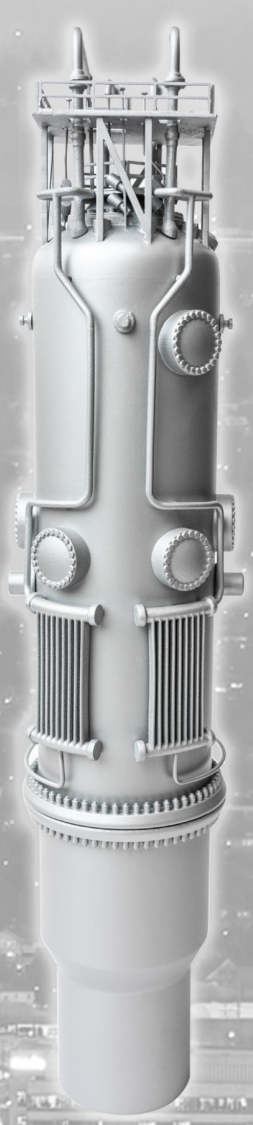
NUSCALE™
Power for all humankind

NuScale Standard Plant
Design Certification Application

Chapter Seven
Instrumentation and Controls



PART 2 - TIER 2

Revision 4
January 2020

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 7.0-29

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 7.1-17

7.1.4 Predictability and Repeatability 7.1-21

7.1.5 Diversity and Defense-in-Depth 7.1-22

7.1.6 Safety Evaluation 7.1-45

7.1.7 Simplicity 7.1-49

7.1.8 Hazards Analysis 7.1-51

7.1.9 References 7.1-59

7.2 System Features 7.2-1

7.2.1 Quality 7.2-1

7.2.2 Equipment Qualification 7.2-30

7.2.3 Reliability, Integrity, and Completion of Protective Action 7.2-33

7.2.4 Operating and Maintenance Bypasses 7.2-37

7.2.5 Interlocks 7.2-41

7.2.6 Derivation of System Inputs 7.2-42

7.2.7 Setpoints 7.2-42

7.2.8 Auxiliary Features 7.2-43

7.2.9 Control of Access, Identification, and Repair 7.2-45

7.2.10 Interaction between Sense and Command Features and Other Systems 7.2-51

7.2.11 Multi-Unit Stations 7.2-53

7.2.12 Automatic and Manual Control 7.2-54

7.2.13 Displays and Monitoring 7.2-56

7.2.14 Human Factors Considerations 7.2-61

TABLE OF CONTENTS

7.2.15 Capability for Test and Calibration 7.2-66
7.2.16 References 7.2-69

LIST OF TABLES

Table 7.0-1: NuScale Instrumentation and Controls Design and Applicable Regulatory Requirements Matrix 7.0-30

Table 7.0-2: Highly Integrated Protection System Topical Report (HIPS TR) Application Specific Information Cross References 7.0-34

Table 7.1-1: Module Protection System Design Basis Events 7.1-61

Table 7.1-2: Variables Monitored by Module Protection System 7.1-62

Table 7.1-3: Reactor Trip Functions 7.1-64

Table 7.1-4: Engineered Safety Feature Actuation System Functions 7.1-65

Table 7.1-5: Module Protection System Interlocks / Permissives / Overrides 7.1-70

Table 7.1-6: Design Basis Event Actuation Delays Assumed in the Plant Safety Analysis. 7.1-74

Table 7.1-7: Summary of Type A, B, C, D, and E Variables 7.1-75

Table 7.1-8: Variables Monitored by Plant Protection System 7.1-77

Table 7.1-9: Sensor Inputs to Module Protection System 7.1-78

Table 7.1-10: Intentional Differences Between Field Programmable Gate Array Architecture 7.1-80

Table 7.1-11: Partial Spurious Actuation Scenarios for Engineered Safety Features Actuation System within Safety Block I 7.1-81

Table 7.1-12: Consequences of Partial Spurious Reactor Trip 7.1-82

Table 7.1-13: Effects of Digital-Based Common Cause Failure of Level Function Type on Sensor Block I 7.1-83

Table 7.1-14: Effects of Digital-Based Common Cause Failure of Digital-Based Pressure Measuring System Function Type on Sensor Block I and II 7.1-84

Table 7.1-15: Effects of Digital-Based Common Cause Failure of Digital-Based Flow Function Type on Sensor Block I and II 7.1-85

Table 7.1-16: Safety-Related Digital Sensors Used by Safety Block I and II 7.1-86

Table 7.1-17: Effect of FPGA Technology Diversity for Postulated Digital-Based CCF of MPS Safety Blocks 7.1-87

Table 7.1-18: Digital Sensors Credited for Mitigating Anticipated Operational Occurrences and Postulated Accidents 7.1-88

Table 7.1-19: Example: Hazard Conditions 7.1-94

Table 7.1-20: Example: Safety Functions 7.1-95

Table 7.1-21: Example: High-level Safety Constraints 7.1-96

Table 7.1-22: Example: Safety Constraints Associated with Plant Conditions 7.1-97

Table 7.1-23: Example: Control Action Analysis 7.1-98

LIST OF TABLES

Table 7.1-24: Example: Identified Hazard Causes. 7.1-99

LIST OF FIGURES

Figure 7.0-1: Overall Instrumentation and Controls System Architecture Diagram 7.0-36
Figure 7.0-2: Module Protection System Boundaries. 7.0-37
Figure 7.0-3: Module Protection System Safety Architecture Overview 7.0-38
Figure 7.0-4: Separation Group A Communication Architecture. 7.0-39
Figure 7.0-5: Separation Group A and Division I Reactor Trip System and Engineered Safety Features Actuation System Communication Architecture . . . 7.0-40
Figure 7.0-6: Reactor Trip Breaker Arrangement 7.0-41
Figure 7.0-7: Equipment Interface Module Configuration 7.0-42
Figure 7.0-8: Equipment Interface Module Output 7.0-43
Figure 7.0-9: Pressurizer Trip Breaker Arrangement. 7.0-44
Figure 7.0-10: Module Protection System Gateway Diagram 7.0-45
Figure 7.0-11a: Module Protection System Power Distribution 7.0-46
Figure 7.0-11b: Module Protection System Power Distribution 7.0-47
Figure 7.0-12: Neutron Monitoring System Ex-Core Block Diagram 7.0-48
Figure 7.0-13: Plant Protection System Block Diagram 7.0-49
Figure 7.0-14: Safety Display and Indication System Boundary 7.0-50
Figure 7.0-15: Safety Display and Indication Hub 7.0-51
Figure 7.0-16: Display Interface Module 7.0-52
Figure 7.0-17: Module Control System Internal Functions and External Interfaces. 7.0-53
Figure 7.0-18: Automatic Control Shared Between Networked Processors 7.0-54
Figure 7.0-19: Automatic Control Shared Between MCS and PCS Processors 7.0-55
Figure 7.0-20: Plant Control System Internal Functions and External Interfaces 7.0-56
Figure 7.1-1a: Module Protection System And Plant Protection System Trip or Bypass Switch Logic 7.1-100
Figure 7.1-1b: Source Range and Power Range Trips. 7.1-101
Figure 7.1-1c: Power Range High-2 Power Trip and N-2 Interlocks, Low and Low Low RCS Flow Trips 7.1-102
Figure 7.1-1d: Power Range and Intermediate Range Rate Trips. 7.1-103
Figure 7.1-1e: Pressurizer Pressure and Level Trips. 7.1-104
Figure 7.1-1f: Reactor Coolant System Hot Temperature Trip, Temperature Interlocks 7.1-105
Figure 7.1-1g: Pressurizer Level Interlock and Trip, High Containment Pressure, and High Containment Level Trips 7.1-106
Figure 7.1-1h: Steam Generator Low and Low Low Main Steam Pressure Trips. 7.1-107

LIST OF FIGURES

Figure 7.1-1i: High Main Steam Pressure and Steam Generator Low and High Steam Superheat Trips 7.1-108
Figure 7.1-1j: Reactor Trip and Reactor Tripped Interlock RT-1 . . . . . 7.1-109
Figure 7.1-1k: ESFAS - Containment System Isolation and Chemical and Volume Control System Isolation Interlocks 7.1-110
Figure 7.1-1l: ESFAS - Decay Heat Removal System and Secondary System Isolation Actuation, FWIV Interlock. 7.1-111
Figure 7.1-1m: ESFAS - Demineralized Water System Isolation, Pressurizer Heater Trip 7.1-112
Figure 7.1-1n: ESFAS Emergency Core Cooling System Actuation, Low Temperature Overpressure Protection Actuation 7.1-113
Figure 7.1-1o: Decay Heat Removal System Valve Actuation 7.1-114
Figure 7.1-1p: Main Steam Isolation Valve Actuation. 7.1-115
Figure 7.1-1q: Main Steam Isolation Bypass Valve Actuation 7.1-116
Figure 7.1-1r: Secondary Main Steam Isolation Valve Actuation. 7.1-117
Figure 7.1-1s: Secondary MSIV Bypass Valve Actuation 7.1-118
Figure 7.1-1t: Feedwater Isolation Valve Actuation 7.1-119
Figure 7.1-1u: Feedwater Regulating Valve Isolation. 7.1-120
Figure 7.1-1v: Chemical and Volume Control System RCS Injection and Discharge Valve Actuation 7.1-121
Figure 7.1-1w: Chemical and Volume Control System Pressurizer Spray and High Point Degasification Valve Actuation 7.1-122
Figure 7.1-1x: Containment Flooding and Drain and Containment Evacuation Valve Actuation 7.1-123
Figure 7.1-1y: Reactor Component Cooling Water System Valve Actuation 7.1-124
Figure 7.1-1z: Demineralized Water Supply Valve Actuation 7.1-125
Figure 7.1-1aa: Emergency Core Cooling System Reactor Vent Valve 1 & 2 Actuation 7.1-126
Figure 7.1-1ab: Emergency Core Cooling System Reactor Recirculation Valve Actuation. 7.1-127
Figure 7.1-1ac: Emergency Core Cooling System Reactor Vent Valve 3 Actuation 7.1-128
Figure 7.1-1ad: Reactor Trip Breaker Division I A 7.1-129
Figure 7.1-1ae: Reactor Trip Breaker Division I B 7.1-130
Figure 7.1-1af: Pressurizer Heater Trip Breaker Proportional Heater A 7.1-131
Figure 7.1-1ag: Pressurizer Heater Trip Breaker Proportional Heater B 7.1-132
Figure 7.1-1ah: Loss of AC Power to ELVS Battery Chargers. 7.1-133
Figure 7.1-1ai: Loss of AC Power to ELVS 24 Hour Timers Division I. 7.1-134

LIST OF FIGURES

Figure 7.1-1aj: Loss of AC Power to ELVS 24 Hour Timers Division II 7.1-135
Figure 7.1-1ak: Reactor Trip Breaker Division II A. 7.1-136
Figure 7.1-1al: Reactor Trip Breaker Division II B. 7.1-137
Figure 7.1-1am: Pressurizer Heater Trip Breaker Backup Heater A 7.1-138
Figure 7.1-1an: Pressurizer Heater Trip Breaker Backup Heater B 7.1-139
Figure 7.1-1ao: Actuation Priority Logic Nonsafety Input Control Logic 7.1-140
Figure 7.1-2: Post-Accident Monitoring General Arrangement Drawing 7.1-141
Figure 7.1-3a: Plant Protection System Trip or Bypass Switch Logic. 7.1-142
Figure 7.1-3b: Plant Protection System Loss of Normal Control Room HVAC System AC and Loss of Highly Reliable DC Power System AC 7.1-143
Figure 7.1-3c: Plant Protection System Radiation Monitors and Actuation Logic 7.1-144
Figure 7.1-3d: Plant Protection System Actuation Logic (1 of 3) 7.1-145
Figure 7.1-3e: Plant Protection System Actuation Logic (2 of 3) 7.1-146
Figure 7.1-3f: Plant Protection System Actuation Logic (3 of 3) 7.1-147
Figure 7.1-4: Blocks Selected for Defense-in-Depth Analysis 7.1-148
Figure 7.1-5: Blocks Selected for Defense-in-Depth Analysis 7.1-149
Figure 7.1-6: Four Echelons of Defense within Chosen Blocks 7.1-150
Figure 7.1-7: Common Cause Failure of Division I Safety Display and Indication System 7.1-151
Figure 7.1-8: Common Cause Failure of Safety Block I with Correct Indication 7.1-152
Figure 7.1-9: Common Cause Failure of Safety Block I with False Indication. 7.1-153
Figure 7.1-10: Common Cause Failure of Non-Class 1E Monitoring and Indication 7.1-154
Figure 7.1-11: Digital-Based Common Cause Failure of Level Function Type in Sensor Block I 7.1-155
Figure 7.1-12: Digital-Based Common Cause Failure of Pressure Measuring System Function Type in Sensor Block I and II 7.1-156
Figure 7.1-13: Digital-Based Common Cause Failure of Flow Function Type in Sensor Block I and II 7.1-157
Figure 7.1-14: Direction of Information and Signals between Analysis Blocks 7.1-158
Figure 7.1-15: Basic Control Loop with Example Flawed Control Actions 7.1-159
Figure 7.1-16: Example Module Protection System High Level Control Structure. 7.1-160
Figure 7.1-17: Example Neutron Monitoring System High Level Control Structure 7.1-161
Figure 7.1-18: Safety Function Module Low-Level Logic Structure. 7.1-162
Figure 7.1-19: Basic Module Protection System Configuration. 7.1-163

LIST OF FIGURES

Figure 7.2-1: Instrumentation and Controls Safety System Development Processes. 7.2-72

Figure 7.2-2: NuScale System and Software Technical Development Life Cycle Processes 7.2-73

Figure 7.2-3: NuScale Software Lifecycle Comparisons. 7.2-74

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, which includes safety-related and nonsafety-related 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)
- health physics network (HPN)
- fixed area radiation monitoring (RM)

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

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

Consideration is also given to the attributes of integrated hazard analysis, system architecture, and simplicity in the design of the NuScale Power, LLC I&C 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). This includes 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 Topical Report," (Reference 7.0-3) listed in Table 7.0-2 for application specific action item (ASAI) number 1.

7.0.2 Instrumentation and Control System Classification

NuScale 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 NuScale I&C systems (e.g., PPS, SDIS, MCS, PCS, ICIS, HPN and RM) are classified as nonsafety-related.

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 safety-related MPS and NMS, and a nonsafety-related MCS and ICIS. One nonsafety-related PPS, SDIS, PCS, HPN and RM 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. The classification of I&C systems is also depicted in Figure 7.0-1.

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, providing 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:

- monitors plant variables and trips the reactor when specified setpoints, which are based on the 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
- monitors plant variables and actuates engineered safety features actuation system (ESFAS) equipment when specified setpoints, which are 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 workstation (MWS), and SDIS, and performs monitoring for post-accident monitoring (PAM) functionality.

The MPS is built on the highly integrated protection system platform (See TR-1015-18653-P-A), which is a field programmable gate array (FPGA)-based system. The MPS incorporates the fundamental I&C design principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth as used by TR-1015-18653-P-A. 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 2, 18 and 57. There are no deviations in the application specific NuScale I&C architecture presented in this Chapter from what is described and approved in TR-1015-18653-P-A.

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

- separation group sensor electronics and input panels
- four separation groups of signal conditioning
- four separation groups of trip determination
- manual actuation switches in the main control room
- main control room isolation switches in the remote shutdown station
- Class 1E components to provide isolation from the nonsafety-related highly reliable DC power system (EDSS) power supply
- power supplies for sensors and MPS components, which also provide isolation from the nonsafety-related EDSS
- eight voltage sensors for detecting loss of 480 VAC to the EDSS battery chargers
- four reactor trip breakers and associated cabling
- four pressurizer heater trip breakers and associated cabling
- two nonsafety-related MWSs
- two nonsafety-related MPS gateways
- three nonsafety-related 24-hour timers per division for PAM-only mode
- two divisions of RTS voting and actuation equipment (see Section 7.0.4.1.2)
- two divisions of ESFAS voting and actuation equipment (see Section 7.0.4.1.3)
- four under-the-bioshield temperature sensors

The MPS boundary extends from the output connections of the sensors and detectors to the input connections of the actuated components as 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 as 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.

An SFM performs three main functions:

- signal conditioning
- trip determination
- communication engines

The signal conditioning function is comprised of input modules that are part of the SFM consisting of a signal conditioning circuit, an analog-to-digital converter, and a serial interface. The signal condition function is responsible for conditioning, measuring, filtering, and sampling field inputs.

The trip determination receives process and detector input values in a digital format through a serial interface from the signal conditioning block. The trip determination performs the safety function algorithm and makes a trip determination based on a predetermined setpoint, and provides a trip or not-trip demand signal to each RTS division through isolated, redundant, transmit only, serial connections. The SFM also makes an ESFAS actuation determination based on a predetermined setpoint, and provides an actuate or do-not-actuate demand signal to each ESFAS division through isolated, transmit only, serial connections.

There are two other logic functions within the SFM: monitoring and indication bus (MIB) functionality, and calibration and testing bus (CTB) functionality. The MIB logic function obtains the parameters, trip determination, status, and diagnostic information from each of the core logic paths and provides that to the MIB. The CTB functional logic allows the MWS to update the tunable parameters in nonvolatile memory when the SFM is out of service.

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

The SFM communication engine sends the trip and actuate data to the three safety data buses (SDB1, SDB2, and SDB3) on the chassis backplane and the data is received on the scheduling and bypass modules (SBM SD1, SBM SD2, and SBM SD3). The scheduling and bypass modules (SBMs) are the bus masters of their associated communication bus and are responsible for scheduling the communications. The SFMs are slaves to the SBMs on the safety data communication buses and the MIB-CM on the monitoring and indication communication bus. 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., 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 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 all 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 is received by each division of RTS and ESFAS as shown in Figure 7.0-5.

All status and diagnostics information for the SFM and SBM is provided to the MIB. The MIB communication module 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 communication module also generates an alarm.The MIB communication module 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 communication module also provides a communication path from the MWS to the SFM through the 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 communication module 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. For additional information on access controls of the MWS see Section 7.2.9.1.

An MIB communication module is included for each separation group and each division. A divisional MIB communication module 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 limit as defined by the NuScale Power, LLC, TR-616-49121, "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 (EIM) 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 all 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 with power from EDSS-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 EDSS-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 7.1-1ad through Figure 7.1-1ae and Figure 7.1-1ak through Figure 7.1-1al for the Division I and II reactor trip breakers, respectively.

The RTS also provides manual trip capability. Manual switches in the main control room (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 three sources:

- digital trip signal from the SFM
- 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 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 limit, 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 of the associated ESF system 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 Figure 7.0-7. This 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 that communication bus on the EIM is to demand a trip or actuation of all 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, all four switching outputs from the EIM open, as shown in Figure 7.0-8, 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 trip 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 with power from EDSS-MS. Either action causes pressurizer heater trip breakers to open. The shunt trip circuit and coil are provided as a nonsafety-related, diverse means to open the pressurizer heater trip breakers for increased reliability should

de-energization of the undervoltage coil fail to cause a pressurizer heater trip breaker to open, and nonsafety-related electrical power from EDSS-MS is still available. Power is then removed from the pressurizer heaters. The undervoltage and shunt trip circuits are shown in Figure 7.1-1af through Figure 7.1-1ag and Figure 7.1-1am through Figure 7.1-1an for the proportional and backup pressurizer heater trip 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 7.0-9.

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 SFM
- 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 always can 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, as well as reads the status of the three 24-hour timers. All of 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 7.0-10. There is one MPS gateway for each division.

The EDSS is the power source for the MPS as described in Section 8.1.2.2 and 8.3.2.1.1. 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 EDSS channel, and then distributed to the loads by sharing or auctioneering. Configuration of the EDSS channels and DC-to-DC voltage converters for MPS Division I and separation groups A and C are shown in Figure 7.0-11a. The MPS Division II and separation groups B and D are similar and are shown in Figure 7.0-11b. The EDSS power channels A and C that supply power to MPS Division I are completely independent from EDSS power channels B and D that supply power to MPS Division II and are shown in Figures 8.3-7a and 8.3-7b.

To ensure EDSS batteries supply power for their full mission time of 24 hours for A and D batteries and 72 hours for B and C batteries, only loads associated with maintaining the ECCS valves closed or PAM instrumentation functional remain energized during ECCS hold mode and PAM-only mode. These loads include the MPS and NMS cabinets including power to sensors, ECCS valve solenoids, RM bioshield radiation monitors, and the EDSS battery monitors. If two out of four sensors detect a loss of voltage on both B and C battery charger switchgear, the MPS automatically generates a reactor trip, decay heat removal system (DHRS) actuation, pressurizer heater trip, demineralized water supply isolation, containment isolation, 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 power has not been restored within 24 hours to the B and C battery switchgear, the 24-hour timers time out. At this time, the ESFAS and RTS chassis and MWS for both MPS divisions are automatically de-energized. This action de-energizes the ECCS solenoid trip valves and ECCS is actuated. The PAM instrumentation remains powered by the B and C EDSS batteries for an additional 48 hours (for a total of 72 hours). This configuration is defined as the PAM-only mode.

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 drives, has been disconnected or disabled prior to NPM movement.

- The NMS consists of NMS-excore, NMS-refuel, and NMS-flood.

7.0.4.2.1 Neutron Monitoring System-Excore

Neutron flux level signals generated by the 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 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 across three overlapping detector ranges the source range, intermediate range, and power range.

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

- four wide-range ex-core detectors functioning over the source, intermediate, and power ranges distinguished by processing electronics
- four pre-amplifiers
- NMS-excore cabinets with 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 EDSS power supply

The NMS-excore detectors are qualified to Seismic Category I and located within the operation bays of the Reactor Building (RXB). They are placed outside the containment vessel. The NMS-excore detectors are 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 just outside the containment vessel to monitor neutron flux leakage from the reactor which is directly proportional to reactor power level.

To support NPM movement, the NMS-excore detector support mechanisms are retracted to reposition the NMS-excore detectors away from the containment vessel to allow for NPM movement.

The NMS-excore signal processing cabinets are located in the RXB. Separation Group A and C cabinets are located in the MPS equipment rooms on the 75'0" elevation of the RXB (see Figure 1.2-14). The NMS-excore separation group B and D equipment is located in the MPS equipment rooms on the 86' elevation of the RXB (see Figure 1.2-15). Figure 7.0-12 shows the NMS-excore block diagram.

7.0.4.2.2 Neutron Monitoring System-Refuel

The NMS-refuel detectors are located within the refueling bay of the plant. There is one NMS-refuel subsystem for the plant as 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 five decade range from 10^0 to 10^5 counts per second with a 5 percent sensor accuracy.

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 operating bay and refueling bay.

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, pre-amplifiers, cabling and signal conditioning and processing equipment. The NMS-flood detectors monitor the neutron flux over a range of five decades.

The NMS-flood detectors 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 near the outer wall of the CNV in the retractable supporting structure, common to the NMS-excore detectors. The NMS-flood detectors have the capability to be moved away from the CNV for maintenance. Following maintenance, they are moved into their fixed operating position outside the CNV. During plant startup, the NMS-flood detectors are verified operational. To minimize the activation of the NMS-flood detectors and to protect them during module operation at power, a movable protective shielding sleeve is put in position around the NMS-flood detectors. Upon detection of a flooded containment condition, the protective shielding sleeve is automatically moved away from the NMS-flood detector to allow the detector to sufficiently monitor neutron flux during flooded containment conditions.

The NMS-flood sub-system is powered by the nonsafety-related EDSS, 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 Type B and D post-accident monitoring variable (see Table 7.1-7) and provided to the SDIS to support post-accident monitoring of neutron flux levels.

7.0.4.3 Plant Protection System

The PPS monitors process variables at the plant level and executes actuations in response to normal and off-normal conditions. The PPS monitors and controls systems common to up to 12 NPMs. 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 CRHS and CRVS can be found in Section 9.4.1.

The PPS is built on the highly integrated protection system platform (See TR-1015-18653-P-A) and is an FPGA-based system. Figure 7.0-13 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. Also included in the PPS boundary are the ELVS AC voltage sensors, which are 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.

An individual SFM is included in each division for each function performed by the PPS. Each SFM can accept input from up to four sensors. Signal conditioning is performed to convert the sensor signals into a digital representation. With the digital signals, the SFM performs algorithms and setpoint comparisons necessary to determine if actuation is required for the function. The actuation decision is output to three separate communication buses to provide redundant communication between the SFMs and EIMs. The SFMs also provide communication outputs for parameter values, status information, and alarms to be sent to the PCS and SDIS. Diagnostic information for each SFM is also sent to the MWS.

The architecture of the PPS uses three independent data busses dedicated to actuation signals. The three communication safety data buses (SDB1, SDB2, and SDB3) are each configured in a master-slave communication protocol. The three redundant SBMs (SBM1, SBM2, and SBM3) are the masters for their associated bus and provide the redundant SDB communications from the SFM to the EIM. The SDB1, SDB2, and SDB3 are dedicated to processing the actuation signals.

The MIB communication module is independent of the three SDB communication modules and is the master of the MIB. It processes the information using the same master-slave communication protocol and interfaces with registers on the SFM, communication module, and EIM. These registers are different from the registers that are used for the actuation data path. The MIB communication module uses the MIB to communicate to the CTB communication module to update the MWS. One-way data to the PCS and SDIS are transmitted through the MIB communication module isolated data paths. This interface is designed so that no credible failure of the nonsafety equipment can prevent the PPS from performing its functions.

The CTB communication module is the master of the CTB; however, during normal operation there are no transactions on this bus. The CTB is only active if the channel is removed from service during calibration or changing of parameters. The CTB communication module isolated data path transmits one-way data to the MWS.

An EIM is included in each division for each piece of equipment actuated or monitored by the PPS. Each EIM has two separate logic paths to allow for connection to a "primary" component and a "secondary" component. Each component is connected to two separate EIMs, resulting in two EIMs providing redundant control to each component. This allows an EIM to be taken out of service and replaced online without actuating any equipment.

The actuation signals from the redundant SDBs are combined and delivered to the APL within the EIM. The APL accepts commands from three sources: (1) the digital actuation signal from the SFM, (2) the non-digital manual actuate input signal from its own PPS division, and (3) non-digital manual control signals from the PCS. The non-digital signals are diverse from the digital portion of the PPS. 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 of actions can be initiated at the division level. When the appropriate configuration is enabled by the operator, component-level control can be achieved through the use of the PCS.

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

Each division of PPS has a dedicated MWS. In order to perform maintenance activities, the ability to perform write commands from the MWS to the equipment is required. The process for using the MWS to perform maintenance on the PPS is identical to the process described for the MPS in Section 7.2.9.1.

Each PPS division cabinet has an HWM that accepts external signals and makes them available on the backplane for the other modules. These signals include the manual switches and nonsafety-control signals.

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 to support the ability to initiate protective actions manually, if required. 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 that 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 the data necessary to ensure that 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 interfaces with the MPS and PPS through communication modules. The MPS interface is referred to as an MPS gateway, while the interface with the PPS is through an MIB communication module. 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 7.0-14.

The SDIS hub receives data from the MPS gateway and plant protection system MIB communication module. Each NuScale Power Module's 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 for each SDIS hub rack is aggregated into a single communication module. This module polls each of the communication modules on its rack through the backplane for the rack. The communication module then sends the aggregated information to the PCS through a unidirectional, optically-isolated interface.

The SDIS hub is separated into two chassis of communication modules per division. The first chassis contains the communication modules for MPS associated with NPM 1 through 6 and the PPS communication modules. The second chassis houses the communication modules for only MPS associated with NPM 7 through 12. Both the first and second chassis of communication modules contain a communication module for interfacing with nonsafety systems. The SDIS hubs are located in the PPS rooms. The SDIS hub is shown in Figure 7.0-15.

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. Figure 7.0-16 represents the DIM.

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 on its own 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 the remote shutdown station as described in Section 7.2.13 and Section 7.2.14.

The principal function of the MCS is to control and monitor nonsafety systems and components. This includes nonsafety-related primary and secondary systems, including chemical, utility, and support process systems to the NPM. 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 isolation 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 7.0-17 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 remote shutdown station, and other locations where MCS 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 (HMI) network layer and the control network layer. A one-way deterministic isolation device between the connection from the MCS to the plant network is provided. The one-way deterministic isolation device between the MCS and plant network shown in Figure 7.0-1 transmits network traffic from the MCS to the plant network in one direction only, which is enforced in the hardware design, not software. No software configuration or misconfiguration will cause the boundary device to reverse the direction of data flow.

The MCS uses logic processing in the cases where redundant input/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: A COL applicant that references the NuScale Power Plant design certification is responsible for demonstrating the stability of the NuScale Power Module during normal and power maneuvering operations for closed-loop module control system subsystems that use reactor power as a control input.

The NuScale power plant 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 (MTCS) 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 MTCS
- 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. During load following, operator input via the MCR human-system interface establishes the turbine generation limit. The turbine bypass valves divert 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/unloading by diverting steam flow to and from the turbine bypass valves.

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 valves are closed. During load following, operator input via the MCR HSI establishes the turbine generation limit. The turbine bypass valves divert excess steam energy to the main condenser to limit turbine generation to the generation target. On a turbine trip, turbine bypass valves automatically open 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
- 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 as determined by the secondary system calorimetric. The feedwater regulating valves (FWRV) remain static and opened to the optimum position to support feedwater pump speed control.

Feedwater Regulating Valve Control

The feedwater regulating valve 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 flow
- RCS boron concentration
- RCS average coolant temperature
- CVCS letdown line flow
- CVCS makeup line flow
- CVCS makeup boron concentration
- source, intermediate and power range nuclear instrumentation
- main steam line flow

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
- BAS 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 BAS to raise RCS boron concentration. CVCS letdown flow is discharged to the liquid radwaste system (LRWS) 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 LRWS. 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 three groups of pressurizer heaters are used to raise pressurizer pressure based on the deviation from the normal operating pressure of 1850 psia. One group of pressurizer heaters uses modulating proportional control, and two other groups of pressurizer heaters are 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
- reactor power

During normal power operation, pressurizer water level control is achieved using the CVCS makeup and letdown flows. The CVCS makeup and letdown flow rates are adjusted to maintain pressurizer level on a ramped linear program from 50 percent level at 0 percent reactor power to 60 percent level at 100 percent reactor power.

7.0.4.5.1 Module Control System Segmentation

Segmentation is used in the MCS architecture to provide functional independence between major control functions. The segmentation is a key defensive and preventive measure against a failure in one controller group from causing an undesirable condition in another controller group. Preventive and limiting measures are determined by a susceptibility analysis that considered malfunctions and spurious actuations, as set forth in NRC DI&C-ISG-04, Section 3.1, staff position 5. The purpose of the susceptibility analysis is to identify control groups that may lead to the following effects:

- reactivity addition to the reactor coolant system
- primary coolant pressure increase or decrease
- primary coolant temperature increase or decrease
- primary coolant level increase or decrease
- radioactive material release to the environment

The MCS control architecture is separated into multiple control segments based on their functions. The major MCS control segments are described below for those segments that have a direct impact on the effects listed above and serve functions relating to power generation; protection of plant assets; remove fuel assembly heat; reactivity control; and radioactivity control:

- CVCS, CFDS, and DHRS segments - The chemical and volume control system (CVCS), containment flooding and drain system (CFDS), and the decay heat removal system (DHRS) use the same segment of the MCS for automatic and remote control functions. Major control functions of the CVCS within the MCS include the makeup of either borated or demineralized water into the reactor coolant system (RCS), the letdown of used coolant into the liquid radwaste management system, and the degasification and pressurizer spray within the pressurizer. Due to concerns with postulated digital-based common cause failures (CCFs) of the CVCS control functions on this segment, the CVCS letdown function is separated onto its own separate, independent control segment. The major control function of the CFDS within the MCS is opening and closing the NPM-specific isolation valve that provides the inlet to the containment module. The inlet of the piping into the NPM containment is isolated by a containment isolation valve, which is controlled by the safety-related MPS. There are no control functions of the DHRS provided by the MCS; only indications are provided for certain variables. Control functions for the DHRS are provided by the MPS.

- RCS, CFWS, MSS, and RCCWS segment - The RCS, condensate and feedwater system (CFWS), main steam system (MSS), and reactor component cooling water system (RCCWS) use the same segment of the MCS for automatic and remote control functions.
- CRDS segment - The control rod drive system (CRDS) uses its own segment of the MCS for automatic and remote control functions. The CRDS control processor does not control the individual mechanics of each rod's movement; rather, the CRDS control processor provides supervisory control and data acquisition to the power converter and control assembly cabinets which is in the scope of the CRDS. Rod withdrawal is performed by an operator, although supervisory control of rod insertion may be performed by the MCS controller if reactor power demand requires rod insertion to reduce power. Automatic rod withdrawal may not be performed when thermal reactor power is between zero and 15 percent.
- TGS and EHVS segment - The turbine generator system (TGS), and 13.8 kV and switchyard system (EHVS) use the same segment of the MCS for automatic and remote control functions. For the EHVS, the MCS only controls the breaker that connects the turbine generator to the off-site customer loads. For the TGS, the MCS provides supervisory control and data acquisition services to the packaged control system, which is included with the TGS, as well as a means to interface the operators in the MCR with each TGS.

7.0.4.5.2 Postulated digital-based Common Cause Failure Evaluation of the Module Control System

Evaluation of Digital-Based CCFs of the CVCS, CFDS, and DHRS Segment of the MCS

The digital-based failure scenarios were analyzed for the CVCS, CFDS and DHRS segments of the MCS. To preclude digital-based CCF of the CVCS segment related to the CVCS letdown and makeup functions, the CVCS letdown function is allocated to a separate, independent segment. The separation of CVCS letdown, makeup and CVCS pressure control on to different MCS segments precludes postulated digital-based CCFs causing events that are not bounded by the plant safety analysis.

CVCS letdown segment failure 1: Postulated failures are limited to the CVCS letdown function and are bounded by the design basis event analyses for increases in reactor coolant inventory (see Section 15.5) and decreases in reactor coolant inventory (Section 15.6).

CVCS, CFDS, and DHRS segment failure 1: A digital-based CCF of this segment is postulated to result in maximum dilution of boron during startup operations, which would be the worst case reactivity addition event in this segment. The analysis for the inadvertent decrease in reactor coolant system boron concentration envelopes Modes 1 through 5, and therefore, bounds all postulated dilution scenarios with this segment (see Section 15.4.6).

Evaluation of Digital-Based CCFs of the RCS, CFWS, MSS, and RCCWS Segment of the MCS

The most-limiting failure scenarios were analyzed for the RCS, CFWS, MSS, and RCCWS segments of the MCS. The results are summarized below.

RCS, CFWS, MSS, and RCCWS segment failure 1: A digital-based CCF in this segment is postulated to cause a reactivity addition event by causing the feedwater pumps to generate excessive feedwater flow to the steam generator while the reactor is in power operation.

The reactivity addition due to increase in feedwater flow is bounded by the design basis analysis of the increase in feedwater flow (see Section 15.1.2).

RCS, CFWS, MSS, and RCCWS segment failure 2: A digital-based CCF is postulated to cause both secondary main steam isolation valves to close while at 100 percent rated thermal power (RTP). This will cause a decrease in heat removal event. Additionally, because the pressurizer heaters are controlled by this segment, the failure also causes all the pressurizer heaters to be continuously energized even when the setpoint to secure the heaters is exceeded. The pressurizer heaters will add to the RCS pressure rise. However, the pressurizer spray valve is expected to operate since this control is not part of this segment.

The postulated failure is bounded by the design basis analysis of the closure of the main steam isolation valve (See Section 15.2.4).

Although the analysis assumes that the pressurizer heaters remain at their initial steady-state output level, the postulated heater controller failure at "high output" is considered to be inconsequential to the outcome of the analysis. This is because of generation of an early DHRS actuation signal by the MPS, which de-energizes all three banks of the pressurizer heaters. Furthermore, the allowed credit for spray actuation in best-estimate analysis offsets the impact of the pressurizer heater malfunction prior to their MPS-based de-energization.

RCS, CFWS, MSS, and RCCWS segment failure 3: A digital-based CCF is postulated to cause both feedwater regulating valves to close while at 100 percent power. The effect of this failure is similar to the failure described above in that it will cause a decrease in heat removal event. Because the pressurizer heaters are controlled by this segment, the failure also causes all the pressurizer heaters to be continuously energized even when the setpoint to secure the heaters is exceeded. The pressurizer heaters will add to the RCS pressure rise. However, the pressurizer spray valve is assumed to operate since this control is not part of this segment.

RCS, CFWS, MSS, and RCCWS segment failure 4: In this failure scenario, a digital-based CCF is postulated to occur during an increase in reactor power where the pressurizer heaters do not energize when the RCS pressure declines below the setpoint for turning on the pressurizer heaters. This is an RCS pressure decrease event.

In this scenario, the pressurizer heaters are not credited to arrest the depressurization rate associated with RCS cooldown events. Furthermore, the failure of the pressurizer heaters to energize as an initiating event is not a design-basis accident presented in Chapter 15 or evaluated as a part of the normal operational transients. This event would result in a reactor trip on low pressurizer pressure or level which is bounded by other RCS overcooling scenarios (see Section 15.1).

Evaluation of Digital-Based CCFs of the CRDS Segment of the MCS

The two most-limiting failure scenarios were analyzed for the CRDS segment of the MCS. The results are summarized below.

CRDS segment failure 1: A digital-based CCF in this segment causes continuous rod withdrawal at the maximum rate of 15 inches per minute of the regulating control rod group. The reactor is critical at 100 percent power and the regulating group is at the power dependent insertion limit (PDIL). This postulated scenario is bounded by the analysis of the rod withdrawal event at power, subcritical, or low-power operation (see Sections 15.4.1 and 15.4.2).

CRDS Segment Failure 2: A digital-based CCF in this segment is postulated to cause the insertion of the regulating or shutdown groups into the core (beyond the PDIL for the regulating bank or allowed insertion steps for the shutdown groups). This postulated failure is not expected to create a new unanalyzed event scenario due to the availability of early indications in the control room (e.g., rod position indication and control rod deviation alarms)

Rod position indication is a variable controlled by the Technical Specifications and off normal condition indications in the control room would alert operators to take appropriate actions. To provide defense-in-depth, the rod position indication function is contained on a separate segment from the CRDS segment of the MCS.

Evaluation of Digital-Based CCFs of the TGS and EHVS Segment of the MCS

The two limiting failure scenarios were analyzed for the TGS and EHVS segment of the MCS. The results are summarized below.

TGS/EHVS segment failure 1: A digital-based CCF in this segment is postulated to cause the turbine bypass valve to spuriously open completely during 100 percent power, resulting in an increase in heat removal event. This postulated failure is bounded by the increase in steam flow design basis analysis event (see Section 15.1.3).

TGS/EHVS segment failure 2: A digital-based CCF in this segment is postulated to cause the turbine generator output breaker to open during 100 percent full power operation, and the turbine bypass valve remains closed. This failure results in a decrease in heat removal by the secondary side event. This postulated failure is bounded by the design basis analysis of the Loss of External Load, Turbine Trip, Loss of Condenser Vacuum (see Section 15.2). The turbine bypass function is a

nonsafety-related function and as such, it is not credited in the design-basis accident analysis.

