action is required to be operable. Indication is provided in the control room if some part of the system has been bypassed or

taken out of service. The operating bypasses are also shown on the MPS functional logic diagrams in Figure 7.1-1b through Figure 7.1-1i.

Manual operating bypasses have two switches, one per division. The only manual operating bypasses used for the design use a permissive in conjunction with the manual bypass in order to achieve the function of the bypass.

The postulated failures of the operating bypass switches are evaluated, as described in Section 7.1.3. The operating bypass switches are momentary-contact switches and normally are open, and only closed momentarily to enact an operating bypass function.

In the identified events evaluated, the failures are limited to one of two MPS divisions. The other MPS division is fully operable and capable of performing the safety function and no single failure disables a safety function. Inadvertent bypasses of a safety function are limited to one MPS division. The other MPS division is able to perform the required safety function.

For automatic and manual operating bypasses, a trip determination is used for the permissive or interlock from the separation group and is similar to the trip determination for a protective action. A three-out-of-four coincidence is used to determine when an operating bypass is warranted. To remove the operating bypass, two-out-of-four of the separation groups are needed to determine that the permissive or interlock is no longer valid and the operating bypass is automatically reset.

Information on displaying system bypass status information is provided in Section 7.2.13.

7.2.4.2 Maintenance Bypass

Module protection system variables are monitored by four redundant channels that actuate the protective functions, using two-out-of-four coincident logic. This configuration allows required safety functions to remain operable in the event of a single random failure of a protection channel concurrent with a channel in maintenance bypass.

The MPS is designed to permit the administrative bypass of a protection channel for maintenance, test, or repair. Indication is provided in the control room if an MPS channel has been administratively bypassed or taken out of service. The time period allowed for removal from service in maintenance bypass is administratively controlled by the plant technical specifications.

To perform maintenance on the MPS, there are two associated switches: a trip/bypass switch associated with each safety function module (SFM) that performs a safety function and an out of service switch on the front of the SFM to allow removal of the SFM from service for maintenance and repair. With the out of service switch activated, the safety function is placed in trip or bypass based on the position of the trip/bypass switch for that SFM. Activating the out of service switch permits modification of the tunable parameters and setpoints in nonvolatile

memory via the MWS. The trip bypass switch status input is received through the hard-wired module (HWM) that converts the switch position into a logic level signal and places this information onto the backplane.

The data packet received from the SFM contains the position of the out of service switch on the SFM. The scheduling and bypass module (SBM) determines if the SFM is out of service from the out of service switch position information received in the data packet from the SFM. If the SFM is out of service and the trip/bypass switch is in bypass, the SBM transmits a non-actuate or no-trip condition to the schedule and voting module (SVM) regardless of the output of the SFM. There is no change to the 2-out-of-4 voting coincidence logic; with one separation group providing a no trip to the SVM, requiring two of the remaining three channels received by the SVM to vote to trip/actuate. In this case, the MPS is still capable of performing the safety function with the required level of redundancy and continues to meet the single failure criteria.

If the SFM is out of service and the trip/bypass switch is in trip, the SBM transmits a trip/actuate signal to the SVM regardless of the output of the SFM. There is no change to the 2-out-of-4 voting coincidence logic. The SBM forces one channel to trip/actuate; with one separation group providing a trip/actuate input to the SVM, requiring one other separation group to issue a vote to trip/actuate to cause a trip/actuate to occur for the particular safety function. In this case, the MPS is in a "partial trip" condition, but still meets the single failure criteria and is capable of performing the safety function with the required level of redundancy.

The maintenance trip/bypass switches are located on a panel in the separation group cabinets located in the I&C equipment rooms. The switches are connected to the HWM in the SFM chassis (Figure 7.0-4).

If the SFM is not out of service, the SBM transmits the safety function algorithm result is calculated and transmitted from the SFM to the SBM.

If the SBM does not receive a valid response from the SFM, an alarm is generated and the SBM uses the position of the trip/bypass switch to determine what to transmit to the SVM.

Using the out of service function of the SFM allows for periodic parameter updates of certain tunable parameters during an outage and during the fuel cycle. Periodic testing is required to verify operability of the safety function.

The MPS is designed to allow periodic and corrective maintenance during normal operation and during outages. For maintenance to be performed, the safety function must be removed from service. The affected channel is placed in a trip condition or bypass subject to technical specification limitations.

Safety functions within a separation group can be taken to bypass or trip for testing or corrective maintenance. The RTS and ESFAS divisions do not have bypass functionality; however the modules have continuous self-testing coverage. The RTBs can be tested at power because of the breaker configuration by opening one breaker at a time. RTB configuration allows for RTB testing without

the need for a maintenance bypass associated with the RTBs. Most of the ESFAS components are not tested at power because they cause a trip or engineered safety feature (ESF) actuation and need to be tested during an outage. The manual trip and actuate switches in the MCR cannot be tested at power and are tested during shutdown conditions in accordance with plant technical specifications.

Four RTBs are associated with each of two divisions of the MPS. The MPS divisions are configured so that opening a single division of breakers de-energizes the control rod drive mechanisms, thus causing the reactor trip (Figure 7.0-6). During testing of the trip actuation logic, the trip signals to the undervoltage trip mechanism of the RTBs are not actuated. The MPS is designed to permit overlapping online testing of MPS logic and RTBs.

The part of MPS that is not tested at power is the actuation priority logic circuit on the EIM, the manual MCR switches and the enable nonsafety control switch that provide inputs to the actuation priority logic. The actuation priority logic consists of discrete components and directly causes actuation of field components that cause the reactor to shutdown or adversely affect operation. The actuation priority logic is tested when the reactor is shut down. Because of the simplicity of the actuation priority logic circuit, testing during shutdown conditions is sufficient to ensure the actuation priority logic function performs as required.

For maintenance bypass purposes, the NMS is treated as a sensor input into the MPS where the MPS provides the bypass capability for maintenance purposes.

Indication is provided in the control room if an MPS channel has been administratively bypassed or taken out-of-service. The time period allowed for removal from service in maintenance bypass is administratively controlled by the technical specifications.

The MPS conforms to the guidance in RG 1.47. The MPS equipment status information is automatically sent to the MCS and SDIS. The display of the status information allows the operator to identify the operability of the safety functions. The capability to manually activate the bypass indication in the control room is provided by the MCS.

Information on displaying system bypass status information is provided in Section 7.2.13.

7.2.5 Interlocks

Interlocks ensure the reactor trip and ESF actuations are in the correct configuration for the current plant status. They ensure protection system functions are available and operational during plant conditions under which the interlocks are assumed to function in the plant safety analyses.

The design of MPS interlocks conforms to the requirements of IEEE Std 603-1991. Computer-based interlocks conform to IEEE Std 7-4.3.2-2003.

7.2.5.1 Instrumentation and Controls System Interlocks

The I&C interlocks performed within the MPS are summarized in Table 7.1-5.

The MPS interlocks and operating bypasses are implemented within the individual divisions, which ensures that the applicable requirements of IEEE Std 603-1991 for redundancy, independence, satisfaction of the single failure criterion, qualification, bypasses, status indication, and testing are met.

Neutron monitoring system sensors and signal processing equipment are used to provide signal inputs for reactor trip functions and MPS interlocks. The NMS equipment used to provide the MPS functions meet the NMS single failure requirements.

The MPS interlocks are compatible with the functions and performance assumed in the events analyzed in Chapter 15.

7.2.5.2 Mechanical System Interlocks

The ECCS reactor recirculation valves (RRV) contain an inadvertent actuation block feature that minimizes the probability of a spurious opening of an RRV at operating pressure (Section 6.3). In the event of an inadvertent signal from MPS to actuate the RRVs at nominal plant pressure, the valves do not open until a low differential pressure between the reactor pressure vessel (RPV) and the containment vessel (CNV) is reached allowing the operator to respond to the inadvertent signal without the opening of the RRVs and the resulting plant transient.

Plant conditions during a valid ECCS actuation per the nominal trip setpoint should allow the RRVs to open when the inadvertent actuation block interlock is satisfied. If plant conditions do not allow the inadvertent actuation block interlock to be satisfied, the completion of the ECCS protective action does not occur until the inadvertent actuation block allows the RRVs to open and the open valve position signal is received by the MPS. There are no other safety-related mechanical system interlocks.

7.2.6 Derivation of System Inputs

This section describes the derivation of system inputs to the MPS used for the safety-related protective functions performed by the MPS. The MPS and NMS sensor and process measurement design conforms to the requirements of Section 6.4 of IEEE Std 603-1991.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI number 41.

The process variables associated with MPS safety-related functions are listed in Table 7.1-3 and Table 7.1-4. These process variables are used by the redundant sense and command features of MPS to generate required protective actions. These

variables are monitored by variables identified in Table 7.1-2. The instrument range that accounts for normal, abnormal, and accident conditions is also specified for each variable. MPS variables used for safety-related functions are normally derived from process signals that are direct measurements of the process variables credited in the plant safety analysis (Chapter 15). Some variables such as steam superheat are calculated. Use of steam pressure and temperature is the only practical and feasible approach to obtaining the steam superheat variable credited in the plant safety analysis. Additional sensor measurement details for variables associated with the nuclear steam supply system (NSSS) are provided in Section 7.2.16.

The safety-related NMS sense and command features provide input to the MPS. The four redundant inputs to the MPS are direct measurements of the variables credited in the plant safety analysis. The ranges that account for normal, abnormal, and accident conditions for these variables are also provided in Table 7.1-2.

7.2.7 Setpoints

This section describes the determination and establishment of safety-related instrument setpoints for the protective functions performed by the MPS. The design of the MPS with respect to instrumentation setpoints conforms to the requirements of Section 6.8.1 of IEEE Std 603-1991. When there are multiple setpoints established for a protective function, operating bypasses are provided that are either automatically activated or require the operator to manually activate the bypass of a particular setpoint when the permissive conditions are satisfied. When the operating bypass condition is no longer satisfied, both the automatic and manual operating bypasses are automatically removed, and the more restrictive setpoint is automatically enabled. These are positive means to ensure the more restrictive setpoint is used when required and conform to IEEE Std 603-1991 Section 6.8.2. The operating bypasses are described in Section 7.2.4.1 and Table 7.1-5.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI number 44.

NuScale Power, LLC, technical report “NuScale Instrument Setpoint Methodology Technical Report” (Reference 7.2-25) describes the instrument setpoint determination methodology applied to the safety-related I&C functions. This methodology establishes performance and test acceptance criteria to evaluate setpoints during surveillance testing and calibration for setpoint drift. The analytical limits, uncertainties, and setpoints for the RTS and ESFAS functions are summarized in Reference 7.2-25.

The methodology described is established to ensure that the RTS and ESFAS setpoints are consistent with the assumptions made in the plant safety analysis and conform to the setpoint-related requirements of industry standard ISA-67.04.01-2018, “Setpoints for Nuclear Safety-Related Instrumentation,” (Reference 7.2-22) as endorsed by RG 1.105.

Setpoints for the RTS and ESFAS are selected to provide sufficient allowance between the trip setpoint and the analytical limit to account for instrument channel

uncertainties. The instrument setpoint methodology determines calibration uncertainty allowances, including as-found and as-left tolerances, that are used in plant surveillance tests to verify that setpoints for safety-related protective functions are within technical specification limits. The methodology also establishes acceptance criteria to evaluate setpoints during surveillance testing and calibration for setpoint drift.