7.0.4.5.3 Preventive and Limiting Measures Used in the Module Control System

The segmentation of major control functions represents a key defensive and preventive measure in the NuScale Power Plant MCS design. Measures are also taken to prevent and limit the effects of MCS software design errors that could result in spurious control actions. The following preventive and limiting measures are used in the overall NuScale MCS I&C architecture to protect against a CCF in the process control systems.

- Enable nonsafety control switch — While discrete actuations may be sent from the nonsafety process control systems, the use of the safety-related enable nonsafety control switch is required in order for actuation signals to pass through to the safety-related actuation logic, which is prioritized such that the safety-related actuations are passed in the absence of a required protective action. Because a second, positive operator action is required to perform this actuation, this measure is preventive in nature in accordance with DI&C-ISG-04, Section 3.1, staff position 5.
- Network handling of messages — Three networking layers comprise the MCS architecture of the process control systems: the HMI layer, the control network layer, and the input/output network layer. The platform servers for the MCS act as an interface between the control network and the HMI network.
- Automatic control within MCS — In the case where the process control system uses closed-loop control across multiple networked processors, but within the same control system, the network signal path follows the data acquisition from an analog (e.g., 4-20 mA) input card or from a discrete input card based on the state of a process sensor. The process variable is first input to the remote input/output cards, after which it is sampled and held in the firmware for the remote input/output rack. The firmware converts the digital value corresponding to the 4-20 mA signal that is sent by the remote input/output protocol to the sensing segment processor, which is communicated to another processor by the control network protocol as input to the calculation of the control variable. The process variable is processed by the control algorithm within the necessary control processor, then the input/output network receives the control variable from the control processor, which then sends a converted digital-to-analog (e.g., 4-20 mA) output to the final control element corresponding to the processed control variable. Figure 7.0-18 depicts a block diagram of the signal handling for this type of control. In the case of a final control element which is placed into an open or closed state only (i.e., "discrete"), the digital value corresponding to the "open" or "closed" command is sent to the actuator. A signal is applied to the actuator from its input/output card, which opens or closes the actuator, based on an input sensor state (in the case of a discrete input) or based on the comparison of an input process variable to a setpoint held in the processing logic for the actuator.
- Automatic control shared between the MCS and the PCS — In the case where the process control system uses closed-loop control across multiple networked processors, but within the same control system, the network signal path

follows the data acquisition from an analog (e.g., 4-20 mA) input card. The process variable is first input to the remote input/output cards, after which it is sampled and held in the firmware for the remote input/output rack. The firmware converts the digital value corresponding to the 4-20 mA signal, then is sent via the remote input/output protocol to the sensing segment processor, which is communicated to another processor via the control network protocol as input to the calculation of the control variable. The process variable is processed by the control algorithm within the necessary control processor, then the input/output network receives the control variable from the control processor, which then sends a converted digital-to-analog (e.g., 4-20 mA) output to the final control element corresponding to the processed control variable. Figure 7.0-19 depicts a block diagram of the signal handling for this type of control. In the case of a final control element which is placed into an open state or closed state only (i.e., "discrete"), the digital value corresponding to the "open" or "closed" command will be sent to the actuator. A signal is applied to the actuator from its input/output card, which opens or closes the actuator based on an input sensor state (in the case of a discrete input) or based on an input process variable comparison to a setpoint held in the processing logic for the actuator. The process systems supported by both the MCS and the PCS, which share information and control signals between the MCS and PCS, are not systems that would immediately or directly affect reactor criticality. They are primarily systems which are utility in nature; that is, systems which provide heating, cooling, water, air, chemical, or power to the process systems.

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 7.0-20 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 remote shutdown station, and other locations where PCS HSIs 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 HMI network layer and the control network layer. A one-way deterministic isolation device between the connection from the PCS to the plant network is provided. The one-way deterministic isolation device between the PCS and plant network shown in Figure 7.0-1 transmits network traffic from the PCS to the plant network in one direction only, which is enforced in the hardware design, not software. No software configuration or misconfiguration will cause the boundary device to reverse the direction of data flow.

The PCS uses logic processing in the cases where redundant input/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.

7.0.4.6.1 Plant Control System Segmentation

Segmentation is used in the PCS control architecture to provide functional independence between major control functions. The segmentation is a key defensive preventive measure against a failure in one controller group from causing an undesirable condition in another controller group. Preventive and limiting measures are determined by a susceptibility analysis that considers malfunctions and spurious actuations, as set forth in NRC DI&C-ISG-04, Section 3.1, staff position 5. The purpose of the susceptibility analysis is to identify control groups that may lead to the following effects:

- reactivity addition
- primary coolant pressure increase or decrease
- primary coolant temperature increase or decrease
- primary coolant level increase or decrease
- radioactive material release to the environment

The PCS control architecture is separated into multiple control segments based on their functions. The major PCS control segment subject to a coping analysis is described below. This segment has a direct impact on the effects listed above and serves functions relating to protection of plant assets, human habitability, and radioactivity control as follows:

- EHVS, EMVS, and ELVS Segment — The EHVS, medium voltage AC electrical distribution system (EMVS), and ELVS use the same segment of the PCS for automatic and remote control functions. For the EHVS, the PCS controls each breaker except for the breaker that connects the turbine generator to the off-site customer loads.

7.0.4.6.2 Postulated digital-based Common Cause Failure Evaluation of the Plant Control System

Evaluation of Digital-Based CCFs of the EHVS, EMVS, and ELVS Segment of the PCS

The two most-limiting failure scenarios were analyzed for the EHVS, EMVS and ELVS segments of the PCS. The results are summarized below.

EHVS/EMVS/ELVS segment failure 1: A digital-based CCF is postulated to cause the following breakers to open simultaneously during power operations:

- Site Cooling Water Pumps
- Cooling Tower Fans
- Circulating Water Pumps

- Chiller packages

This failure results in a loss of the normal balance-of-plant heat sink and therefore is considered a decrease in heat removal event. This failure results in a loss of condenser vacuum on all operating turbine generators. The loss of the chiller packages would cause a loss of HVAC cooling. The postulated failure impacts multiple modules and results in a turbine trip due to loss of condenser vacuum, which is addressed in the design basis Loss of Condenser Vacuum Analysis (see Section 15.2.3). HVAC cooling is a nonsafety-related function and is not credited in the design basis accident analysis for environmental qualification of mechanical or electrical equipment and systems.

EHVS/EMVS/ELVS segment failure 2: A digital-based CCF in this segment is postulated to cause all the EHVS switchyard breakers to open simultaneously, causing a loss of normal AC power during power operations. The loss of offsite EHVS distribution system translates into the Loss of External Load design basis event which is analyzed in Section 15.2.1. The postulated scenarios are bounded by the consideration of loss of power coincident with an initiating event or decrease in secondary heat removal initiated by equipment failures (e.g. Loss of Feedwater, Turbine Trip, Loss of Condenser Vacuum, see Section 15.2).

7.0.4.6.3 Preventive and Limiting Measures Used in the Plant Control System

The segmentation of major control functions represents a key defensive measure in the PCS design. Measures are also taken to prevent and to limit the effects of a PCS software design errors that could result in spurious control actions. The following preventive and limiting measures were used in the overall NuScale PCS I&C architecture to be hardened against a CCF in the process control systems:

- Enable nonsafety control switch — same as for MCS, see Section 7.0.4.5.3
- Network handling of messages — Three networking layers comprise the PCS architecture of the process control systems: the HMI layer, the control network layer, and the input/output network layer. The HMI layer consists of the PCS power operations HMI network, and the PCS radwaste handling HMI network. The separations of function between the PCS power operations and radwaste handling functions prevent input from the waste management control room from adversely affecting power operations. The platform servers for the PCS act as an interface between the control network and the HMI network.
- Automatic control within PCS — same as for MCS, see Section 7.0.4.5.3
- Automatic control shared between the MCS and the PCS — same as for MCS, see Section 7.0.4.5.3

7.0.4.7 In-core Instrumentation System

The ICIS monitors the neutron flux distribution within the reactor core and provides core inlet and exit temperature information to the MPS for monitoring core cooling during post-accident conditions. The neutron flux information is also used to verify operation and calibrate the NMS-excore detectors. The ICIS has the ability to 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 also provides a pressure boundary for the RPV which is a safety-related function as described in Section 7.1.1.2.8.

The ICIS includes:

- self-powered neutron detectors located in the reactor core for monitoring neutron flux.
- thermocouples located at the inlet and exit of the core to provide temperature information to the MPS for monitoring post-accident conditions.
- instrument assemblies in which the neutron detectors and thermocouples are housed.
- signal conditioning and processing electronics.

The in-core instrumentation system has a total of six detectors integral to each instrument assembly. There are four self-powered neutron detectors and two thermocouples. The neutron detectors are equally spaced 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 mineral-insulated, pressure-retaining cabling which contains the in-core instrumentation assemblies. Section 4.3.2 provides additional information on the in-core instrumentation system. Figure 4.3-18 provides the ICIS core locations.

7.0.4.8 Health Physics Network

The HPN is used to interconnect the radiological controls equipment as part of the Operational Radiation Protection Program, which is established to provide an effective means of radiation protection for station personnel, visitors, and the general public.

The principal function of the HPN is to provide the permanently installed communications infrastructure necessary to support the Operational Radiation Protection Program.

The HPN includes communications cabling and equipment mounting racks.

For more information on radiation protection, see Chapter 12.

7.0.4.9 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:

- continuously 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 that are 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," TR-1015-18653-P-A, Rev. 2.

7.0-4 NuScale Power, LLC, "NuScale Instrument Setpoint Methodology Technical Report," TR-616-49121, Rev. 0.

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

Regulatory Requirements and Guidance	Applicable DCD 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
10 CFR																				
50.34(b)(2)(i)													x							
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		
50.34(f)(2)(xiv)					x															
50.34(f)(2)(xix)																		x		
50.36(c)(l)(ii)(A)												x								
50.36(c)(3)												x								x
50.49							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															
52.47(a)(2)													x							
GDC 1						x														
GDC2							x													
GDC4							x													
GDC 5																x				
GDC 10	x																			
GDC 13		x		x	x							x						x		
GDC 15	x																			
GDC 16	x																			
PDC 19	x																	x		
GDC20	x											x								
GDC21		x	x	x																x
GDC22		x			x															

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

Regulatory Requirements and Guidance	Applicable DCD 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
GDC24		x	x		x															
GDC 25																				
GDC 28																				
GDC29				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 1.97																		x		
RG 1.100																		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 1.175		x												x						
RG 1.180							x													
RG 1.204							x													
RG 1.209							x													
IEEE Std 603-1991																				
4.1	x																			
4.2	x																			

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

Regulatory Requirements and Guidance	Applicable DCD 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
4.3	x																			
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

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

Regulatory Requirements and Guidance	Applicable DCD 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
6.6									x											
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														
RIS 2006-17												x								
GL 91-04												x								

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

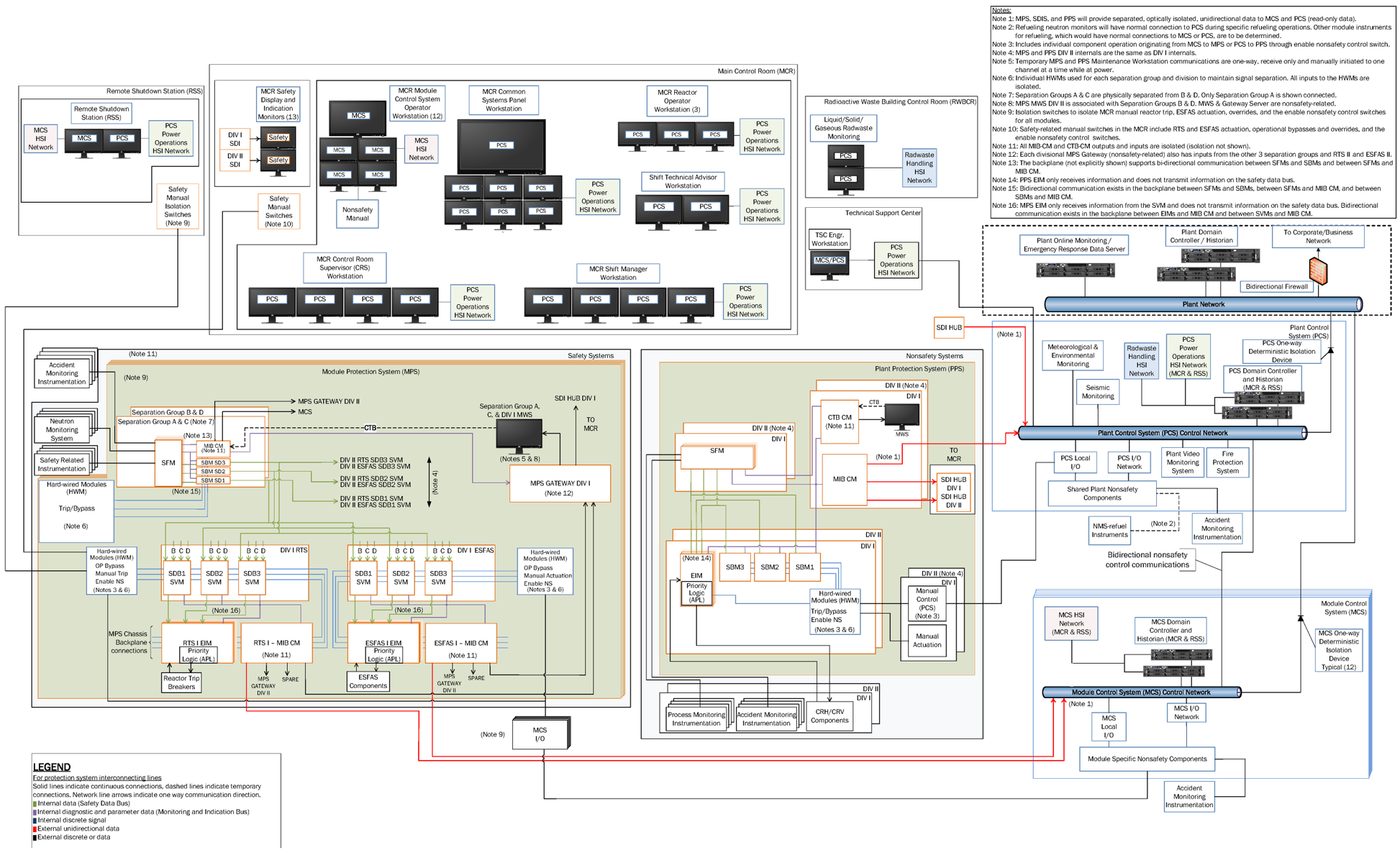
HIPS TR Application Specific Action Item Number	Section 7.0 - Introduction and Overview				Section 7.1- Fundamental Design Principles								Section 7.2 - System Characteristics													
	7.0.1	7.0.2	7.0.3	7.0.4	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.1.6	7.1.7	7.1.8	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	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 (HIPS TR) 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	7.1.6	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 ASAIs 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.

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



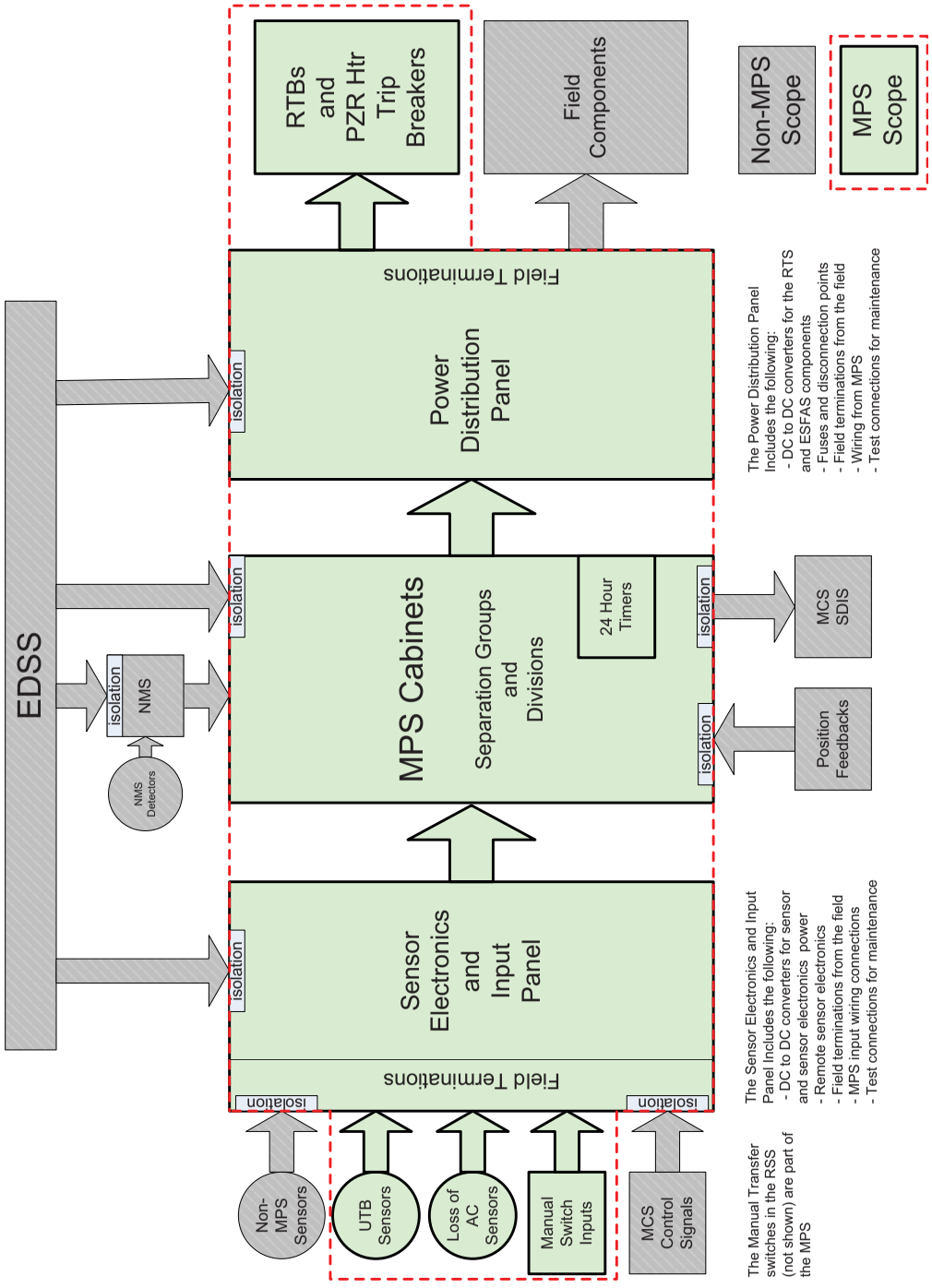


Figure 7.0-2: Module Protection System Boundaries

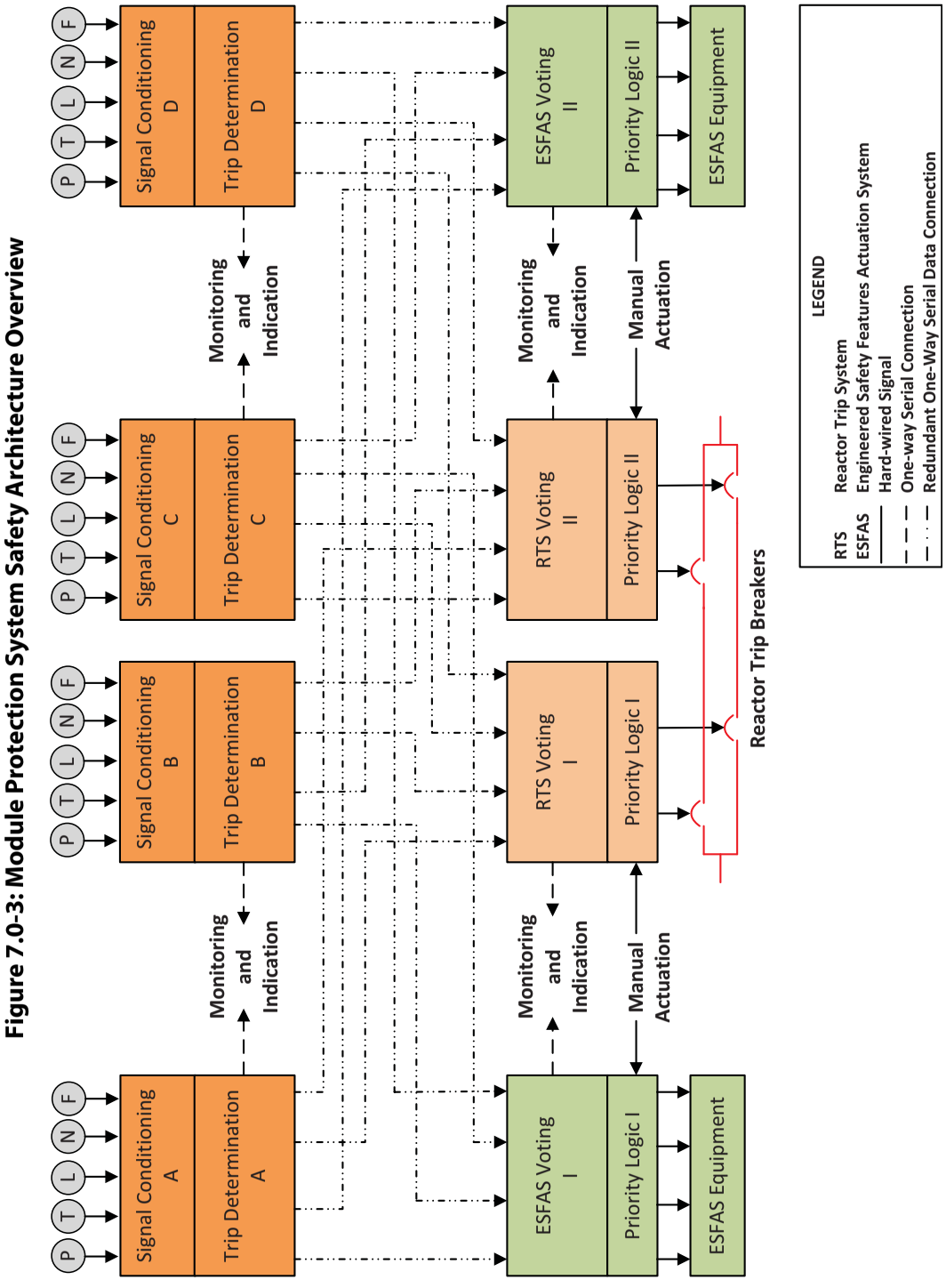


Figure 7.0-3: Module Protection System Safety Architecture Overview

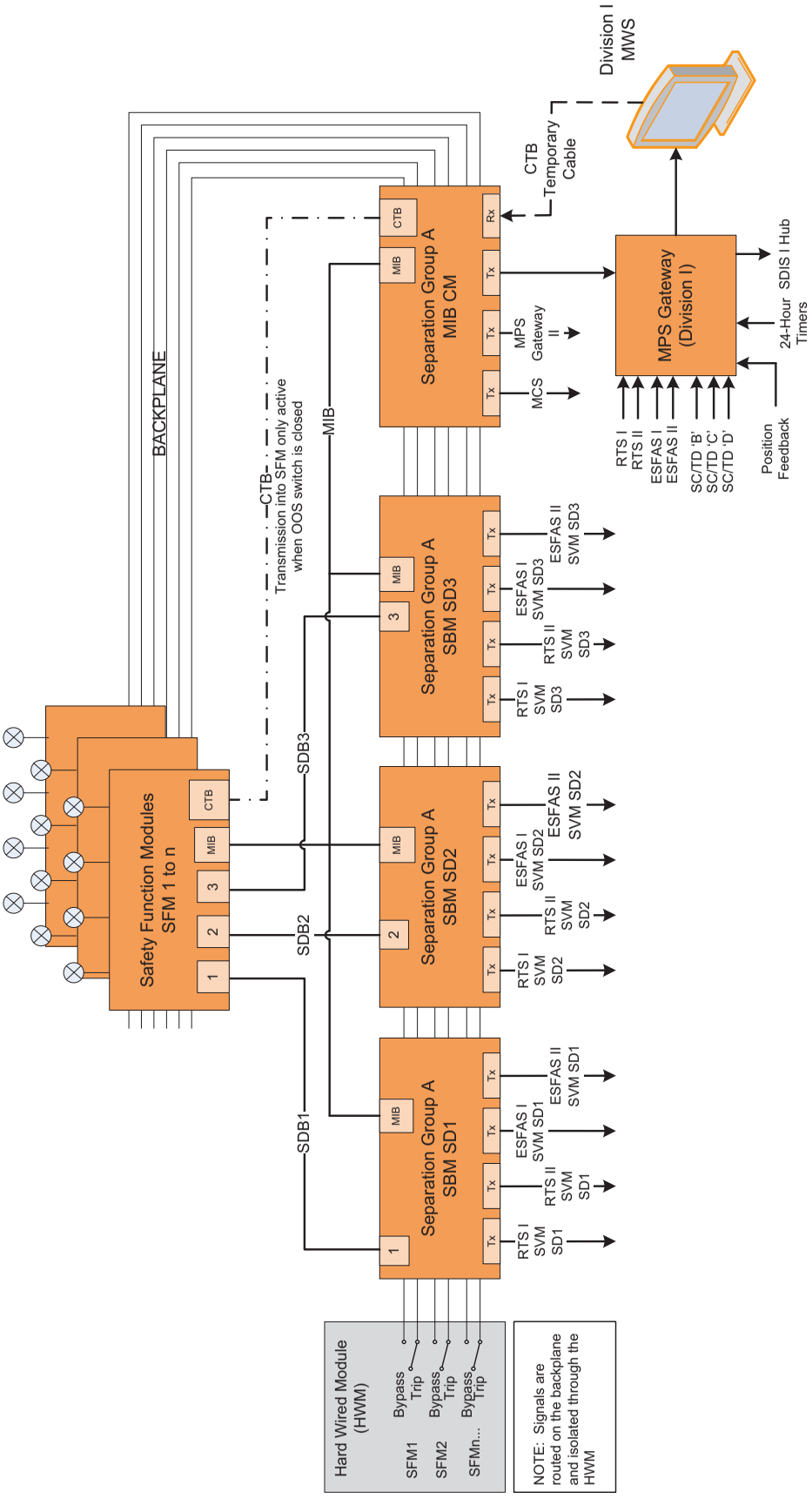


Figure 7.0-4: Separation Group A Communication Architecture

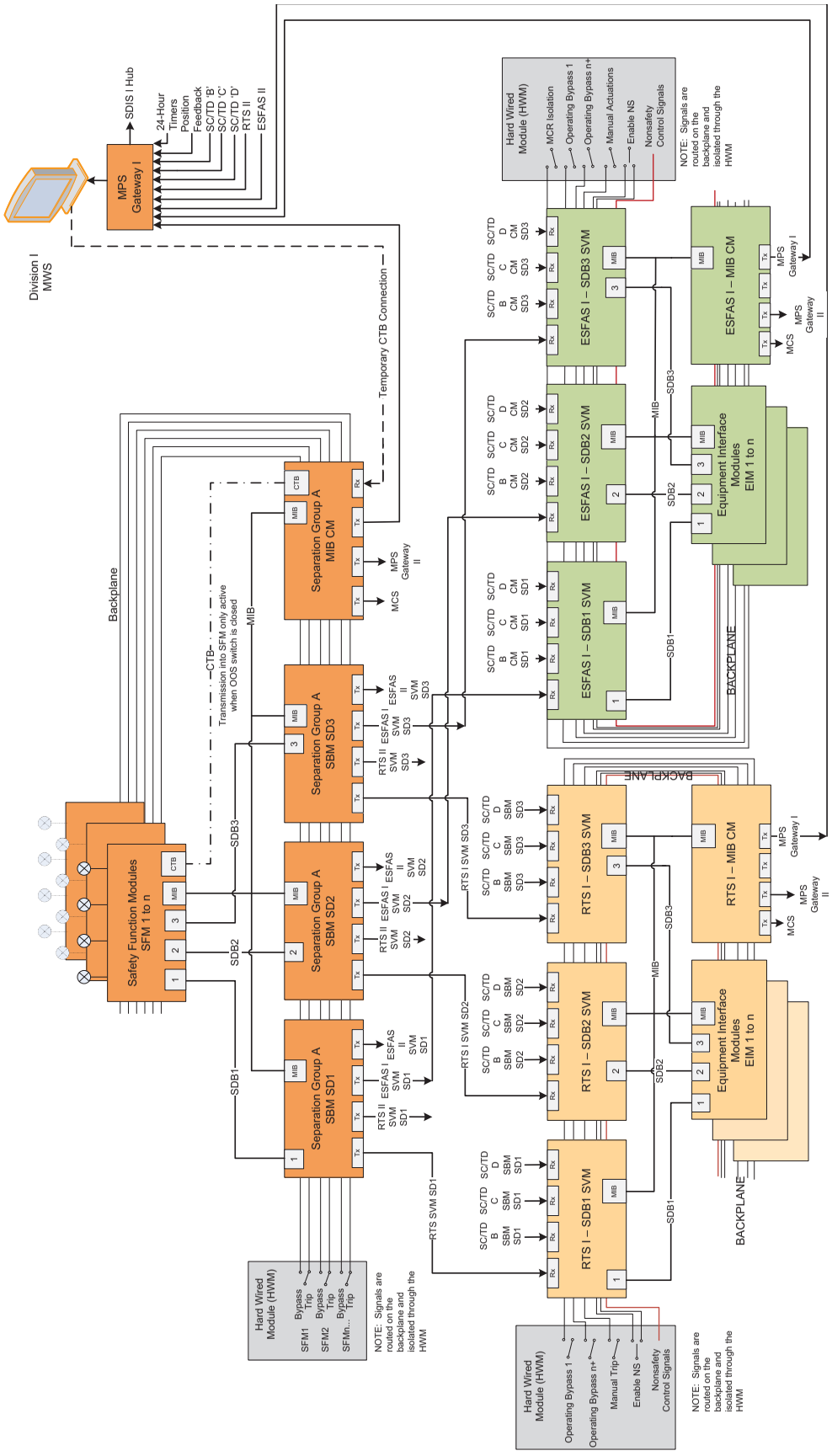


Figure 7.0-5: Separation Group A and Division I Reactor Trip System and Engineered Safety Features Actuation System Communication Architecture

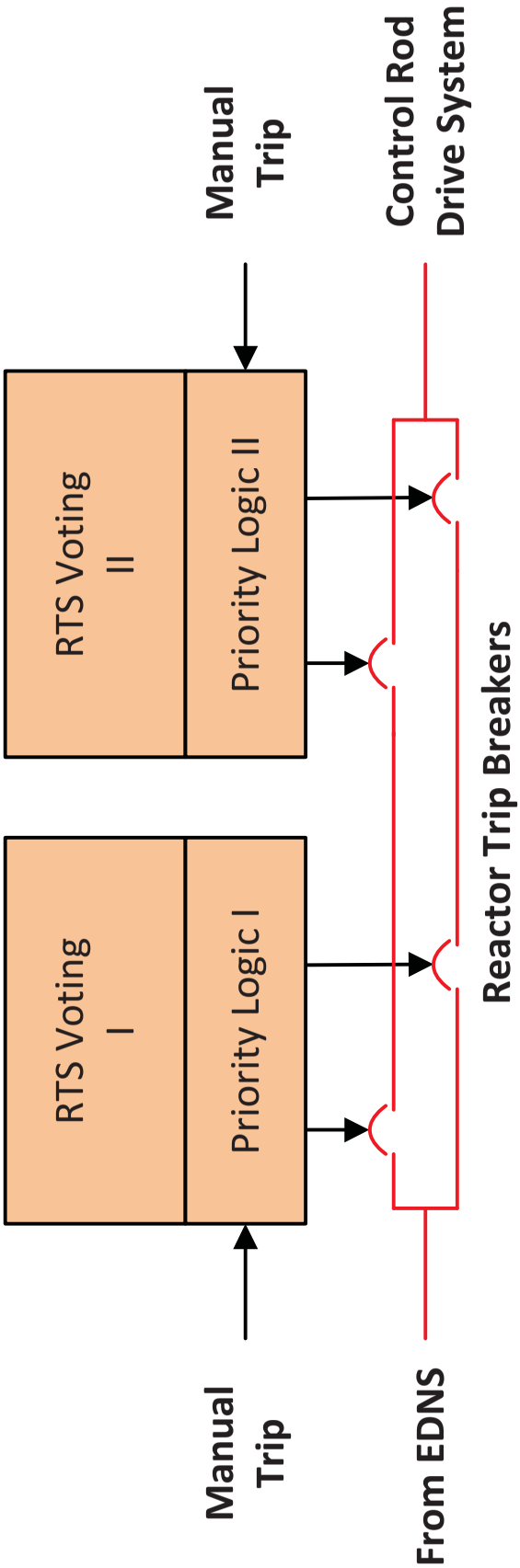


Figure 7.0-6: Reactor Trip Breaker Arrangement

Figure 7.0-7: Equipment Interface Module Configuration

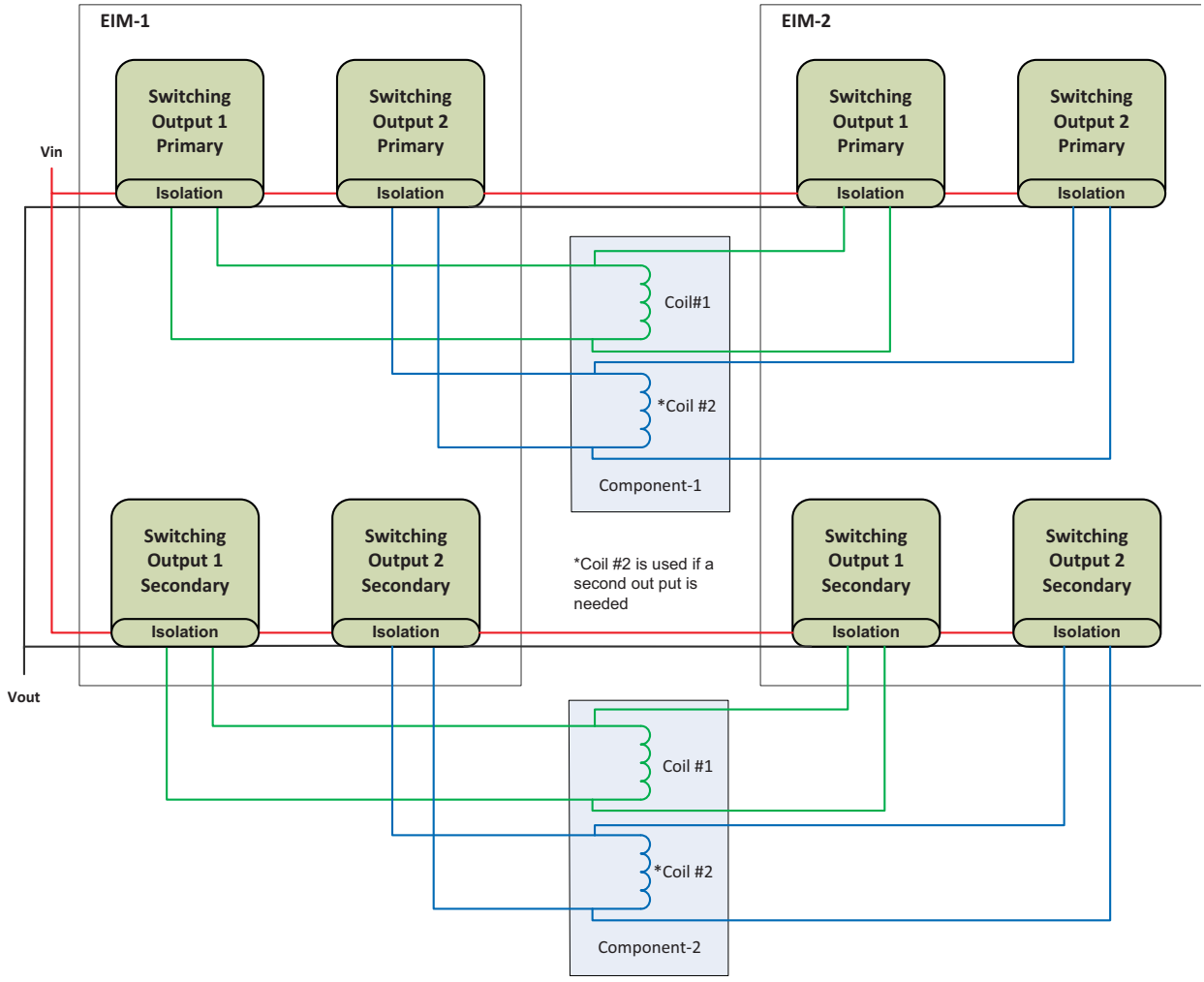
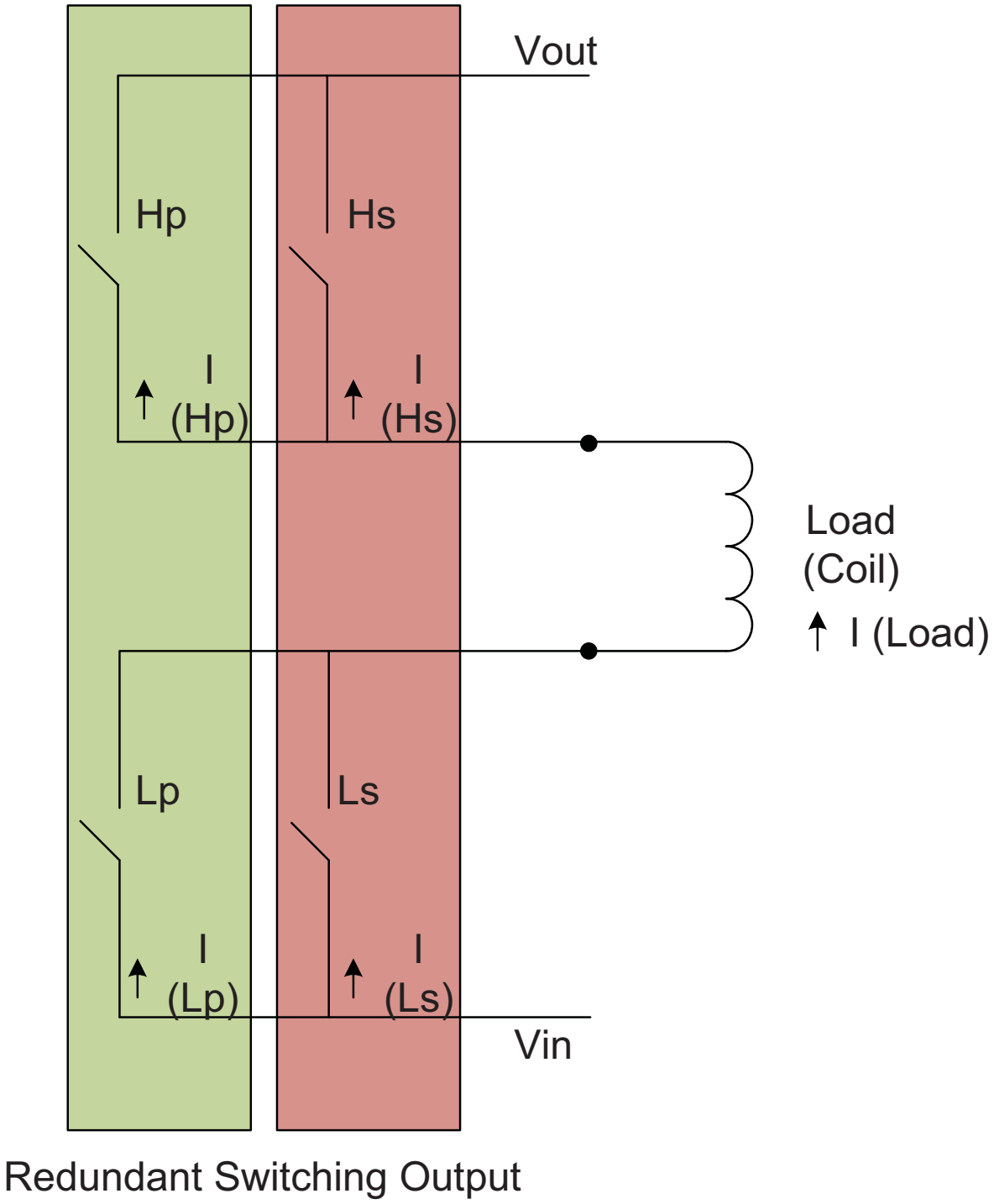