The methodology includes uncertainty and calculated setpoints based on assumptions for instrument uncertainties. This methodology only applies to safety-related instrumentation used for RTS and ESFAS functions and does not include provisions for using a graded approach for nonsafety-related or less important instrumentation.

7.2.8 Auxiliary Features

This section describes the auxiliary features associated with the safety-related I&C systems described in Section 7.0 and Section 7.1. These features meet the requirements of IEEE Std 603-1991, Section 5.12.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI numbers 34, 47, and 49.

7.2.8.1 Auxiliary Supporting Features

There are no auxiliary supporting features that are part of the safety-related MPS or the NMS. The MPS and NMS are designed to not rely on auxiliary supporting features such as electrical power or environmental controls to perform their safety functions; therefore, IEEE Std 603-1991 sub-clause 5.12.1 does not apply to the design of the MPS and the NMS.

7.2.8.2 Other Auxiliary Features

Other auxiliary features of the MPS that are part of the MPS by association (i.e., not isolated from the MPS) but are not required for the MPS to perform its safety functions include the following:

- 1) Continuous online self-testing and diagnostics. The continuous online self-testing and diagnostic functions are described in Section 7.2.15. These functions are designed and qualified as part of the MPS as described in TR-1015-18653-P-A (Reference 7.2-24) such that the self-testing and diagnostics functions do not adversely affect the MPS from performing its safety functions.
- 2) Communication from safety-related portions of the MPS to nonsafety-related components. Communication interfaces from safety-related SFMs, SBMs, SVMs, or EIMs to the MIB communications module are provided in order to transmit data to nonsafety-related systems and nonsafety-related displays. Communication interfaces on safety-related SFMs, SBMs, SVMs, and EIMs are designed and qualified as part of the MPS such that the communications

do not adversely affect the MPS from performing its safety functions as described in Section 7.1.2.

- 3) Capability for control of safety-related components by using nonsafety-related module control system through the actuation priority logic function within the EIM. These features are designed to not adversely affect the MPS as described in Section 7.1.2 and Section 7.2.3.
- 4) Isolation devices and circuitry. Electrical power for the MPS is supplied by the nonsafety-related augmented DC power system (EDAS) as described in Section 8.3 through a Class 1E isolation device that provides isolation between the Class 1E components within the MPS and non-Class 1E components as described in Section 7.1.2. The Class 1E isolation devices are designed and qualified to comply with IEEE Std 603-1991.
- 5) Shunt trip relay/coil circuitry in RTBs and pressurizer heater breakers. The shunt trip coil and relays of the RTBs and the pressurizer heater trip breakers do not affect the MPS in accomplishing its safety functions. Each breaker uses its own nonsafety-related shunt trip coil and relay as a backup to the safety-related undervoltage coil as described in Section 7.0.4.1. The shunt trip coil and relay are nonsafety-related diverse means for opening the reactor trip and pressurizer heater trip breakers and are not capable of closing these breakers once opened.
- 6) 24-Hour timers for PAM only mode. The 24-hour timers and associated components of the MPS are used to ensure a 72-hour EDAS-MS battery capacity by shedding loads on EDAS as described in Section 7.0.4.1.4. These components do not affect the ability of the MPS in accomplishing its safety functions. The 24-hour timers are normally de-energized and are energized by an MPS equipment interface module. On a loss of AC to both B and C 480 VAC buses, the MPS generates a reactor trip, actuates the decay heat removal system (DHRS), demineralized water supply isolation (DWSI), containment system isolation (CSI), Chemical and Volume Control System Isolation (CVCSI), Secondary System Isolation (SSI), trips the Pressurizer Heater Breakers, and de-energizes the MWS for both MPS divisions, thereby reducing loads, and starts the 24-hour timers using SVMs. If AC power is not restored within 24 hours, the 24-hour timers time out and de-energize the RTS chassis, ESFAS chassis and actuate ECCS reducing the loads on batteries for buses B and C. Failure of the 24-hour timers or failure to shed loads does not impact the MPS capability of initiating protective actions. Instead, these failures have the potential of impacting the nonsafety-related function of providing PAM information to the operator.

Other auxiliary features of the NMS-excore that are part of the NMS-excore by association (i.e., not isolated from the NMS-excore) but are not required for the NMS-excore to perform its safety functions include the electrical isolation devices and circuitry. Electrical power for the NMS-excore is supplied by the EDAS as described in Section 8.3 through a Class 1E isolation device that provides isolation between the Class 1E components within the NMS-excore and

non-Class 1E components as described in Section 7.1.2. The Class 1E isolation devices are designed and qualified to comply with IEEE Std 603-1991.

7.2.9 Control of Access, Identification, and Repair

The design of the MPS control of access, identification and repair features conforms to IEEE Std 603-1991, Sections 5.9, 5.10, and 5.11, IEEE Std 7-4.3.2-2003, Section 5.11, and conforms to the guidance contained in RG 1.75 and RG 1.152.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI numbers 11, 22, 31, 32, 33, 53, 54, and 58.

7.2.9.1 Control of Access

The Digital Safety System SDOE Plan establishes the approach for applying security-related regulatory guidance to the digital I&C system life cycle.

The SDOE plan applies to digital components, hardware or software, of a system or component that performs a safety-related function to ensure they are free from security vulnerabilities that could affect the reliability of the system.

A Secure Development Environment, as described in RG 1.152, is applied to the system development through the test phase. Secure operational environment design or cyber-security features intended to ensure reliable system operation and to help satisfy the licensee's cyber requirements is evaluated and implemented during the development of the system and verified not to adversely affect the reliability of the system.

The Secure Operational Environment and the Cyber Security requirements of 10 CFR 73.54 apply to the latter phases of the life cycle that occur at a licensee site (i.e. site installation, operation, maintenance, and retirement).

Regulatory Guide 1.152 provides guidance for an SDOE. The SDOE for the development of digital safety-related system software satisfies the requirements of 10 CFR 50.55a(h) and IEEE Std 603-1991, Sections 5.6 and 5.9.

The digital I&C system development process is outlined in the Digital Safety System Project Plan and the Digital I&C Software Quality Assurance Plan that provide detailed information on the life cycle processes (Section 7.2.1).

There are three distinct digital system life cycle development elements: basic design, detailed design, and system integration, installation and testing.

Regulatory Guide 1.173 endorses IEEE Std 1074-2006 with several clarifications. The security objectives for development of a system with high functional reliability commensurate with the safety functions performed include a secure software and system development environment, secure operational environment, and cyber-security controls of the installed system.

Security analyses are performed in accordance with IEEE Std 1012-2004 as endorsed by RG 1.168.

Digital system software is assigned a SIL per the Software Integrity Level Classification Procedure at the beginning of the software development life cycle.

For systems that are classified as SIL 4, the Digital I&C Software Development Plan requires the software development life cycle and procurement activities to be in accordance with the SDOE plan.

An initial SDOE Vulnerability Assessment is performed during the basic design stage to identify design requirements that are verified or added to the requirements specification for each system.

The detailed design process element includes production hardware, software, and programmable logic development. The detailed design activities correspond to the requirements, design, implementation, and test phases of a typical software life cycle.

During the detailed design process production software, firmware, and programmable logic are developed and implemented. The controls established by the Secure Development Environment ensure that unwanted, unneeded, and undocumented functionality (e.g., superfluous code) is not introduced.

Administrative controls for the secure operational environment are developed prior to the operational phase.

The transition from a secure development environment to a secure operational environment includes system integration at the site, SAT, installation, and post installation testing.

Access to protected areas that contain MPS equipment is controlled with the use of security devices. Separation group A and C, and Division I are in different rooms from Separation Group B and D, and Division II. Each separation group, MWS, and division cabinet of the MPS is locked using different keys. During plant operations, routine planned maintenance activities are limited to one division and one separation group at a time.

Remote access to the MPS is prohibited. However the MPS permits administrative control of direct access to safety system equipment. Access to manually bypassed protection channels and manually blocked protective functions is limited by administrative controls. Administrative controls are also provided for access to MWS test points, setpoint adjustments, and channel calibration.

Physical and logical controls prevent modifications to a safety channel when it is being relied upon to perform a safety function. A temporary cable is required to be connected and an out of service switch on the SFM activated before any changes can be made to the SFM. To enable MWS communication, the hardware disconnect must be physically enabled and the affected safety channel must be

placed into bypass, either of which generates an alarm in the control room. By placing the safety channel in bypass, the channel is no longer being relied upon to perform a safety function.

The MPS gateway that supplies information to the SDIS hub is located in the MPS room dedicated to each module. The SDIS hub is located in the PPS room. SDIS displays and the associated display interface modules are located in the MCR.

The communication interfaces for each MPS separation group have unidirectional links to nonsafety-related plant systems.

The FPGA logic in the MPS can only be modified using special tools and only upon removal of an SFM. Certain MPS parameters, such as setpoints, can be adjusted using the MWS during plant operation when the equipment is bypassed or when its safety function is no longer required to be operable.

A nonsafety-related MWS is used to make changes to tunable parameters. Two manual actions are required before write capability of the MWS is established. First, the SFM must be placed out of service by positioning the out of service switch and manual bypass switch into their desired positions. Second, a temporary cable must be connected between the MWS and MPS. Upon completion of these two manual actions, one-way communications are established between the MWS and the MIB communications module for calibration or parameter and setpoint changes. Additional administrative controls (e.g., MWS password login) are required to make changes. Enabling MWS communication initiates alarms at the device level and in the MCR.

Adjustments to MPS parameters are performed in accordance with plant operating procedures that govern the parameter's adjustment, including procedures that establish the minimum number of redundant safety channels that must remain operable for the current operating mode and conditions (Section 13.5). Each safety division has a dedicated nonsafety-related MWS to prevent connection to multiple safety divisions. The FPGA logic circuits and configuration settings for digital data communication interfaces are not adjustable. As a result, the FPGA logic is protected from alterations while in operation.

The MPS provides status and diagnostics information to the MCS, SDIS, and the MWS through one-way, transmit only, isolated outputs.

The I&C architecture is designed with four security levels of which Security Level 4 is the highest. The MPS is identified as a Security Level 4 digital system. The design of the MPS prohibits remote access.

The NMS-excore is an analog system with no digital components, and therefore has no vulnerabilities that require assessment.

7.2.9.2 Identification

Redundant divisions of MPS equipment are marked so that equipment can be clearly identified without frequent referral to reference material. Redundant divisions are distinguished by color-coded equipment tags or nameplates.

The MPS equipment is divided into four separation groups and two divisions. Non-rack mounted module protection system SSC are provided with an identification tag or nameplate. Small electrical components such as power supplies and logic cards have nameplates on the enclosure that houses them. Cables are provided with identification tags.

Electrical and control equipment, assemblies, devices, and cables are grouped into separate divisions and are identified such that the electrical divisional assignment is apparent. The identification method uses color coding and the markers within a division are the same color.

The cables and raceways for Class 1E systems (except those routed in conduits) are tagged at periodic intervals prior to or during installation. Cables and raceways are marked in a manner of sufficient durability to be legible throughout the life of the plant, and to facilitate initial verification that the installation is in conformance with the separation criteria. Cable and raceway markings are colored to uniquely identify the division (or non-division) of the cable. Non-divisional cables within such cabinets are appropriately marked to distinguish them from the divisional cables. The method used for identification is readily distinguished among different divisions of Class 1E systems, between Class 1E and non-Class 1E systems, and among associated cables of different divisions. Associated cables are uniquely identified as such by a longitudinal stripe or other color-coded method.

Class 1E cable raceways are marked with the division color, and with their proper raceway identification at periodic intervals. Neutron-monitoring cables carry the unique voltage class markings superimposed on the divisional color markings, and placed at the same nominal intervals.

For computer systems, software and hardware identification is used to verify that the correct software is installed in the correct hardware component. A configuration control document or drawing is used to identify the correct software, including version, installed in digital I&C systems in accordance with IEEE Std 7-4.3.2-2003, as endorsed by RG 1.152 (Section 7.2.1).

Module protection system programming information is stored in the board's non-volatile memory device attached to the FPGA device. This configuration information is local to the board, and contains local settings, such as channel setup, sequencer setup, timing setup, and build information, including the version and revision of the programming. FPGA build information is created when the FPGA image is generated and is integral to the FPGA logic. The information can be read by the MWS.

The additional requirements from IEEE Std 7-4.3.2-2003 are not applicable to NMS because the NMS is an entirely analog design.

The Digital I&C Software Configuration Management Plan describes the following related to identification with digital I&C systems (Section 7.2.1):

- identification of the program version as well as a means to identify the version after the software is compiled and loaded onto a computer or the FPGA programming is completed
- assurance that the correct control parameters and constants are initially installed in the computers and digital devices and that these control parameters and constants are maintained and updated correctly
- identification that includes a unique revision identifier and that is traceable to configuration control documentation that identifies and justifies the changes made by that revision
- how computer hardware, programs, and software are distinctly identified in accordance with the guidance in Section 5.11 of IEEE Std 7-4.3.2-2003

7.2.9.3 Repair

The MPS incorporates a combination of continuous self-testing and periodic surveillance testing, as described in Section 7.2.15. The self-test features provide a comprehensive diagnostic system ensuring system status is continually monitored. Detectable failures are announced to station personnel and an indication of the impact of the failure is provided to determine the overall status of the system.

The MPS facilitates the recognition, location, replacement, repair, and adjustment of malfunctioning components or modules. The built-in diagnostics support timely recognition of problems by providing a mechanism for periodically verifying the operability of MPS modules, and of locating malfunctioning assemblies. Continuous online error checking detects and locates failures. Channel bypass for the MPS permits replacement of malfunctioning sensors or channel components without jeopardizing plant availability. Detailed information regarding an alarm or fault is available in the MWS to facilitate the timely location of problems.

Without the use of MWS, a status light is provided on the module to indicate any issues with that component. Timely replacement is dependent on the licensee and the component needing replacement. Sensors located in harsh environments or inaccessible areas may be replaceable during an outage. In this instance, the channel can be placed in bypass or trip depending on the technical specifications. Placing a channel in bypass or trip permits continued operation while still meeting the single-failure criterion. For SFMs, SBMs, SVMs, MIB communication module and EIMs self-test and operability checks are performed in accordance with the technical specifications. Detected failures or inoperable status are provided to the operators as an alarm and the channel can be bypassed for repair. Adjustments are only possible on tunable parameters through the use of the MWS.

Periodic parameter updates of certain tunable parameters are required during an outage and during the fuel cycle. Periodic testing is required to verify operability of the MPS. Failure of MPS components require replacement and the ability to replace the MPS components with the plant at power.

The MPS allows periodic and corrective maintenance during normal power operation and during outages. For maintenance to be performed, the equipment must be removed from service. The affected channel in a separation group can be placed in a trip condition or bypass subject to technical specification requirements.

Safety functions within a separation group can be taken to bypass or trip for testing or corrective maintenance. The RTS and ESFAS divisions do not have bypass functionality, however the modules have continuous self-testing coverage. The RTB configuration can be tested at power by opening one breaker at a time.

Removing a channel from service requires the following steps:

- 1) Determine what mode the safety function needs to be in: bypass or trip.
- 2) Place the trip/bypass switch to the position determined in Step 1.
- 3) Place the out of service switch on the associated SFM to the out of service position.
- 4) Verify the correct out of service and bypass or trip alarms have been received in the MCR.

The safety function is now out of service. The maintenance trip/bypass switches are located on a panel in the separation group's cabinet. The switches are connected to the HWM in the SFM chassis and the bypass or trip signal is placed on the backplane to make it available to the modules in the chassis.

The normal configuration of MPS is designed with one-way communication from the module protection system SFMs to the MWS through the MIB communications module and the MPS gateway. The MIB communications module provides Class 1E isolation from safety to nonsafety and communicates status and data to be displayed on the MWS. Changing of parameters is not possible with the SFM in service.

In order to write parameters to the SFM, the following steps are required:

- 1) Verify the SFM is removed from service as described above.
- 2) Connect a temporary calibration and test bus cable from the MWS to the associated separation group's MIB communications module calibration and test bus connection.
- 3) Login on the MWS to a security level that allows changing parameters.
- 4) Select the desired SFM and make the required changes.

5) Verify the changes are correct.

The removal from service of an SFM, corrective maintenance, parameter update, and return to service processes are administratively controlled with approved plant procedures.

The safety function logic cannot be changed on a module when it is installed in the chassis. It must be removed and special equipment used to modify the logic. The MPS design meets the guidance of interim staff guidance DI&C-ISG-04 for changing of parameters by requiring the SFM to be removed from service and a temporary cable to be connected. There is one cable from the MWS so one separation group or division in the I&C equipment room can be connected and updated at one time. Because there are two separate I&C equipment rooms with an MWS, the limitation of having one separation group or division being changed at a time is administratively controlled. The out of service switch on the SFM provides one more level of defense-in-depth where no parameters can be changed unless the SFM is out of service. The switch provides a physical disconnect between the calibration and test bus data and the SFM.

During outage periods when the MPS is not required to be in service, multiple MWSs could be connected to multiple separation groups at the same time under administrative controls.

7.2.10 Interaction between Sense and Command Features and Other Systems

The I&C systems minimize the interactions between safety and nonsafety systems to those that are necessary for the proper functioning of the plant. The boundaries between safety and nonsafety systems are formed by isolation devices that prevent failures or malfunctions in the nonsafety systems from interfering with the safety systems; therefore, conditions that prevent the safety systems from completing protective functions within the sense and command features do not exist in the MPS.

The MPS sense and command features and interaction with other nonsafety systems are designed to meet the requirements of IEEE Std 603-1991, Section 6.3.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI number 40.

Variables used for both protection and control are inputs into the MPS for monitoring, signal conditioning, and trip determination. These variables are then provided to the MCS for plant control functions through isolated, one-way communication paths (Section 7.1.2).

Variables monitored by MPS channels (Table 7.1-2) such as pressurizer pressure or main steam pressure are also used to control the NPM via the nonsafety MCS. Sharing variables between MPS and nonsafety I&C systems reduces the number of penetrations into critical pressure boundaries, such as the RPV and steam lines. Isolated output signals maintain MPS channel independence (Section 7.1.2). The

MCS uses a median signal select algorithm to prevent a single failure in MPS from causing a transient in the control system that would require a protective action.

A median select algorithm in the nonsafety MCS is used so a malfunctioning protection channel does not cause a spurious control system action within MCS. The MCS median select algorithm rejects the failed input and uses the remaining redundant MPS channels monitoring that variable for control. Where protection signals are used for control, robust design features exist to prevent adverse interactions between the MPS and MCS.

Module protection system safety-related variables are monitored by four redundant channels with safety functions actuated by two-out-of-four coincident logic. This logic ensures the required safety function remains operable in the event of a single random failure of a protection channel concurrent with a channel in maintenance bypass, as described in Section 7.1.3 and Section 7.2.4.

When the sense and command features equipment for the MPS are in maintenance bypass, the capability of a safety system to accomplish the safety function is retained, and during such operation, the sense and command features continue to meet the single failure requirements contained in Section 7.2.4.

The MCS utilizes logic processing in the cases where redundant input/output (I/O) channels are used. Some logic supports the redundant-channel architecture used by the MPS, while other logic directly supports the process systems. The logic processing of multiple channels can include two, three, or four input signals.

Median Signal Selection

The MCS performs quality and validation checks on the input process variable data. The MCS determines if the process value is "good." The operator has the ability to select a signal for control if the inputs are determined to be good. If four process values are good, the MCS uses the median value of the four inputs. If one of the inputs is "bad" because of a failure or bypass, a notification is sent to the operator workstation. MCS selects the appropriate selection methodology for the number of remaining good signals for use.

For a two signal input, there are three possible configurations for a selection algorithm. When both inputs are good, the operator has the option to select which signal is used as an input to the process controller. When both signals are bad the loop control is transferred to the operator for manual control. When one signal is good, then the process controller uses that signal.

For a three input signal, a determination is made on the value of three inputs: lowest, median and highest. When three inputs are determined to be good, the median signal is transferred as the input to the control process. If one of the input signals is tagged as bad, then an average of the two remaining signals is used as the input to the control process. When two of the inputs are marked as bad, the one remaining good signal is used by the control process. When all signals are bad, the loop control is transferred to the operator for manual control and the operator is alerted.

For four input signals, if the four channel inputs are determined by MCS to be good, MCS uses the median value of the four inputs. If one channel is bypassed for maintenance, or if the channel fails (i.e., is marked as bad), the channel is disregarded by the signal select algorithm. The signals from the remaining three channels are then processed as described for three inputs. When two of the four signals are bad, the MCS uses the average value of the remaining two valid inputs. When a single value is good, MCS uses the value of the single good input for control. When four signals are bad, the loop control is transferred to the operator for manual control and the operator is alerted.

7.2.11 Multi-Module Stations

This section describes the multi-module station design of the NPP. The I&C safety systems use the term modules vice units to describe the individual NPMs. The design of the I&C systems conforms to the requirements of IEEE Std 603-1991, Section 5.13.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-25) listed in Table 7.0-2 for ASAI number 35.

The NPP includes up to six individual NPMs. The modules have a separate MPS and NMS-excore to provide safety-related protective functions. The MPS and NMS-excore for the NPM do not share information with the other NPMs and are isolated from them. Design-basis events occurring in one module do not impair the ability of the I&C systems in another module from performing their required safety functions. Chapter 19 provides more details on multi-module effects on safety systems.

The electrical power provided by the module-specific EDAS is not shared among NPMs. The common portion of EDAS provides electrical power to shared plant SSC (Section 8.3). Class 1E isolation is provided between the EDAS and MPS, and the isolation devices are classified as part of the safety system. Cross-tie capabilities between NPMs are not provided in the EDAS design.

The NPP is designed for the monitoring and control up to six NPMs from a single control room by utilizing human factors engineering (HFE) and increased automation to optimize staffing levels and reduce human errors. There is no sharing of safety-related I&C structures, systems, and components among modules. The plant protection system, PCS, and SDIS, which are nonsafety-related I&C systems, are the I&C systems that are shared across multiple NPMs. Electrical power supply for the PPS and SDIS is provided by the common portion of the EDAS (Section 8.3). There are no interfaces or connections between the PPS or PCS to any NPM's module protection system or NMS. The SDIS is isolated from the MPS through the MPS gateways, as described in Section 7.1.2. The SDIS is analyzed such that no credible failure of the SDIS can cause a loss of multiple NPM display functions. The SDIS human system interface is designed as described in Section 18.7.