Figure 7.0-8: Equipment Interface Module Output



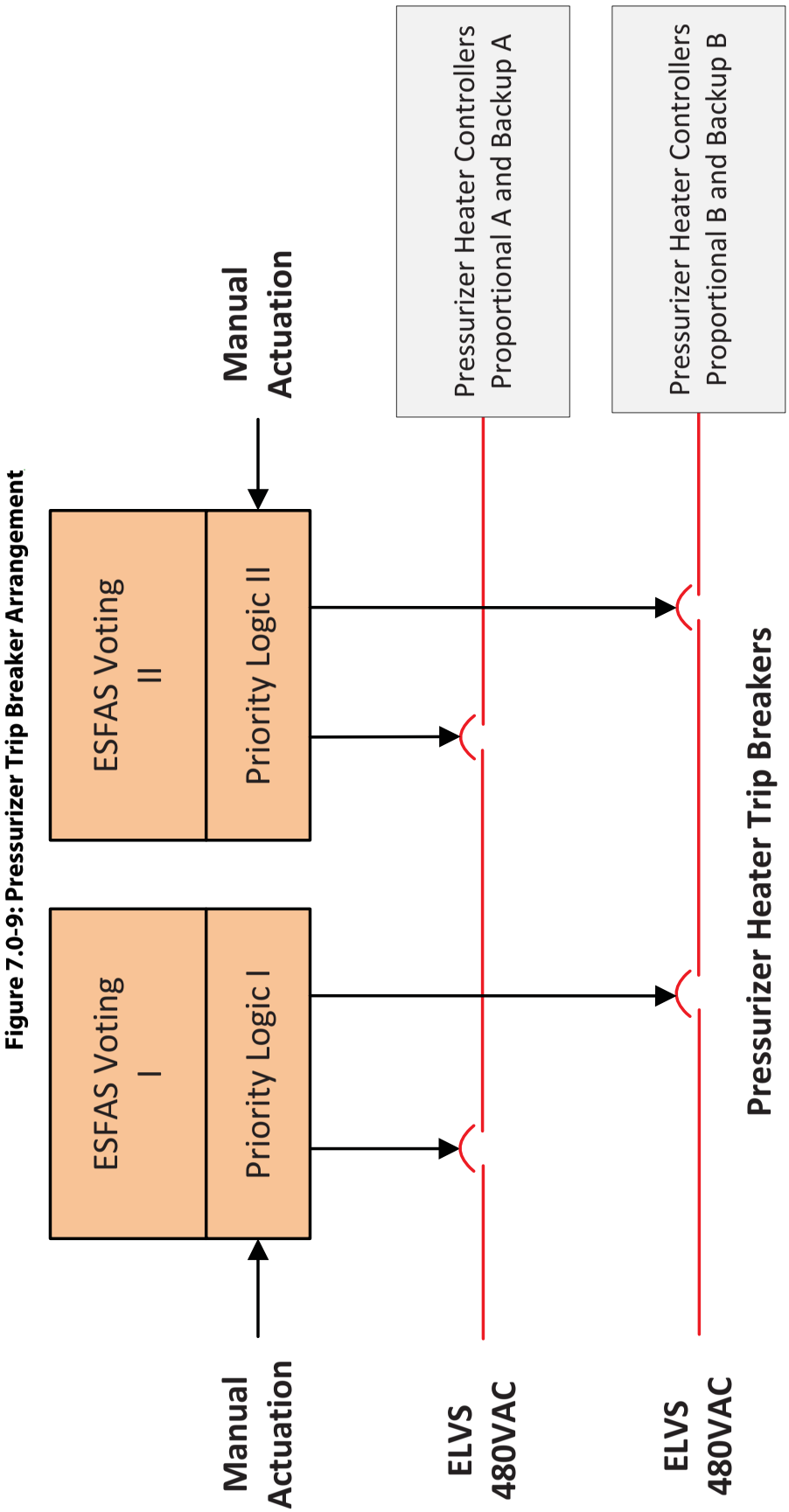


Figure 7.0-9: Pressurizer Trip Breaker Arrangement

Figure 7.0-10: Module Protection System Gateway Diagram

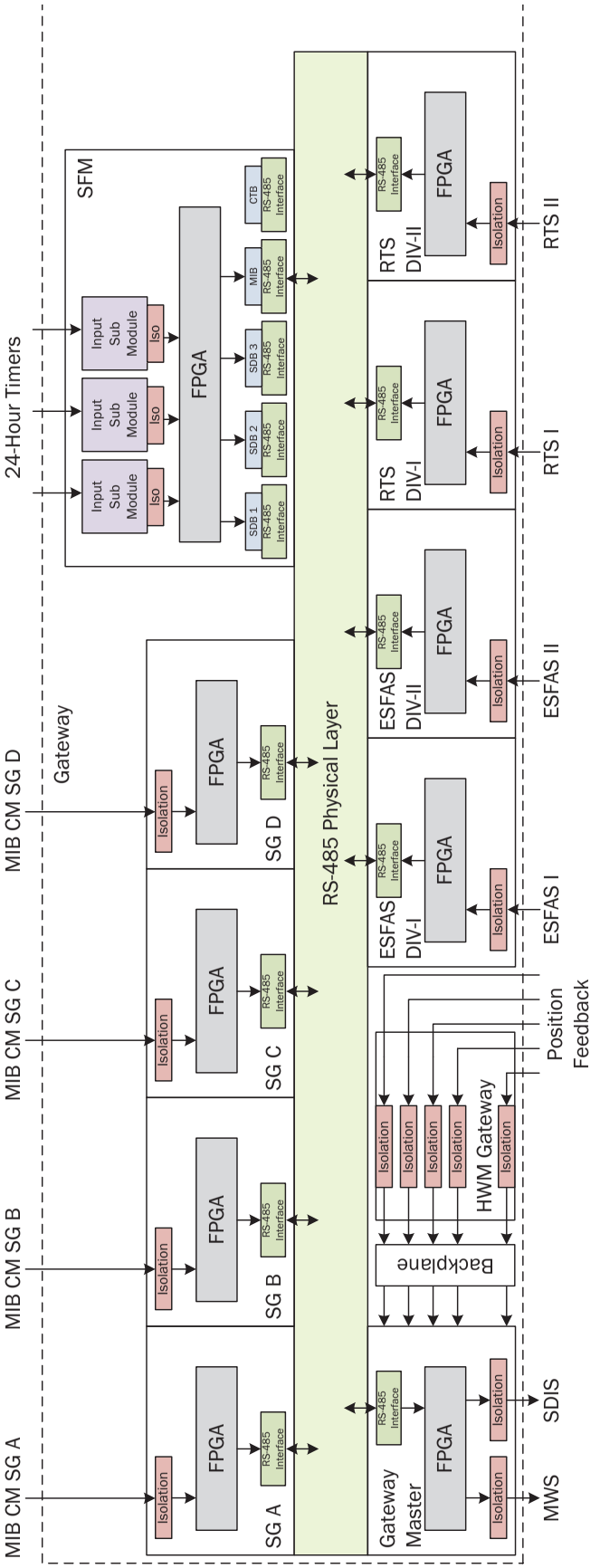
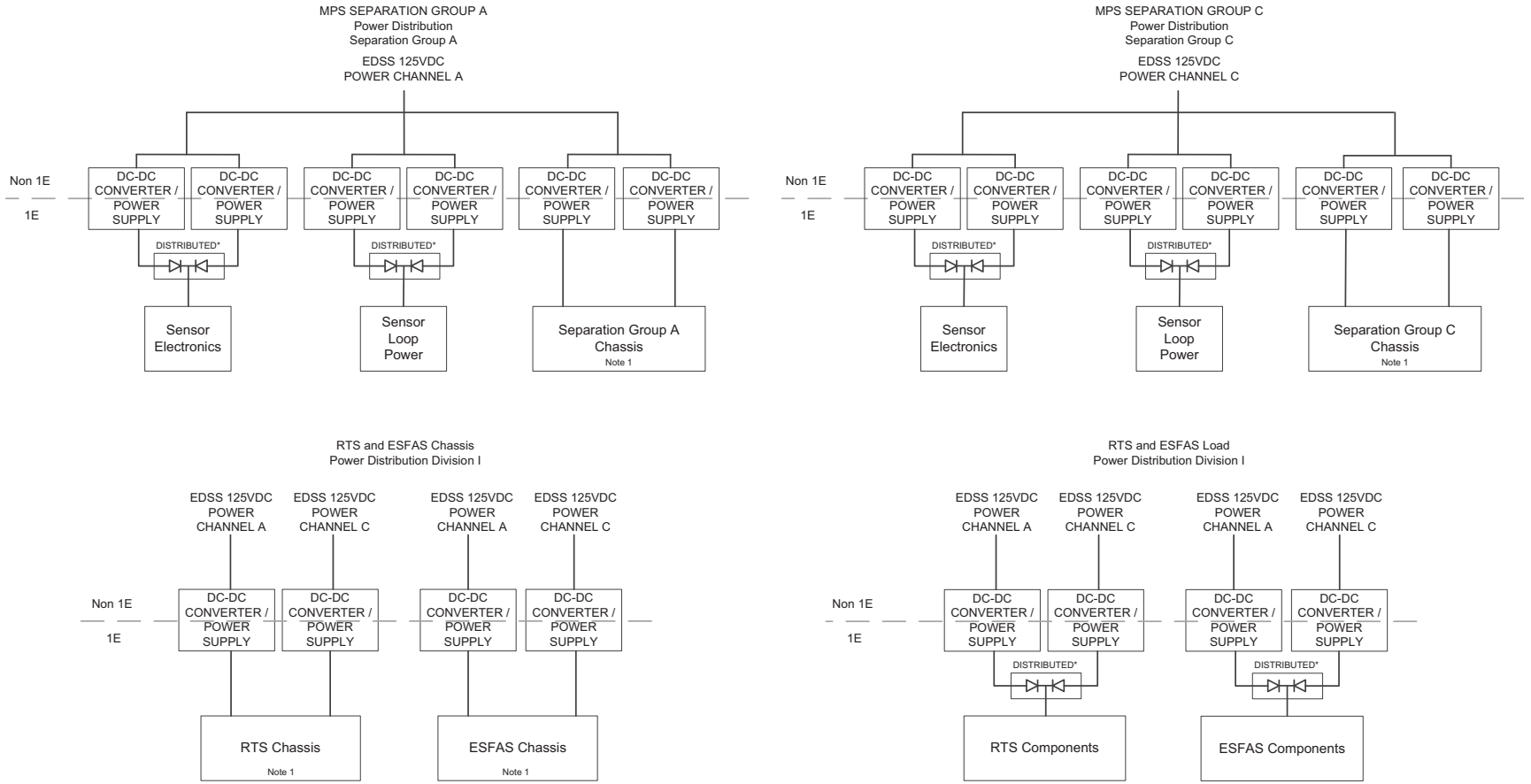


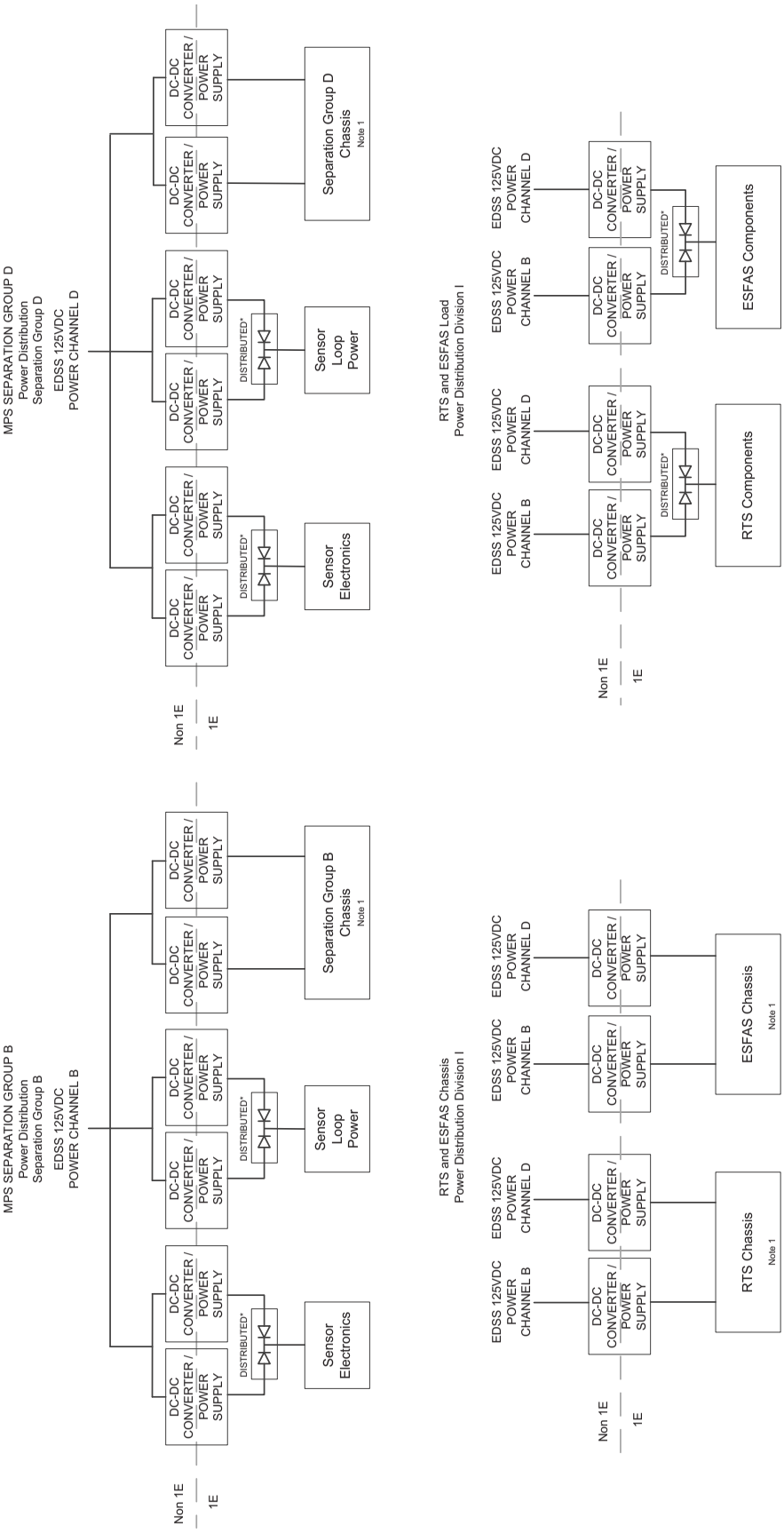
Figure 7.0-11a: Module Protection System Power Distribution



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

*Shared or auctioneered

Figure 7.0-11b: Module Protection System Power Distribution



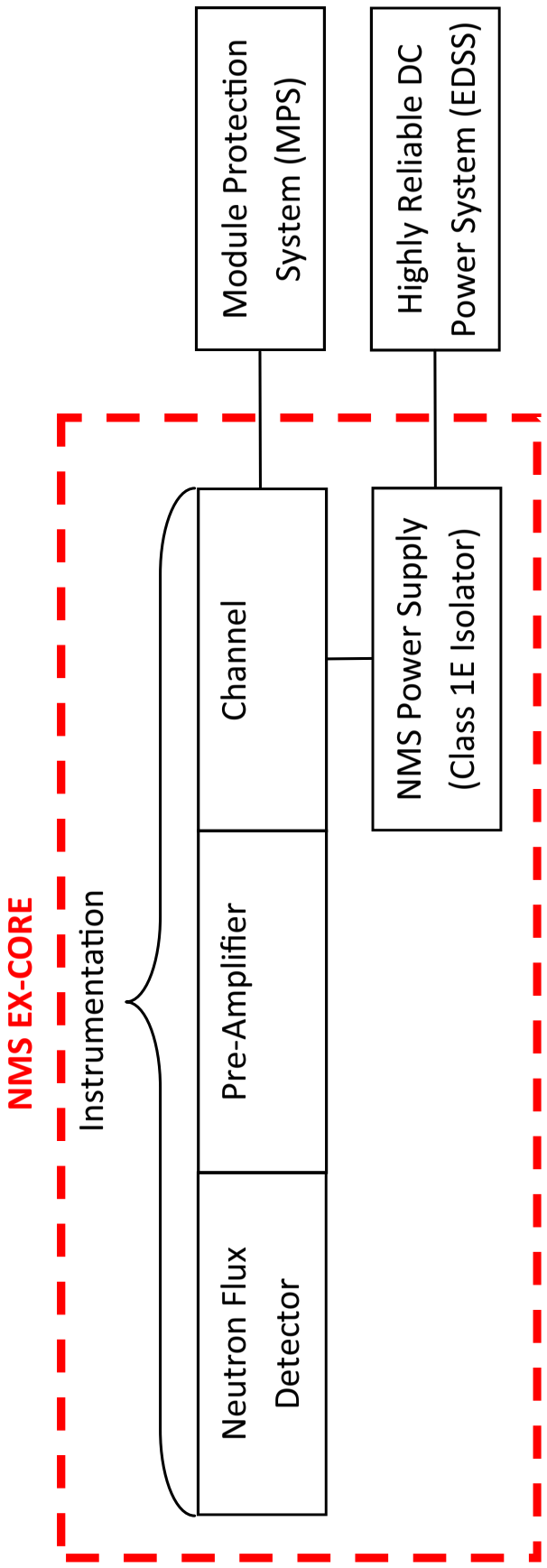


Figure 7.0-12: Neutron Monitoring System Ex-Core Block Diagram

Figure 7.0-13: Plant Protection System Block Diagram

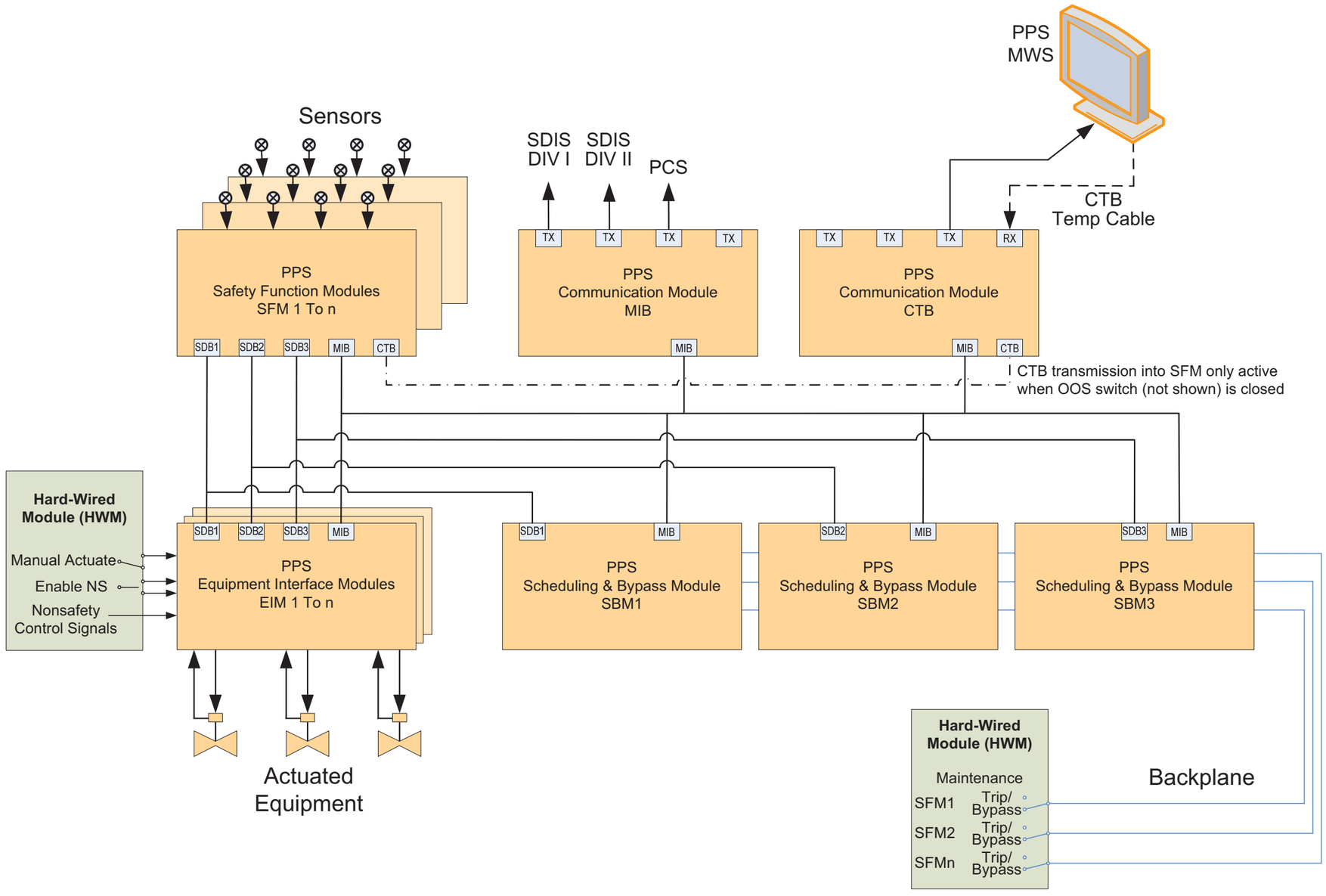
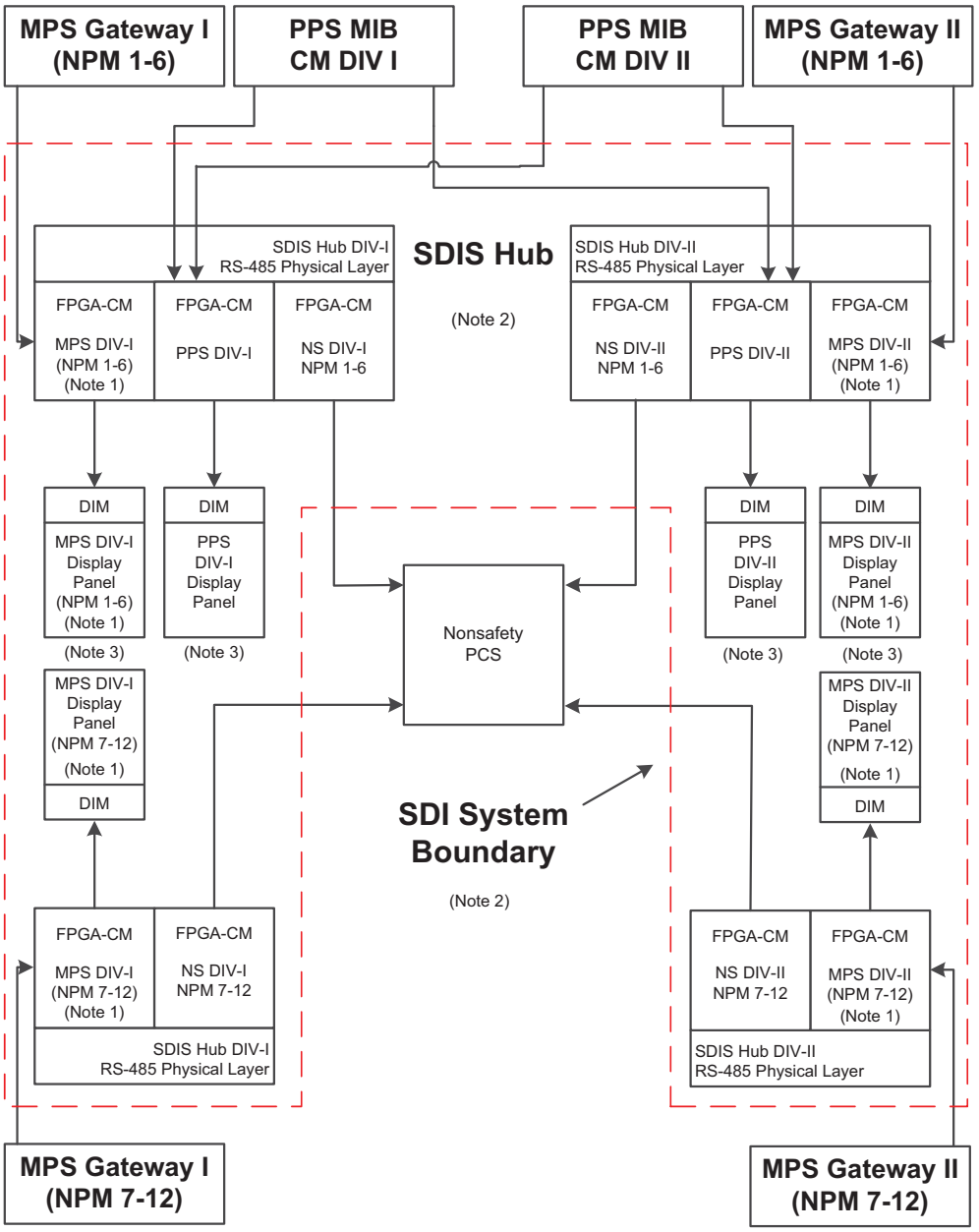


Figure 7.0-14: Safety Display and Indication System Boundary



Notes:
1. The MPS gateway, FPGA-CM, DIM, & display panels shown are typical for NPM 1-12.
2. Only one MPS communication module is shown. Hub communication modules for NPM 1 through 6 will be grouped together with one PPS communication module and a nonsafety communication module. The Hub communication modules for NPM 7 through 12 will be grouped together with only a nonsafety communication module.
3. DIM/display panels will be separate for each NPM. PPS will have separate display panels. Although no cabling is shown, there is a cable connection between the DIM and the display panels.

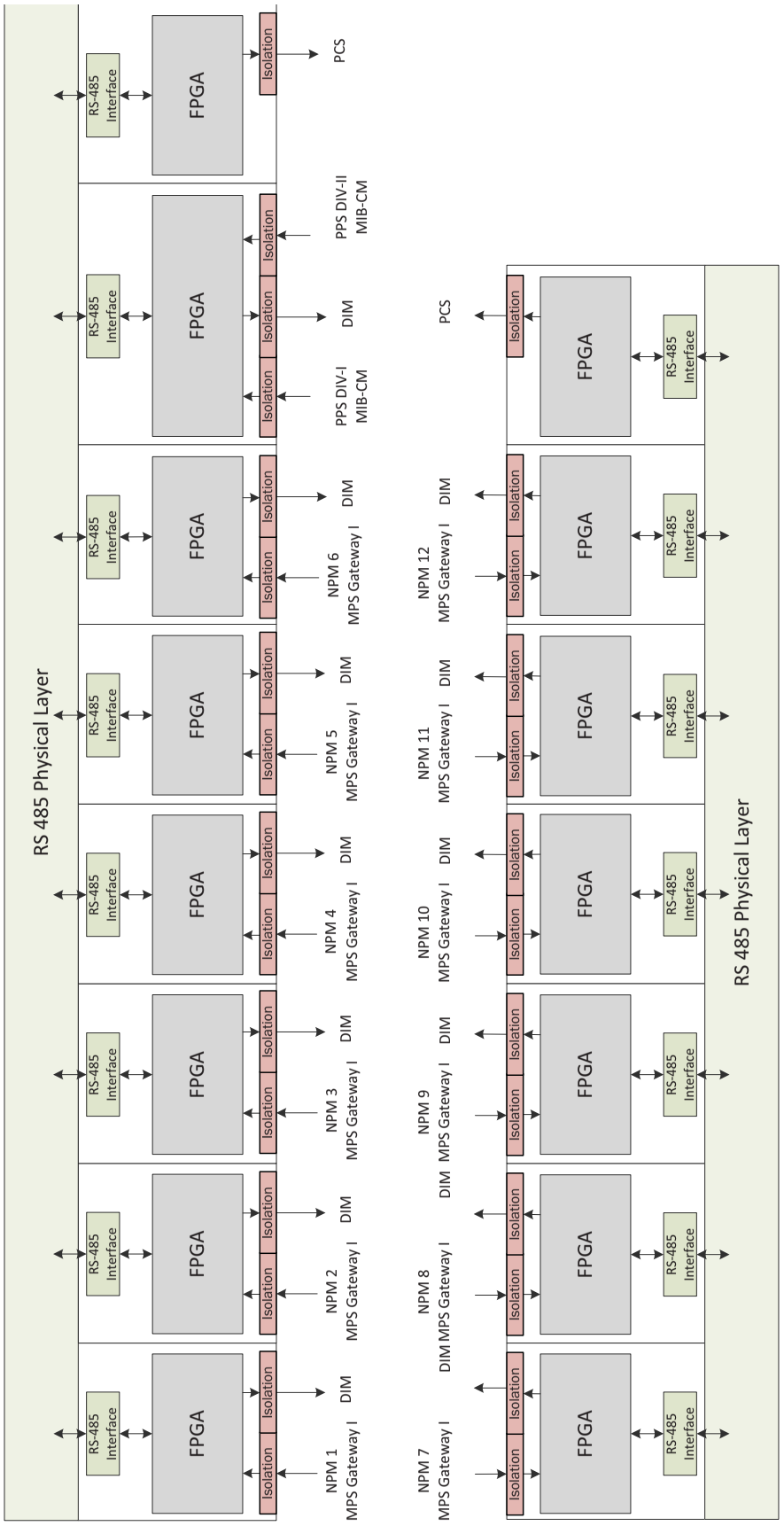


Figure 7.0-15: Safety Display and Indication Hub

Figure 7.0-16: Display Interface Module

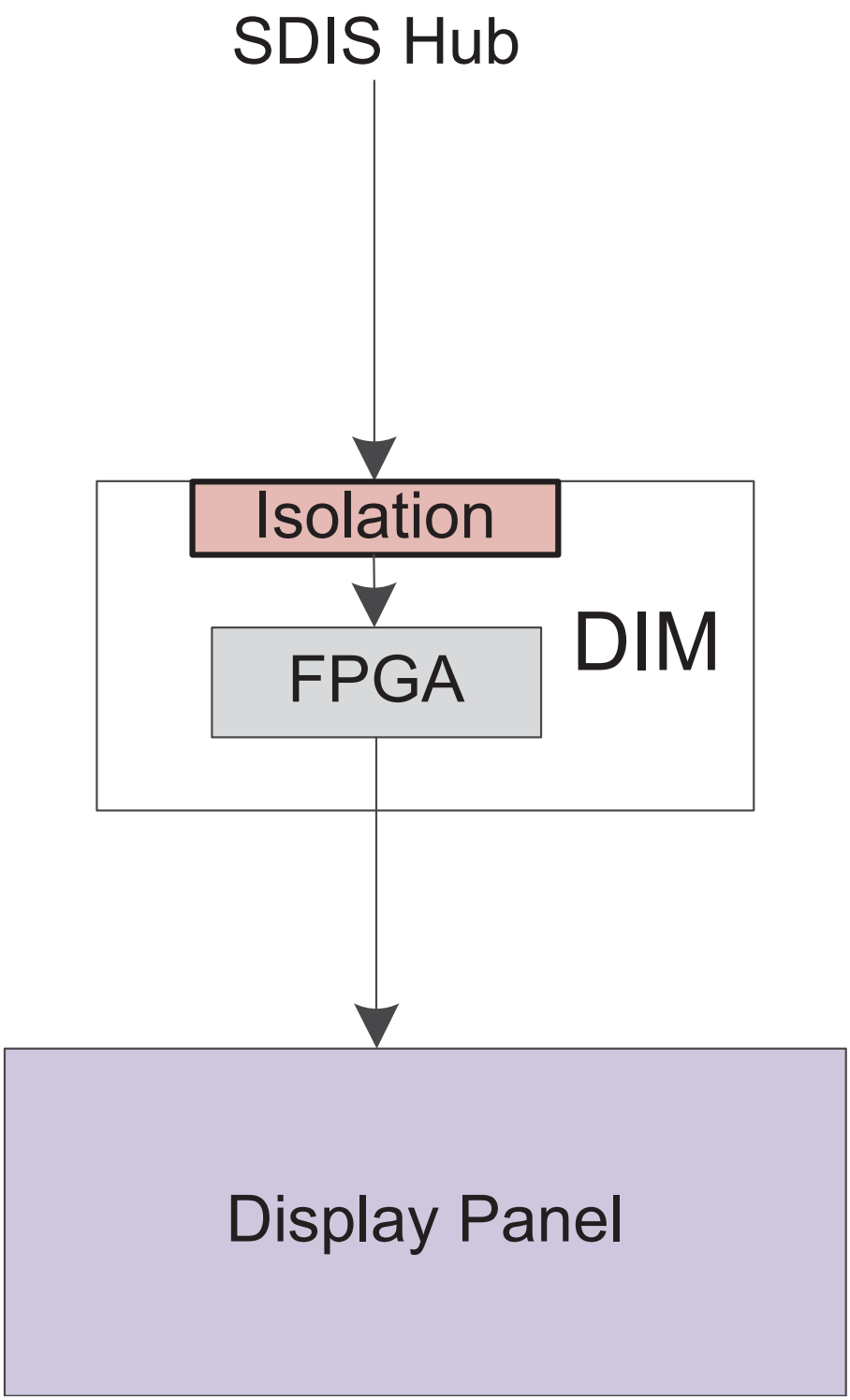
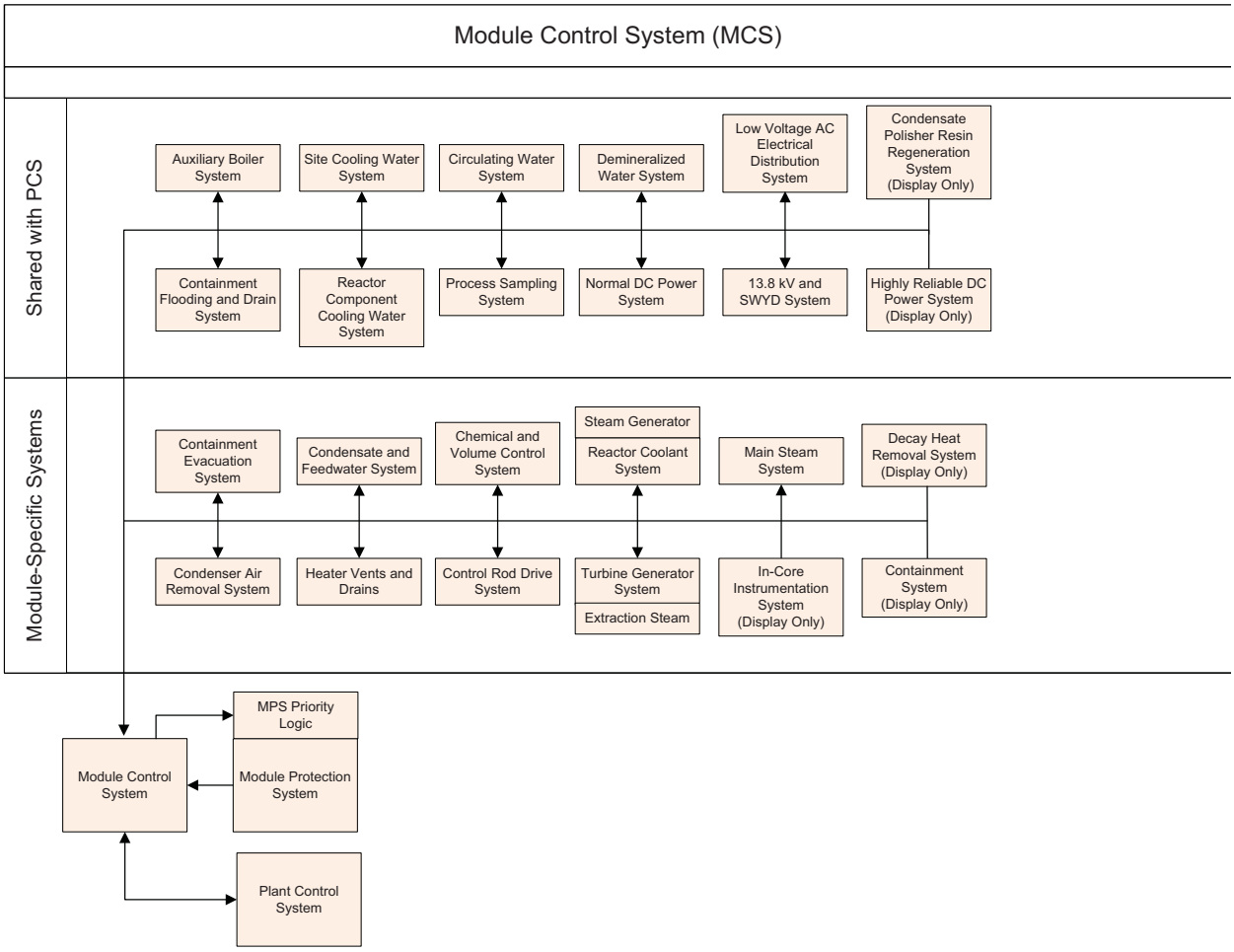