The independence and redundancy discussions in Section 7.1.2 and Section 7.1.3, along with the hazards analyses described in Section 7.1.8, demonstrate that single failure or transient within an I&C safety system of one NPM does not adversely affect

or propagate to another NPM. The safety-related I&C systems are module-specific, and there are no safety-related I&C systems that share functions across multiple NPMs.

7.2.12 Automatic and Manual Control

The MPS provides means for automatic and manual initiation of required functions; however, there are no credited manual actions required to enable the plant to mitigate AOOs and postulated accidents. The automatic and manual features accomplish the reactor trip and ESF actuation functions necessary to shut down and maintain the reactor in a safe condition, thereby restricting the release of radionuclides to the environment.

The automatic and manual control functions of the MPS are designed to conform to Sections 6.1, 6.2, 7.1, and 7.2 of IEEE Std 603-1991, and meet the guidance of RG 1.62.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAls 38 and 39.

7.2.12.1 Automatic Control

The MPS automatically initiates the protective actions necessary to mitigate the effects of the DBEs identified in Table 7.1-1. The variables monitored by MPS to initiate safety-related functions are identified in Table 7.1-2. The safety-related reactor trip and ESFAS functions of MPS are listed in Table 7.1-3 and Table 7.1-4, respectively.

The MPS is designed using the HIPS platform. The HIPS platform is designed to have predictable and repeatable time responses. Information for how the MPS utilizes the predictable and repeatable features of the HIPS platform is detailed in Section 7.1.4. Functional logic implemented within MPS is shown in Figure 7.1-1a through Figure 7.1-1al.

7.2.12.2 Manual Control

The MPS conforms to RG 1.62, and is designed to manually initiate the protective actions listed in Table 7.1-4 at the divisional level. Manual initiation of a protective action is a backup to the automatic function.

A Division I and Division II set of manual switches are provided for manual initiation of protective actions and are connected to the HWM of the corresponding RTS and ESFAS division. Input signals to the HWM are isolated, converted to logic level signals and placed on the backplane. These signals are provided to the associated EIM actuation priority logic circuits downstream of the FPGA logic components that generate automatic signals.

A Division I and Division II manual actuation switch is provided in the MCR for each of the following protective actions. Each manual actuation switch actuates

the respective protective function within its associated division. Actuation of either divisional switch is sufficient to complete the safety function. The manual actuation switches are shown in the MPS functional logic diagrams as shown in Figure 7.1-1j through Figure 7.1-1n:

- reactor trip
- ECCS actuation
- decay heat removal actuation
- containment isolation
- demineralized water system isolation
- chemical and volume control system isolation
- pressurizer heater trip
- secondary system isolation
- low temperature overpressure protection
- pressurizer line isolation

Because the hard-wired manual actuation switch input is downstream of digital components within the MPS, failure of the MPS automatic function does not prevent the manual initiation of the required protective action.

If enabled by the operator using the safety-related enable nonsafety control switch, the capability for manual component level control of ESF equipment is possible using nonsafety discrete hard-wired inputs from the MCS to the HWM. These signals are then input to the actuation priority logic circuit on the EIM. Any automatic or manual safety-related signal overrides the nonsafety signal and is prioritized within the actuation priority logic. For beyond design-basis events and for a limited number of actuated equipment, a safety-related override switch can be used to prioritize a nonsafety signal over certain automatic signals. Override switches are provided for the containment system isolation override function as shown below.

Override - two switches / one per division

- The manual override switches allow for manual control of the containment flooding and drain system, the reactor coolant system (RCS) injection isolation, and the pressurizer spray containment isolation valves if an automatic containment system isolation actuation signal or a chemical and volume control system isolation actuation signal is present with the exception of the High Pressurizer Level chemical and volume control system isolation actuation signal.
- The manual override switches generate an alarm when activated.

The MPS functional logic diagrams provide additional details (Figure 7.1-1j through Figure 7.1-1al). The manual controls are controlled administratively through approved plant procedures.

No manually controlled actions are assumed in the NPP safety analyses in order to accomplish required safety-related functions. No Type A post-accident monitoring variables have been identified as defined in IEEE Std 497-2016 "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations" (Reference 7.2-28). The MPS provides outputs of monitored variables to two redundant divisions of the main control room SDIS displays for accident monitoring and to aid in manual operations. MCS human system interface displays in the MCR are also used to support manual controls.

In the event of a fire in the MCR, the operators evacuate the MCR. There are two MCR isolation switches for each NPM that when repositioned, isolate the MPS manual actuation switches and the enable nonsafety switch for each NPM's module protection system in the MCR to prevent spurious actuation of equipment due to fire damage. An alarm is annunciated in the MCR when the MCR hard-wired switches are isolated using the MCR isolation switches located outside the control room (Figure 7.1-1j).

7.2.13 Displays and Monitoring

This section describes the I&C display and monitoring systems, which provide information for the safe operation of the plant during normal operation, AOOs, and postulated accidents, for supporting manual initiation and control of safety systems, and for the normal status and the bypassed and inoperable status of safety systems.

The design of the SDIS conforms to IEEE Std 603-1991, Section 5.8, and the guidance in RG 1.97, with exceptions as described in this section.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI numbers 27, 28, 29, and 30.

The displays for the SDIS are located in the MCR and provide accurate, complete, and timely information pertinent to MPS and PPS status and informational displays. These displays minimize the possibility of ambiguous indications to the operator. SDIS displays can be used to support manual initiation of protective actions, but the SDIS does not directly initiate protective actions.

The MCR displays are developed following the guidance contained in NUREG-0700 as described in Section 18.7, Human-System Interface Design. Display ambiguity factors have been addressed to minimize the chances of operational error due to misreading or misunderstanding displayed data. Each SDIS display panel presents data and status information derived from both divisions of MPS or PPS.

The SDIS receives inputs from the MPS and PPS through communication modules. Status information regarding process variable values, logic status, equipment status, and actuation device status are provided to the SDIS from the separation group and each division of the RTS, ESFAS, and PPS. The MPS interfaces through the divisional MPS gateway while the PPS interfaces through its MIB communication module.

The principal function of the SDIS is to display PAM variables used by plant operators to assess plant conditions during and following an accident. The principal functions of PAM instrumentation are to provide

- primary information to the control room operators to assess the plant critical safety functions.
- primary information to the control room operators to indicate the potential for breach or the actual breach of fission product barriers.
- information to the control room operators indicating the performance of those safety systems and auxiliary supporting features necessary for mitigating DBEs.
- information to the control room operators indicating the performance of other systems necessary to achieve and maintain a safe shutdown condition.
- information to the control room operators to verify safety system status.
- information to the control room operators for determining the magnitude of the release of radioactive materials and continually assessing such releases.

7.2.13.1 Displays for Manually Controlled Actions

Manual controls are a backup to the automatic functions provided by the MPS. There are no credited manual actions required to mitigate DBEs, and there are no Type A PAM variables. There are no safety-related information displays in the MCR.

7.2.13.2 System Status Indication

The initiation of a protective action is identified and indicated down to the channel-level. Status information is nonsafety-related. As such, it is transmitted to the MCR for indication and recording from the MPS using the SDIS and MCS. The plant protection system uses the PCS in conjunction with the SDIS.

Module protection system and PPS status information is provided in four types:

- process variable values and setpoints
- logic status
- equipment status
- actuation device status

Deviations from normal operating conditions using any combination of these four variable types are alerted to the operator through the use of alarms and annunciators. The task analysis process is used to identify the controls, alarms, and displays needed in the MCR to manage the plant safety functions (Section 18.7).

The Human Factors Program is described in Chapter 18, which includes the application of Functional Requirements Analysis and Function Allocation (Section 18.3) and Task Analysis (Section 18.4) in the design of the I&C human system interfaces for the NPP design.

Post-accident monitoring variables are displayed in the MCR on the SDIS, MCS, and PCS. The PAM variables displayed on SDIS are also displayed on MCS or PCS. Some PAM variables are only displayed on MCS and PCS. Additional description on PAM is in the PAM Section 7.1.1.2.2.

An interdisciplinary team consisting of I&C engineering, probabilistic risk assessment and severe accidents, reactor systems, and HFE have conducted a review of the variables identified for PAM based on the criteria established in IEEE Std 497-2016. The SDIS meets the display criteria of IEEE Std 497-2016. The SDIS display panels display variables required for mitigation of design-basis accidents, and the required variables for PAM requirements identified in Table 7.1-1. The ranges of the identified variables are presented in Table 7.1-7. The accuracy for each PAM variable listed in Table 7.1-7 is established based on the variable's assigned function.

The NuScale HFE Program Management Plan (Reference 18.1-1) outlines how human factors are incorporated into the SDIS. The SDIS displays are designed to minimize the possibility of ambiguous indications that could be confusing to the operator. The SDIS displays continuous real time data of PAM variables. There are no identified Type A PAM variables required to be displayed by the SDIS. The SDIS has the capability of displaying up to 30 minutes of trending data. Continuous self-tests within the SDIS detect and annunciate any signal validation errors.

The SDIS displays are in a separate location in the MCR from those used during normal plant operations. The SDIS displays the PAM variables to the operator during both normal plant operation as well as during post-accident conditions. Information sent to the SDIS from the MPS and PPS is also made available to the plant historian for recording and trending purposes.

7.2.13.3 Alternate Operator Workstation Controls and Monitoring

The Alternate Operator Workstation Controls and Monitoring is described in Section 7.1.1.2.3. There is a set of MCS and PCS displays located at various locations throughout the plant (alternate operator workstations) that allow operators to monitor the NPMs if evacuation of the MCR is required. Safety display and indication system displays are not provided locally as there is no manual control of safety-related equipment allowed outside the control room.

7.2.13.4 Indication of Bypasses

The MCS provides continuous indication of the MPS protective actions that are bypassed or deliberately rendered inoperable. The display of the status information allows the operator to identify the specific bypassed functions and to determine system status and operability. In addition to the status indication, an alarm is sounded in the MCR by the MCS if more than one MPS bypass is attempted for a given protection function. Section 7.2.4 provides details on the operating and maintenance bypasses.

Equipment status information is automatically sent from the MPS to the MCS and SDIS. The MCS displays provide the operator with continuous indications of bypass, trip, and out of service status. The display of the status information allows the operator to identify the operability of the safety functions.

The capability to manually activate the bypass indication in the control room is provided by the MCS.

The display and bypass status information functions are evaluated as part of the MPS failure modes and effects analysis. There are no safety-related trips or actuation functions associated with the display and bypass status information function. Loss of displayed indication would be readily apparent and noticed by MCR operators.

7.2.13.5 Annunciator Systems

Alarms are available for deviation from setpoint, excessive rate-of-change, high or low process value, and contact change of state from normal. Generation of alarms and notifications integrate the requirements from HFE task analysis and alarm philosophy as discussed in Section 18.7.

Alarms are not required to support manually controlled actions relied upon to enable the safety systems to accomplish their safety functions. Manually controlled actions are not assumed in the safety analyses in order to accomplish required safety functions. Operator actions are not required to maintain the plant in a safe and stable condition.

The MCS provides the operators with alarm and status information for viewing and historical trending. The MCS provides the alarms, alarm history, and trending information to the plant operators via the MCS human-system interfaces.

The alarms generated by the MCS for each NPM and PCS, are aggregated for display to the operator by the PCS HSIs in the MCR and local workstations. The MCS and PCS operator workstations are separate and independent from the control processors such that a failure of the control processors does not affect the MCS or PCS operator workstations' alarm functions. Additionally, an independent monitoring system monitors the mutual status of the MCS and PCS to detect and alert the operator to a loss of the overall I&C system.

The MCS and PCS provide redundancy in the control processors, networking components, power supplies, power sources and operator workstation displays to maintain alarm system reliability in the MCR in accordance with item II.T of SECY-93-087.

The MCS provides a first-out alarm resolution capacity. In the case of an avalanche of alarms, the system is able to discriminate between them and date tag the alarms in order of their occurrence. Process alarms are logged with a time stamp that includes the year, month, day, hour, minutes, and second that provides the operator the ability to understand and diagnose major plant upsets.

7.2.13.6 Three Mile Island Action Items

The under-the-bioshield radiation monitor provides the primary means to satisfy the requirements of 10 CFR 50.34(f)(2)(xix) as well as the following variables used to identify inadequate core cooling to satisfy the requirements of 10 CFR 50.34(f)(2)(xviii):

- core exit temperatures
- wide range RCS pressure
- RCS hot temperature
- RPV riser level

The bypassed and operable status indication of safety interlocks is automatically provided in the control room as described in Section 7.2.13.4 and satisfies the requirements of 10 CFR 50.34(f)(2)(v) and RG 1.47.

The SDIS conforms to 10 CFR 50.34(f)(2)(iv) by providing the capability to display the Type B and Type C variables identified in Table 7.1-7 over anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions.

The reactor safety valve position indication is processed by the MPS and then sent to the SDIS and the MCS for display in the MCR. The reactor safety valve position indication is seismically qualified to Seismic Category I requirements and meets the requirements of 10 CFR 50.34(f)(2)(xi).

Consistent with 50.34(f)(2)(xvii) the SDI system provides the capability to monitor containment pressure, containment water level, and the reactor containment atmosphere for radioactivity released from postulated accidents. The MCS provides the recording function for the containment parameters. The PCS provides display and record capability for the noble gas effluent release points.

The design supports an exemption from the hydrogen monitoring requirement of 10 CFR 50.34(f)(2)(xvii)(C).

As described in Table 1.9-5, the design supports an exemption from the power supply requirements for pressurizer level indication included in 10 CFR 50.34(f)(2)(xx).

7.2.13.7 Other Information Systems

There is a unidirectional communication interface between the MCS and PCS networks and the plant network and is shown in Figure 7.0-1. The one-way deterministic isolation devices transmits network traffic from the MCS and PCS to the plant network in one direction only, which is enforced in the hardware design, not software. No software configuration or misconfiguration causes the boundary device to reverse the direction of data flow. The MCS and PCS systems provide monitoring data through one-way communication interfaces to the plant network that provides data recording, trending, and historical retention that can be

retrieved on the emergency operations facility (EOF) stations and technical support center (TSC) engineering workstations.

Additionally, there is a link from the plant network to the NRC emergency response data system through dedicated communication servers that connect to the plant network and provide data communication of required plant data to off-site emergency response facilities.

The TSC engineering work stations are located on the 125' level of the Control Building and separated from the operator workstations, which are located in the MCR. The TSC engineering work stations have fully licensed operating systems, configuration software, and a software package for complete configuration, tuning, trending, and diagnostics of the system. The TSC engineering work stations provide a means to make changes and test software code prior to loading into the controllers.

The non-operator workstation PCS displays (TSC engineering, shift manager, shift technical advisor, and emergency operations facility) provide monitoring functionality to plant process and equipment controls.

7.2.14 Human Factors Considerations

The NuScale HFE program is described in Chapter 18. The program provides a systematic method for integrating HFE into plant analysis, design, evaluation, and implementation to achieve safe, efficient, and reliable operation, maintenance, testing, inspection, and surveillance of the plant. It also ensures the application of HFE principles in the design and verification of the following:

- physical control room structures
- MCR equipment and furnishings
- environments and structures where human tasks must be performed
- control panels and instruments throughout the plant
- controls and tools
- operating procedures
- operator training
- staffing planning

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI number 36.

Human interface considerations for the MPS, PPS, and SDIS alarms and plant status information, as well as the nonsafety-related MCS and PCS are provided in this section.

7.2.14.1 Module Protection System

There are four types of MPS status information:

- 1) process variable values and setpoints
- 2) logic status
- 3) equipment status
- 4) actuation device status

The alarms and status information provided by MPS are used to confirm that protective actions have been actuated as required and that plant conditions have stabilized. Alarms and status information can be used for manual initiation of protective actions; however, there are no manual protective actions that have no automatic action. Alarms associated with MPS are designed to alert the operator of abnormal conditions that may lead to automatic reactor trip or ESF actuation, of inoperable channel or division-level components, or of a need for maintenance activities.

Process Variable Values and Setpoints

The MPS provides status information for its sensors and equipment to the SDIS and the MCS for indication and alarms. The display instrumentation provides accurate, complete, and timely information that improves operator awareness and assists in making appropriate decisions. The MPS provides information for PAM variables through the MPS gateway to the SDIS displays in the MCR.

Logic Status

The module protection system uses four separation groups to make a reactor trip or ESF actuation determination. An alarm is provided at the separation group and division-level for the protective action. As an example, when an overpower condition is identified in one separation group, an alarm is generated. With two or more separation groups indicating an overpower condition, a first out alarm is generated to indicate the cause of the reactor trip. A first out alarm identifies the first condition to cause a major change in plant state. This is illustrated in the MPS functional logic diagrams in Figure 7.1-1a through Figure 7.1-1al. This information is made available to the operators in the MCR and, in more detail, through the MWS.

Equipment Status

A trouble alarm is generated if there are equipment errors or inoperable channels or divisions, which are monitored continuously. Detailed information regarding the trouble alarm is available from the MWS to aid in determining the course of action needed to correct problems.

These notifications allow operators to remain aware of system status during the performance of maintenance or testing.

Actuation Device Status

Execute features relied on by the MPS to accomplish a protective action provide component position feedback to the MPS. Component feedback is essential in confirming that protective actions have been initiated and completed. Valve position, for example, is shown on SDIS displays and allows an operator to identify safety valves in motion or in the safety position. Because of the simplified design of the NPM, actuation device status is limited to valve or breaker positions.

7.2.14.2 Plant Protection System

A component of human interface with the PPS is the MWS. The MWS is located close to the PPS equipment to facilitate troubleshooting activities. Diagnostics data for the PPS, as well as sensor and equipment status information, are accessible via the MWS.

The PPS provides status information for sensors and equipment to the SDIS and the PCS for indication and alarms. The PPS status information provided to the operator is of four types:

- process variable values and setpoints
- logic status
- equipment status
- actuation device status

The alarms and status information provided for PPS are used to confirm that the required PPS actions have been actuated, and remain actuated, as required, and that plant conditions have stabilized. Alarms and status information may be used for manual initiation of the required PPS actions; however, there are no manual PPS actions that have no automatic action. Alarms associated with PPS are designed to alert the operator of abnormal plant conditions, equipment actuation, inoperable division-level components, or malfunctions that require maintenance.

Process Variable Values and Setpoints

Variables monitored by PPS, including setpoints, are provided for display to the operator via the PCS and the SDIS. Accident monitoring variables are available through the SDIS. The display instrumentation provides accurate, complete, and timely information that improves operator awareness and assists in making appropriate decisions.

Logic Status

The plant protection system utilizes two fully redundant divisions to perform required functions. When process logic determines that a protective function actuation is required (e.g., control room habitability system actuation), an alarm is

provided at the division level for the required PPS protective function actuation. There are no connections between divisions. In terms of human factors, this ensures that the source of the alarm can be readily determined.

Equipment Status

With continuous self-diagnostics, system modules generate a trouble alarm if there are equipment errors or inoperable channels or divisions. Detailed information regarding the trouble alarm is available from the MWS. This aids in determining the course of action to correct any problems.

The PPS allows periodic testing during normal operation. The affected channel can be placed in bypass. Any channel in bypass generates an alarm for that particular function. These notifications allow operators to remain aware of system status during the performance of maintenance or testing.

Actuation Device Status

Status feedback is provided for the execute features relied on by the PPS to accomplish a required action.

Periodic surveillance testing (e.g., actuation of device) is used to verify operability, in accordance with applicable technical specification limits (Section 7.2.15). Additional self-diagnostics are implemented in PPS to provide device status in the event of a component issue. The results of this testing are provided to the operators and maintenance personnel through the MCR status displays and the MWS local to the PPS equipment.

Component feedback is essential in confirming that the required actions have been initiated and completed. Valve position, for example, is shown on MCR displays and allows an operator to identify valves in motion or in their actuated position. Because of the simplistic design of the NPP, actuation device status in the PPS is limited to valve or damper positions.

7.2.14.3 Safety Display and Indication System

The SDIS is designed to meet the requirements of IEEE Std 1023-1988. The HFE Program Management Plan (Reference 18.1-1) outlines how human factors are incorporated into the design of systems such as the SDIS.

The SDIS provides the following information to the operator:

- MPS and PPS post-accident monitoring parameter values
- MPS, PPS, and SDIS equipment status
- MPS and PPS actuation device status

The operator uses the SDIS for validation that a protective action goes to completion and that the NPMs are being maintained in a safe condition. Because

the SDIS does not perform actions, the operators use the SDIS to aid in decision making regarding plant operations.

Variables monitored by the MPS and PPS identified for PAM (Table 7.1-7) are available on the SDIS displays for the operator in an accurate, complete and timely manner. Process variables are displayed such that when they exceed set limits, they are easily noticeable by the operator.

Alarms associated directly with the SDIS are for failures of a communication module or a display. If an alarm occurs, the identified piece of equipment must be removed and replaced. The SDIS displays the status of the actuation devices controlled by MPS and PPS. The operators use this information to verify the completion of protective actions during DBEs requiring actuation of devices through the MPS or PPS.

7.2.14.4 Module Control System and Plant Control System

The MCS and PCS human-system interface design is described in Section 18.7.

The MCS and PCS human-system interface is developed with integration of the HFE functional allocation, task analysis and alarm philosophy. The HFE functional allocation, task analysis, and alarm philosophy specify the level of automation and indication required for each process and electrical system.

The MCS and PCS provide a high level of automation with minimal local operation to reduce operator burden and optimize staffing levels while ensuring personnel safety, equipment protection, and system availability.

Coordination with HFE analysis determines the level of automation for the various plant systems and components. This process determines the need for human interfaces to be manual control, shared control, or automatic control. Alarms are developed in accordance with the HFE alarm philosophy and are discussed in Section 18.7.

The MCS and PCS human-system interface is a collection of both hardware, in the form of physical screens and input devices, and software, in the context of the displays designed to represent real-time plant operations and enable the user to monitor and manage the process.

The human-system interface has a windowing type display that can display multiple windows and any combination of graphic pictorials, bar charts, and trend displays as selected by the operator. Displays are hierarchical and are designed in accordance with the HFE function allocation, minimum inventory of controls, task analysis and alarm philosophy.

Operator Workstation Displays

The MCS operator workstation displays are located in the MCR.

The PCS operator workstation displays are located in the MCR and the radwaste building control room.