Figure 7.0-17: Module Control System Internal Functions and External Interfaces



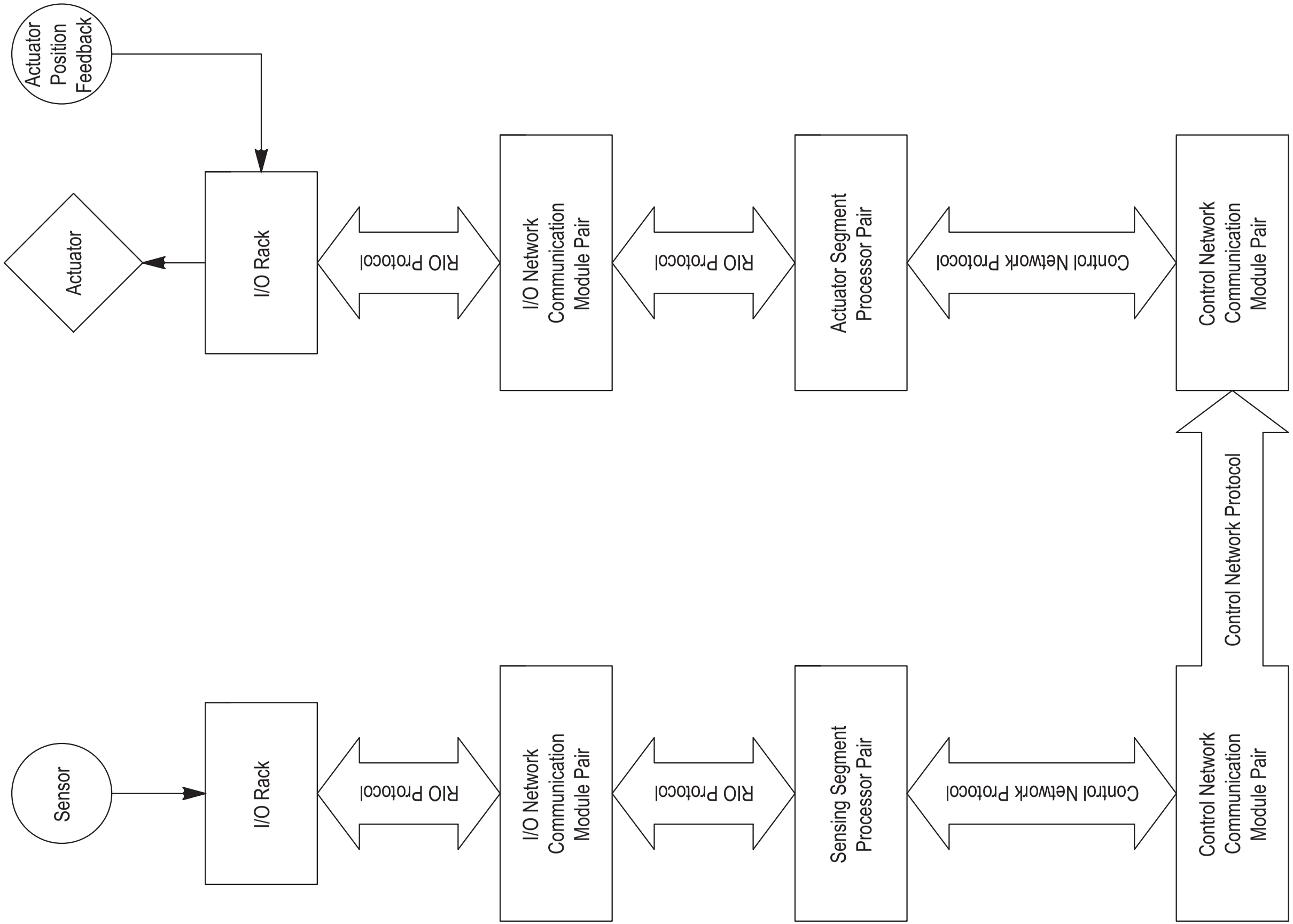


Figure 7.0-18: Automatic Control Shared Between Networked Processors

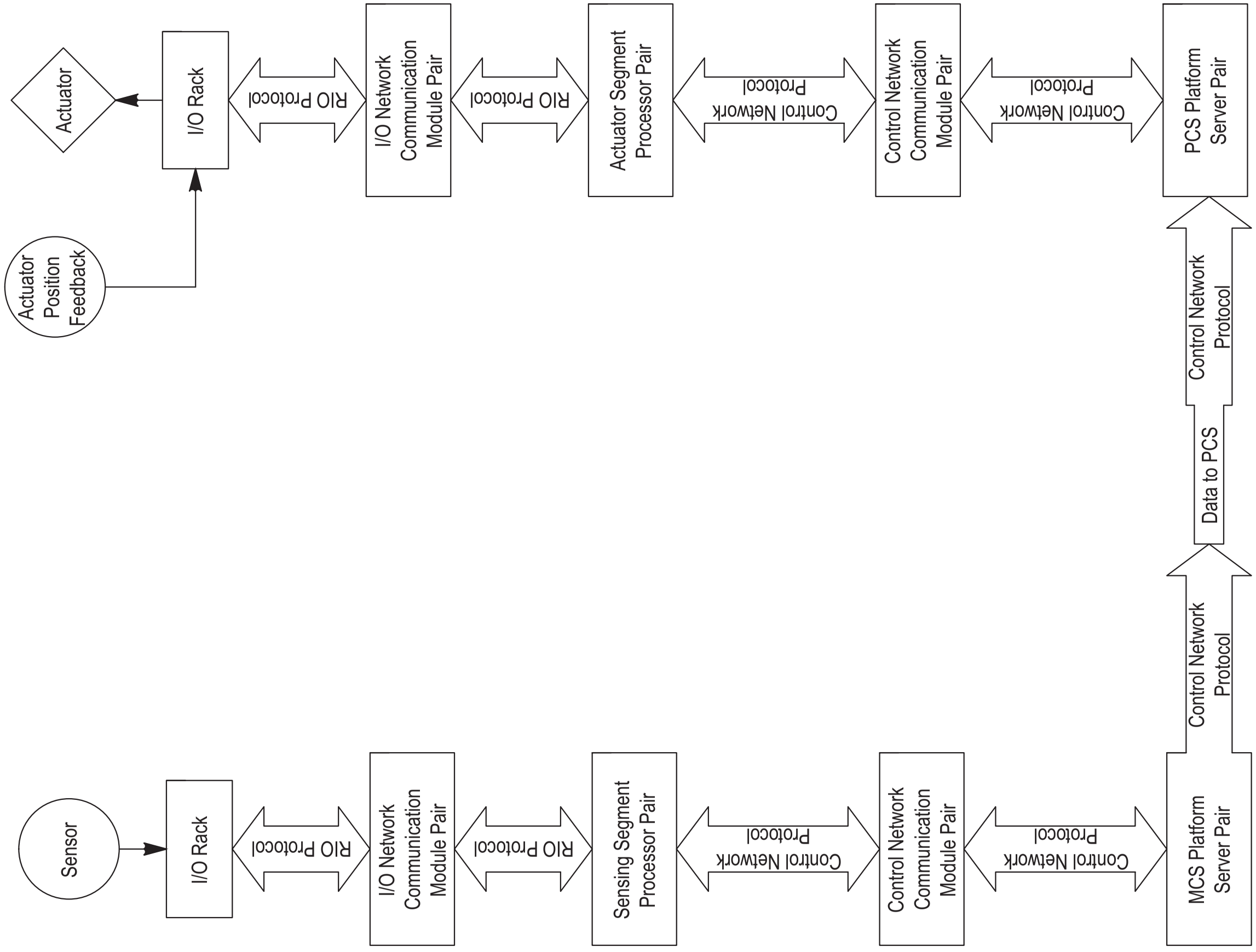
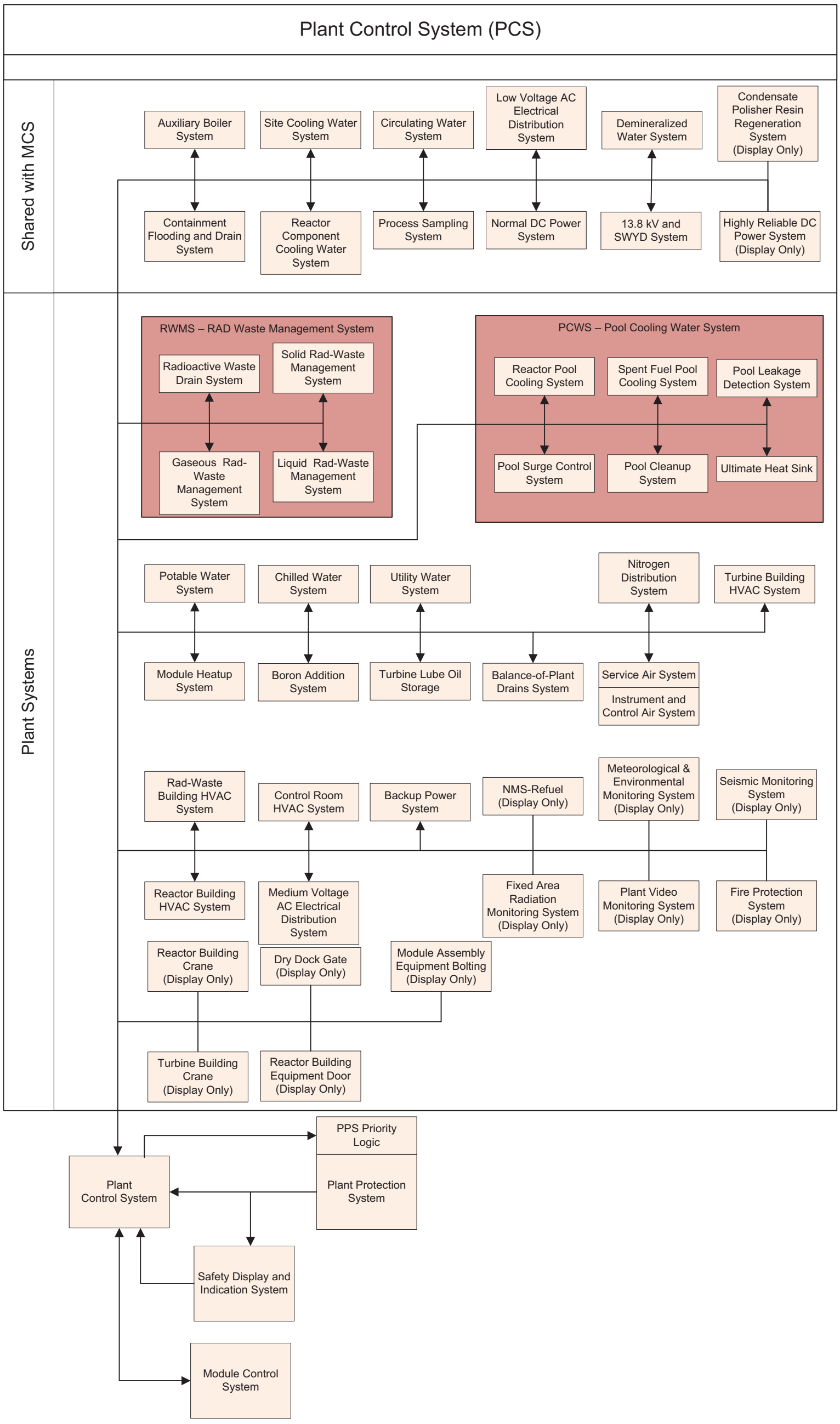


Figure 7.0-19: Automatic Control Shared Between MCS and PCS Processors

Figure 7.0-20: Plant Control System Internal Functions and External Interfaces



7.1 Fundamental Design Principles

The design of NuScale 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 is the safety evaluation and describes how the NuScale design conforms to applicable regulations.

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

Section 7.1.8 describes how hazard analyses have been used to examine the NuScale 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 NuScale Power, LLC, TR-1015-18653-P-A, "Design of the Highly Integrated Protection System Platform Topical Report," (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, Rev. 1, which endorses IEEE Std 603-1991 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 7.1-3) and the correction sheet dated January 30, 1995. Because the HIPS platform uses programmable digital devices, RG 1.152, Rev. 3, IEEE Std 7-4.3.2-2003 "IEEE Standard Criteria for Digital Computers and Safety Systems of Nuclear Power Generating Stations" (Reference 7.1-5), Digital I&C Interim Staff Guidance 04 (D&IC ISG-04), and the Staff Requirements Memorandum for SECY 93-087 were also used for the general platform design.

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 Criteria (GDC) 1, I&C systems are designed to the quality assurance program described in Section 17.5. The quality and safety classifications of structures, systems, and components (SSC) are identified in Section 3.2.

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

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 be required to function.

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

Consistent with GDC 10, the MPS provides reactor trips and engineered safety feature (ESF) actuations which ensure specified fuel design limits are not exceeded during normal operations and anticipated operational occurrences (AOOs).

Consistent with GDC 13, the I&C systems monitor variables and systems over their anticipated ranges for normal operations, AOOs, and accident conditions.

Consistent with GDC 15, the MPS and NMS initiate safety-related functions that 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 the containment design conditions are not exceeded for the duration of a postulated accident.

Consistent with PDC 19, the I&C systems are designed to ensure the ability to control each NPM during normal and accident conditions. The NuScale main control room (MCR) is designed with the ability to place the reactors in safe shutdown in the event of an MCR evacuation event, and for safe shutdown to be maintained without operator action thereafter. Prior to 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 MPS equipment rooms within the reactor building. Following shutdown and initiation of passive cooling from either the MCR or the MPS equipment rooms, the NuScale design does not rely on operator action, instrumentation, or controls outside of the MCR to maintain safe shutdown condition. There are no displays, alarms, or controls in the RSS credited to meet the

requirements of principal design criterion (PDC) 19 as there is no manual control of safety-related equipment allowed from the RSS.

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 that specified fuel design limits are not exceeded as a result of AOOs.

Consistent with GDC 21, MPS and NMS have sufficient redundancy and independence to ensure that no single failure results in the loss of the protection function. Individual SSC of the MPS and NMS may be removed from service for testing without loss of protection functions.

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

Consistent with GDC 23, the MPS fails into a safe state upon loss of electrical power or if adverse environmental conditions 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.

Consistent with GDC 25, the MPS initiates reactor trip functions to ensure that specified fuel design limits are not exceeded for any single malfunction of the reactivity control system. Compliance with GDC 25 is discussed in Section 4.6.2

Consistent with GDC 28, the MPS initiates reactor trip functions to limit the potential amount and rate of reactivity increase and to ensure sufficient protection from reactivity accidents. Compliance with GDC 28 is discussed in 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.

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 50.34(b)(2)(i), the design of the I&C systems and auxiliary features of the I&C system design is 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.

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

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

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

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.

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

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.

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

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

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

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.

Consistent with 10 CFR 50.55a(h), the MPS and NMS are designed in accordance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

Compliance with these regulatory requirements is described in Section 7.1.6.

As described in Table 1.9-5, 10 CFR 50.34(f)(2)(xii) and 10 CFR 50.34(f)(2)(xxii) are not applicable to the NuScale design. As described in Table 1.9-5, the NuScale design supports an exemption from the power supply requirements for pressurizer level indication included in 10 CFR 50.34(f)(2)(xx).

7.1.1.2 Additional Design Considerations

7.1.1.2.1 Protection Systems

The protection systems are used to facilitate protective actions of the MPS (reactor trip and ESF functions) in response to monitored variables exceeding pre-established limits. Table 7.1-1 identifies the specific DBEs and classifications for which MPS protective actions are credited in Chapter 15 analyses. The DBEs, including AOOs, infrequent events (IEs), and postulated accidents for the NuScale

Power Plant design are listed in Table 15.0-2. The MPS functional logic diagrams are shown in Figure 7.1-1a through Figure 7.1-1ao.

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 across three overlapping detector ranges: the source range, intermediate range, and power range.

Certain 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). For additional information on the MPS interlocks and permissive, see Table 7.1-5. 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 don't include the delay times associated with the actuation device (e.g. valve stroke times) with the exception of opening the pressurizer heater breakers.

There are manual trip or actuate switches for each automatic trip or actuate function in the MCR. 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.

All of the 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 all that are needed for reactor trip and ESF actuations, and post-accident monitoring (PAM) variables that would be required for monitoring after an event. 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.

All 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 does not result in spatial dependence concerns because of core radial symmetry.

The RCS temperature is measured by resistance temperature detectors (RTDs) located in thermowells on the side of the reactor pressure vessel (RPV). Each RPV quadrant contains a redundant separation group of RTDs. Temperature-streaming effects may result in variations in the measured reactor coolant system (RCS) temperature as a function of RTD position. Multiple sensors are provided to minimize spatial dependence in temperature measurement.

The RCS narrow range T_{hot} is measured by three RTDs in each MPS separation group. One RTD separation group is located in each RPV quadrant at the top of the hot leg riser. The MPS averages the three RTD inputs to compensate for temperature-streaming effects that may be present at the RTD location.

The RCS narrow range T_{cold} is measured by two RTDs in each MPS separation group. One RTD separation group is located in each RPV quadrant in the lower downcomer. Although reactor coolant flow is expected to be thoroughly mixed as it passes through the steam generator (SG) tube region of the RPV downcomer, some temperature-streaming effects are possible. The MPS averages the two T_{cold} inputs to compensate for temperature-streaming effects that may be present in the RPV downcomer region.

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 between 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, IE, 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 Reactor Building, 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 Reactor Building, 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 unit.

The MPS and NMS rack-mounted equipment is installed in a mild environment. The MPS 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) was conducted for both the MPS and the NMS. This is a systematic procedure for addressing failures for all components of a system and for evaluating their 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 all equipment is in the actuated position and the plant conditions are stabilized. The MPS may 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, and is described in Section 7.2.3.3. The NMS does not initiate any protective functions; it only provides safety-related input to the MPS.

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

7.1.1.2.2 Post-Accident Monitoring

The post-accident monitoring (PAM) 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 497-2002 "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations" (Reference 7.1-11), as modified by RG 1.97, Revision 4.

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. Since 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 the 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) (see Section 19.1).
- operator actions identified during human factors engineering (HFE) task analysis (see Section 18.4).
- industry operating experience
- engineering judgment.
- the identification process and its results reviewed by a multidisciplinary group (see Section 7.2.13.2).

The PAM Type B, C, D, and E 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 which processes the sensor input is also provided in Table 7.1-7 and Figure 7.1-2. The NuScale reactor design has no Type A variables because there are no operator actions credited in any Chapter 15 anticipated operational occurrence, infrequent event, or accident, nor the station blackout or anticipated transient without scram analysis.

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

Type B Variables

Type B variables are those variables that provide primary information to the control room operators to assess the plant's critical safety functions that have been defined for the NuScale power plant. These are accomplishing or maintaining the following three critical safety functions:

- reactivity control
- remove fuel assembly heat
- containment integrity

NuScale has selected these three critical safety functions based on the plant design. 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 reactor coolant system (RCS) integrity. This is

due to 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 —it is done to maintain core cooling and protect the fuel clad fission product barrier. This is automatically actuated when there is an existing loss of RCS integrity as indicated by low reactor pressure vessel (RPV) riser water level or high containment water level.

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 inlet and exit temperature.

Remove Fuel Assembly Heat Critical Safety Function Variables

The Type B variables selected that provide direct indication and verification and 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, containment water level, degrees of subcooling, 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) which serves as the primary means to control radioactive effluent releases. The same variables that are used to provide direct indication and support the containment integrity critical safety function are: narrow range containment pressure, wide range containment pressure, containment isolation valve position, containment water level, and inside bioshield area radiation monitor.

Type C Variables

Type C variables are those variables that 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.

The selection of these variables represents 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 monitor 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 the 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 where the core is not damaged due to inadequate core cooling.

Reactor Coolant System Fission Product Barrier Variables

The primary variables used to assess the status of the reactor coolant system fission product barrier are the RPV riser level and RCS pressure. RPV riser level can show a loss of boundary through a loss of inventory, resulting in a reduction in 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 (Maintain Containment Integrity) and a fission product barrier which 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, containment isolation valve position, containment water level, and inside bioshield area radiation monitor.

Type D Variables

The Type D variables listed in Table 7.1-7 are those variables that 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 design-basis events.
- indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
- verify safety system status.

The Type D 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.

Type E Variables

Type E variables identified and 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 that are 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).

7.1.1.2.3 Remote Shutdown Station

If the MCR is evacuated, the RSS serves as a central location for the operators to monitor the modules in a safe shutdown condition with DHRS in service for each module. Additionally, the RSS provides defense-in-depth capability to monitor the plant remotely from the MCR and control balance of plant equipment to support asset protection and long-term plant recovery in events where the MCR becomes uninhabitable. An MCR evacuation occurrence is a special event and is not postulated to occur simultaneously with any DBE, nor does it cause fuel damage, or result in consequential loss of function of the RCPB or primary containment barriers. The RSS provides a safe alternate location during an MCR evacuation occurrence to allow monitoring of each NPM.

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

Despite these considerations, events for the RSS design and licensing basis include smoke due to 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 prior to leaving the MCR. Following evacuation of the MCR, the ability to isolate the MPS manual switches to prevent spurious actuations is provided in the RSS as described in Section 7.2.12. An alarm is annunciated in the MCR when the MCR hard-wired switches are isolated using the MCR isolation switches in the RSS, see Figure 7.1-1j.

The MPS manual isolation switches are mounted in a Seismic Class I enclosure to allow them to remain functional following an earthquake. Controls are available outside the MCR in the associated MPS equipment rooms that provide the capability to trip the reactors, initiate DHRS and initiate containment isolation, which will initiate passive cooling and places and maintains the NPMs in safe shutdown. The MCS equipment in the RSS provides nonsafety-related human-system interface (HSI) and direct readings of the process variables necessary to monitor safe shutdown of each NPM. Figure 1.2-14 shows the location of the RSS equipment.

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 Section 9A.

Access to the RSS is under administrative controls.

7.1.1.2.4 Safety Display and Indication System

The safety display and indication system (SDIS) as described in Section 7.0.4.4, provides HSI for the MPS and PPS to monitor and display PAM variables, and provides the capability for control inputs and status information. The SDIS is a nonsafety-related, nonrisk-significant system; however, because it supports the PAM function, the SDIS meets augmented quality and regulatory requirements as described in Table 3.2-1.

7.1.1.2.5 Plant Protection System

The PPS as described in Section 7.0.4.3 provides monitoring and control of plant systems that are common to multiple NPMs. The PPS is nonsafety-related; however, because it supports the PAM function, the PPS is designed to meet augmented quality and regulatory requirements as described in Table 3.2-1. The PPS functional logics are shown in Figure 7.1-3a through Figure 7.1-3f.

All of the variables monitored by the PPS listed in Table 7.1-8 are sent to the SDIS and the PCS to be displayed in the MCR as required by those systems. These provide the display and indication to support actuation of the control room habitability system and required PAM variables from the PPS.

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 NuScale NPM-specific components, including manual controls and HSIs necessary for operator interaction. The MCS is a nonsafety-related system; however, the MCS is designed to meet augmented quality and regulatory requirements as described in Table 3.2-1.

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 a nonsafety-related system; however, the PCS is designed to meet augmented quality and regulatory requirements as described in Table 3.2-1.

7.1.1.2.8 In-Core Instrumentation System

In-core instrumentation system (ICIS) described in Section 7.0.4.7 is a nonsafety-related system that monitors neutron flux distribution in the reactor core. The ICIS supports the RCS by providing equipment to accomplish a leak-tight RCPB. The SSC associated with maintaining the RCPB and containment isolation,

and Class 1E isolation devices are classified as safety-related. This equipment is designed to the augmented quality criteria in Table 3.2-1.

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 NuScale 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 497-2002, as endorsed by RG 1.97, Rev. 4.

The physical and electrical independence attributes of the MPS and NMS meet the guidance in RG 1.75 Rev.3, which endorses IEEE Std 384-1992 "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 7.1-14).

The communication independence attributes of the MPS meet the guidance in RG 1.152, 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 is used to achieve separation of 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 rooms on the 75'-0" elevation of the Reactor Building (RB) and Separation Groups B, D, and Division II equipment are located on the 86'-0" elevation (see Figure 1.2-14 and Figure 1.2-15, respectively). The MPS equipment rooms are seismically qualified and located in separate fire zones. The rooms containing Separation Group A and C (Division I) MPS and NMS equipment are in a separate fire zone from the MPS equipment rooms containing Separation Group B and D (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, seismically qualified equipment rooms. The NMS Separation

Group A and C signal processing equipment is located in the MPS Separation Group A and C (Division I) equipment rooms on the 75'-0" elevation of the RB, and NMS Separation Group B and D signal processing equipment is located in the MPS Separation Groups B and D (Division II) equipment rooms on the 86'-0" elevation of the RB (see Figure 1.2-14 and Figure 1.2-15, respectively).

The SDIS has two separate and independent hubs. The SDIS hubs are located in the seismically qualified Control Building (CRB) at the 50' level 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. See Section 8.3 for additional details on the design and routing of nonsafety-related cabling.

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 as part of the MPS in accordance with IEEE Std 384-1992. The isolation devices are tested to confirm that credible failures on the nonsafety side of the isolation device do not prevent the associated safety system channel from meeting the minimum performance requirements.

Electrical isolation between the safety-related MPS and associated nonsafety-related systems is provided by the following devices (see 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. For additional information, see Section 4.2 of TR-1015-18653-P-A.
- 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 highly reliable DC power system (EDSS). The MPS provides Class 1E isolation from the nonsafety-related EDSS by using Class 1E isolation devices that are part of the MPS and are used as the safety system boundary (see 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 (see Figures 7.0-11a and 7.0-11b).

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

The PPS, SDIS, ICI, MCS, and PCS are nonsafety-related SSC and are separated from safety-related SSC in accordance with the NuScale Electrical Design Criteria. The SDIS receives electrical power from the EDSS. The SDIS divisions are powered from independent EDSS sources.

7.1.2.3 Communication Independence

The NuScale 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 for the 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 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 NuScale 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 SDB) are functionally independent from the division components (SVM, EIM) 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 module protection system (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 all 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 that 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 NuScale I&C systems, and conforms to the single-failure criterion in IEEE Std 603-1991, Section 5.1 and the criteria of IEEE Std 497-2002, 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 NuScale safety-related I&C systems are designed to meet the guidance in RG 1.53, Rev. 2, which endorses IEEE Std 379-2000 "IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 7.1-8).

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 that 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 NuScale 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 that 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 (see Section 8.2.6 of TR-1015-18653-P-A for more detail). 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 was 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 was divided into four groups to evaluate the effect of a single failure. The first group consisted of those components in the MPS that are common to both the RTS and ESFAS. The second group was made up of the associated RTS functions. The third group was analyzed based on the ESFAS functions. Finally, the last group analyzed the external communications and supporting functions associated with the MPS.

<u>Group 1 - Common Components</u>

- separation group analog sensor/detector associated with monitored systems
- separation group SFM - signal conditioning
- separation group SFM - trip determination
- separation group SBM
- divisional scheduling and voting module
- 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 actuate switch
- divisional automatic ESFAS
- pressurizer heater breakers
- enable nonsafety control switch

Group 4 - External Communication and Supporting Functions

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

Only single failures were considered and evaluated for the MPS design. Failure effects on the system assume no other coincident failures occur. 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.

As described in Section 8.1.2.2, for the EDSS design, the power supplied to the MPS by the EDSS is monitored by the MPS Class 1E isolation devices. Therefore, failures of the

EDSS are bounded by the MPS failure modes and effects analysis 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
- NMS-refuel sub-system (sensor, pre-amplifier, channel, and associated power supply)
- NMS-flood sub-system (sensor, pre-amplifier, channel, and associated power supply)

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 I/O network layer. The flow of data is uninterrupted by a single component, cable, or device failure. In addition, redundant process system components are segregated onto alternate I/O modules to ensure that MCS and PCS component-level failures do not impact redundant process equipment.

Redundancy is incorporated into the RSS by providing redundant MCS and PCS operator workstations for plant monitoring when the MCR is evacuated. When the operators evacuate the MCR and occupy the RSS, 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 failure modes and effects analysis 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 interface 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 NuScale 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 that 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 reactor trip breakers 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 comprised of the analog input delay plus the digital time response delay plus the analog output delay and includes the time for the reactor trip breakers 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 comprised 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 trip breakers to open.

7.1.5 Diversity and Defense-in-Depth

The NuScale I&C system design includes features and processes to mitigate a common cause failure (CCF) in the MPS because of digital-based failures which could disable a safety function.

The D3 assessment of the NuScale 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 requirement memorandum to SECY- 93-087 is summarized in Section 7.1.5.3. Conformance to 10 CFR 50.62, and 10 CFR 50.34(f)(2)(xiv)(C) are summarized in Section 7.1.6. See Section 15.8 for the discussion on ATWS.

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 the NUREG/CR-6303 guidelines to the D3 of the NuScale 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 7.1-4 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).

Non-Class 1E Monitoring and Indication Block

The non-Class 1E 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 Control 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 all four separation groups and both MPS divisions of RTS and ESFAS. The SDIS displays are for indication only and do not provide any control functionality. Each protective action automatically initiated by MPS can be manually actuated at the division level by safety-related manual switches. 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 7.1-4 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 7.1-5 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 non-Class 1E 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 non-Class 1E controls 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 7.1-9. 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., degrees of subcooling, 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 non-Class 1E 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 significantly. For example, the logic implemented for trip determination on an SFM is different than the logic implemented for two-out-of-four voting on a 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 analog 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 analog 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 accident 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 certain 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 7.1-9 can be grouped into the following function types as described in the NuScale Power, LLC, TR-0316-22048 "Nuclear Steam Supply Systems Advanced Sensor Technical Report," (Reference 7.1-15):

- digital-based level measurements
- digital-based pressure measurement
- 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, pressure, 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, pressure, 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., vendor or supplier).

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 SDIS

There are no diversity attributes within this block.

Division I or II of Manual Controls

There are no diversity attributes within this block.

Non-Class 1E Monitoring and Indication Block

There are no diversity attributes within this block.

Module Control System

There are no diversity attributes within this block for the monitoring functions.

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 7.1-17 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., vendor or supplier). 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 7.1-10.

The MCS block and non-Class 1E 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 certain blocks. The SDIS and safety blocks are based on an FPGA platform while the non-Class 1E 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).

Due to 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, as needed, to initiate a reactor trip and ESF actuations to mitigate a DBE.

The monitoring and indication blocks allow for 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 certain operational transients.

Sensor Block I and II function is 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 non-Class 1E 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 1, 2 and 3 system failures as described in NUREG/CR-6303 are considered in Guidelines 10 and 11.

Type 1 Failures

Type 1 failures occur when a plant transient is induced by the instrumentation system for which reactor trip or ESF function is needed, but may not occur, because of an interaction between echelons of defense. Type 1 failures typically begin with a challenge presented by the control system to the RTS or to the ESFAS due to failure of a common sensor or signal source. Defense against such failures depends upon means of accomplishing safety functions that are diverse to the shared signals or equipment (i.e., not impaired by the postulated CCF). Defense-in-depth analysis of Type 1 failures is required by general analysis Guideline 12.

Type 2 Failures

Type 2 failures do not directly cause plant transients, but are undetected until environmental effects or physical equipment failures cause a plant transient or DBE to which protective equipment may not respond. Failure to respond is due to

postulated CCF of redundant protection system divisions or portions thereof. Type 2 failures can have serious consequences only if the event needing safety action occurs while the protection system is in the failed state and before the failure is repaired. Defense against type 2 failures depends upon some combination of diverse control system, RTS, ATWS mitigation equipment, ESFAS, and monitoring and indication functions that are sufficient to mitigate the postulated incident. Defense-in-depth analysis of Type 2 failures is required by general analysis Guidelines 10 and 11.

Type 3 Failures

Type 3 failures occur because the primary sensors expected to respond to a DBE produce anomalous readings. For instance, accident conditions may have modified instrument response or an unanticipated event sequence may have modified the process variable values seen by the instrumentation. Because Type 3 failures are unpredictable by definition, a strategy dictated by experience is to ensure sufficient signal diversity that alternate means of detecting significant events exist. At a minimum, there is sufficient signal diversity to ensure that for each AOO in the design basis in conjunction with postulated CCFs, the plant is brought to a stable hot standby condition. For each accident in the design basis in conjunction with postulated CCFs, the plant response calculated using best-estimate (using realistic assumptions) analyses does not result in exceedance of the 10 CFR 100 dose limits, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment. Defense-in-depth analysis that supports signal diversity required for Type 3 failures is required by general analysis Guidelines 10 and 11.

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 7.1-6.

The monitoring and indication echelon consists of five blocks: Division I SDIS, Division I Manual Controls, Division II SDIS, Division II Manual Controls, and non-Class 1E 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 that 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 any 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 analog 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 analog 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 non-Class 1E 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 non-Class 1E 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 SDIS and Manual Controls

The SDIS and manual control 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 non-Class 1E Monitoring and Indication block and the MCS block but only if non-Class 1E controls are enabled from the manual control 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 prior to 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 non-Class 1E Monitoring and Indication block. The information provided to the SDIS blocks from the safety blocks is also provided to the non-Class 1E 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 non-Class 1E Monitoring and Indication block. The operator is able to resolve the discrepancy in indication.

Figure 7.1-7 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 protection 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 due to the 2-out-of-4 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,

eight possible partial spurious actuation scenarios are identified in Table 7.1-11. For scenarios 1 and 2, a D3 coping analysis was performed to demonstrate that 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 7.1-12.

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 7.1-8 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 7.1-9 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).

Non-Class 1E Monitoring and Indication Block

Non-Class 1E Monitoring and Indication block includes controls for safety and nonsafety equipment. Because non-Class 1E Monitoring and Indication is used for normal day-to-day operations, any spurious actuation of a major control function (e.g., rod control, feedwater control) by a digital-based CCF within non-Class 1E Monitoring and Indication block is immediately identifiable and, if it exceeds operating limits, is mitigated by Safety Blocks I or II. Figure 7.1-10 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 non-Class 1E controls; however, this can only be enabled by the operator using a safety-related switch. Without this feature being enabled, the non-Class 1E signals to the actuation priority logic are ignored. Because of the limited period in time in which safety-related components are controlled by non-Class 1E 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 non-Class 1E 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 certain 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 non-Class 1E controls; however, this can only be enabled by the operator using a safety-related switch. Without this feature being enabled, the non-Class 1E signals to the actuation priority logic are ignored. Because of the limited period in time in which safety-related components are controlled by non-Class 1E 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 7.1-13 through Table 7.1-16 identify how a digital-based CCF affects either one or both sensor blocks. For Table 7.1-13, 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 7.1-11) causes:

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

Failed Low Signal

The affected variables are pressurizer level and containment water level. Because protective actions are actuated when at least two-out-of-four separation groups demand a reactor trip or ESF actuation, a failed low signal results in a spurious reactor trip, containment system isolation, chemical and volume control system (CVCS) isolation, pressurizer heater trip, and secondary system isolation.

Failed low signals received by Safety Block I are transmitted to MCS, displayed in the MCR, and used for nonsafety control functions. With the spurious actuation of a

reactor trip, containment system isolation, demineralized water system isolation, and pressurizer heater trip, the MCS response to two correct and two incorrect sensor values has no further impact. Out of the failed low signals, pressurizer level is the only signal used for nonsafety-related controls; however, with CVCS isolated, MCS cannot use CVCS makeup and letdown pumps to change pressurizer level.

Failed High Signal

The affected variables are pressurizer level and containment water level. Because protective actions are actuated when at least two-out-of-four separation groups demand a reactor trip or ESF actuation, a failed high signal results in a spurious reactor trip, CVCS isolation, demineralized water system isolation, and ECCS actuation.

Failed high signals received by Safety Block I are transmitted to MCS, displayed in the MCR, and used for nonsafety control functions. With the spurious actuation of a reactor trip, and CVCS isolation, the MCS response to two correct and two incorrect sensor values has a no further impact. Out of the failed high signals, pressurizer level is the only signal used for nonsafety controls; however, with CVCS isolated, 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 variables are pressurizer level and containment water level. The failed as-is condition for two of the four sensors for each affected variable 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. Failed as-is signals may go unnoticed until the valid signals significantly deviate from the failed signals.

Digital-Based CCF of Pressure Measuring System Function Type

A digital-based CCF of pressure measuring system function type for Sensor Block I (Figure 7.1-12) causes

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

Failed Low Signal

The affected variables are pressurizer pressure and wide-range RCS pressure. Failed low signals in the four sensors for each affected variable can result in a spurious

reactor trip, demineralized water system isolation, CVCS isolation, and secondary system isolation.

Failed low signals received by Safety Block I and II are provided to MCS to be displayed in the MCR and to be used for nonsafety controls. With the spurious reactor trip, demineralized water system isolation, and CVCS isolation, the MCS response to four incorrect sensor values is to turn on the pressurizer heaters, which is bounded by the spectrum of heatup event analyses described in Chapter 15.

Failed High Signal

The affected variables are pressurizer pressure and wide-range RCS pressure. A failed high signal affecting the four sensors for the affected variables can result in a spurious reactor trip, CNTS isolation, DHRS actuation, demineralized water system isolation, pressurizer heater trip, and secondary system isolation.

Failed high signals received by Safety Block I and II are provided to MCS to be displayed in the MCR and to be used for nonsafety controls. With the spurious reactor trip, containment system isolation, demineralized water system isolation, and pressurizer heater trip, the MCS response to four incorrect sensor values has a no further impact. The automatic MCS response to a rise in pressure is to use pressurizer spray; however, with the closure of the containment isolation valves, pressurizer spray is unavailable.

Failed As-Is

The affected variables are pressurizer pressure and wide-range RCS pressure. The failed as-is condition for the four sensors of each affected variable does not result in spurious actuations; however, it can prevent initiation of protective actions if a DBE were to occur. 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.

Digital-Based CCF of Flow Measurement Function Type

A digital-based CCF of flow measurement function type for Sensor Block I (Figure 7.1-13) causes

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

Failed Low Signal

The affected variable is RCS flow. A failed low signal for the four channels results in a spurious reactor trip, demineralized water system isolation and CVCS 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; however, the RCS flow sensor is not relied upon for detection or mitigation of AOOs or postulated accidents as described in Section 7.1.5.2 and Table 7.1-18. 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

The digital-based flow and pressure measuring system 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 7.1-14 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 any 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.

Non-Class 1E Monitoring and Indication Block

The non-Class 1E 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. Any fault within the MCS block cannot propagate backwards into the safety blocks.

Communications between MCS and non-Class 1E 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 7.1-16 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 pressure measuring systems to have a digital-based CCF concurrent with an AOO. Digital-based CCF of pressure measuring system and digital-based level sensors concurrent with an AOO is not considered credible due to the technology diversity. The AOOs and credited digital sensors are summarized in Table 7.1-18.

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 pressurizer pressure and 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 100 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. The results of the D3 coping analysis for each design basis event are shown in Table 7.1-18.

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 only one safety block.

Safety Block I and II depend on both analog and digital sensors for detecting the need for protective actions. Table 7.1-16 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 pressure measuring systems to have a digital-based CCF concurrent with a postulated accident. Digital-based CCF of pressure measuring systems and digital-based level sensors concurrent with a postulated accident is not considered credible because

of the technology diversity. Postulated accidents and credited digital sensors are summarized in Table 7.1-18. A postulated accident may have multiple credited signals, depending on the event sequence; however, Table 7.1-18 only identifies the digital sensors. The event and signal credited are obtained from the plant safety analysis.

Although pressurizer level is a digital-based sensor that 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 that a Type 3 failure concurrent with a postulated accident does not result in radiation release exceeding 10 CFR 100 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. The results of the D3 coping analysis for each design basis event are shown in Table 7.1-18.

7.1.5.1.12 Guideline 12 - Diversity among Echelons of Defense

As shown in Figure 7.1-6, 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 (see Section 7.1.5.1.6). For example, during normal operations, it is possible that the pressurizer spray valves are open (or partially open) as commanded by the MCS to reduce pressure to the normal operating pressure. If we assume that during this process the four pressurizer pressure transmitters fail as-is due to a digital-based CCF, then:

- MCS continues to demand a reduction in pressurizer pressure (failure of control system echelon)
- RTS does not receive the sensor signal needed to initiate a reactor trip when pressure drops below the low pressure setpoint (failure of RTS echelon)
- ESFAS does not receive the sensor signal needed to initiate CVCS isolation when pressure drops below the low pressure setpoint (failure of ESFAS echelon)
- the operator is not be able to see an uncontrolled pressure 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 Class 1E.

As discussed in Section 7.1.5.1.6, 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 analog components and downstream of the automatic digital portion of the safety system. The SDIS and manual controls blocks are sufficiently diverse that any 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
   - decay heat removal system actuation
   - emergency core cooling system actuation
   - containment system isolation

- chemical and control volume system isolation
- pressurizer heater trip
- demineralized water system isolation
- low temperature overpressure protection (LTOP)
- secondary system 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 7.1-11.