Operator workstation displays provide real-time information regarding the operation and status of the plant process and equipment and control functions for those processes and equipment. Operator workstation displays provide a manual and automatic control station interface to process controls. Displays are provided for operator adjustment of setpoints, bias, output, and manual and automatic control switching and indication of the associated equipment status and process values.

Diagnostic displays are provided at operator workstations that allow the operator to identify system faults. Diagnostic displays provide sufficient detail to allow the operator to determine if a problem is hardware or software related and which system node, card input or output (I/O) point, power supply, or other aspect fails.

The operator workstation displays are designed as described in Section 18.7.2.

Workstations in locations outside of the Main Control Room

The HSIs in the locations outside of the MCR (Module Maintenance Center, Radioactive Waste Building Control Room, Technical Support Center, and Emergency Operations Facility) are MCR derivatives (i.e., operated from the same platform and connected to either the MCS or PCS network).

7.2.15 Capability for Test and Calibration

The I&C systems provide testing and calibration features for functional tests and checks, calibration verification, and time response measurements. Online testing and periodic testing during outages in conjunction with continuous self-testing are used to verify the performance of I&C systems.

The testing and calibration functions of the MPS and the NMS are designed to conform to Sections 5.7 and 6.5 of IEEE Std 603-1991, Section 5.7 of IEEE Std 7-4.3.2-2003, and meet the guidance in RG 1.22, RG 1.118, and RG 1.47.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A (Reference 7.2-24) listed in Table 7.0-2 for ASAI numbers 14, 24, 25, 26, 32, 47, 49, 50, and 51.

7.2.15.1 System Calibration

The MPS and the NMS are designed with the capability for calibration and surveillance testing, including channel checks, calibration verification, and time response measurements, as required by the technical specifications to verify that I&C safety systems perform required safety functions.

The normal configuration of MPS is designed with one-way communication from the MPS safety function modules to the MWS through the MPS gateway. Adjustments to parameters are performed in accordance with plant operating

procedures that govern the parameter adjustment. Technical specifications establish the minimum number of redundant safety channels that must remain operable for the current operating mode and conditions.

Changing of setpoints and tunable parameters within the MPS is not allowed when the SFM is in service. Using one MWS, only one separation group may be calibrated at a time during normal operation at power. To perform calibrations on the MPS, the affected SFM must be taken out of service subject to technical specification limits (Section 7.2.4). Any SFM in maintenance bypass generates an alarm in the MCR. While a channel is bypassed, the redundant MPS separation groups are fully capable of completing the safety function with the remaining three redundant channels.

Once the SFM is out of service, a temporary cable is connected between the MWS and the calibration and test bus communication port on the associated MIB communications module. The removal from service of an SFM, corrective maintenance, parameter update, and return to service processes are administratively controlled.

The MPS provides the capability to bypass an NMS channel to support NMS system calibration.

7.2.15.2 Instrumentation and Controls System Testing

The MPS is designed to support testing as specified in IEEE Std 338-1987 “Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems,” (Reference 7.2-29) as endorsed and modified by RG 1.118, and IEEE Std 603-1991 with supplemental guidance in RG 1.22, and RG 1.47.

The MPS and the NMS allow SSC to be tested while retaining the capability to accomplish required safety functions. The MPS uses modules from the HIPS platform that are designed to eliminate non-detectable failures through a combination of built-in self-testing and periodic surveillance testing.

Testing from the sensor inputs of the MPS through to the actuated equipment is accomplished through a series of overlapping sequential tests, and the majority of the tests can be performed with the NPM at power. Where testing final equipment at power has the potential to upset plant operation or damage equipment, provisions are made to test the equipment when the NPM is shut down.

Performance of periodic surveillance testing does not involve disconnecting wires or installation of jumpers for at-power testing. The self-test features maintain separation group and division independence by being performed at within the separation group or within the division.

The part of MPS that cannot be tested at power is the actuation priority logic circuit on the EIM, the manual MCR switches, and the nonsafety-related controls that provide inputs to the actuation priority logic. The actuation priority logic consists of discrete components and directly causes actuation of field

components that cause the reactor to shutdown or adversely affect operation. The actuation priority logic is a very simple circuit and has acceptable reliability to be tested when the reactor is shut down.

The manual trip and actuate switches in the MCR cannot be tested at power and require an outage. These switches are standby, low demand components such that testing every refueling outage is acceptable to maintain sufficient system reliability.

The SDIS supports MPS and PPS by providing the displays for PAM variables. Post-accident monitoring instrument channels have testing capability to verify, on a periodic basis, functional requirements to support calibration of the channels.

Continuous self-tests within the SDIS detect and annunciate communication failures.

The SDIS and PPS are designed to support periodic testing, calibration, and maintenance. Either division of SDIS and PPS can fully accomplish their required functions, such that if a single division is removed from service for testing, maintenance, or calibration the other division remains available to perform the required functions. SDIS and PPS are not required to meet the single failure criterion during maintenance, test or calibration activities consistent with the guidance contained in IEEE Std 497-2016. The time periods that SDIS or PPS is bypassed or removed from service are administratively controlled.

While the MPS is in normal operation, self-tests run without affecting the performance of the safety function, including its response time.

Module protection system data communications are designed with error detection to enhance data integrity. The protocol features ensure communications are robust and reliable with the ability to detect transmission faults. Similar data integrity features are used to transfer diagnostics data.

The MPS provides a means for checking the operational availability of the sense and command feature input sensors relied upon for a safety function during reactor operation.

This capability is provided by one of the following methods:

- perturbing the monitored variable
- cross-checking between channels that have a known relationship (i.e., channel check)
- introducing and varying a substitute input to the sensor

7.2.15.3 Fault Detection and Self-diagnostics

The MPS platform incorporates failure detection and isolation techniques. Fault detection and indication occurs at the module level, which enables plant personnel to identify the module that needs to be replaced. Built-in self-testing

generates an alarm and report a failure to the operator and place the component (e.g., SFM, SVM, or EIM components) in a fail-safe state.

Diagnostic data for the separation group and division of the MPS are provided to the MWS for the division. The MWS is located close to the equipment to facilitate troubleshooting activities. The interface between the MPS gateway and the MWS is an optically isolated, one-way diagnostic interface. Diagnostics data are communicated through the MIB which is a physically separate communications path from the safety data path, ensuring the diagnostics functionality is independent of the safety functionality. Further discussion on how the MWS does not prevent or have adverse influence on the MPS performing safety functions can be found in Section 7.1.2.

The operation of the MPS is deterministic in nature and allows the systems to monitor themselves in order to validate functional performance. The self-test features provide a comprehensive diagnostic system ensuring system status is continually monitored. Detectable failures are alarmed to the operator in the MCR, and an indication of the impact of failure is provided to determine the overall status of the system. More detail on the MPS diagnostics functions are provided in TR-1015-18653-P-A (Reference 7.2-25).

The NMS uses a health monitoring circuit in the electronic process blocks that checks the continuity of the circuit inputs. Detected faults within the NMS are provided to the MPS to trip the channel and for alarm and display in the MCR.

7.2.16 Sensors

This section provides information on sensor functions, requirements, design, installation, maintenance, and qualification.

7.2.16.1 Design Bases

Spatial requirements are described in Section 7.1.1 (IEEE Std 603-1991, Sections 4.4 and 4.6).

Single failure and redundancy are described in Section 7.1.3 (IEEE Std 603-1991, Section 5.1).

Regulatory requirements that govern sensors include GDC 2, GDC 4, GDC 13, 10 CFR 50.49, and 10 CFR 50.34(f)(2)(xviii) as described in Section 7.1.1.

Sensor diversity including conformance with NUREG/CR-6303 is described in Section 7.1.5.

Equipment qualification including conformance with Regulatory Guide 1.89, Regulatory Guide 1.209, IEEE Std 7-4.3.2-2003, and IEEE Std 323 are described in Section 7.2.2.

Seismic qualification is described in Section 3.10.1 including conformance with IEEE 344-2013. Advanced sensors located inside the CNV are required to withstand earthquakes and have a seismic classification of Category I.

Sensor supporting structures planned for insertion in the RPV (as part of the RPV pressure boundary) are classified as Seismic Category I.

7.2.16.2 Design

The following design attributes are applicable to the sensors described in this section.

- The instruments are accessible, retrievable, and replaceable while in the refueling bay dry dock.
- The in-vessel instruments are capable of calibration and capable of an in-situ function test upon vessel return to the operating bay.
- Space is provided for electronics associated with sensors on or near the platform, above the containment head if required, or in an electronics room.
- Sensors located in the top of containment or underneath the bioshield are protected, shielded, or located away from the impact of spray effects of a high energy line break by pipe whip restraints, local shielding, or sensor location.
- Taps or sensing lines through the CNV are double isolated.
- Advanced sensors' accuracies and ranges are consistent with Section 15.0.

7.2.16.3 Functions

NSSS sensors primary functions, range, quantity, and safety classification are provided in Table 7.2-1. Table 7.1-2 provide additional information on variables including core exit temperature monitoring. Section 7.0.4.2 provides information on NMS equipment. The following provides additional information related to individual sensor functions.

Reactor Coolant System Hot Temperature

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in MCS using an isolated signal output from MPS rather than a direct connection to the sensors.

Reactor Coolant System Cold Temperature

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in the MCS using an isolated signal from the MPS rather than a direct connection to the sensors.

Pressurizer Liquid Temperature

Nonsafety-related functions are implemented in the MCS using an isolated signal from the MPS rather than a direct connection to the sensors.

Pressurizer Vapor Temperature

Nonsafety-related functions are implemented in the MCS from a direct connection to the sensors.

Main Steam Temperature

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in the MCS using an isolated signal from the MPS rather than a direct connection to the sensors.

Under-the-Bioshield Temperature

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in MCS using an isolated signal from MPS rather than a direct connection to the sensors.

Pressurizer Pressure

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in the MCS using an isolated signal from the MPS rather than a direct connection to the sensors.

Wide Range Reactor Coolant System Pressure

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in the MCS using an isolated signal from the MPS rather than a direct connection to the sensors.

Narrow Range Containment Pressure

An isolated output of the narrow range containment pressure signal is provided to the MCS for NSSS control functions. The narrow range containment pressure is scaled to measure in a narrow band around expected operating pressures with margin. Narrow range containment pressure is also used to supply control room alarms, control room displays, and the plant historian.

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in the MCS using an isolated signal from the MPS rather than a direct connection to the sensors.

Main Steam Pressure

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in MCS using an isolated signal from MPS.

Feedwater Pressure/Decay Heat Removal Outlet Pressure

One pressure instrument is used to measure both functions because there are no valves between the feedwater plenum of the steam generator and the DHRS

condenser in the area near the bottom of the decay heat removal condenser. This instrument performs its feedwater pressure function when the DHRS valves (at the inlet to the decay heat removal) are closed, and performing its DHRS outlet pressure function when the decay heat removal valves are open (indicating the DHRS unit is active and main steam and feedwater are isolated).

Pressurizer Level

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in the MCS using an isolated signal from the MPS rather than a direct connection to the sensors.

Containment Water Level

Nonsafety-related functions are implemented in the MCS using an isolated signal from the MPS rather than a direct connection to the sensors.

Reactor Coolant System Flow Measurement

Safety-related functions are implemented by the MPS. Nonsafety-related functions are implemented in the MCS using an isolated signal output from the MPS rather than a direct connection to the sensors.