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, CVCS isolation, demineralized water system isolation, pressurizer heater trip, and secondary system isolation
   - spurious reactor trip, CVCS isolation, demineralized water system isolation, and ECCS actuation

4) Potential digital-based CCF of pressure measuring system function type within Sensor Block I and II may result in one of the following (Section 7.1.5.1.6):

   - spurious reactor trip, CVCS isolation, demineralized water system isolation, and secondary system isolation
   - spurious reactor trip, containment isolation, DHRS actuation, demineralized water system isolation, and secondary system isolation
   - Type 3 failure for the digital-based pressure measuring system function type sensors

5) 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, demineralized water system isolation, and CVCS isolation
   - Type 3 failure of flow function type sensors (See Item 6 and 7 below)

6) Type 3 failures of digital sensors may lead to failure of MPS to initiate protective action(s) during AOOs and postulated accidents. Table 7.1-18 identifies the digital sensors credited for AOOs and postulated accidents that were addressed with a D3 coping analysis. 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 very 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 that the spurious actuation of containment system isolation due to a digital-based CCF is the bounding analysis with

regard to the reactor coolant pressure boundary integrity. Concurrent actuations of any combination of RTS, DHRS or PZR heater trip have been evaluated to be less limiting due to the additional heatup effects on the delay of reactor trip, DHRS actuation valve opening or PZR heaters being tripped off. CSI actuation includes CVCSI actuation which increases the heatup event slightly and negates any possible effects of DWSI actuation. The consequences of a digital-based CCF that leads to spurious initiation of any 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 identified in Table 7.1-18, 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 which 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 exceeding 10 percent of 10 CFR 100 dose limits for AOOs and 100 percent of 10 CFR 100 dose limits for postulated accidents. The analysis summary is provided below for the flow and pressure safety-related digital-based sensors.

<u>High Pressurizer Pressure</u>

The plant safety analyses described in Chapter 15 credit high PZR pressure for detection and mitigation of heatup and reactivity excursion DBEs.

There are two reactor safety valves each of which are sized to relieve the pressure generated by a total loss of secondary cooling without credit for a reactor trip. The D3 coping analysis concluded that a conservative postulated heatup event that did not trip on high pressure would not violate the RCS pressure boundary integrity due to the sizing of the reactor safety valves.

For the events described in Chapter 15 and listed in Table 7.1-18 that result in a high RCS pressure condition, the analyses conservatively do not take credit for normal pressurizer spray control. In the secondary plant events that result in the loss of main steam flow, the high main steam pressure signal is credited to generate reactor trip and DHRS actuations in addition to the high PZR pressure. In the case of the loss of feedwater and feedwater line break events, the high RCS hot temperature is a diverse signal. Therefore, sufficient signal diversity exists such that postulated digital-based CCFs of the high pressurizer pressure function are bounded by the plant safety analyses in Chapter 15.

Low Pressurizer Pressure

The plant safety analyses described in Chapter 15 credit low PZR pressure in the steam generator tube failure and CVCS line breaks outside containment events. Both the low pressurizer pressure trip and the low low pressurizer pressure trip are credited in the steam generator tube failure event while only the low low pressurizer pressure trip is credited in the CVCS line breaks outside containment event. The limiting radiological scenarios include assumed loss of AC power concurrent with the breaks which results in an RCS pressurization that delays the low pressurizer level and low pressurizer pressure trips. This assumption bounds the cases where loss of offsite power is not assumed in a best-estimate analysis and the D3 coping analysis concluded the plant safety analyses are bounding.

For the events described in Chapter 15, and listed in Table 7.1-18 that result in a low RCS pressure condition, the analyses do not credit normal operation of the PZR heaters. The best-estimate analysis of these events concludes that pressurizer heaters are able to mitigate events. Low pressurizer pressure (via the low low pressurizer pressure trip) is also credited for generating a CVCS isolation signal for small CVCS line failure event and a DHRS actuation signal for the steam generator tube failure event after the RTS and PZR heater trip occurs on low pressurizer level. In these cases, the low-low PZR level trip is identified as the diverse signal for CNV isolation, in order to mitigate the consequences of the radiological release. The best estimate analysis of a larger break of the PZR spray line outside containment does not generate a condition that relies on the low low pressurizer pressure function due to the back flow and overflow prevention (check valves) located on the CVCS lines. If the CVCS pressure drops sufficiently to seat these valves, then the RCS inventory will be preserved and the NPM will continue to operate until operators noticed the failed CVCS line. For breaks/leaks in the CVCS lines that are small enough to not generate the system pressure drop required to seat the check valves, the transient response is a slow degradation of the of RCS inventory that is detected and mitigated by the low low PZR level actuation function.

Low Reactor Coolant System Flow

RCS flow rate is a function of reactor power in the NuScale design, such that low RCS flow is only possible during startup conditions. The low-low RCS flow protective function is credited for actuating RTS and CVCS isolation in the event of a MHS malfunction that causes an RCS flow reversal. This event is not considered credible in combination with a digital-based CCF of the RCS flow sensor due to the very short, and limited operating window where the MHS failure could occur.

The low RCS flow ESFAS actuation is used as a boron dilution initial condition but is not credited as part of the transient detection or mitigation. The minimum RCS 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 mitigating actuations of RTS or DWS isolation. Because this is not a credited signal, this event is non-limiting.

7.1.5.3 Diversity and Defense-in-Depth Assessment Regulatory Conformance

Conformance with SRM 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

"The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed."

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 that plant response to vulnerabilities is either bounded by Chapter 15 analyses or within acceptable limits.

Point 2

"In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events."

The D3 assessment demonstrates that there is adequate diversity within the MPS for each event that is evaluated in the accident analysis section of the Safety Analysis Report.

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 that plant response to vulnerabilities is either bounded by Chapter 15 analyses or within acceptable limits.

Point 3

"If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

The D3 assessment demonstrates that sufficient diversity exists within the MPS to prevent a postulated digital-based CCF from disabling the capability to perform any of 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

"A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above."

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 analog components and is downstream of the automatic digital portion of the safety system. The MCS, SDIS, and manual controls are sufficiently diverse that any failure does not prevent the operator from obtaining or resolving conflicting information (Section 7.1.5.1.6).

7.1.6 Safety Evaluation

Conformance with 10 CFR 50 Appendix A

General Design Criterion 1

The I&C systems are designed to the quality assurance program requirements as described in Section 7.1.1, Section 7.2.1, and Section 17.5.

General Design Criterion 2

The I&C systems and components required to function during natural phenomena events are located within structures that protect them against natural phenomena. See Section 7.1.1 and Section 7.2.2.

General Design Criterion 4

The I&C systems are designed for the environmental conditions that are associated with normal operation, maintenance, testing, and postulated accidents to which they may be subjected and required to function. See Section 7.1.1 and Section 7.2.2.

General Design Criterion 5

The MPS, NMS, MCS, and ICISs are not shared between NPMs. The PCS and PPS are shared between multiple NPMs and are designed to not adversely affect the ability of I&C platforms to perform safety-related functions. See Section 7.1.1 and Section 7.2.11.

General Design Criterion 10

The MPS provides the reactor trips and ESF actuations based on analytical limits with appropriate margin to ensure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of AOOs. The MPS also monitors NPM variables and provides these signals to the MCS for control and indication. The NMS monitors and provides neutron flux levels to the MPS. See Section 7.1.1.

General Design Criterion 13

The I&C systems monitor variables and systems over their anticipated ranges for normal operations, AOOs, and accident conditions to ensure adequate safety. See Section 7.1.2, Section 7.1.4, Section 7.1.5, Section 7.2.7, and Section 7.2.13.

General Design Criterion 15

The MPS and NMS provide the appropriate controls to the NPM with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during normal operations or as a result of an AOO. See Section 7.1.1.

General Design Criterion 16

The MPS initiates containment isolation and safety-related functions. In addition, MPS removes power to the secondary main steam isolation valves (MSIVs) and the main feedwater regulating valve upon DHRS actuation, providing a backup containment isolation function. See Section 7.1.1.

Principal Design Criterion 19

The I&C systems ensure the ability to control each NPM during normal and accident conditions. The NuScale MCR is designed with the ability to place the reactors in safe shutdown in the event of an MCR evacuation event, and for safe shutdown to be maintained without operator action thereafter. Prior to 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 MPS equipment rooms within the reactor building. Following shutdown and initiation of passive cooling from either the MCR or the MPS equipment rooms, the NuScale design does not rely on operator action, instrumentation, or controls outside of the MCR to maintain safe shutdown condition. The design includes an RSS for monitoring of the plant if the MCR is evacuated. There are no displays, alarms or controls in the RSS credited to meet the requirements of principal design criterion (PDC) 19 as there is no manual control of safety-related equipment allowed from the RSS. See Section 7.1.1 and Section 7.2.13.

General Design Criterion 20

The MPS, with inputs from the NMS, senses when specified parameters are exceeded and initiates reactor trips and ESF actuations to ensure that 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. See Section 7.1.1 and Section 7.2.7.

General Design Criterion 21

The MPS and NMS have sufficient redundancy and independence to ensure that no single failure results in the loss of the protection function. The MPS and NMS components may be removed from service to permit periodic testing during operation, including the capability to test channels independently to determine failures and losses of redundancy that may have occurred. See Section 7.1.2, Section 7.1.3, Section 7.1.4, and Section 7.2.15.

General Design Criterion 22

The MPS and NMS have sufficient functional diversity to prevent the loss of a protection function. See Section 7.1.2 and Section 7.1.5.

General Design Criterion 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 on some other defined basis if conditions such as disconnection of the system, loss of power, or postulated adverse environments are experienced. See Section 7.1.1.

General Design Criterion 24

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. See Section 7.1.2, Section 7.1.3, and Section 7.1.5.

General Design Criterion 25

The MPS initiates reactor trip functions to ensure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control system. See Section 4.6.2 and Section 7.1.1.

General Design Criterion 28

The MPS initiates reactor trip functions to limit the potential amount and rate of reactivity increase and to ensure sufficient protection from reactivity accidents. See Section 4.6.2, and Section 7.1.1.

General Design Criterion 29

The MPS and NMS are designed with sufficient redundancy and diversity to ensure high probability of accomplishing their safety-related functions in the event of AOOs. See Section 7.1.3.

General Design Criterion 64

The MCS and PCS provide monitoring of radioactivity releases, reactor containment atmosphere, and plant environments for radioactivity that may be released from normal operations, AOOs, and postulated accidents. See Section 7.1.1.

Conformance with Other 10 CFR 50 Requirements

10 CFR 50.34(b)(2)(i)

The NuScale 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.

10 CFR 50.34(f)(2)(iv)

The SDIS, MCS, and PCS provide the capability to display important plant variables over their anticipated ranges for normal operation, AOOs, and accident conditions. See Section 7.2.13.

10 CFR 50.34(f)(2)(v)

The MCR displays bypassed and operable status indication of safety interlocks. See Section 7.2.4 and Section 7.2.13.

10 CFR 50.34(f)(2)(xi)

The MCR displays reactor safety valve position indication. See Section 7.2.13.

10 CFR 50.34(f)(2)(xiv)(C)

Containment isolation is initiated by two diverse signals from the MPS that ensure the isolation valves do not re-open upon logic reset, as shown in Section 7.1.5 and Section 7.2.3.3.

10 CFR 50.34(f)(2)(xvii)

The 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. See Section 7.2.13.

10 CFR 50.34(f)(2)(xviii)

The MPS and NMS provide MCR indications of inadequate core cooling. See Section 7.2.13.

10 CFR 50.34(f)(2)(xix)

The MPS and NMS provide instrumentation for monitoring plant conditions following an accident that includes potential core damage. See Section 7.2.13.

10 CFR 50.36(c)(1)(ii)(A)

The MPS initiates automatic protective actions prior to exceeding a safety limit. See Section 7.2.7.

10 CFR 50.36(c)(3)

The I&C systems are designed to meet surveillance requirements to ensure that the necessary quality of SSC is maintained such that operation is within safety limits and limiting conditions of operations are met. See Section 7.2.7 and Section 7.2.15.

10 CFR 50.49

The I&C equipment that perform the functions in 10 CFR 50.49(b) remain functional during and following DBEs. See Section 7.2.2.

10 CFR 50.44(jj) and 10 CFR 50.55(i)

The I&C systems are designed, tested, and inspected to quality standards commensurate with the safety function to be performed. See Section 7.2.1.

10 CFR 50.55a(1h)

The MPS and the 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.

10 CFR 50.62

An ATWS was considered in the design of I&C systems as it relates to the design provisions of subpart (c)(1). The portion of (c)(1) related to automatic initiation of the auxiliary feedwater system is not applicable to the NuScale design. The NuScale design supports an exemption from the portion of (c)(1) related to diverse turbine trip capability. The diversity internal to MPS ensures safety function performance in the presence of CCF. The MPS design leads to a simpler overall I&C architecture than other previously accepted solutions for 10 CFR 50.62 that involved separate diverse actuation systems. The MPS design also results in higher quality and simpler system interfaces than other previously accepted solutions for 10 CFR 50.62 that involved nonsafety-related diverse actuation systems. The D3 coping analyses meet the intent of the subpart (c)(2), which is not applicable to the NuScale design, by demonstrating that MPS digital-based CCF vulnerabilities do not result in consequences that exceed accepted regulatory criteria. See Section 7.1.5.

7.1.7 Simplicity

This section provides a description the simplicity attributes that have been considered and incorporated into the design of the NuScale I&C system architecture. Simplicity is a cross-cutting design element and an evaluation of the simplicity of the NuScale 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 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, the testing and maintenance is enhanced because each protective function can be taken out of service or bypassed for testing, maintenance, or repair without any 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 rigorously segmented into five separate and distinct communication domains based on the safety function of the communication:
  - SDB (3 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 any safety functions. The calibration test bus provides for calibration of tunable parameters and is used during maintenance of the MPS. Communications within the MIB and calibration test bus are performed on separate, isolated communication paths that have no interaction with any 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 MCS to 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 may 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 NuScale 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 NuScale 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 NuScale I&C architecture is composed of a series of building blocks. Each safety block is composed of three types of FPGA-based modules: SFMs, communication modules, and EIMs. Because each type of module performs different functions, the logic implementations differ significantly. For example, logic implemented for trip determination on an SFM is significantly 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 NuScale 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 NuScale 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 7.1-16). 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 that 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 that 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 that 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 that the SIL 3 and 4 portions of the logic design are correctly implemented in the logic and that the logic introduces no new hazards.

Testing Phase

Software safety test analysis is performed during the test phase to confirm that the SIL 3 and 4 portions of the software or configurable logic device logic design are correctly implemented in the logic and that the logic introduces no new hazards. For example, software stress testing is performed to ensure that 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 that 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 NuScale 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 all 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 NuScale I&C system hazard analysis is intended to evaluate 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 7.1-9). The STPA methodology departs from the standard failure modes and effects analysis 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 is a methodology in which organizational and process control systems can be modeled to show interactions between processes and components. 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 that 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 7.1-15 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. This can be seen in the high-level control structure diagram in Figure 7.1-16 and the lower level functional diagram in Figure 7.1-18.

By evaluating the control structures on a functional level, the analysis can be performed before any significant design work is completed and 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 the potential for inadequate control of the system 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.

2) Determine how each potentially hazardous control action identified in step 1 could occur.

3) 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 NuScale I&C system as described in Section 7.0 was 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. Any 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 defense-in-depth 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 7.1-19. This list is based on the limits for the MPS as provided in Table 7.1-20.

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 7.1-21 indicate the hazard conditions which 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 7.1-20. This analysis is based on the safety functions initiated by any 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 7.1-22 expands the safety constraints shown in Table 7.1-21 to address the individual safety functions of Table 7.1-20. This is done 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.

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 7.1-20. The SFMs accept up to four 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 7.1-19.

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, MCS; the safety-related protection system, 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 7.1-16. 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 priority logic portions of 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 Neutron Monitoring Control Structure

The control structure for the NMS ex-core sensors and process instrumentation consists of the control and monitoring systems, process instrumentation, and sensors. This structure is shown in Figure 7.1-17. Beginning at the top of Figure 7.1-17, the control and monitoring systems manipulate the different functions and variables that affect the reactor power level that the NMS is monitoring. The NMS monitors the neutron flux levels of the controlled process and supplies the control and monitoring systems with current levels and conditions. The NMS also updates the control and monitoring systems with the status and condition of the NMS circuits. The control and monitoring systems use this information to update the operator.

Example Low-Level Logic Structure - Safety Function Module

The SFM logic (Figure 7.1-18) 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 communications bus, 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. The process variable value signal,

along with generated signal quality information, is sent to the MIB communications module.

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. For example, looking at the signal conditioning in Figure 7.1-18, 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 7.1-23 reflects this in the first row by showing that 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 that the constraint is intended to mitigate. The second number is a unique number that is incremented for each identified SC.
- Possible causes that refer to "algorithm" errors may be due to requirements, design, or implementation. Any FPGA errors, 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 7.1-24 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 most significant differences between the lists are that the preliminary hazard list focused primarily on failures due to physical events. The hazard analysis identified causes such as operator error and procedural error as well as possible design deficiencies such as software and algorithm error. These differences support the use of the STPA methodology for analyzing complex systems such as the MPS.

The NuScale 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 defense-in-depth; however, the hazard conditions identified in the hazards analysis are partially or fully 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 that 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 Rev. 2.

7.1-2 Not Used.

7.1-3 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Standard 603-1991, Piscataway, NJ.

7.1-4 Not Used

7.1-5 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.

7.1-6 Not Used.

7.1-7 Not Used.

7.1-8 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.

7.1-9 Leveson, N.G., "Engineering a Safer World: Systems Thinking Applied to Safety," Massachusetts Institute of Technology, Cambridge, MA, 2011.

7.1-10 Not Used.

7.1-11 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," IEEE Standard 497-2002, Piscataway, NJ.

7.1-12 Not Used.

7.1-13 Not Used.

7.1-14 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," IEEE Standard 384-1992, Piscataway, NJ.

7.1-15 NuScale Power, LLC, "Nuclear Steam Supply Systems Advanced Sensor Technical Report," TR-0316-22048 Rev. 0.

7.1-16 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	Event Type	Credited Signals
Decrease in Feedwater Temperature	Cooldown Event	Described in Section 15.1.1.2
Increase in Feedwater Flow	Cooldown Event	Described in Section 15.1.2.2
Increase in Steam Flow	Cooldown Event	Described in Section 15.1.3.2
Inadvertent Opening of Steam Generator Relief or Safety Valve	Cooldown Event	Described in Section 15.1.4.2
Steam System Piping Failures Inside and Outside of Containment	Cooldown Event	Described in Section 15.1.5.2
Loss of Containment Vacuum/Containment Flooding	Cooldown Event	Described in Section 15.1.6.2
Loss of External Load	Heatup Event	Described in Section 15.2.1.2
Turbine Trip	Heatup Event	Described in Section 15.2.2.2
Loss of Condenser Vacuum	Heatup Event	Described in Section 15.2.3.2
Closure of Main Steam Isolation Valve(s)	Heatup Event	Described in Section 15.2.4.2
Loss of Nonemergency AC Power to the Station Auxiliaries	Heatup Event	Described in Section 15.2.6.2
Loss of Normal Feedwater Flow	Heatup Event	Described in Section 15.2.7.2
Inadvertent Operation of DHRS	Heatup/Cooldown Event	Described in Section 15.2.9.2
Feedwater System Pipe Breaks Inside and Outside of Containment	Heatup Event	Described in Section 15.2.8.2
Uncontrolled Control Rod Assembly Withdrawal from a Subcritical or Low Power or Startup Condition	Reactivity Event	Described in Section 15.4.1.2
Uncontrolled Control Rod Assembly Withdrawal at Power	Reactivity Event	Described in Section 15.4.2.2
Control Rod Misoperation	Reactivity Event	Described in Section 15.4.3.2
Inadvertent Decrease in Boron Concentration in the Reactor Coolant System	Reactivity Event	Described in Section 15.4.6.2
Spectrum of Rod Ejection Accidents	Reactivity Event	Described in Section 15.4.8.2
Chemical and Volume Control System Malfunction	Increase in RCS Inventory Event	Described in Section 15.5.1.2
Failure of Small Lines Carrying Primary Coolant Outside Containment	Decrease in RCS Inventory Event	Described in Section 15.6.2.2
Steam Generator Tube Failure	Decrease in RCS Inventory Event	Described in Section 15.6.3.2
Loss-of-Coolant Accidents Resulting from Spectrum of Postulated Piping Breaks within the Reactor Coolant Pressure Boundary	Decrease in RCS Inventory Event	Described in Section 15.6.5.2
Inadvertent Operation of Emergency Core Cooling System	Decrease in RCS Inventory Event	Described in Section 15.6.6.2
Instability Events	Special Event	Described in Section 15.9
Station Blackout	Special Event	Described in Section 8.4

Table 7.1-2: Variables Monitored by Module Protection System

VARIABLE	Range	Nominal (100% RTP)
Pressurizer Level	0 to 100%	50% full scale
Pressurizer Pressure	1500 to 2200 psia	1850 psia
RPV Riser Level	0 to 100%	100%
Wide Range RCS Pressure	0 to 2500 psia	1850 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 1200 psia	0.1 psia
Containment Isolation Valve Positions	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 Hot Temperature (NR RCS Thot)	400 to 650 °F	589 °F
Wide Range RCS Hot Temperature (WR RCS Thot)	40 to 700 °F	589 °F
Wide Range RCS Cold Temperature (WR RCS Tcold)	40 to 700 °F	507 °F
Core Exit Temperature	0 to 2300 °F	595 °F
Core Inlet Temperature	0 to 2300 °F	501 °F
Degrees of Subcooling (calculated from WR RCS Thot and WR RCS Pressure)	calculated variable	30 °F
RCS Flow	0 to 110%	100%
Main Steam Pressure (DHR Inlet Pressure)	0 to 1200 psia	500 psia
Main Steam Temperature (DHR Inlet Temperature)	100 to 700 °F	575 to 585 °F
Power Range Linear Power	0 to 125% RTP	100% RTP
Intermediate Range Linear Power	3 decades: 10^7 to 10^{10} cps	100% RTP equivalent
Intermediate Range Log Power	6 decades: 10^4 to 10^{10} cps	100% RTP equivalent
Intermediate Range Doubling Time	-5 to +5 seconds	0 seconds
Source Range Count Rate	5.5 decades: 5 to 10^6 cps	-
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 Supply Fault	Fault/No Fault	No Fault
Inside Bioshield Area Radiation Monitor	$1x10^0$ to $1x10^7$ R/hr	$1x10^0$ to $1x10^2$ R/hr
Reactor Trip Breaker Position Feedback	Open/Closed	Closed
Pressurizer Heater Trip Breaker Position Feedback	Open/Closed	Closed
DHRS Outlet Temperature	40 to 440 °F	90 to 110 °F
DHRS Outlet Pressure	0 to 1200 psia	500 psia
Module Operating Bay Pool Temperature	40 to 220 °F	85-100 °F
EDSS Bus Voltage	0 to 150 VDC	125 VDC
ELVS Voltage	0 to 600 VAC	480 VAC
Reactor Safety Valve Position	Open/Closed	Closed

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

VARIABLE	Range	Nominal (100% RTP)
Under-the-Bioshield Temperature	40 to 700 °F	130 °F
NMS-Flood	5 decades (cps)	-
Containment Evacuation System Pressure	0 to 14.7 psia	1 psia

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

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 = 120% RTP	4	2/4↑
High Intermediate Range Log Power Rate	3 dpm	4	2/4↑
High Power Range Positive and Negative Rate	+/- 15% RTP/minute	4	2/4↕
High Source Range Count Rate	$5x10^5$ cps	4	2/4↑
High Source Range Log Power Rate	3 dpm	4	2/4↑
High Narrow Range RCS Hot Temperature (NR RCS T_{hot})	610°F	4	2/4↑
High Narrow Range Containment Pressure	9.5 psia	4	2/4↑
High Pressurizer Pressure	2000 psia	4	2/4↑
Low Pressurizer Pressure	1720 psia	4	2/4↓
Low Low Pressurizer Pressure	1600 psia	4	2/4↓
High Pressurizer Level	80%	4	2/4↑
Low Pressurizer Level	35%	4	2/4↓
High Main Steam Pressure	800 psia	4	2/4↑
Low Main Steam Pressure	300 psia	4	2/4↓
Low Low Main Steam Pressure	20 psia	4	2/4↓
High Main Steam Superheat (MS Temperature and Pressure)	150°F	4	2/4↑
Low Main Steam Superheat (MS Temperature and Pressure)	0.0°F	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↑

Note 1: Normal AC voltage is monitored at the bus(es) supplying the battery chargers for the highly reliable DC power system.

Table 7.1-4: Engineered Safety Feature Actuation System Functions

ESF Function	Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Emergency Core Cooling System (ECCS)	High Containment Water Level	264" - 300" (elevation) (Note 3)	4	2/4↑	Removes Electrical Power to the trip solenoids of the reactor vent valves. Removes electrical power to the trip solenoids of the reactor recirculation valves
	Low ELVS voltage 24-hour Timer	24 hours	3	2/3	
Decay Heat Removal System (DHRS)	High Pressurizer Pressure	2000 psia	4	2/4↑	Removes electrical power to the trip solenoids of the decay heat removal valves Removes electrical power to the trip solenoids of the of the following valves in the containment, main steam, and feedwater systems: • main steam isolation valves • main steam isolation bypass valves • secondary main steam isolation valves • secondary main steam isolation valve bypass valves • feedwater isolation valves • feedwater regulating valves
	High Narrow Range RCS Hot Temperature (NR RCS Thot)	610°F	4	2/4↑	
	High Main Steam Pressure	800 psia	4	2/4↑	
	Low AC Voltage to Battery Chargers	80% of normal ELVS voltage Actuation Delay of 60 seconds (Note 4)	4	2/4↓	

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

ESF Function	Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Secondary System Isolation	High Pressurizer Pressure	2000 psia	4	2/4↑	Removes electrical power to the trip solenoids of the of the following valves in the containment, main steam, and feedwater systems: • main steam isolation valves • main steam isolation bypass valves • secondary main steam isolation valves • secondary main steam isolation valve bypass valves • feedwater isolation valves • feedwater regulating valves
	High Narrow Range RCS Hot Temperature (NR T_{hot})	610°F	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 Pressure	800 psia	4	2/4↑	
	Low Main Steam Superheat (MS Temperature and Pressure)	0.0°F	4	2/4↓	
	High Main Steam Superheat (MS Temperature and Pressure)	150°F	4	2/4↑	
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	
	Low Low Pressurizer Pressure	1600 psia (Note 2)	4	2/4↓	
	Low Low Pressurizer Level	20%	4	2/4↓	
	Low ELVS 480VAC to EDSS Battery Chargers	80% of normal ELVS voltage Actuation Delay of 60 seconds (Note 4)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	

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

ESF Function	Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Containment System Isolation (CSI) Signal	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	Removes electrical power to the trip solenoids of the following valves: • RCS injection valves • RCS discharge valves • PZR spray valves • RPV high point degasification line valves • feedwater isolation valves • feedwater regulating valves • main steam isolation valves • main steam isolation bypass valves • secondary main steam isolation valves • secondary main steam isolation valve bypass valves • containment evacuation system valves • reactor component cooling water system supply and return valves • containment flooding and drain system valves
	Low Low Pressurizer Level	20%	4	2/4↓	
	Low AC Voltage to Battery Chargers	80% of normal ELVS voltage Actuation Delay of 60 seconds (Note 4)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	
Demineralized Water System Isolation (DWSI)	High Power Range Linear Power	High-1 = 25% RTP High-2 = 120% RTP	4	2/4↑	Removes electrical power to the trip solenoids of the demineralized water supply valves (Note 5)
	High Intermediate Range Log Power Rate	3 dpm	4	2/4↑	
	High Power Range Positive and Negative Rate	+/- 15% RTP/minute	4	2/4↕	
	High Source Range Count Rate	$5x10^5$ cps	4	2/4↑	
	High Source Range Log Power Rate	3 dpm	4	2/4↑	
	High Narrow Range RCS Hot Temperature (NR RCS Thot)	610°F	4	2/4↑	
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	
	High Pressurizer Pressure	2000 psia	4	2/4↑	
	Low Pressurizer Pressure	1720 psia (Note 1)	4	2/4↓	

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

ESF Function	Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Demineralized Water System Isolation (DWSI) (continued)	Low Low Pressurizer Pressure	1600 psia (Note 2)	4	2/4↓	
	High Pressurizer Level	80%	4	2/4↑	
	Low Pressurizer Level	35%	4	2/4↓	
	High Main Steam Pressure	800 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°F	4	2/4↑	
	Low Main Steam Superheat (MS Temperature and Pressure)	0.0°F	4	2/4↓	
	Low RCS Flow	1.7 ft^3/s	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 4)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	
	High Subcritical Multiplication (SCM)	3.2	4	2/4↑	
Chemical and Volume Control System Isolation (CVCSI)	High Pressurizer Level	80%	4	2/4↑	Removes electrical power to the trip solenoids of the following valves: • RCS injection valves • RCS discharge valves • PZR spray valves • RCS high point degasification valves
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	
	Low Low Pressurizer Pressure	1600 psia (Note 2)	4	2/4↓	
	Low Low Pressurizer Level	20%	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 4)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	

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

ESF Function	Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Pressurizer Heater Trip	Low Pressurizer Level	35%	4	2/4↓	Removes electrical power to the PZR heaters
	High Pressurizer Pressure	2000 psia	4	2/4↑	
	High Narrow Range RCS Hot Temperature (NR RCS T_{hot})	610°F	4	2/4↑	
	High Main Steam Pressure	800 psia	4	2/4↑	
	Low AC Voltage to Battery Chargers	80% of normal ELVS voltage Actuation Delay of 60 seconds (Note 4)	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 5.2-10	4	2/4↑	Removes electrical power to the trip solenoids of the reactor vent valves

Note 1: If RCS hot temperature is ≥ 600°F.
Note 2: If RCS hot temperature is < 600°F.
Note 3: Containment vessel water level are presented in terms of elevation where reference zero is the bottom of the reactor pool. The ranges allow ±18" from the nominal ECCS level setpoint of 282".
Note 4: Normal AC voltage is monitored at the bus(es) supplying the battery chargers for the highly reliable DC power system.
Note 5: FSAR Section 9.3.4 describes "demineralized water supply isolation valves" as part of the CVCS system.

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 • Reactor Trip on High Source Range Log Power Rate • Demineralized Water System Isolation actuation on High Source Range Count 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 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.

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

Interlock/ Permissive/ Override	Condition for Interlock/Permissive/ Override	Function
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 • Reactor Trip on High Power Range Negative Rate • Demineralized Water System Isolation actuation on High Power Range Positive Rate • Demineralized Water System Isolation actuation on High Power Range Negative Rate • Reactor Trip on Low Main Steam Pressure • Secondary system isolation (SSI) actuation on Low Main Steam Pressure • Demineralized water system isolation actuation on Low Main Steam Pressure Operating bypasses are automatically removed when interlock condition is no longer satisfied.
V-1 Interlock	FWIV Closed Interlock: Interlock established when one FWIV indicates closed.	Automatically establishes an operating bypass of the following when N-2H is active (below 15% RTP): • Reactor trip on Low Main Steam Superheat. • Secondary system isolation on Low Main 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 F-1, T-2 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 > 325° 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 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 < 350° F	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 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 <600° F	Automatically establishes an operating bypass of the following: • Reactor Trip on Low Pressurizer Pressure • Demineralized water system isolation on Low Pressurizer Pressure 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 420°F AND RT-1 is active.	Automatically establishes an operating bypass of the following: • Secondary system isolation actuation on Low Low Pressurizer Pressure • Demineralized water system isolation actuation that occurs coincident with an automatic reactor trip signal. • Chemical and volume control system isolation actuation on Low Low Pressurizer Pressure.
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 Low Pressurizer Level • Secondary system isolation actuation on Low Low Main Steam Pressure • Secondary system isolation actuation on Low Main Steam Superheat • Secondary system isolation actuation on High Narrow Range Containment Pressure • Containment system isolation actuation on Low Low Pressurizer Level • Chemical and volume control system isolation actuation on Low Low Pressurizer Level Operating bypasses are automatically removed when interlock condition is no longer satisfied.
L-2 Interlock	Pressurizer Level Interlock, L2: Interlock established when 3 of 4 Pressurizer Level channels are greater than 20% AND T-3 interlock is active.	Automatically establishes operating bypass of the ECCS actuation on high containment water level.

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

Interlock/ Permissive/ Override	Condition for Interlock/Permissive/ Override	Function
F-1 Interlock	RCS Flow Interlock: Interlock established after a set time delay when at least 3 of 4 RCS Flow Channels $\leq$ 0.0 ft^3/sec and RT-1 has been established	Automatically establishes operating bypass of CVCS isolation on Low Low RCS Flow. Operating bypasses are automatically removed when interlock condition is no longer satisfied.
O-1 Override	Containment System Isolation Override Function: Override established when manual override switch is active and RT-1 permissive is established	Override allows manual control of the CFDS, 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 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
High Containment Water Level	Containment Level	3.0s
Low AC Voltage to the Battery Chargers	AC Voltage	60.0s
High Under-the-Bioshield Temperature	Under-the-Bioshield Temperature	8.0s

Table 7.1-7: Summary of Type A, B, C, D, and E Variables

Variable	Range	System	Type A	Type B	Type C	Type D	Type E
Neutron Flux (Note 1)	0-200% RTP	MPS		X		X	
Core Exit Temperatures	0-2300°F	MPS		X	X	X	
Core Inlet Temperatures	0-2300°F	MPS		X			
Wide Range RCS Pressure	0-2500 psia	MPS		X	X	X	
Degrees of Subcooling	N/A-calculated variable	MPS		X			
Wide Range RCS T_{HOT}	40-700°F	MPS		X			
RPV Riser Level	Top of upper core plate to top of RPV Riser	MPS		X	X	X	
Narrow Range Containment Pressure	0-20 psia	MPS		X			
Wide Range Containment Pressure	0-1200 psia	MPS		X	X	X	
Containment Water Level	ECCS RRVs to Top of Containment	MPS		X	X	X	
Containment Isolation Valve Positions	Closed	MPS		X	X	X	
Inside Bioshield Area Radiation Monitor	Note 3	MPS		X	X		
ECCS Valve Position	Open/Closed	MPS				X	
Reactor Pool Temperature (Operating Bay)	40-220°F	MPS				X	
Spent Fuel Pool Water Level	Top of spent fuel racks to top of pool	PPS				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	
Main Steam Temperature (DHRS Inlet Temperature)	100-700°F	MPS				X	
Main Steam Pressure (DHRS inlet pressure)	0-1200 psia	MPS				X	
DHRS Outlet Temperature	40-440°F	MPS				X	
DHRS Outlet Pressure	0-1200 psia	MPS				X	
RCS Flow	0-120% flow	MPS				X	
Reactor Trip Breaker Position Feedback	Open	MPS				X	
Pressurizer Heater Trip Breaker Position Feedback	Open	MPS				X	
Demineralized Water Supply Isolation Valve Position	Closed	MPS				X	
Under-the-Bioshield Temperature	40-700°F	MPS				X	
EDSS-MS and EDSS-C Bus Voltage	0-150 Vdc	MPS/PPS				X	
CRHS Air Supply Isolation Valve Position	Open	PPS				X	

Table 7.1-7: Summary of Type A, B, C, D, and E Variables (Continued)

Variable	Range	System	Type A	Type B	Type C	Type D	Type E
CRHS Pressure Relief Isolation Valve Position	Closed	PPS				X	
CRVS Supply Air Damper Position	Open/Closed	PPS				X	
CRVS Smoke Purge Exhaust Damper Position	Open/Closed	PPS				X	
CRVS General Exhaust Damper Position	Open/Closed	PPS				X	
CRVS Return Air Damper Position	Open/Closed	PPS				X	
Reactor Building Plant Exhaust Stack - Flowrate	0-110% flow rate	RBVS					X
Reactor Building Plant Exhaust Stack - Noble Gas Activity	Note 2	RBVS					X
Reactor Building Plant Exhaust Stack - Particulates And Halogens	Note 2	RBVS					X
Reactor Building Continuous Airborne Monitor - Noble Gas Activity	Note 3	RMS					X
Reactor Building Continuous Airborne Monitor - Particulates and Halogens	Note 3	RMS					X
Hot Lab - Area Radioactivity	Note 3	RMS					X
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
EDSS Switchgear Rooms - Area Radioactivity	Note 3	RMS					X
Safety Instrument Rooms - Area Radioactivity	Note 3	RMS					X
Reactor Building Access Tunnel - 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 Specific Environs Radiation and Radioactivity	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 of power range linear power, intermediate range log power, source range count rate; NMS-flood provides the source range count rate indication during conditions when the containment is flooded.
Note 2: The process and effluent radiation monitoring instrumentation ranges are provided in Section 11.5, Table 11.5-1.
Note 3: The fixed area and airborne radiation monitoring instrumentation ranges are provided in Section 12.3, Table 12.3-10.

Table 7.1-8: Variables Monitored by Plant Protection System

Variable	Range
ELVS Voltage 1 (Note 1)	0-600 VAC
ELVS Voltage 2 (Note 2)	0-600 VAC
ELVS Voltage 3 (Note 2)	0-600 VAC
ELVS Voltage 4 (Note 1)	0-600 VAC
CRVS Post Filter Air Radiation Sensor	Particulate: 3E-10 to 1E-6 µCi/cc Iodine: 3E-10 to 5E-8 µCi/cc Noble Gas: 3E-7 to 1E-2 µCi/cc
[[Outside Air Toxic Gas Sensor	Provided by COL applicant based on plant location]]
Outside Air Smoke Detector N/A	N/A
CRE Air Delivery Line Flow Sensor 1	0-150 SCFM
CRE Air Delivery Line Flow Sensor 2	0-1000 SCFM
CRE Differential Pressure Sensor	0-2 in water column
Emergency Pressurized Air Pressure	3000-4000 psig
Reactor/Refueling Pool Level Indication	0-69 ft
Spent Fuel Pool Level Indication	0-69 ft
EDSS-C Bus Voltage	0-150 VDC
CRHS Air Supply Isolation Valve Position	Open, Closed
CRHS Pressure Relief Isolation Valve Position	Open, Closed
CRVS Supply Air Damper Position	Open, Closed
CRVS Smoke Purge Exhaust Damper Position	Open, Closed
CRVS General Exhaust Damper Position	Open, Closed
CRVS Return Air Damper Position	Open, Closed
CRVS Outside Air Isolation Damper Position	Open, Closed

Note 1: This variable monitors AC power supplied to an EDSS-C battery charger and a CRVS air handling unit.
Note 2: This variable monitors AC power supplied to an EDSS-C battery charger.