7.2.16.4 Sensor Selection

Temperature Measurement

Resistance temperature detectors (RTDs) that are conventional for use in existing reactors are used and radiation hardened. Resistance temperature detectors and thermowells are used for measurement of temperature in the presence of thermal streaming.

Pressure Measurement

In-containment method of measuring pressure device uses a pressure transducer mounted inside containment with remote processing electronics. This approach requires minimal space and impact to the NPM baseline design and involves commercial grade dedication or qualification of digital electronics and environmental qualification.

Flow Measurement

Ultrasonic flowmeter is used to measure RCS flow.

Level Measurement

A guided wave radar method is used for measuring the PZR water level. The RPV riser level and CNV level measurements are thermal dispersion switch assemblies consisting of a probe that spans the distance of the measurement range with switches located at various levels to support operational requirements.

The thermal dispersion switches determine the presence or absence of liquid water at discrete locations axially along the probe assembly. Modifications are made as needed to support qualification. The processing electronics for the radar unit is remote from the sensor assembly and located in a mild environment.

The RPV riser level measurement provides input to MPS to actuate ECCS within the specified level range during service conditions typical of when ECCS actuation is expected. The RPV riser level instrumentation is qualified to actuate ECCS within specified analytical limits for the process conditions characteristic of the spectrum of postulated design-basis loss-of-coolant accidents (liquid and vapor) and the associated range of depressurizations. Additionally, qualification confirms the acceptability of the correlation between RPV riser level transient and the modeling approach used in the transient and accident analyses in Chapter 15, as identified in Table 15.0-7.

7.2.16.5 Installation

Sensor signals in containment are transmitted through radiation and temperature tolerant cable and fed through designated containment electrical penetration assemblies. Outside the containment, the signals are routed to the processing electronics located in a mild environment. Power supplies are also housed in the processing cabinets in a mild environment.

Reactor Coolant System Hot Temperature

The sensors are installed in thermowells on the RPV vessel and inside containment. Four sensing elements, one per separation group, are mounted below the pressurizer baffle plate section to obtain safety-related RCS hot temperature measurement.

Reactor Coolant System Cold Temperature

Four RTDs, one per channel, are mounted in thermowells below the steam generators. The RTD lead wires are routed through a support conduit to the CNV penetration assemblies.

Pressurizer Liquid Temperature

The RTDs are mounted in thermowells in the lower section of the pressurizer. The RTD wiring is routed from the RTD in the thermowell location to the designated containment vessel electrical penetration assemblies and then to the MCS cabinets located in a mild environment outside containment.

Pressurizer Vapor Temperature

The two RTDs are installed in thermowells in the vapor section of the pressurizer. The RTD wiring is routed from the RTD in the thermowell location to the designated containment vessel electrical penetration assemblies, and then to the MCS cabinets located in a mild environment outside containment.

Containment Air Temperature

The two RTDs are installed on mountings near the top inside of containment such that the temperature sensing can occur in the environment that the RTD element resides.

Main Steam Temperature

The RTDs are installed in thermowells outside of containment in the main steam pipe section on the reactor module side of the main steam isolation valves.

Feedwater Temperature

The RTDs are installed in thermowells on the containment piping on the separation flange side of the feedwater isolation valves.

Decay Heat Removal System Outlet Temperature

The RTDs are installed in thermowells in the lower condenser section outside of containment, in the pool.

Under-the-Bioshield Temperature

The RTDs are mounted on the reactor pool wall underneath the bioshield. Cabling from the RTDs is routed to the disconnect panel on the pool wall.

Pressurizer Pressure

The pressure transducer is installed on a mounting in the containment annulus and measures pressure using sensing lines.

Wide Range Reactor Coolant System Pressure

The pressure transducer is installed on a mounting in the containment annulus and measures pressure using sensing lines.

Narrow Range Containment Pressure

Four narrow range pressure transducers, one for each separation group, are installed in containment in four different locations, supplying four different separation groups.

Wide Range Containment Pressure

Two wide range pressure transducers are installed in containment in two locations, and cables are routed through separation groups B and C penetration assemblies.

Main Steam Pressure

Standard installation processes are used for these transmitters as the piping that the sensing lines tap into is outside of containment and above the reactor pool water level.

Feedwater Pressure and Decay Heat Removal System Outlet Pressure

The transmitters are located in the reactor pool and mounted to part of the DHRS condenser structure. This location allows them to be in close proximity to their respective sensing lines. The signal cable is waterproof cable that routes the signal from the transmitter to the electrical panel near the platform above the vessel. From there the signal goes to the MPS cabinets.

Pressurizer Level

The radar level sensor consists of an antenna that is the wave-guide for the transmitted signal. This assembly is inserted in the top of the reactor module for pressurizer level measurement such that its signal propagates down the antenna and reflects off the vapor/liquid surface.

Reactor Pressure Vessel Riser Level

The sensors are mounted on top of the CNV with mineral insulated cable extending down to an instrument seal assembly in the RPV head. A probe with multiple level switches extends downward through the PZR and into the RPV riser, spanning the distance of the measurement range, to monitor points below the baffle plate. The probe is routed through guide tubes within the RPV that contain openings to allow for vapor or liquid to be in contact with the probe.

Containment Water Level

The level sensor consists of a single or series of level switches located at points determined by operational requirements.

Decay Heat Removal System Level

The sensor taps are fitted into the DHRS steam piping. The switch inserts into the pipe taps and sends the signal electronically to the disconnect panel using mineral insulated cable or cable of similar nature that is waterproof. From the disconnect panel the signals are sent to the MCS for MCR indication.

Reactor Coolant System Flow

The reactor coolant system flow sensors consist of ultrasonic flowmeter transducers mounted into a nozzle integral to the reactor vessel shell. These transducers are inserted into a well that is machined into the nozzle. This well is the reactor coolant pressure boundary and allows the transducer signal to pass through the well and perform its function.

The transducer is media isolated, and the well is fabricated with materials specified by the vendor for sonic transmission and reception as well as materials acceptable for use in the RPV.

7.2.16.6 Sensor Maintenance

Sensors are located to allow for maintenance and periodic calibration. Sensors are accessible while the module is in dry dock and have the ability to be maintained, removed, and reinstalled.

Reactor coolant system RTD cross calibration is required before or after the refueling outage. The calibration requires access to the MPS cabinets and an RTD cross calibration test set. An in-situ function test is also being planned for post-dry dock testing after the vessel is moved back to its operating bay. The reactor coolant system RTD cross calibration is performed in accordance with the plant procedures and the plant technical specifications. Acceptance criteria are determined based on vendor specifications for the RTDs and the plant safety analysis.

Feedwater and decay heat removal outlet pressure sensors are accessible for maintenance calibrations and replacements during operation and refueling outages.

To ensure accessibility of the RCS flow measurement transducers for maintenance and replacement, the transducers are located in the lower downcomer region that is exposed when the upper reactor module is separated for refueling. Routine maintenance of the transducer during or between cycles is not generally required. The electronics cabinet is located in a mild environment and is readily accessible.

7.2.16.7 Instrument Sensing Lines

The sensors that use instrument sensing lines are pressurizer pressure narrow range, RCS pressure wide range, main steam pressure, feedwater outlet pressure, and DHRS outlet pressure. For these sensors, the instrument sensing lines are designed in accordance with ISA-67.02.01-2014 "Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants," (Reference 7.2-23), as endorsed by RG 1.151.

7.2.17 References

- 7.2-1 American National Standards Institute/American Nuclear Society, "Nuclear Power Plant Simulators for Use in Operator Training and Examination," ANSI/ANS 3.5-2009, LaGrange Park, IL.
- 7.2-2 American Society of Mechanical Engineers, *Quality Assurance Requirements for Nuclear Facility Applications*, ASME NQA-1-2008, New York, NY.

- 7.2-3 American Society of Mechanical Engineers, *Addenda to ASME NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications*, ASME NQA-1a-2009 Addenda, New York, NY.
- 7.2-4 Electric Power Research Institute, "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," TR-106439, EPRI, November 15, 1996.
- 7.2-5 Institute of Electrical and Electronics Engineers, "IEEE Application Guide for Surge Protection of Electric Generating Plants," IEEE Std C62.23-1995 (R2001), Piscataway, NJ.
- 7.2-6 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," IEEE Std 323-2003, Piscataway, NJ.
- 7.2-7 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," IEEE Std 323-1974, Piscataway, NJ.
- 7.2-8 Institute of Electrical and Electronics Engineers, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Std 379-2000 (R2008), Piscataway, NJ.
- 7.2-9 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," IEEE Std 384-1992 (R1998), Piscataway, NJ.
- 7.2-10 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603-1991, Piscataway, NJ.
- 7.2-11 Institute of Electrical and Electronics Engineers, "IEEE Guide for Generating Station Grounding," IEEE Std 665-1995 (R2001), Piscataway, NJ.
- 7.2-12 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std 7-4.3.2-2003, Piscataway, NJ.
- 7.2-13 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Quality Assurance Plans," IEEE Std 730-2002, Piscataway, NJ.
- 7.2-14 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Configuration Management Plans," IEEE Std 828-2005, Piscataway, NJ.
- 7.2-15 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software and System Test Documentation," IEEE Std 829-2008, Piscataway, NJ.

- 7.2-16 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Software Requirements Specifications," IEEE Std 830-1998, Piscataway, NJ.
- 7.2-17 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Unit Testing," IEEE Std 1008-1987 (R2009), Piscataway, NJ.
- 7.2-18 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Verification and Validation," IEEE Std 1012-2004, Piscataway, NJ.
- 7.2-19 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Reviews and Audits," IEEE Std 1028-2008, Piscataway, NJ.
- 7.2-20 Institute of Electrical and Electronics Engineers, "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations," IEEE Std 1050-1996, Piscataway, NJ.
- 7.2-21 Institute of Electrical and Electronics Engineers, "IEEE Standard for Developing a Software Project Life Cycle Process," IEEE Std 1074-2006, Piscataway, NJ.
- 7.2-22 International Society of Automation, "Setpoints for Nuclear Safety-Related Instrumentation," ISA-S67.04.01-2018, Research Triangle Park, North Carolina.
- 7.2-23 American National Standards Institute/International Society of Automation, "Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants," ANSI/ISA 67.02.01-2014, Research Triangle Park, North Carolina.
- 7.2-24 NuScale Power, LLC, "Design of the Highly Integrated Protection System Platform," TR-1015-18653-P-A, Revision 2.
- 7.2-25 NuScale Power, LLC, "NuScale Instrument Setpoint Methodology Technical Report," TR-122844-P, Revision 0.
- 7.2-26 Institute of Electrical and Electronics Engineers, "Standard for Flame-Propagation Testing of Wire & Cable," IEEE Std 1202-2006, Piscataway, N.J.
- 7.2-27 Not used.
- 7.2-28 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," IEEE Std 497-2016, Piscataway, NJ.
- 7.2-29 Institute of Electrical and Electronics Engineers, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," IEEE Std 338-1987, Piscataway, NJ.