Table 7.1-9: Sensor Inputs to Module Protection System

Process Variable	Sensor Type	Output Signal	Safety-Related?	Type A, B, or C PAM Variable?	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	N	X	X	-	X	X	-
RPV riser level	Digital	Analog	N	Y	-	X	-	X	-	-
PZR pressure (Note 1)	Digital	Analog	Y	N	X	X	-	X	X	-
Wide-range reactor coolant system (RCS) pressure (Note 1)	Digital	Analog	Y	Y	X	X	-	X	X	-
Containment water level (Note 1)	Digital	Analog	Y	Y	X	X	-	X	X	-
Narrow-range containment pressure	Analog	Analog	Y	Y	X	X	-	X	X	-
Wide-range containment pressure	Digital	Analog	N	Y	-	X	-	X	-	-
Containment isolation valve positions (except FWIV Valve Position)	Discrete (Analog)	Discrete (Analog)	N	Y	-	-	X	-	-	X
Secondary MSIV position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
Secondary MSIV bypass isolation valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
Feedwater regulation valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
ECCS valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
Narrow-range RCS hot temperature	Analog	Analog	Y	N	X	X	-	X	X	-
Wide-range RCS hot temperature	Analog	Analog	Y	Y	X	X	-	X	X	-
Wide-range RCS cold temperature	Analog	Analog	Y	N	X	X	-	X	X	-
Core exit temperature	Analog	Analog	N	Y	-	X	-	X	-	-
Core inlet temperature	Analog	Analog	N	Y	-	X	-	X	-	-
RCS flow (Note 1)	Digital	Analog	Y	N	X	X	-	X	X	-
Main steam pressure (decay heat removal inlet pressure)	Analog	Analog	Y	N	X	X	-	X	X	-
Main steam temperature (decay heat removal inlet temperature)	Analog	Analog	Y	N	X	X	-	X	X	-
Power range linear power	Analog	Analog	Y	Y	X	X	-	X	X	-
Intermediate range log power	Analog	Analog	Y	Y	X	X	-	X	X	-
Source range count rate	Analog	Analog	Y	Y	X	X	-	X	X	-
Source/intermediate range fault	Discrete (Analog)	Discrete (Analog)	Y	N	X	X	-	X	X	-
Power range fault	Discrete (Analog)	Discrete (Analog)	Y	N	X	X	-	X	X	-
NMS Supply Fault	Discrete (Analog)	Discrete (Analog)	Y	N	X	X	-	X	X	-
Inside bioshield area radiation monitor	Digital	Analog	N	Y	-	X	-	X	-	-

Table 7.1-9: Sensor Inputs to Module Protection System (Continued)

Process Variable	Sensor Type	Output Signal	Safety-Related?	Type A, B, or C PAM Variable?	Sensor Block I			Sensor Block II		
					SG A	SG C	DIV. I	SG B	SG D	DIV. II
FWIV positions	Discrete (Analog)	Discrete (Analog)	Y	Y	-	-	X	-	-	X
Reactor trip breaker position feedback	Discrete (Analog)	Discrete (Analog)	Y	N	-	-	X	-	-	X
Pressurizer heater breaker status	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
DHRS valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
DHRS outlet temperature	Analog	Analog	N	N	-	X	-	X	-	-
DHRS outlet pressure	Analog	Analog	N	N	X	X	-	X	-	-
Demineralized water system isolation valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
Reactor pool temperature	Analog	Analog	N	N	-	X	-	X	-	-
EDS voltage	Analog	Analog	N	N	-	X	-	X	-	-
ELVS voltage	Analog	Analog	Y	N	X	X	-	X	X	-
Reactor safety valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	X	-	X	-	-
Under-the-bioshield temperature	Analog	Analog	Y	N	X	X	-	X	X	-
NMS-Flood	Analog	Analog	N	Y	-	X	-	X	-	-
NMS-Flood Faults	Discrete (Analog)	Discrete (Analog)	N	Y	-	X	-	X	-	-
Containment evacuation vacuum pump suction pressure	Analog	Analog	N	N	X	-	-	-	X	-

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

Table 7.1-10: 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)		
iV&V design simulation tool(s)	Different than Suite A and Suite B	

Table 7.1-11: 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 (Note 1)
3	ECCS and LTOP	ECCS reactor vent valves (Note 1)
4	Containment isolation	Containment evacuation CIV Containment flood & drain CIV Reactor component cooling water CIVs
5	CVCS isolation and containment isolation	CVCS containment isolation valves
6	DWS isolation and loss of AC power	DWS isolation valve
7	PZR heater trip	PZR heater breakers
8	DHRS	DHRS Actuation Valves

Note 1: The ECCS valves include an inadvertent actuation block (IAB) described in Section 7.2.5.2 that is designed to prevent the spurious opening of the ECCS valves at normal operating pressures. The spurious opening of the ECCS valves below the IAB setpoint is bounded by the plant safety analysis described in Chapter 15.

Table 7.1-12: Consequences of Partial Spurious Reactor Trip

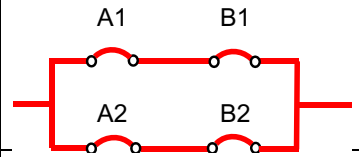
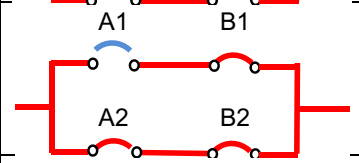
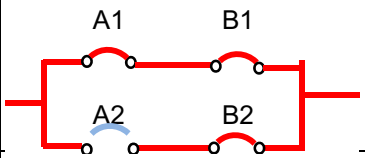
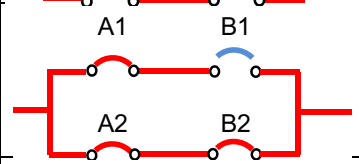
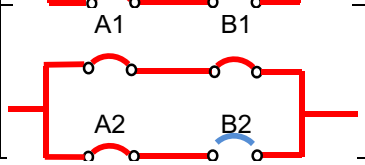
Event		RTS Trip Demand		Reactor Trip Breaker Status	Result	
No.	**Description**				**Reactor Trip**	**Comments /Notes**
1	No trip No failure	A1	B1		**No**	Normal operation
		N	**N**			
		A2	B2			
		N	**N**			
2	Partial spurious Division I trip	A1	B1		**No**	Only one of the two Division I RTBs trip which 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 7.1-13: 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
	Containment water level	Digital-based CCF	OK
Digital-based pressure measurement	PZR pressure	OK	OK
	Wide-range RCS pressure	OK	OK
Digital-based flow measurement	RCS flow	OK	OK

Table 7.1-14: Effects of Digital-Based Common Cause Failure of Digital-Based Pressure Measuring System 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
	Containment water level	OK	OK
Digital-based pressure measurement	PZR pressure	Digital-based CCF	Digital-based CCF
	Wide-range RCS pressure	Digital-based CCF	Digital-based CCF
Digital-based flow measurement	RCS flow	OK	OK

Table 7.1-15: 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
	Containment water level	OK	OK
Digital-based pressure measurement	PZR pressure	OK	OK
	Wide-range RCS pressure	OK	OK
Digital-based flow measurement	RCS flow	Digital-based CCF	Digital-based CCF

Table 7.1-16: Safety-Related Digital Sensors Used by Safety Block I and II

Input Signal	Sensor Technology	Function
Containment water level	Digital-based level	Accident monitoring initiate protective action(s)
PZR water level	Digital-based level	Accident monitoring initiate protective action(s)
Wide-range RCS pressure	Digital-based pressure	Accident monitoring initiate protective action(s)
PZR pressure	Digital-based pressure	Initiate protective action(s)
RCS flow	Digital-based flow	Initiate protective action(s)

Table 7.1-17: Effect of FPGA Technology Diversity for Postulated Digital-Based CCF of MPS 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 7.1-18: Digital Sensors Credited for Mitigating Anticipated Operational Occurrences and Postulated Accidents

Design Basis Event	Typical Signals Credited in Plant Safety Analysis Described in Chapter 15	Signals Credited in D3 Best-Estimate Coping Analysis	Comments
Category 1 Events			
For these events listed in this category, the digital-based sensors subject to a CCF are not relied upon or credited in either the plant safety analysis described in Chapter 15 or the best-estimate D3 coping analysis. The sensors credited do not use digital-based technology and are not subject to a digital-based CCF; therefore, sufficient diversity is provided by the FPGA technology diversity within the MPS as shown in Table 7.1-17.			
Decrease in Feedwater Temperature	high power range linear power high RCS hot temperature high main steam pressure high main steam superheat	high power range linear power	No digital-based sensor relied upon for deterministic plant safety analysis (Chapter 15) or best estimate analysis. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Increase in Feedwater Flow	high power range linear power high main steam pressure high RCS hot temperature low main steam superheat	high power range linear power high main steam pressure	No digital-based sensor relied upon for deterministic plant safety analysis (Chapter 15) or best estimate analysis. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Feedwater System Pipe Breaks Inside of Containment	high CNV pressure	high CNV pressure	No digital-based sensor relied upon for deterministic plant safety analysis (Chapter 15) or best estimate analysis. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Loss of Containment Vacuum	high CNV pressure high main steam pressure	high CNV pressure	No digital-based sensor relied upon for deterministic plant safety analysis (Chapter 15) or best estimate analysis. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Steam System Piping Failures Inside of Containment	high CNV pressure	high CNV pressure	No digital-based sensor relied upon for deterministic plant safety analysis (Chapter 15) or best estimate analysis. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.

Table 7.1-18: Digital Sensors Credited for Mitigating Anticipated Operational Occurrences and Postulated Accidents (Continued)

Design Basis Event	Typical Signals Credited in Plant Safety Analysis Described in Chapter 15	Signals Credited in D3 Best-Estimate Coping Analysis	Comments
Category 2 Events			
For the events listed below in this section, when evaluated by the plant safety analysis described in Chapter 15, the event progresses to a point when a trip condition is generated by the credited signals listed; however, when evaluating these events using best-estimate methods, no setpoint is reached which would require an MPS protective function to actuate.			
Loss of External Load	high main steam pressure high PZR pressure (digital-based)	No sensors credited using best-estimate analysis.	The best-estimate analysis does not generate a trip condition, such that no digital-based sensor is relied upon for best estimate analysis. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Turbine Trip	high main steam pressure high PZR pressure (digital-based)	No sensors credited using best-estimate analysis.	The best-estimate analysis does not generate a trip condition, such that no digital-based sensor is relied upon for best estimate analysis. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Category 3 Events			
For the events listed in this section, the digital-based sensor subject to a CCF is credited in both the deterministic analyses described in Chapter 15 and best-estimate analyses; however, multiple, diverse sensors that do not use digital-based technology provide the required protection in the best-estimate D3 coping analyses; therefore, sufficient sensor diversity exists to provide the required safety function. The FPGA technology diversity in the MPS divisions ensures a digital-based CCF does not prevent the MPS from performing its required safety function.			
Failure of Small Lines Carrying Primary Coolant Outside Containment	low PZR level (digital-based) (note 1) low PZR pressure (digital-based) high PZR pressure (digital-based) high main steam superheat	low PZR level (digital-based) (note 1) low PZR pressure (digital-based) (note 3)	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Inadvertent Decrease in Boron Concentration in the Reactor Coolant System	high PZR pressure (digital-based) high RCS hot temperature high power range linear power high power range rate high source range count rate high intermediate range log power (low power events)	high power range linear power high power range rate high intermediate range log power positive rate high source range count rate high RCS hot temperature high PZR pressure (digital-based) (note 3)	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.

Table 7.1-18: Digital Sensors Credited for Mitigating Anticipated Operational Occurrences and Postulated Accidents (Continued)

Design Basis Event	Typical Signals Credited in Plant Safety Analysis Described in Chapter 15	Signals Credited in D3 Best-Estimate Coping Analysis	Comments
Inadvertent Operation of DHRS	high RCS hot temperature high main steam pressure high PZR pressure (digital-based)	high RCS hot temperature high main steam pressure high PZR pressure (digital-based) (note 3)	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Uncontrolled Control Rod Assembly Withdrawal from a Subcritical or Low Power	high power range linear power high intermediate range log power positive rate high source range count rate high PZR pressure (digital-based)	high power range linear power high intermediate range log power positive rate high source range count rate high PZR pressure (digital-based) (note 3)	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Uncontrolled Control Rod Assembly Withdrawal at Power	high power range linear power high RCS hot temperature high power range positive rate high PZR pressure (digital-based)	high power range linear power high RCS hot temperature high power range positive rate high PZR pressure (digital-based) (note 3)	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Loss of Condenser Vacuum	high main steam pressure high PZR pressure (digital-based)	high main steam pressure high PZR pressure (digital-based) (note 3)	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Loss of Nonemergency AC Power to the Station Auxiliaries	high main steam superheat high PZR pressure (digital-based) high main steam pressure	high main steam superheat high PZR pressure (digital-based) (note 3) high main steam pressure	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Loss of Normal Feedwater Flow	high PZR pressure (digital-based) high RCS hot temperature	high PZR pressure (digital-based) (note 3) high RCS hot temperature high power rate	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.

Table 7.1-18: Digital Sensors Credited for Mitigating Anticipated Operational Occurrences and Postulated Accidents (Continued)

Design Basis Event	Typical Signals Credited in Plant Safety Analysis Described in Chapter 15	Signals Credited in D3 Best-Estimate Coping Analysis	Comments
System Malfunction that Increases Reactor Coolant Inventory	high PZR level (digital-based) (note 1) high PZR pressure (digital-based) high main steam pressure	high PZR level (digital-based) (note 1) high PZR pressure (digital-based) (note 3) high CNV pressure high main steam pressure	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Feedwater System Pipe Breaks Outside of Containment	high PZR pressure (digital-based) high main steam superheat low main steam pressure high main steam pressure high RCS hot temperature	high PZR pressure (digital-based) (note 3) high main steam superheat low main steam pressure high RCS hot temperature	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Steam Generator Tube Failure	low PZR level (digital-based) (note 1) high PZR pressure (digital-based) high main steam pressure low PZR pressure (digital-based)	low PZR level (digital-based) (note 1) low PZR pressure (digital-based) (note 3) high main steam pressure low main steam superheat	Sensor diversity ensures performance of required safety function is satisfied. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Category 4 Events			
For the design basis events listed below, while the deterministic plant safety analyses described in Chapter 15 credit the function provided by the digital-based sensors that are subject to a CCF; however, the evaluation of the plant response for these events using best-estimate analysis methods determined that the plant response does not progress to the point where the digital-based sensor is relied upon to provide required protection. In these events, other sensors that do not use digital-based technology and are not subject to a digital-based CCF provide the required safety function and the FPGA technology diversity in the MPS divisions ensures a digital-based CCF does not prevent the MPS from performing its required safety function (note 2).			
Control Rod Misoperation	high power range linear power high RCS hot temperature high PZR pressure (digital-based) high power rate	high power range linear power high RCS hot temperature high power rate	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Inadvertent Operation of Emergency Core Cooling System (ECCS)	high CNV pressure high CNV level (digital-based) (note 1)	high CNV pressure high CNV level (digital-based) (note 1)	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.

Table 7.1-18: Digital Sensors Credited for Mitigating Anticipated Operational Occurrences and Postulated Accidents (Continued)

Design Basis Event	Typical Signals Credited in Plant Safety Analysis Described in Chapter 15	Signals Credited in D3 Best-Estimate Coping Analysis	Comments
Instability Events	high RCS hot temperature low PZR level (digital-based) (note 1) low PZR pressure (digital-based)	high RCS hot temperature low PZR level (digital-based) (note 1)	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Loss-of-Coolant Accidents from a Spectrum of Postulated Piping Breaks inside CNV	high PZR pressure (digital-based) high CNV level (digital-based) (note 1) high CNV pressure low PZR level (digital-based) (note 1)	high CNV level (digital-based) (note 1) high CNV pressure	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other divisions remains fully functional.
Increase in Steam Flow	high power range linear power high RCS hot temperature high main steam superheat high PZR pressure (digital-based) low main steam pressure	high power range linear power low main steam pressure	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Inadvertent Opening of Main Steam Safety Valve	high RCS hot temperature high main steam superheat high PZR pressure (digital-based) high power range linear power low main steam pressure	low main steam pressure high power range linear power	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Closure of Main Steam Isolation Valve	high main steam pressure high PZR pressure (digital-based)	high main steam pressure	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Steam System Piping Failures Outside of Containment	high power range linear power low main steam pressure high PZR pressure (digital-based) high RCS hot temperature high main steam superheat low main steam superheat	high power range linear power low main steam pressure	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.

Table 7.1-18: Digital Sensors Credited for Mitigating Anticipated Operational Occurrences and Postulated Accidents (Continued)

Design Basis Event	Typical Signals Credited in Plant Safety Analysis Described in Chapter 15	Signals Credited in D3 Best-Estimate Coping Analysis	Comments
Spectrum of Rod Ejection Accidents	high power range linear power high power range positive rate high PZR pressure (digital-based) high RCS hot temperature	high power range linear power high power range positive rate	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.

Note 1: The digital-based level measurement function incorporates equipment diversity between sensor blocks I and II such that a postulated CCF of the digital-based level measurement function is limited to one sensor block only. Since the other sensor block remains functional, sufficient diversity exists for those functions that rely on the digital-based level measurement function, see Section 7.1.5.1.2.

Note 2: The design basis for the digital-based RCS flow sensors in the plant safety analysis described in Section 15.4.6 is to ensure minimum RCS flow rates exist during dilution events to ensure proper mixing within the RCS; therefore, the RCS flow sensors are not included in Table 7.1-18 as they are not relied upon for detection or mitigation of AOOs or postulated accidents as described in Section 7.1.5.2. The plant safety analysis credits the high subcritical multiplication protective function for detection and mitigation of an uncontrolled RCS dilution. Best-estimate analysis of this event concludes the event is non-limiting and does not rely on the digital-based RCS flow sensor to function. The consequences of RCS flow stagnation or reversal during low power conditions are addressed in NuScale Power, LLC topical report, "Non-Loss-of-Coolant Accident Analysis Methodology," TR-0516-49416. The FPGA technology diversity in the MPS divisions ensures a digital-based CCF does not prevent the MPS from performing its required safety function.

Note 3: Reactor module conditions that reach the pressurizer high or low pressure signal may occur in the best estimate transient progression but actuations from this process condition are not credited in the D3 coping analysis.

Table 7.1-19: 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 7.1-20: Example: Safety Functions

Safety Function ID	Safety Function	Initiating Conditions	Setpoint
SF-1a	Reactor trip	High power	10% > nominal
SF-1b		High log power rate	3 decades per minute
SF-1c		High narrow range RCS hot temperature	600 °F
SF-2a	DHRS actuation	High pressurizer pressure	2000 psia
SF-2b		High pressurizer level	80%
SF-2c		Low main steam pressure	300 psia

Table 7.1-21: 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 7.1-22: Example: Safety Constraints Associated with Plant Conditions

Safety Constraint ID	Condition	Constraint
SC-1a	Variable high power	RTBs must be opened when neutron flux = High setpoint
SC-1b	High rate power change	RTBs must be opened when the rate of change of reactor power = High neutron flux rate setpoint
SC-1c	High T_{hot}	RTBs must be opened when narrow range RCS hot temperature $\geq$ High narrow range RCS hot temperature setpoint
SC-2a	Low steam pressure	Decay heat removal must be actuated when steam pressure = Low steam pressure setpoint
SC-2b	High steam pressure	Decay heat removal must be actuated when steam pressure = High steam pressure setpoint
SC-2c	Containment isolation	Decay heat removal must be actuated when containment isolation is actuated

Table 7.1-23: 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 7.1-24: 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	Loss of power
Loss of power	Operates at incorrect time
Module hardware fault	Operates inadvertently
Operator error	Operates incorrectly/erroneously
Power supply voltage too high or low	Receives erroneous data
Procedural error	Sends erroneous data
Reactor trip breaker fault	Failure due to corrosion
Safety-related isolator fault	Failure due to faulty calibration
Sensing line damaged	Failure due to overvoltage or overcurrent
Sensor does not provide an output	Failure due to dust/dirt
Setpoint error	Failure due to EMI/RFI interference
Software/algorithm error	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 OOS 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 OOS 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, ALL SAFETY FUNCTIONS FOR THAT SFM ARE FORCED TO NOT TRIP OR NOT ACTUATE. IF THE TRIP/BYPASS SWITCH IS IN THE TRIP POSITION, THEN ALL SAFETY FUNCTIONS FOR THAT SFM ARE FORCED TO TRIP AND 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. (ASSOCIATED LOGIC IS SHOWN BELOW)

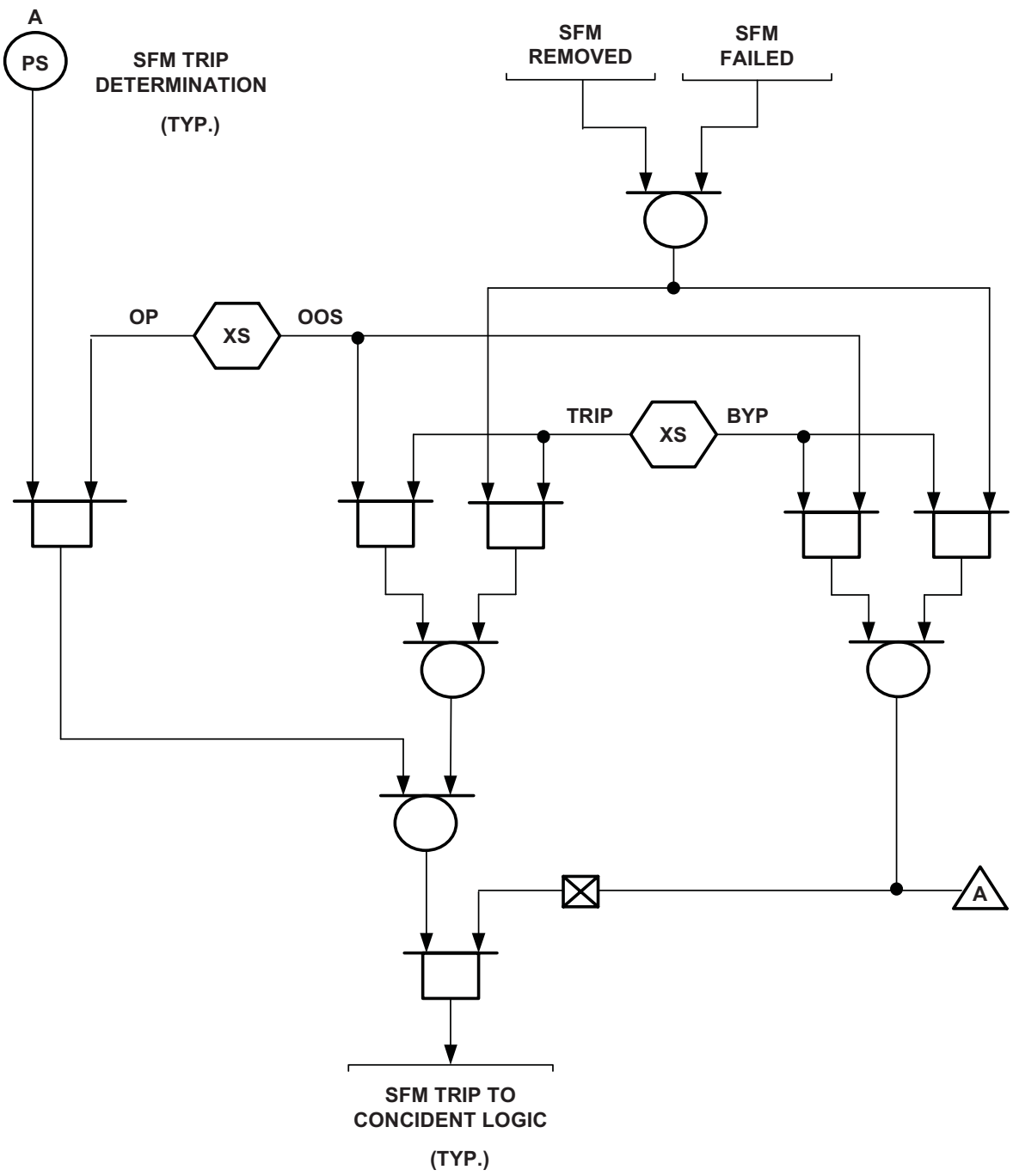
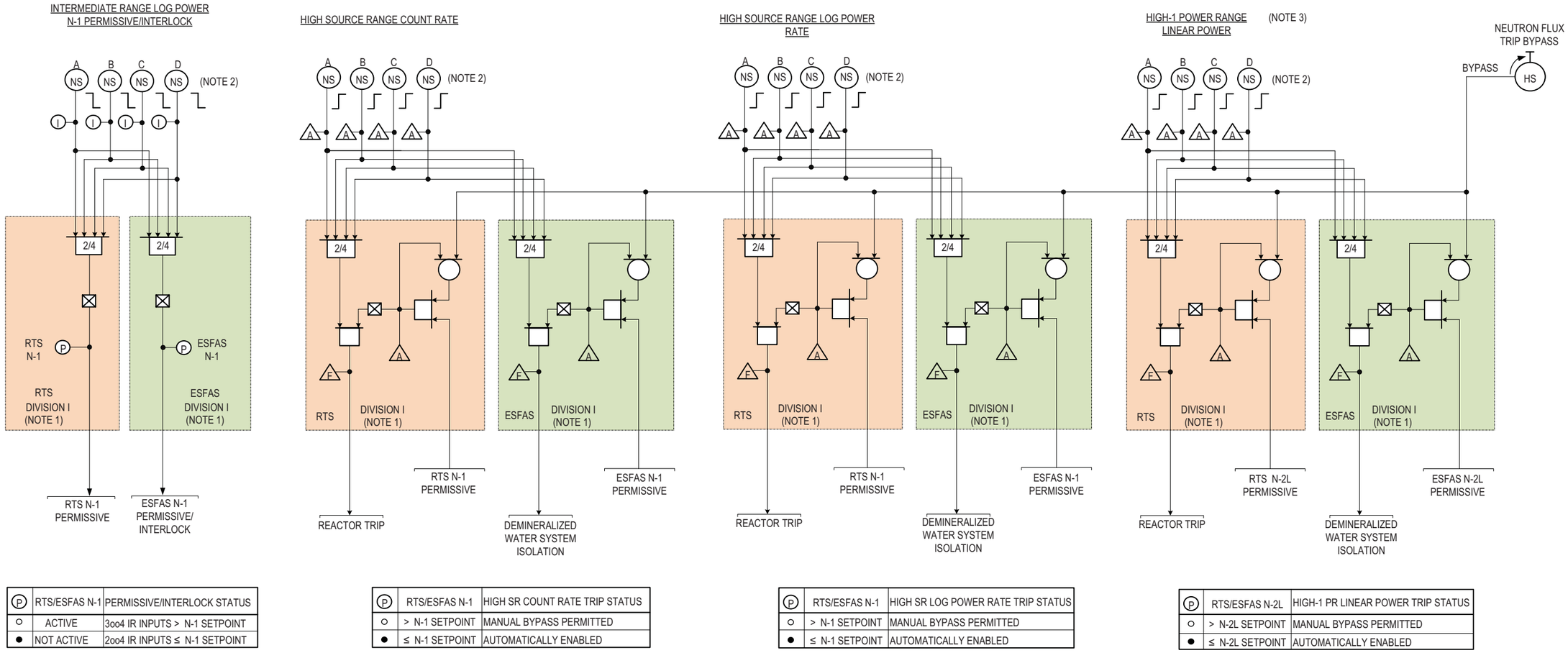


Figure 7.1-1b: Source Range and Power Range Trips



Ⓟ	RTS/ESFAS N-1	PERMISSIVE/INTERLOCK STATUS
○	ACTIVE	3oo4 IR INPUTS > N-1 SETPOINT
●	NOT ACTIVE	2oo4 IR INPUTS ≤ N-1 SETPOINT

Ⓟ	RTS/ESFAS N-1	HIGH SR COUNT RATE TRIP STATUS
○	> N-1 SETPOINT	MANUAL BYPASS PERMITTED
●	≤ N-1 SETPOINT	AUTOMATICALLY ENABLED

Ⓟ	RTS/ESFAS N-1	HIGH SR LOG POWER RATE TRIP STATUS
○	> N-1 SETPOINT	MANUAL BYPASS PERMITTED
●	≤ N-1 SETPOINT	AUTOMATICALLY ENABLED

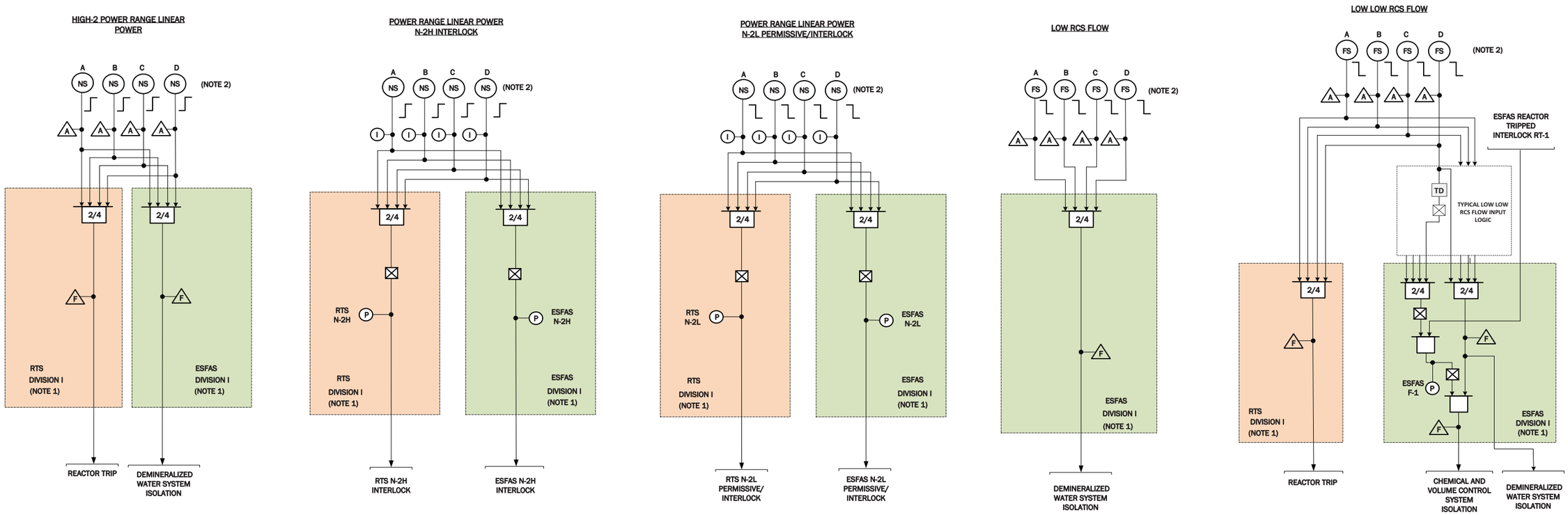
Ⓟ	RTS/ESFAS N-2L	HIGH-1 PR LINEAR POWER TRIP STATUS
○	> N-2L SETPOINT	MANUAL BYPASS PERMITTED
●	≤ N-2L SETPOINT	AUTOMATICALLY ENABLED

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.

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



P	RTS/ESFAS N-2H	PR LINEAR POWER N-2H INTERLOCK STATUS
○	ACTIVE	3oo4 PR INPUTS < N-2H SETPOINT
●	NOT ACTIVE	2oo4 PR INPUTS ≥ N-2H SETPOINT

P	RTS/ESFAS N-2L	PR LINEAR POWER N-2L PERMISSIVE/INTERLOCK STATUS
○	ACTIVE	3oo4 PR INPUTS > N-2L SETPOINT
●	NOT ACTIVE	2oo4 PR INPUTS ≤ N-2L SETPOINT

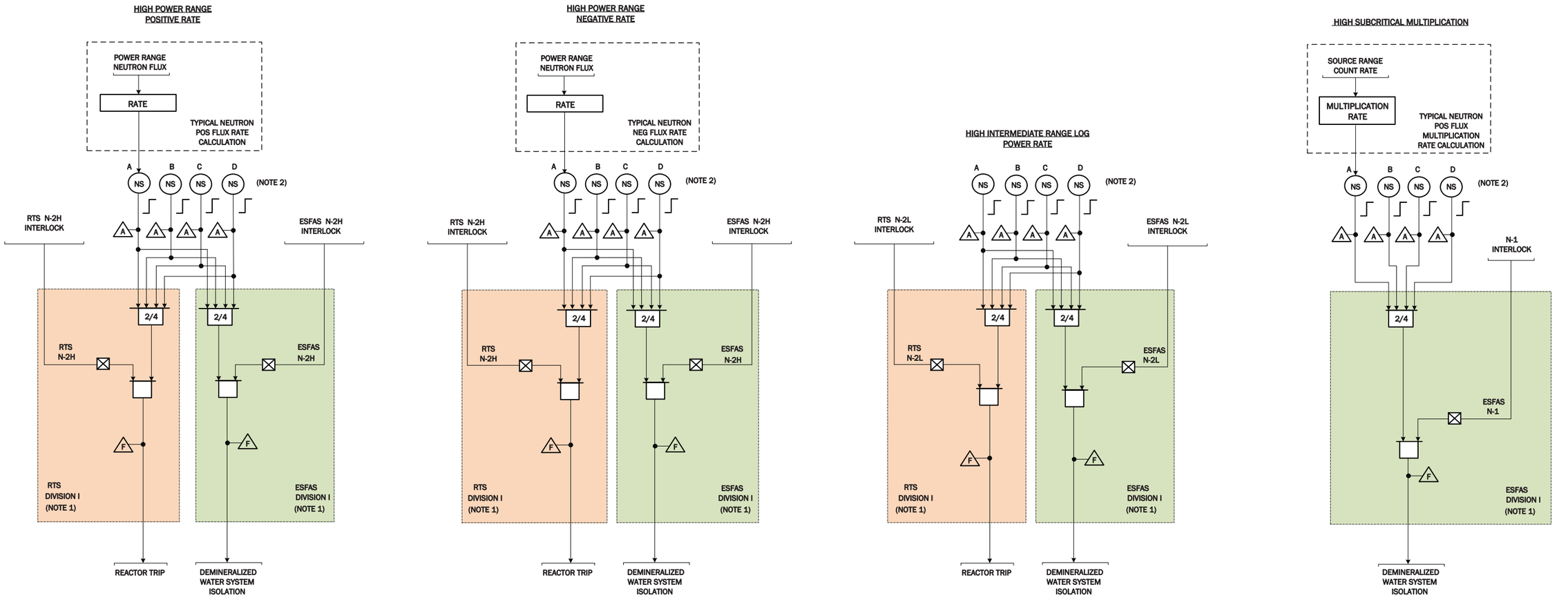
P	ESFAS F-1	CHEMICAL & VOLUME CONTROL SYSTEM ISOLATION
○	< F-1	AUTOMATIC BYPASS
●	≥ F-1	AUTOMATICALLY ENABLED

P	ESFAS F-1	LOW LOW RCS FLOW CVCSI ACTUATION INTERLOCK STATUS
○	ACTIVE	3oo4 RCS FLOW INPUTS < LOW LOW SETPOINT FOR MORE THAN TD, AND RT-1 ACTIVE
●	NOT ACTIVE	2oo4 RCS FLOW INPUTS > LOW LOW SETPOINT FOR MORE THAN TD, OR 3oo4 RCS FLOW INPUTS < LOW LOW SETPOINT FOR LESS THAN TD, OR RT-1 NOT ACTIVE

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



P	RTS/ESFAS N-2H	HIGH PR POSITIVE RATE TRIP STATUS
○	≥ N-2H SETPOINT	AUTOMATICALLY ENABLED
●	< N-2H SETPOINT	AUTOMATIC BYPASS

P	RTS/ESFAS N-2H	HIGH PR NEGATIVE RATE TRIP STATUS
○	≥ N-2H SETPOINT	AUTOMATICALLY ENABLED
●	< N-2H SETPOINT	AUTOMATIC BYPASS

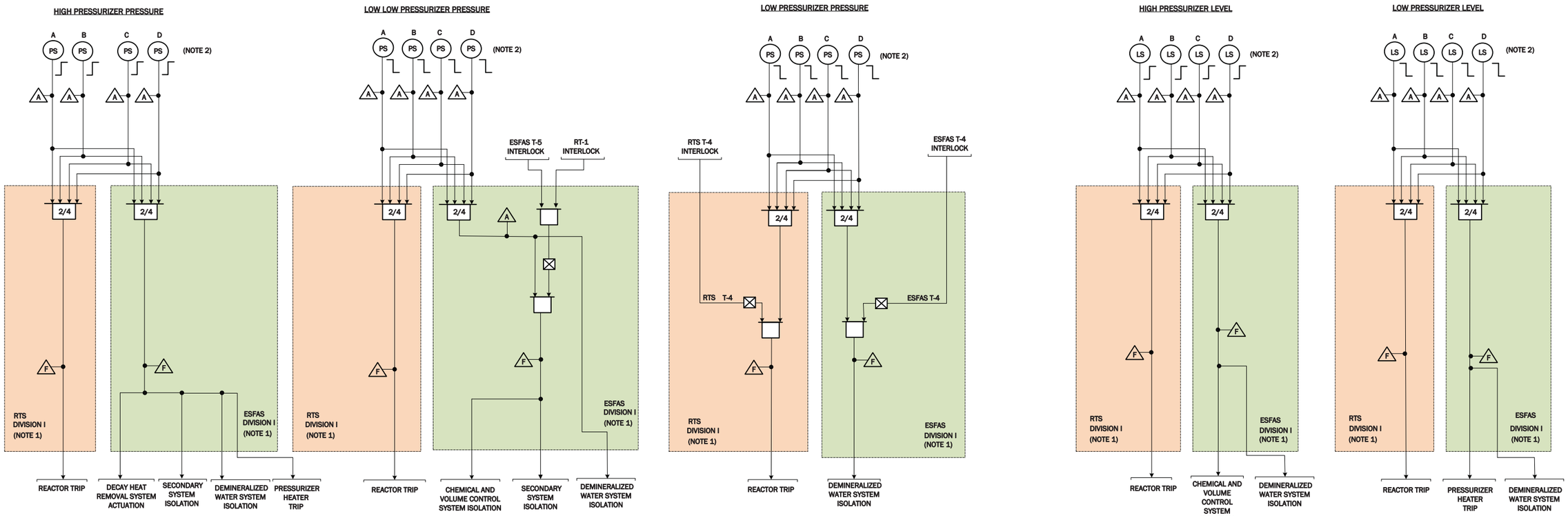
P	RTS/ESFAS N-2L	HIGH IR LOG POWER RATE TRIP STATUS
○	> N-2L SETPOINT	AUTOMATIC BYPASS
●	≤ N-2L SETPOINT	AUTOMATICALLY ENABLED

P	ESFAS N-1	HIGH SUBCRITICAL MULTIPLICATION TRIP STATUS
○	> N-1 SETPOINT	AUTOMATIC BYPASS
●	≤ N-1 SETPOINT	AUTOMATICALLY ENABLED

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



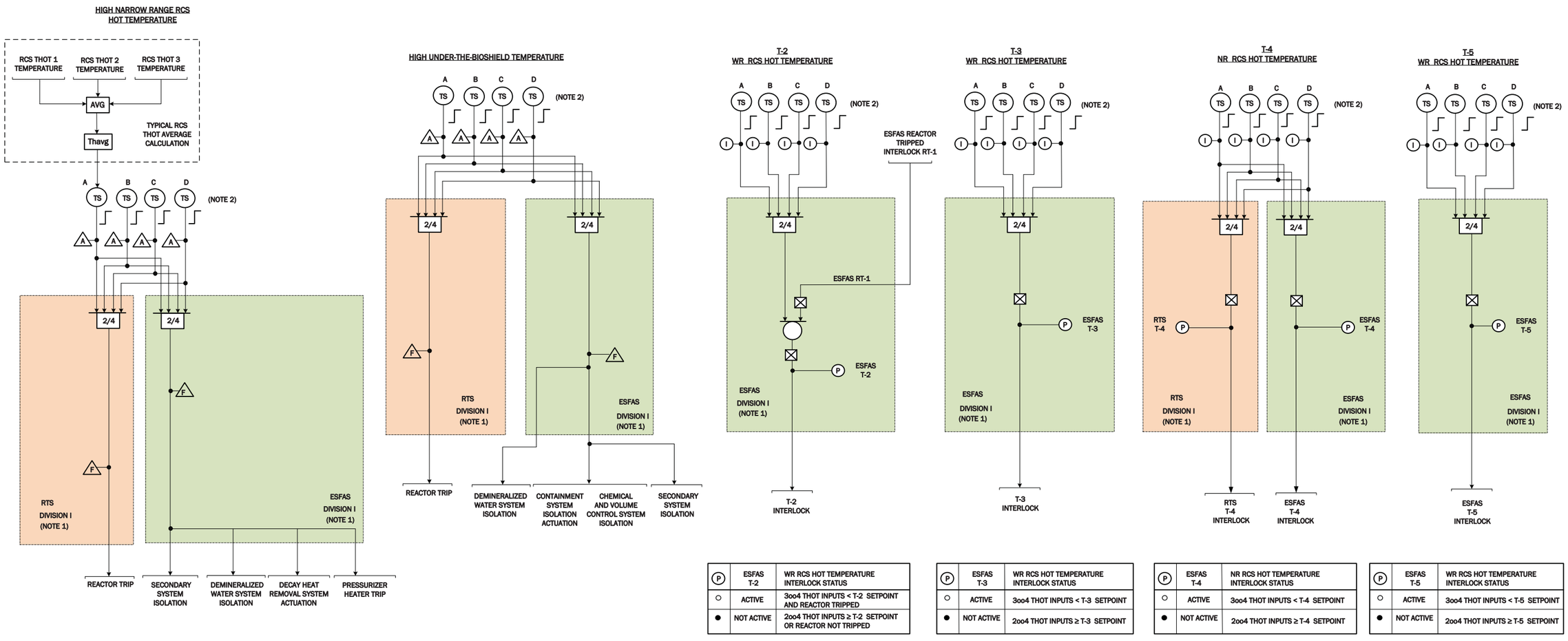
(P)	ESFAS T-5 AND RT-1	LOW LOW PRESSURIZER PRESSURE CVCSI AND SSI TRIP STATUS
○	< T-5 AND RT-1	AUTOMATIC BYPASS
●	≥ T-5 OR NO RT-1	AUTOMATICALLY ENABLED

(P)	RTS/ESFAS T-4	LOW PRESSURIZER PRESSURE TRIP STATUS
○	< T-4 SETPOINT	AUTOMATIC BYPASS
●	≥ T-4 SETPOINT	AUTOMATICALLY ENABLED

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



P	ESFAS T-2	WR RCS HOT TEMPERATURE INTERLOCK STATUS
○	ACTIVE	3oo4 THOT INPUTS < T-2 SETPOINT AND REACTOR TRIPPED
●	NOT ACTIVE	2oo4 THOT INPUTS ≥ T-2 SETPOINT OR REACTOR NOT TRIPPED

P	ESFAS T-3	WR RCS HOT TEMPERATURE INTERLOCK STATUS
○	ACTIVE	3oo4 THOT INPUTS < T-3 SETPOINT
●	NOT ACTIVE	2oo4 THOT INPUTS ≥ T-3 SETPOINT

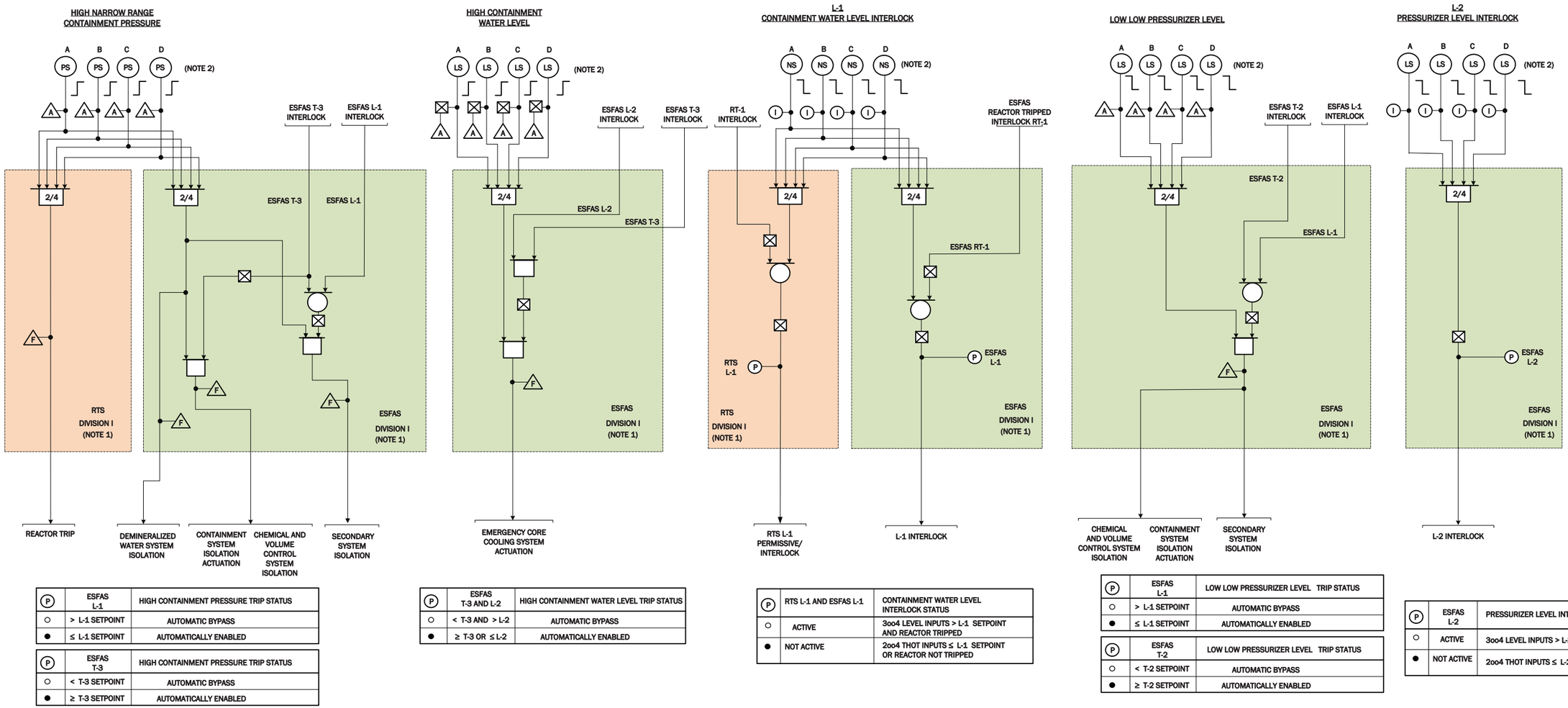
P	ESFAS T-4	NR RCS HOT TEMPERATURE INTERLOCK STATUS
○	ACTIVE	3oo4 THOT INPUTS < T-4 SETPOINT
●	NOT ACTIVE	2oo4 THOT INPUTS ≥ T-4 SETPOINT

P	ESFAS T-5	WR RCS HOT TEMPERATURE INTERLOCK STATUS
○	ACTIVE	3oo4 THOT INPUTS < T-5 SETPOINT
●	NOT ACTIVE	2oo4 THOT INPUTS ≥ T-5 SETPOINT

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



P	ESFAS L-1	HIGH CONTAINMENT PRESSURE TRIP STATUS
○	> L-1 SETPOINT	AUTOMATIC BYPASS
●	≤ L-1 SETPOINT	AUTOMATICALLY ENABLED

P	ESFAS T-3	HIGH CONTAINMENT PRESSURE TRIP STATUS
○	< T-3 SETPOINT	AUTOMATIC BYPASS
●	≥ T-3 SETPOINT	AUTOMATICALLY ENABLED

P	ESFAS T-3 AND L-2	HIGH CONTAINMENT WATER LEVEL TRIP STATUS
○	< T-3 AND > L-2	AUTOMATIC BYPASS
●	≥ T-3 OR ≤ L-2	AUTOMATICALLY ENABLED

P	RTS L-1 AND ESFAS L-1	CONTAINMENT WATER LEVEL INTERLOCK STATUS
○	ACTIVE	3oo4 LEVEL INPUTS > L-1 SETPOINT AND REACTOR TRIPPED
●	NOT ACTIVE	2oo4 THOT INPUTS ≤ L-1 SETPOINT OR REACTOR NOT TRIPPED

P	ESFAS L-1	LOW LOW PRESSURIZER LEVEL TRIP STATUS
○	> L-1 SETPOINT	AUTOMATIC BYPASS
●	≤ L-1 SETPOINT	AUTOMATICALLY ENABLED

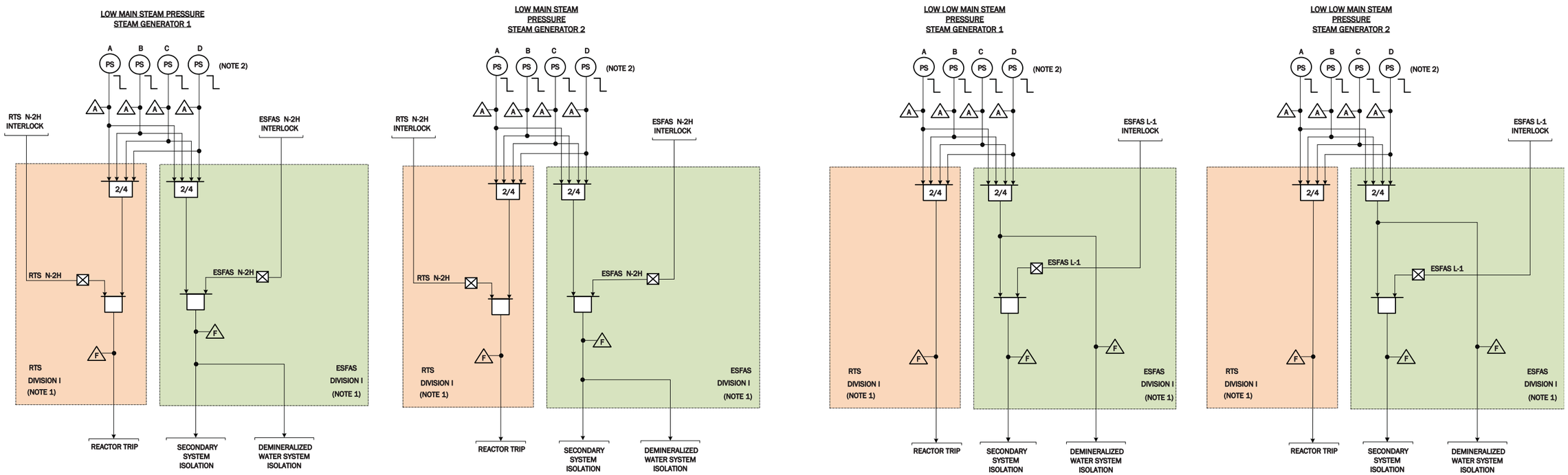
P	ESFAS T-2	LOW LOW PRESSURIZER LEVEL TRIP STATUS
○	< T-2 SETPOINT	AUTOMATIC BYPASS
●	≥ T-2 SETPOINT	AUTOMATICALLY ENABLED

P	ESFAS L-2	PRESSURIZER LEVEL INTERLOCK STATUS
○	ACTIVE	3oo4 LEVEL INPUTS > L-2 SETPOINT
●	NOT ACTIVE	2oo4 THOT INPUTS ≤ L-2 SETPOINT

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



P	RTS/ESFAS N-2H	LOW MAIN STEAM PRESSURE SG 1 TRIP STATUS
○	≥ N-2H SETPOINT	AUTOMATICALLY ENABLED
●	< N-2H SETPOINT	AUTOMATIC BYPASS

P	RTS/ESFAS N-2H	LOW MAIN STEAM PRESSURE SG 2 TRIP STATUS
○	≥ N-2H SETPOINT	AUTOMATICALLY ENABLED
●	< N-2H SETPOINT	AUTOMATIC BYPASS

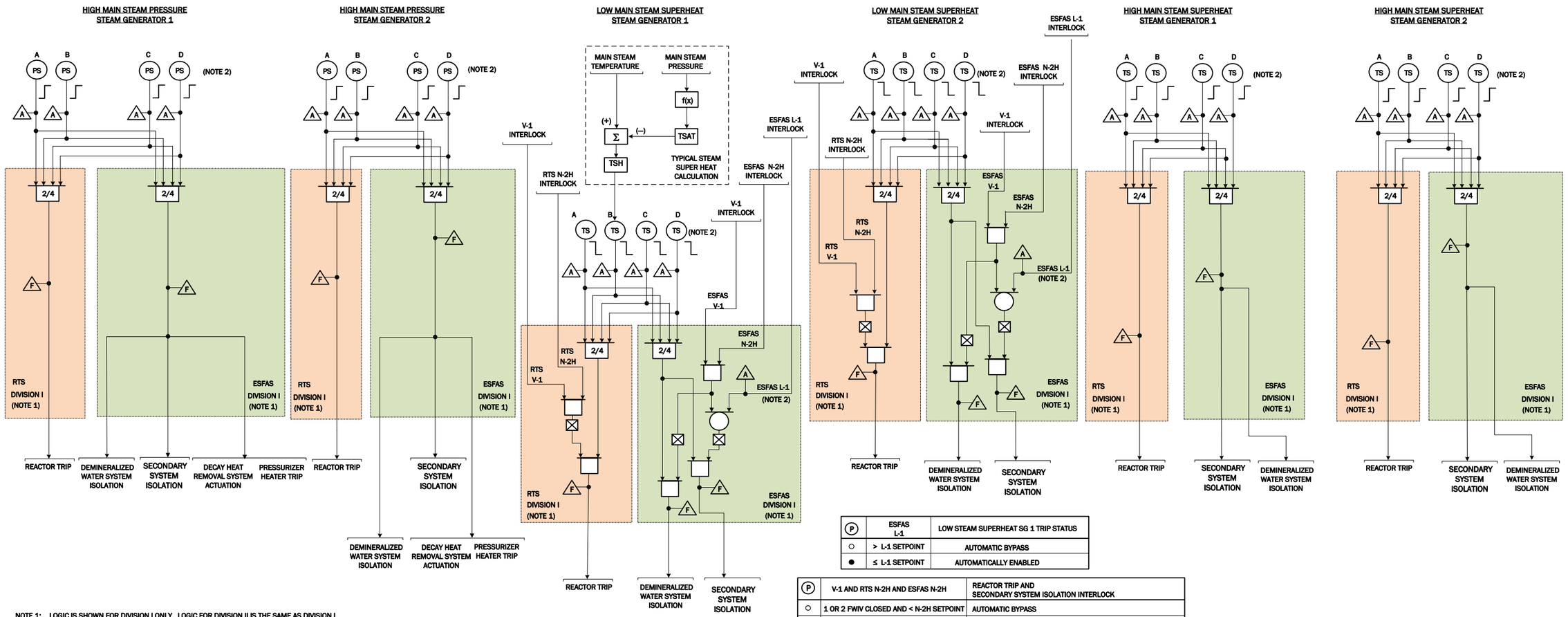
P	ESFAS L-1	LOW LOW MIAN STEAM PRESSURE SG 1 TRIP STATUS
○	> L-1 SETPOINT	AUTOMATIC BYPASS
●	≤ L-1 SETPOINT	AUTOMATICALLY ENABLED

P	ESFAS L-1	LOW LOW MAIN STEAM PRESSURE SG 2 TRIP STATUS
○	> L-1 SETPOINT	AUTOMATIC BYPASS
●	≤ L-1 SETPOINT	AUTOMATICALLY ENABLED

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



P	ESFAS L-1	LOW STEAM SUPERHEAT SG 1 TRIP STATUS
○	> L-1 SETPOINT	AUTOMATIC BYPASS
●	≤ L-1 SETPOINT	AUTOMATICALLY ENABLED

P	V-1 AND RTS N-2H AND ESFAS N-2H	REACTOR TRIP AND SECONDARY SYSTEM ISOLATION INTERLOCK
○	1 OR 2 FWIV CLOSED AND < N-2H SETPOINT	AUTOMATIC BYPASS
●	NO FWIV CLOSED OR ≥ N-2H SETPOINT	AUTOMATICALLY ENABLED

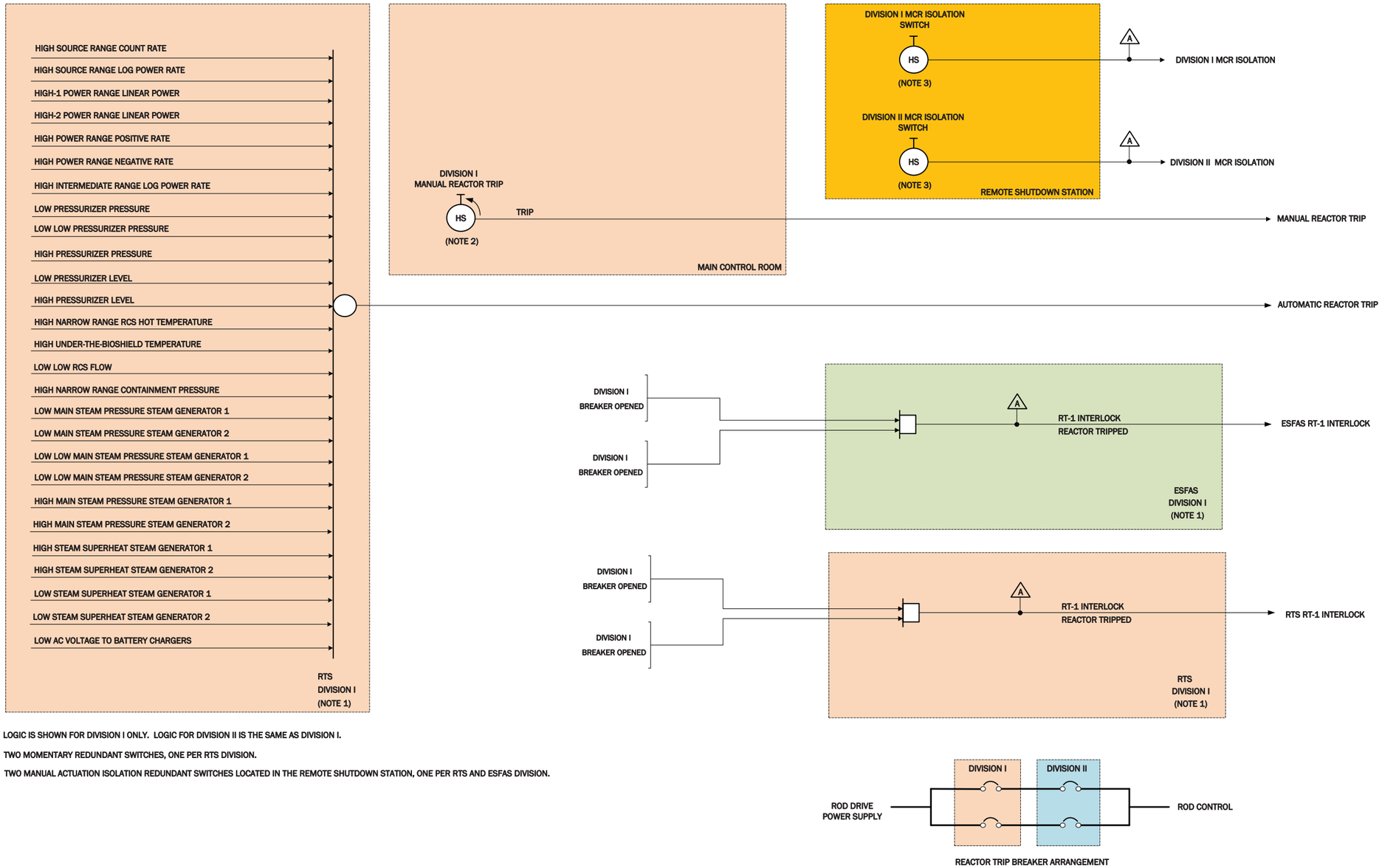
NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

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

P	ESFAS L-1	LOW STEAM SUPERHEAT SG 1 TRIP STATUS
○	> L-1 SETPOINT	AUTOMATIC BYPASS
●	≤ L-1 SETPOINT	AUTOMATICALLY ENABLED

P	V-1 AND RTS N-2H AND ESFAS N-2H	REACTOR TRIP AND SECONDARY SYSTEM ISOLATION INTERLOCK
○	1 OR 2 FWIV CLOSED AND < N-2H SETPOINT	AUTOMATIC BYPASS
●	NO FWIV CLOSED OR ≥ N-2H SETPOINT	AUTOMATICALLY ENABLED

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

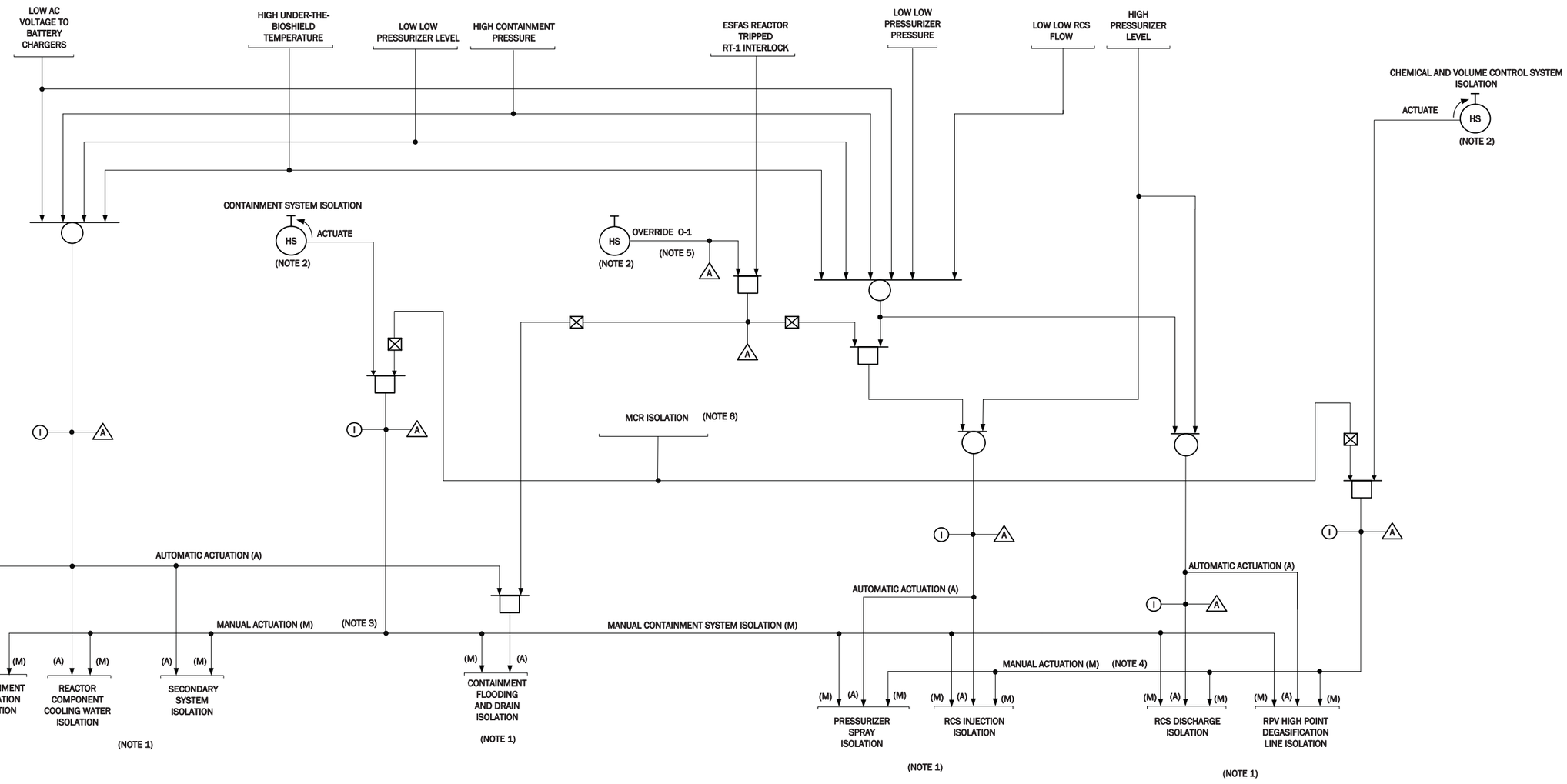


NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

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

NOTE 3: TWO MANUAL ACTUATION ISOLATION REDUNDANT SWITCHES LOCATED IN THE REMOTE SHUTDOWN STATION, ONE PER RTS AND ESFAS DIVISION.

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.

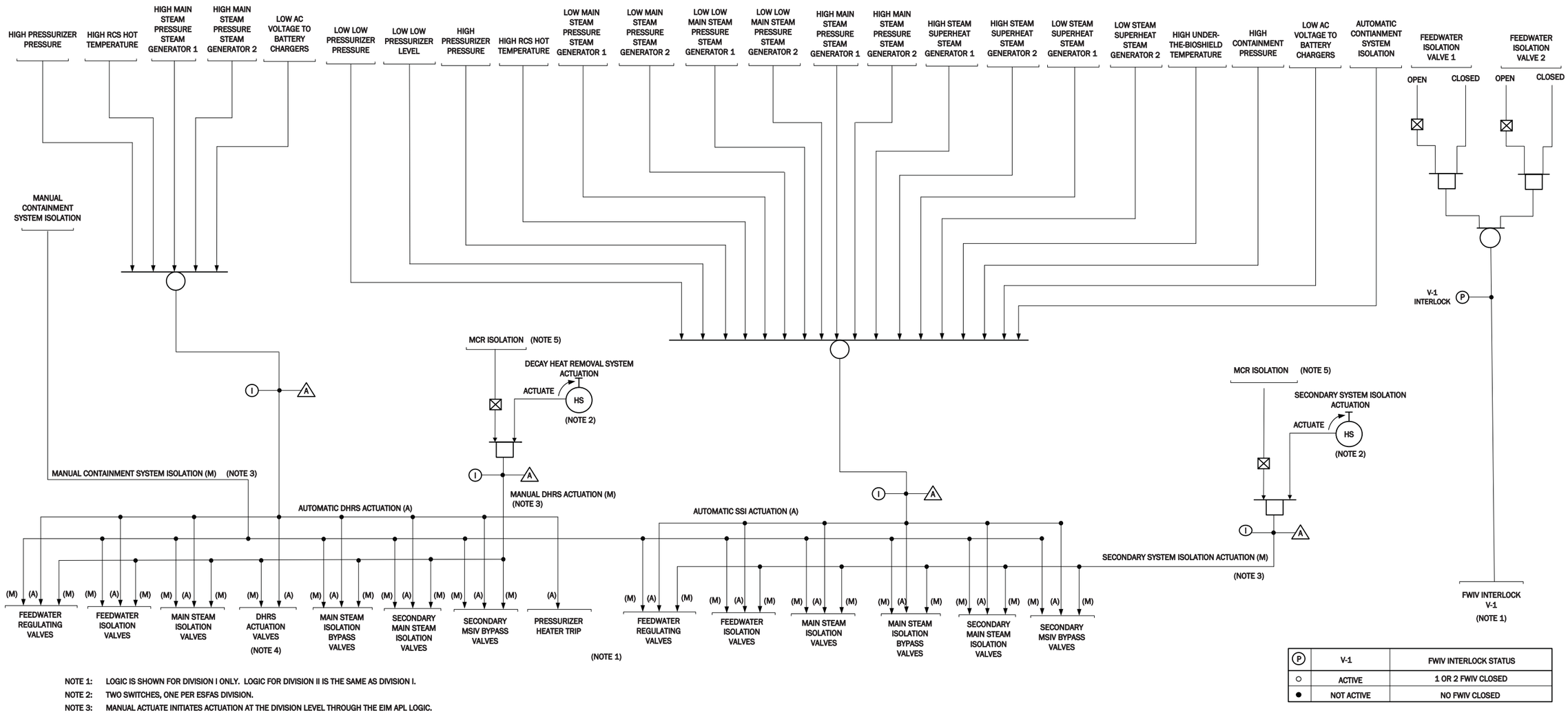
NOTE 3: MANUAL ACTUATION INITIATES CONTAINMENT SYSTEM ISOLATION AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.

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 RTS/ESFAS DIVISION.

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



P	V-1	FWIV INTERLOCK STATUS
○	ACTIVE	1 OR 2 FWIV CLOSED
●	NOT ACTIVE	NO FWIV CLOSED

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

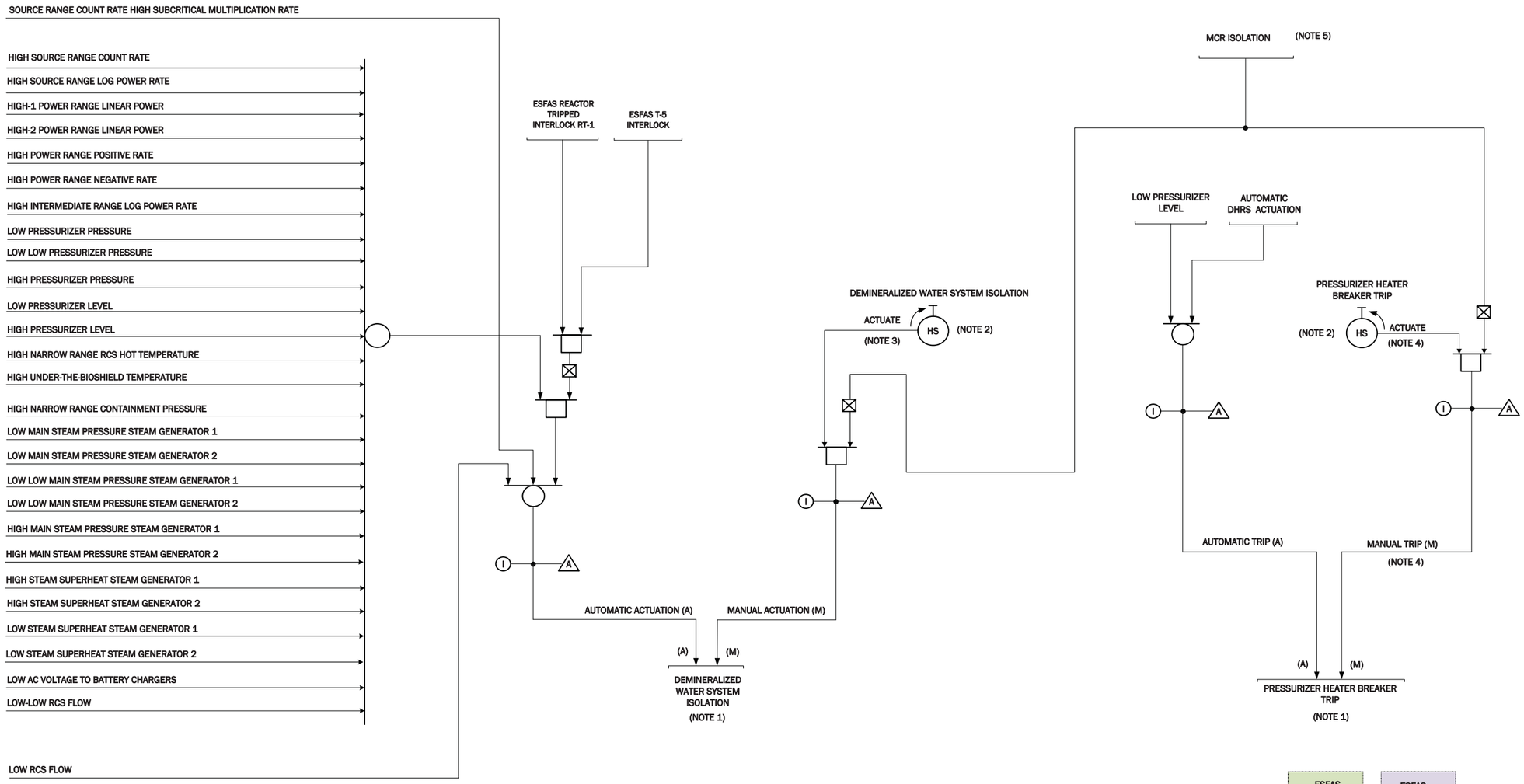
NOTE 2: TWO SWITCHES, ONE PER ESFAS DIVISION.

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 RTS/ESFAS DIVISION.

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



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

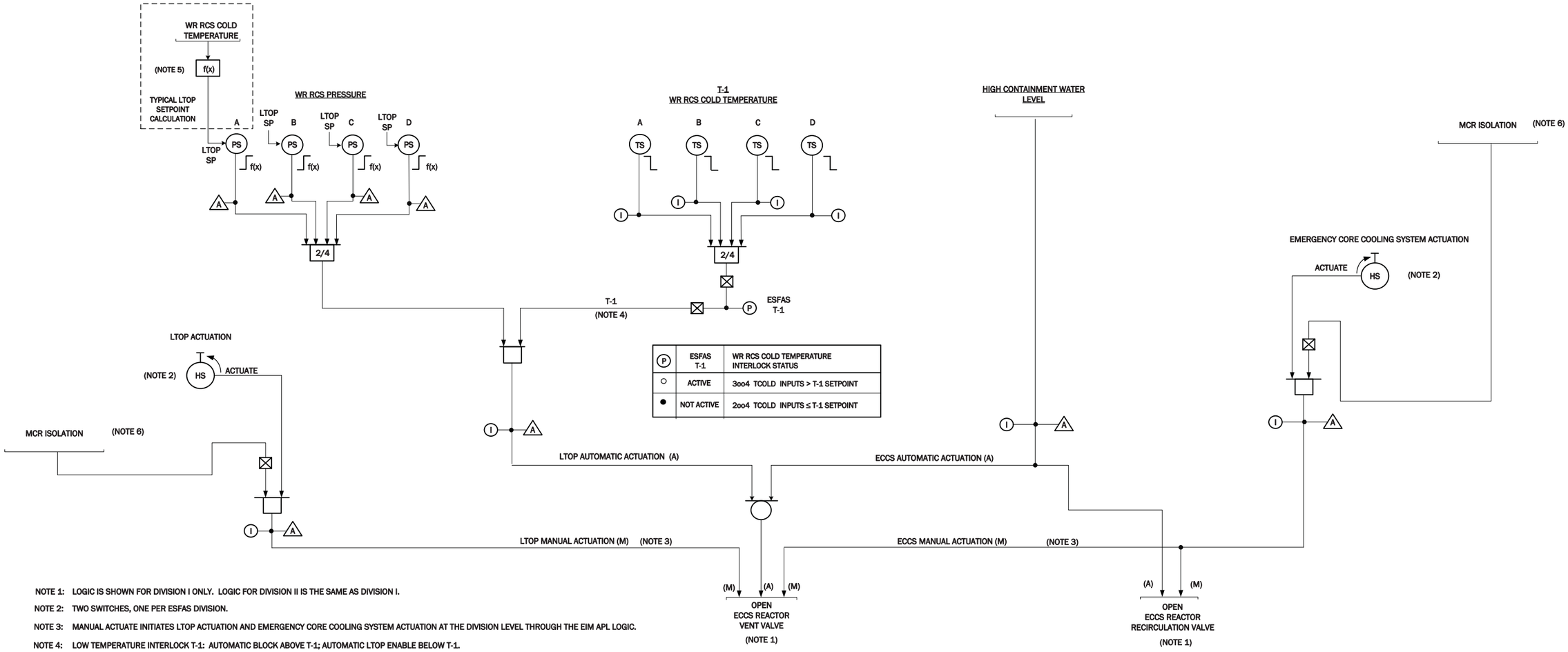
NOTE 2: TWO SWITCHES, ONE PER ESFAS DIVISION.

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

NOTE 4: MANUAL ACTUATION INITIATES PRESSURIZER HEATER BREAKER TRIP AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.

NOTE 5: TWO MANUAL ACTUATION ISOLATION SIGNALS, ONE PER RTS/ESFAS DIVISION.

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.

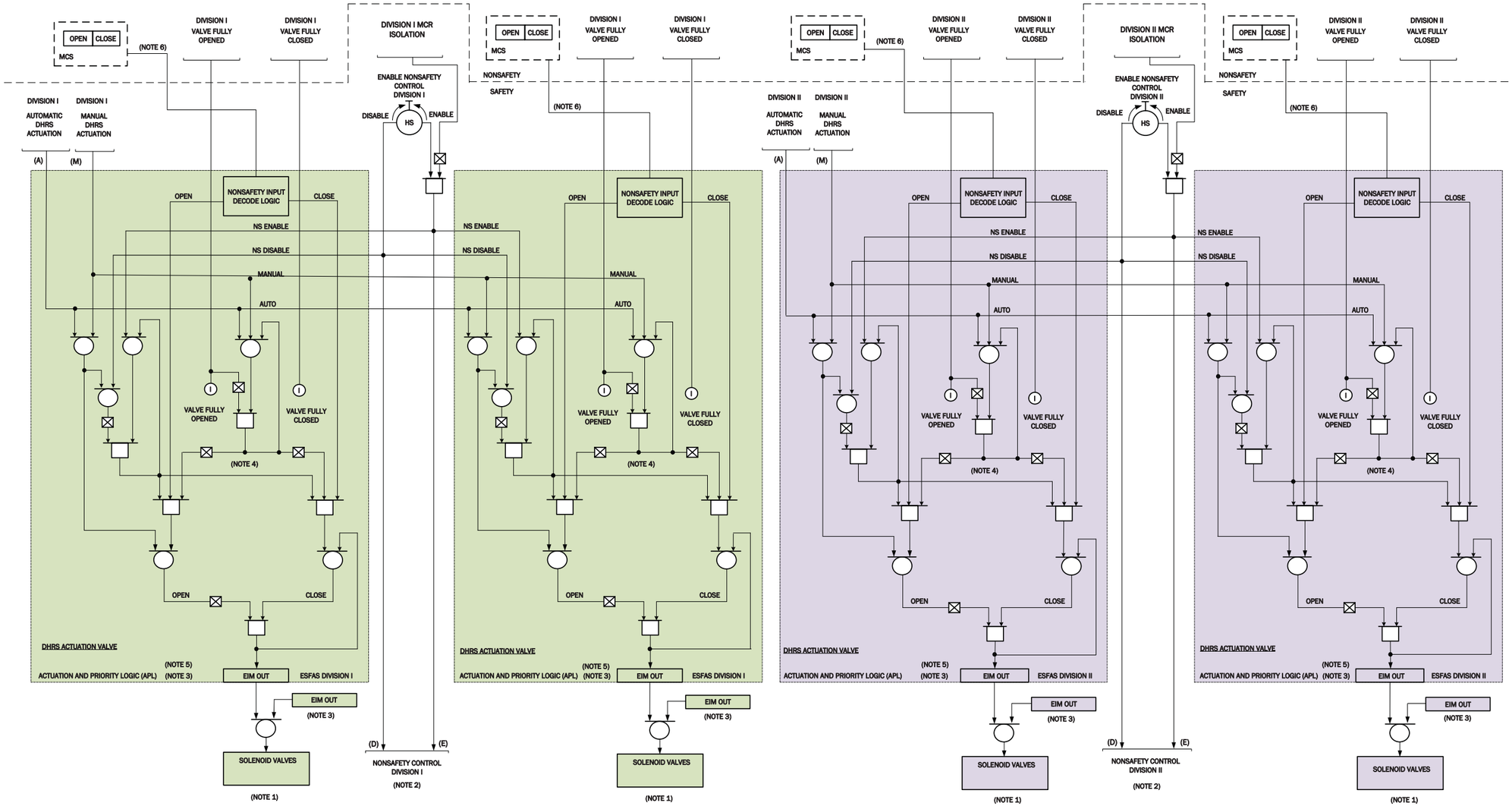
NOTE 3: MANUAL ACTUATE INITIATES LTOP ACTUATION AND EMERGENCY CORE COOLING SYSTEM ACTUATION AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.