Table 7.2-1: Nuclear Steam Supply System Sensor List

Sensor	Range	Quantity	Function	Location	Classification	Receiving System
Temperature						
RCS hot temperature	40°F to 700°F	4	RTS ESFAS T-2, T-3, T-4 interlocks PAM NSSS control MCR indication Degrees of subcooling Input to calorimetric calculation Plant historian	Top of downcomer	A1	MPS
RCS cold temperature	40°F to 700°F	4	LTOP T-1 interlock T-5 interlock NSSS control MCR indication Input to calorimetric calculation Plant historian	Downcomer below steam generator	A1	MPS
PZR liquid temperature	40°F to 800°F	2	NSSS control MCR indication Plant historian	Lower PZR	B2	MCS
PZR vapor temperature	40°F to 800°F	2	NSSS control MCR indication Plant historian	Upper PZR	B2	MCS
CNV air temperature	40°F to 600°F	2	NSSS control MCR indication Plant historian	Upper part of containment	B2	MCS
Main steam temperature	100°F to 700°F	8	RTS ESFAS Input to calorimetric calculation Degrees of superheat MCR indication NSSS control Plant historian	Upstream of main steam isolation valve (MSIV) on main steam pipe	A1	MPS
Feedwater temperature	40°F to 440°F	6	NSSS control MCR indication Input to calorimetric calculation Plant historian	Upstream of feedwater isolation valve (FWIV) on feedwater (FW) pipe	B2	MCS
DHRS outlet temperature	40°F to 440°F	4	MCR indication Plant historian	Bottom of DHRS unit	A2	MCS
Under-the-bioshield temperature	40°F to 700°F	4	RTS ESFAS PAM MCR indication Plant historian	Under the bioshield	A1	MPS

Table 7.2-1: Nuclear Steam Supply System Sensor List (Continued)

Sensor	Range	Quantity	Function	Location	Classification	Receiving System
Pressure						
Pressurizer pressure	1100 to 2200 psia	4	RTS ESFAS NSSS control MCR indication Plant historian	Near top of PZR in CNV	A1	MPS
Wide range RCS pressure	0 to 2500 psia	4	LTOP PAM Degrees of subcooling NSSS control MCR indication Plant historian	Near top of PZR in CNV	A1	MPS
Narrow range containment pressure	0 to 20 psia	4	RTS ESFAS NSSS control MCR indication Plant historian	Upper part of CNV	A1	MPS
Wide range containment pressure	0 to 1400 psia	2	PAM MCR indication Plant historian	Upper part of CNV	B2	MPS
Main steam pressure (decay heat removal inlet pressure)	0 to 1400 psia	8	RTS ESFAS MCR indication Degrees of superheat NSSS control Input to calorimetric calculation Plant historian	Upstream of MSIVs on DHRS tee	A1	MPS
Feedwater pressure and DHRS outlet pressure	0 to 1400 psia	6	NSSS control MCR indication Input to calorimetric calculation Plant historian	Bottom of DHRS heat exchanger	A2	MCS
Level						
Pressurizer level	0 to 100%	4	RTS ESFAS NSSS control MCR indication Plant historian	Top of PZR to baffle plate	A1	MPS
RPV riser level	Multiple discrete points	4	ESFAS PAM MCR indication Plant historian	RPV head penetration to the top of the upper core plate	A1	MPS
Containment water level	Multiple discrete points	4	L-1 interlock Excore compensation MCR indication NSSS control Plant historian	Top of containment to below the ECCS reactor recirculation valves	A1	MPS
DHRS level switch	N/A (Single discrete point)	8	MCR indication Plant historian	On DHRS steam piping	B2	MCS

Table 7.2-1: Nuclear Steam Supply System Sensor List (Continued)

Sensor	Range	Quantity	Function	Location	Classification	Receiving System
Flow						
Reactor coolant system flow	0 to 110%	4	RTS ESFAS PAM MCR indication Input to calorimetric calculations NSSS control Plant historian	Downcomer below SG	A1	MPS

Figure 7.2-1: Instrumentation and Controls Safety System Development Processes

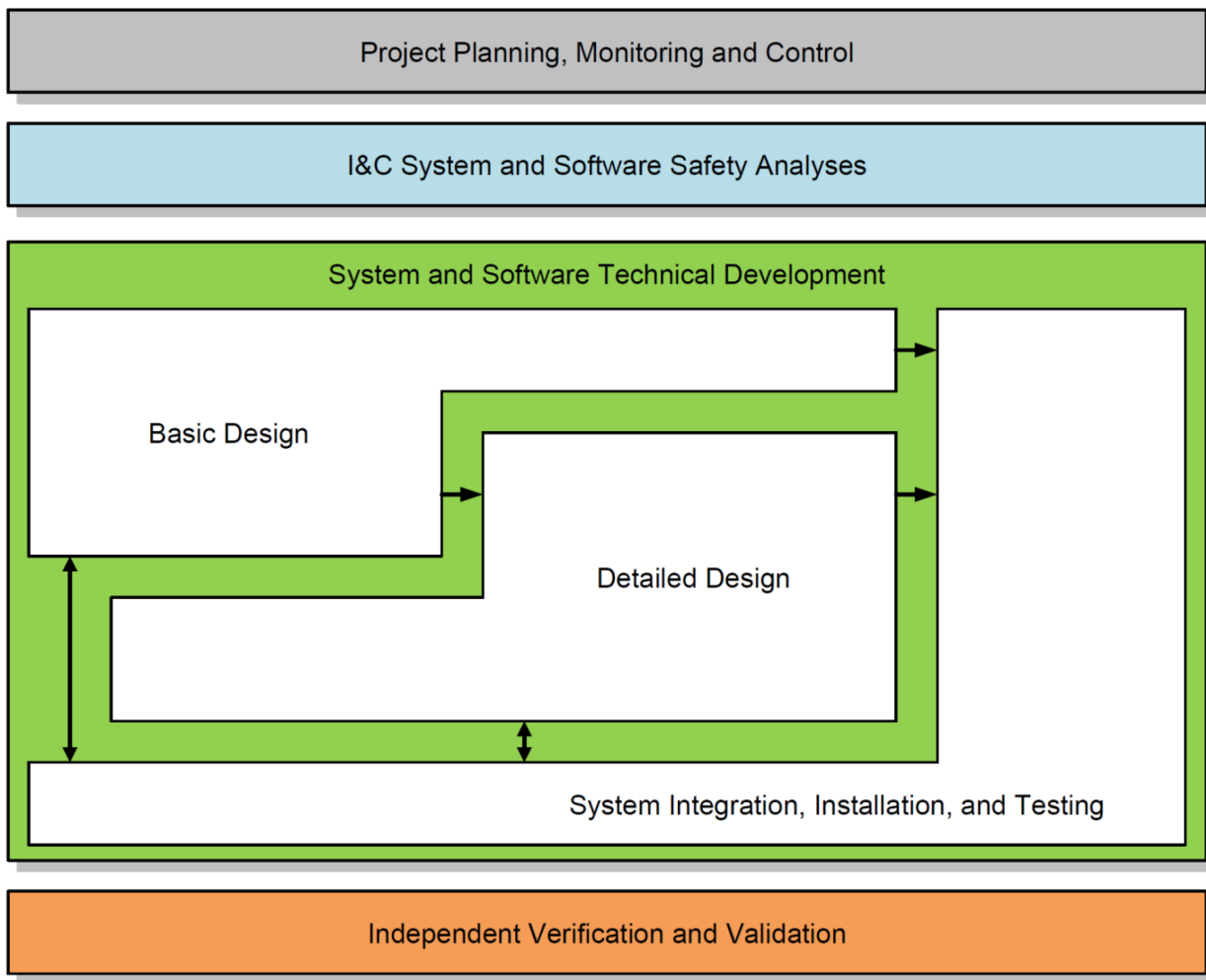


Figure 7.2-2: System and Software Technical Development Life Cycle Processes

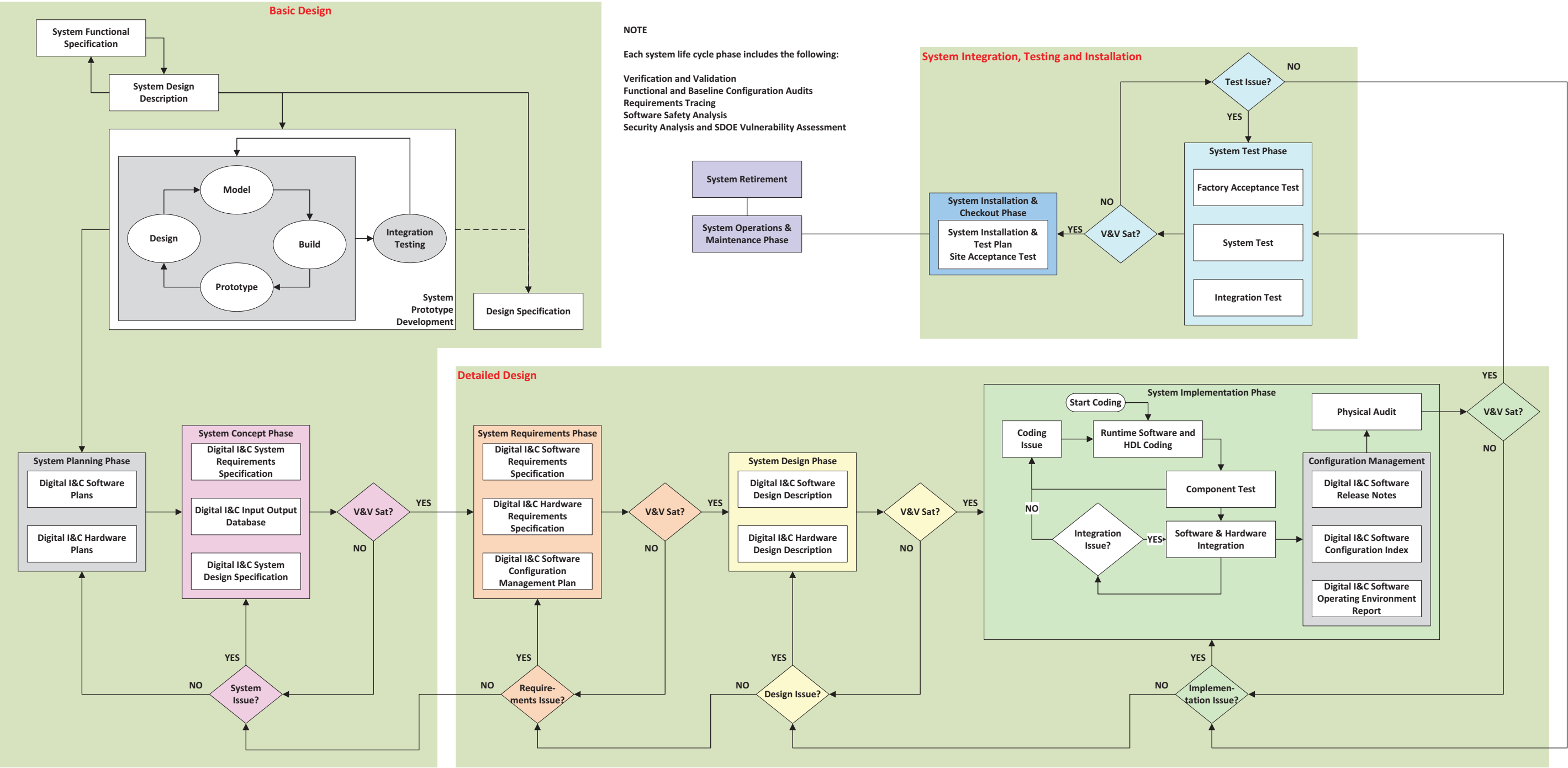


Figure 7.2-3: Software Lifecycle Comparisons