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 RTS/ESFAS DIVISION.

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



DECAY HEAT REMOVAL SYSTEM VALVE ACTUATION

NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO CLOSE VALVE; SOLENOIDS ARE DE-ENERGIZED TO OPEN 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 ESF COMPONENTS.

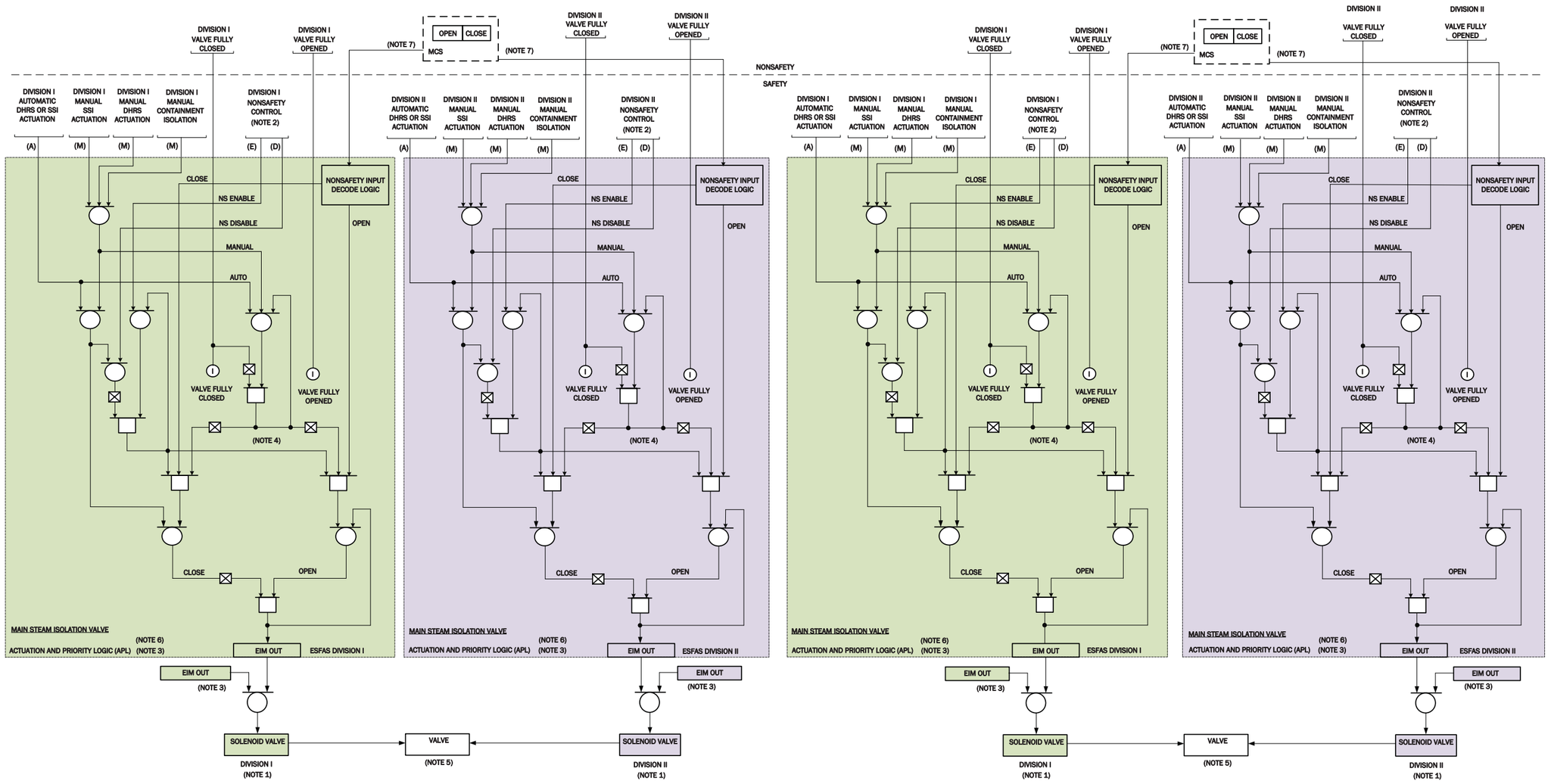
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

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 7.1-1p: 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 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.

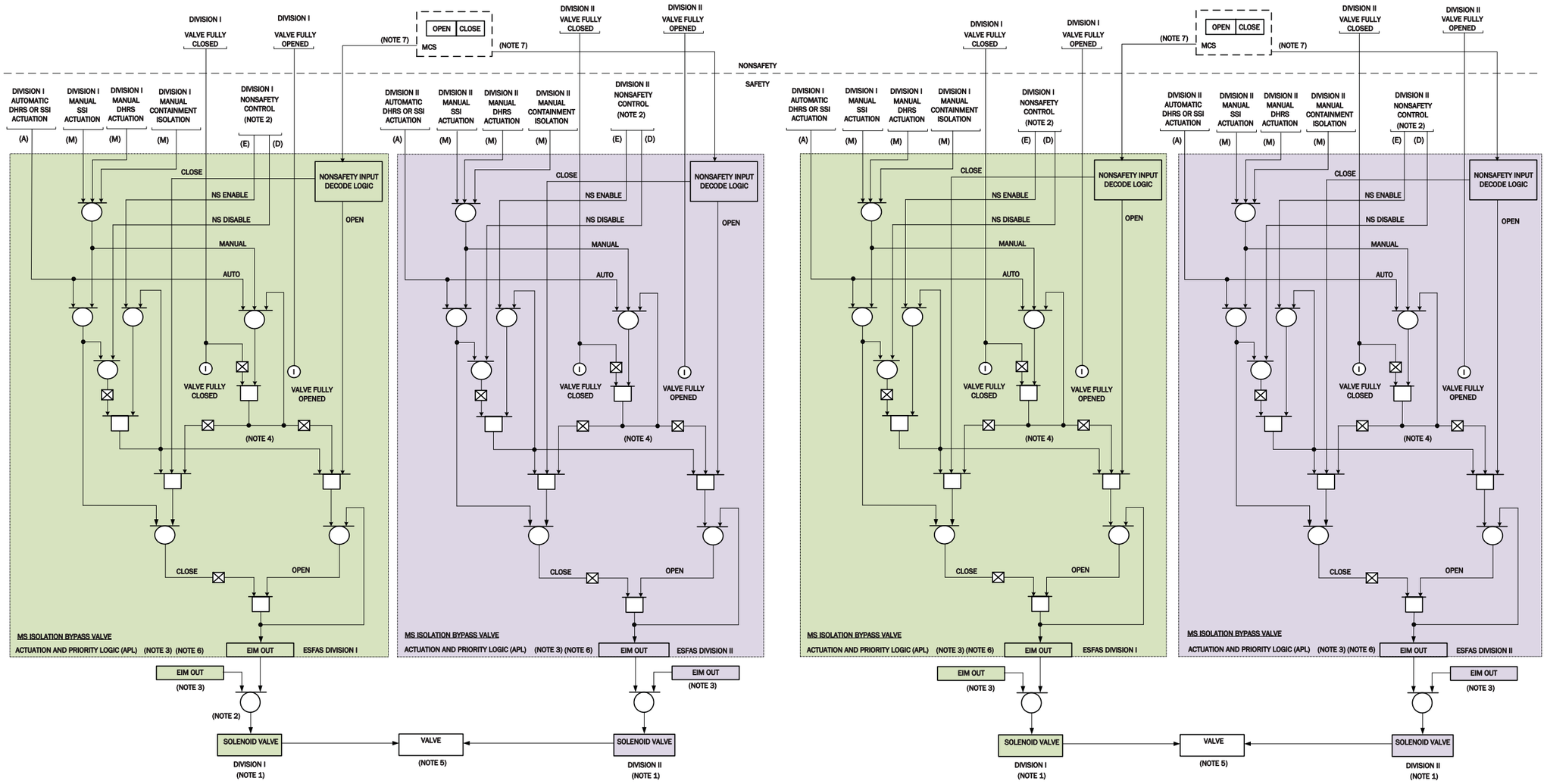
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES 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 7.1-1q: 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 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.

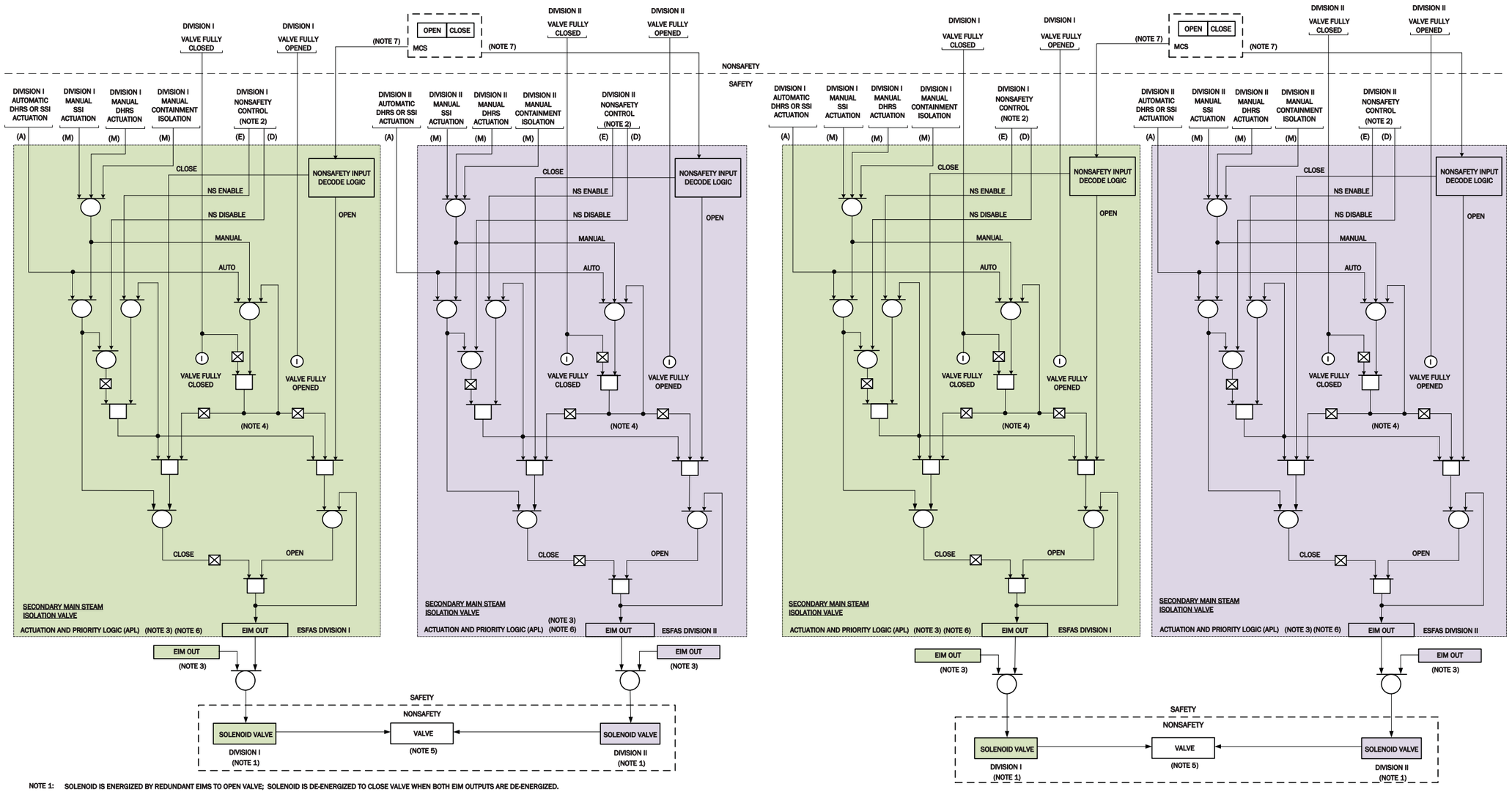
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES 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



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 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.

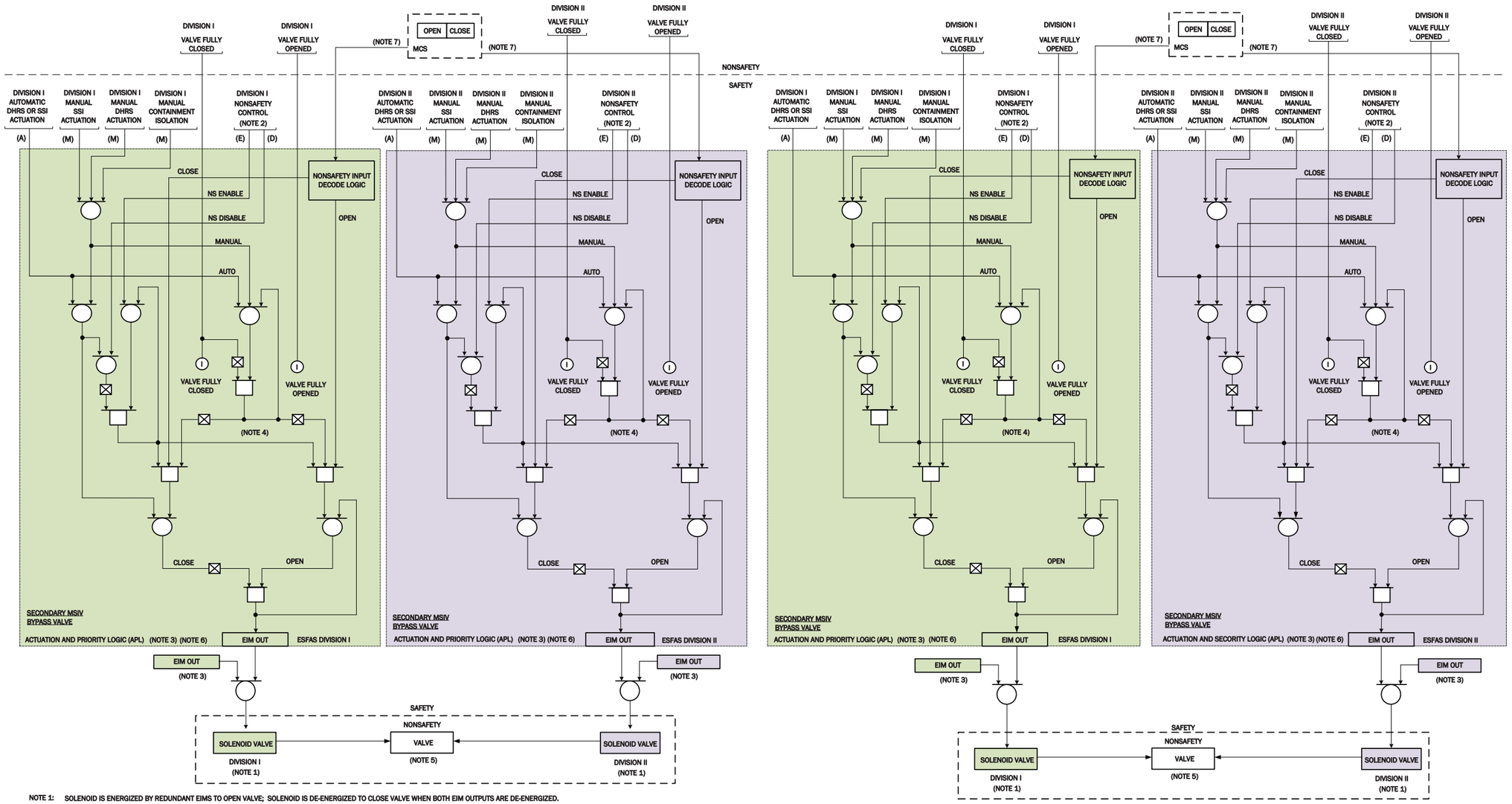
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES 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 7.1-1s: Secondary MSIV 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 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.

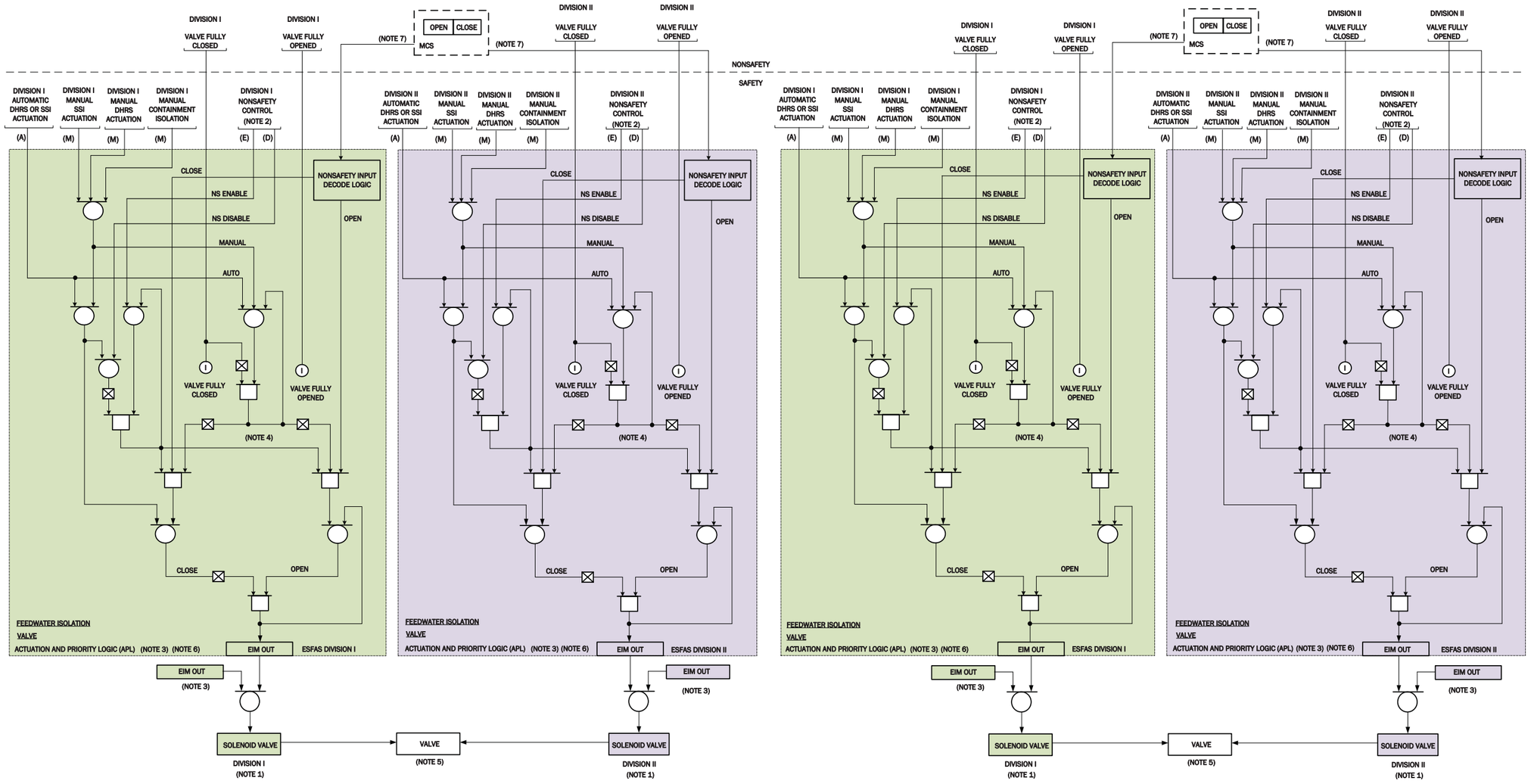
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES 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 7.1-1t: 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 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.

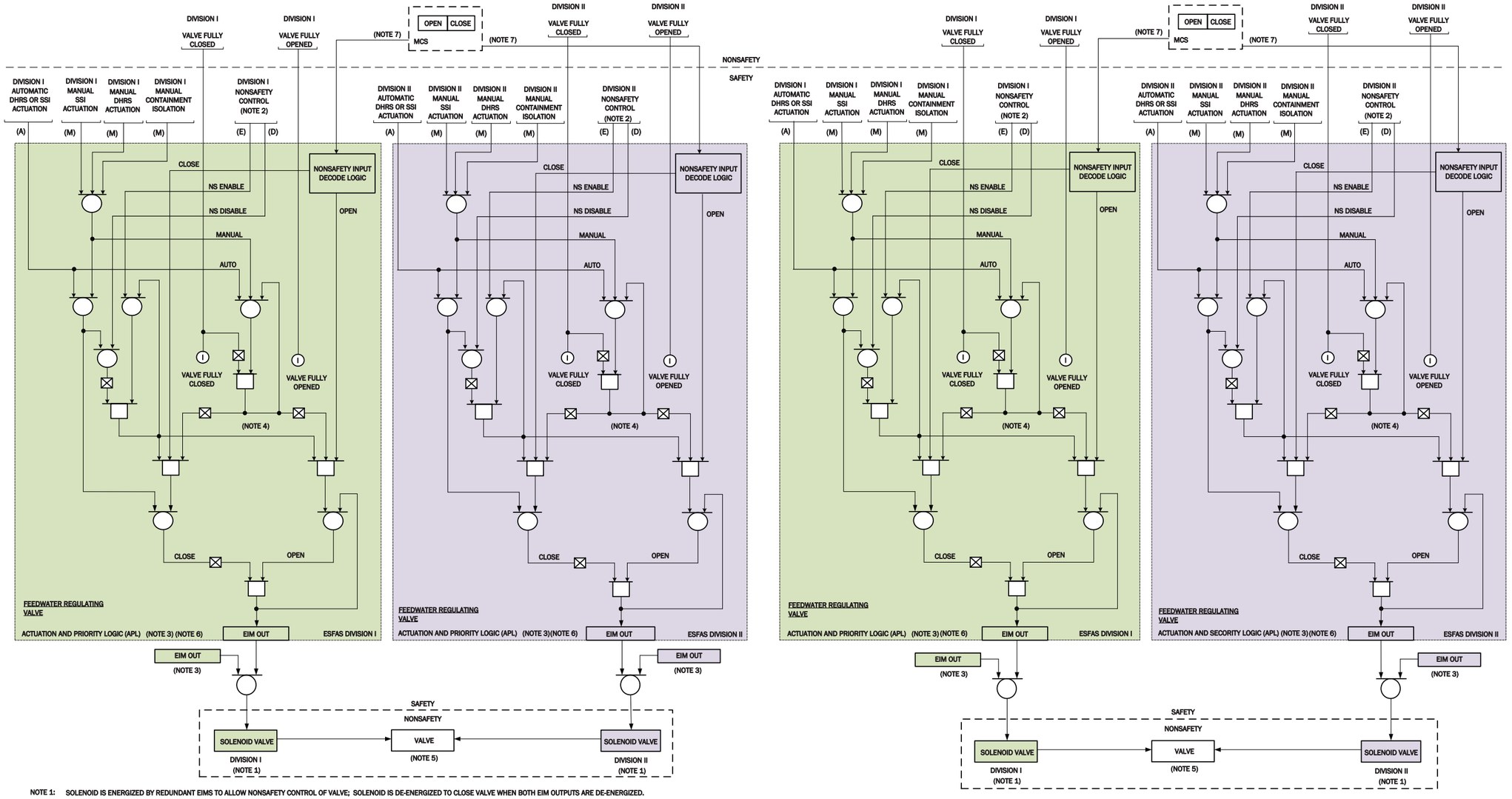
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES 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



NOTE 1: SOLENOID IS ENERGIZED BY REDUNDANT EIMS TO ALLOW NONSAFETY CONTROL OF 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 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.

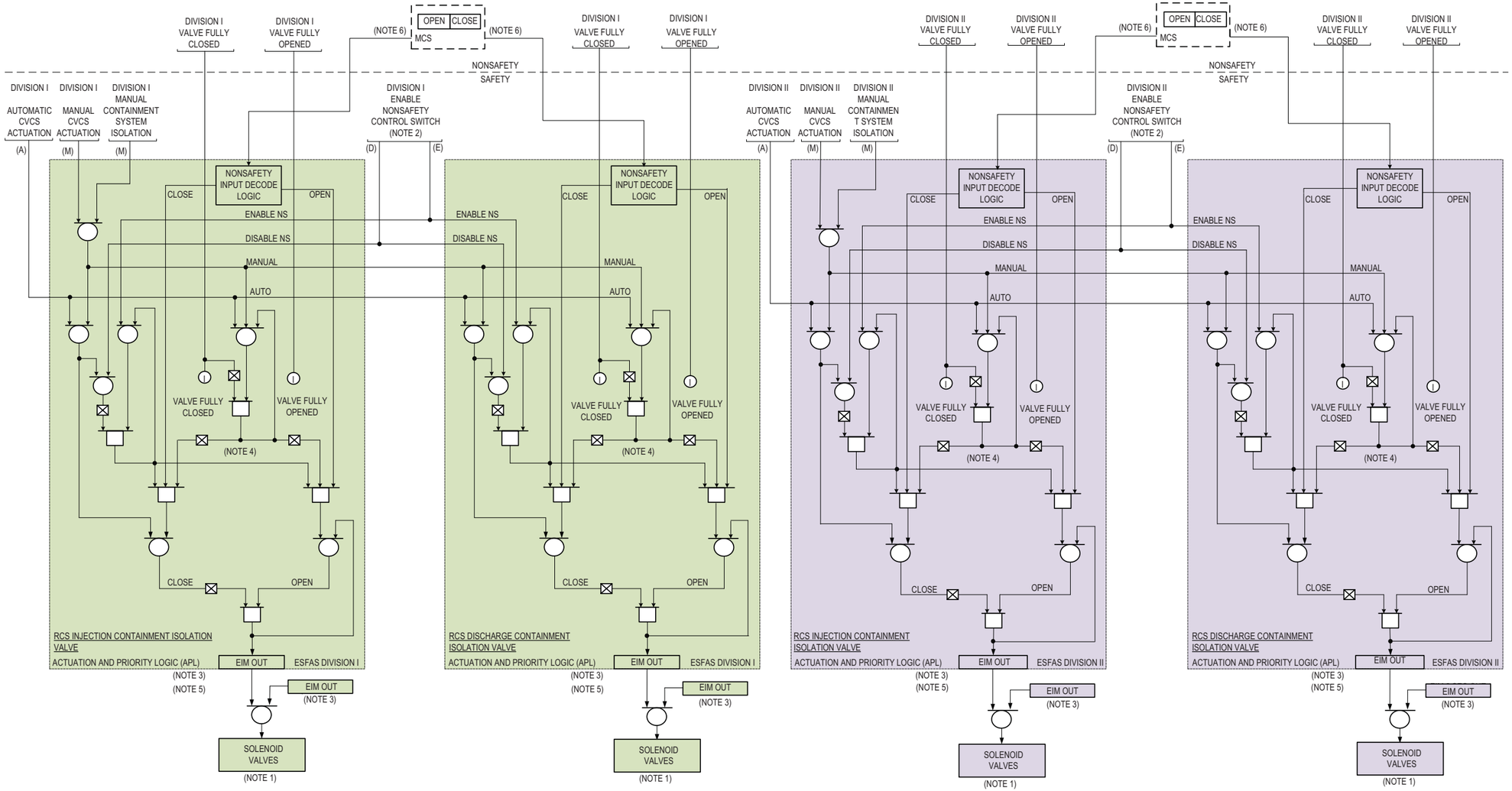
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES 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 7.1-1v: 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 ESF COMPONENTS.

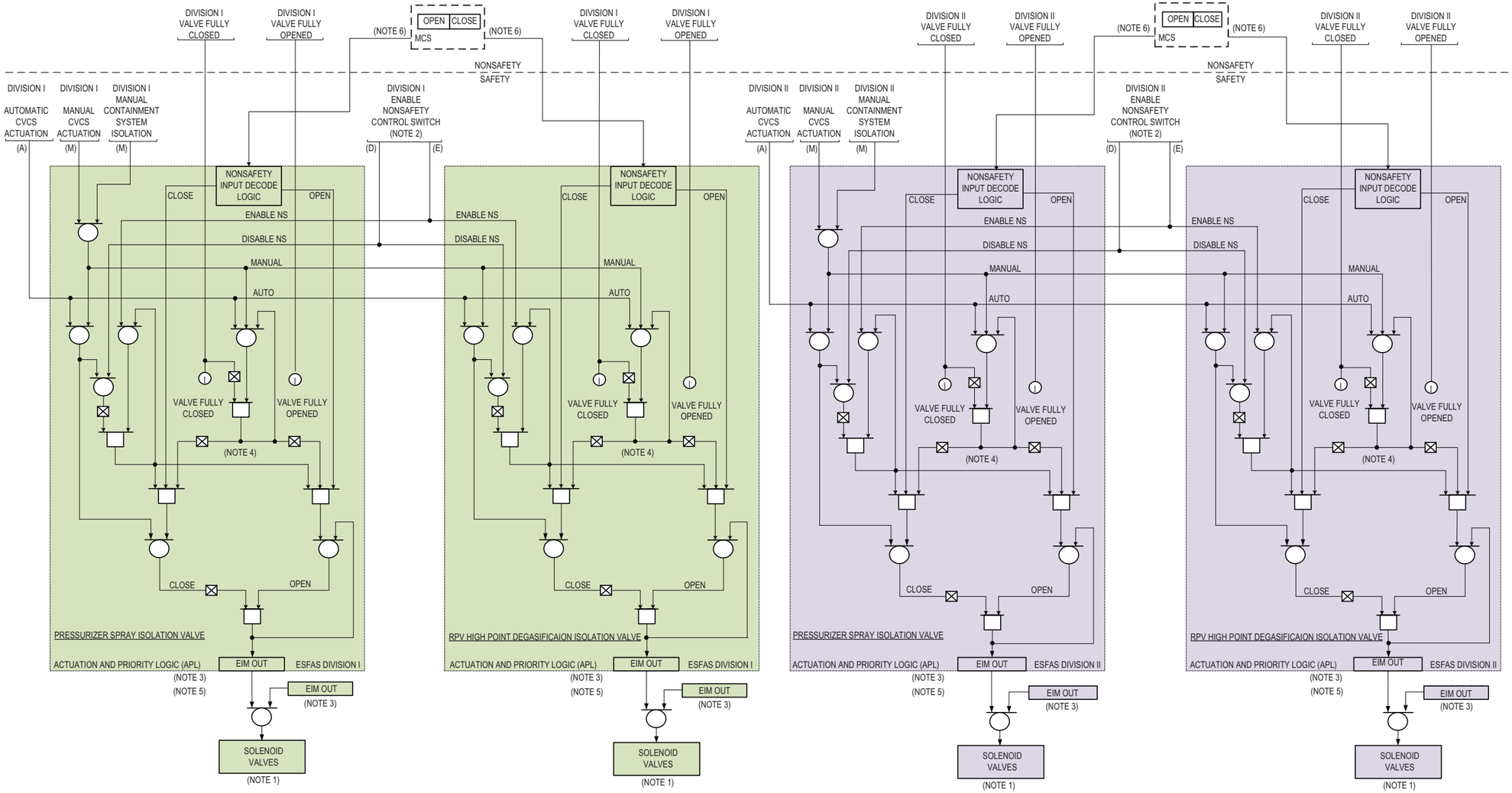
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

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 ESF COMPONENTS.

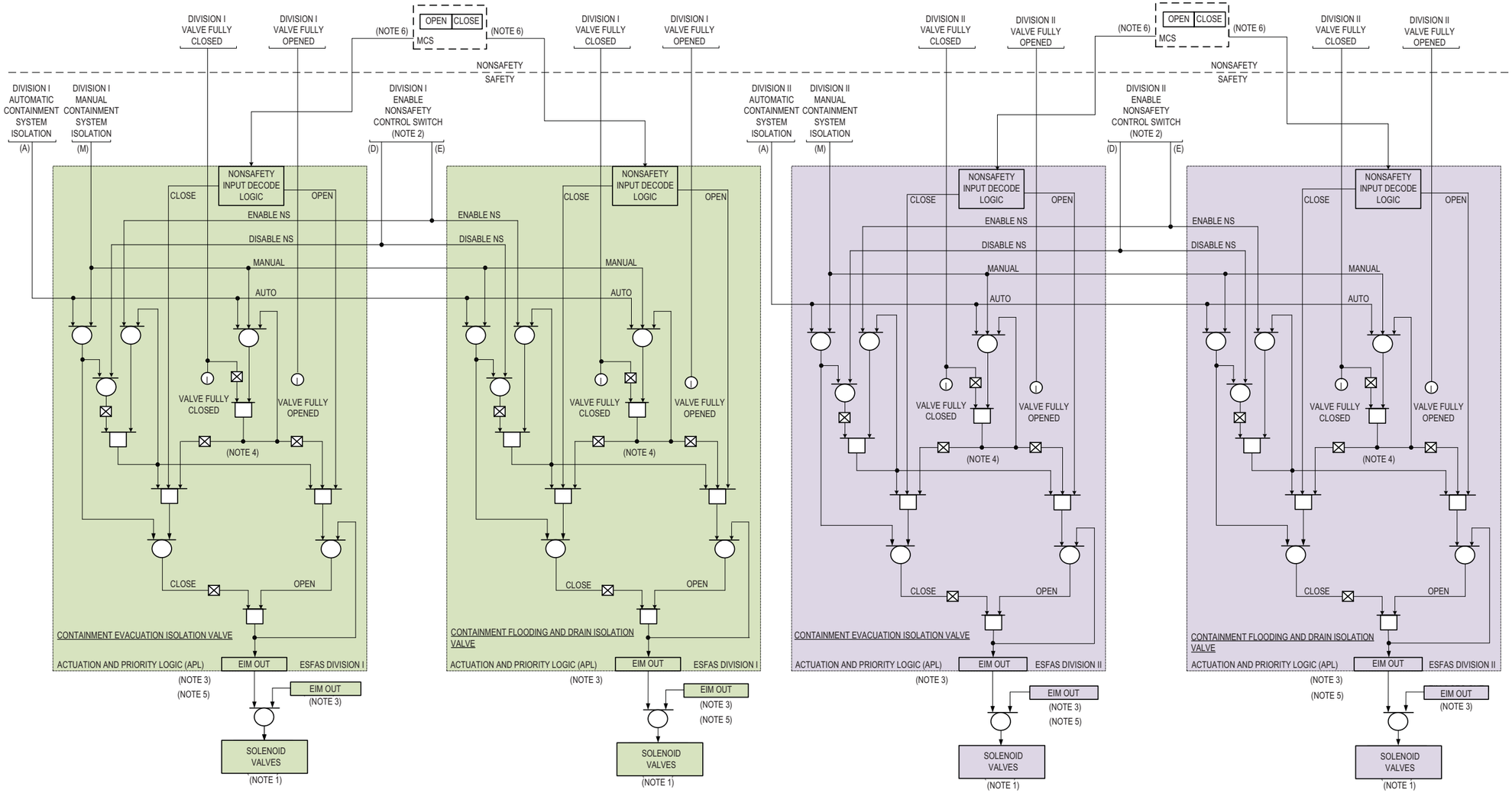
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

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 ESF COMPONENTS.

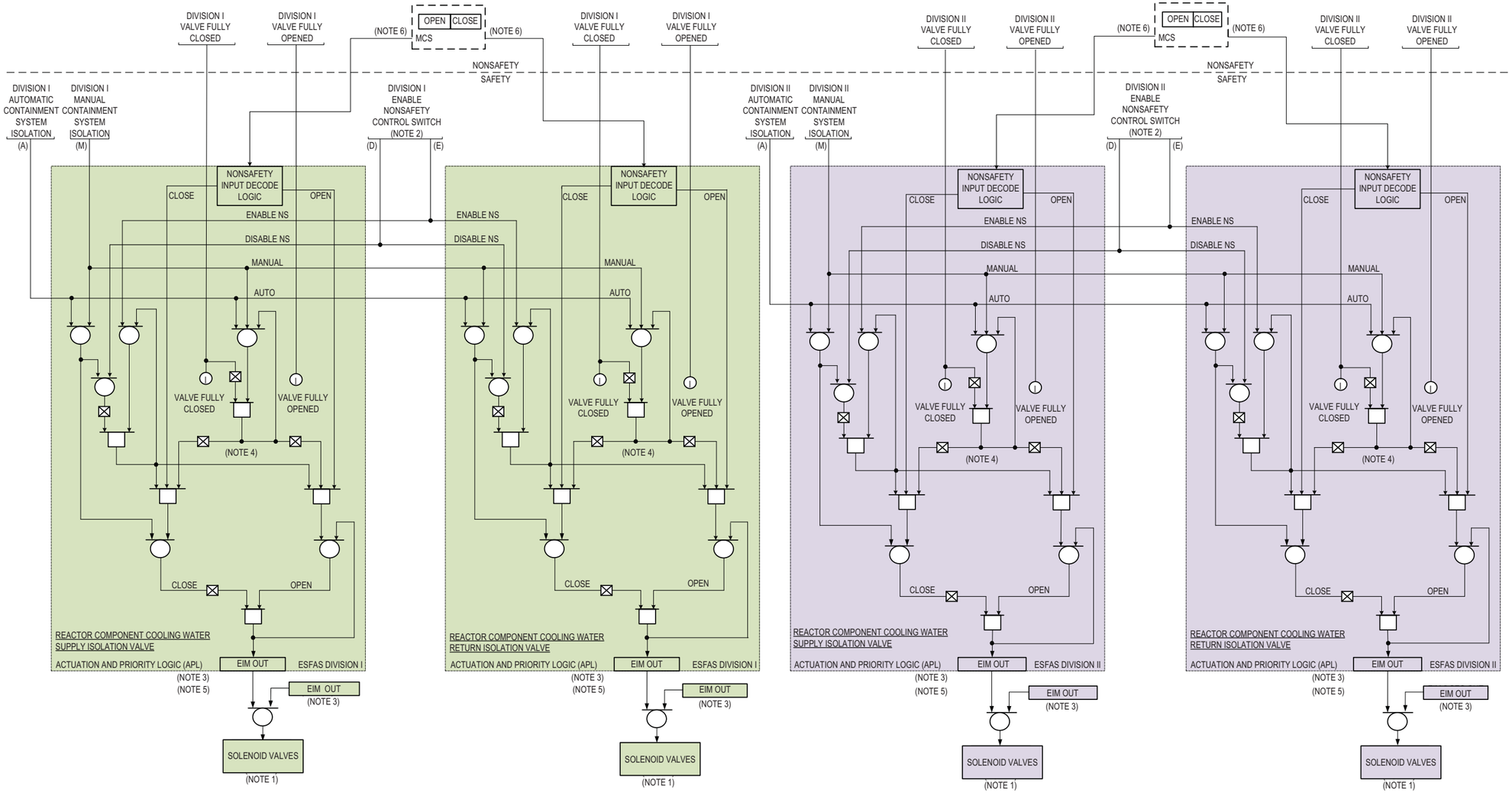
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

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 ESF COMPONENTS.

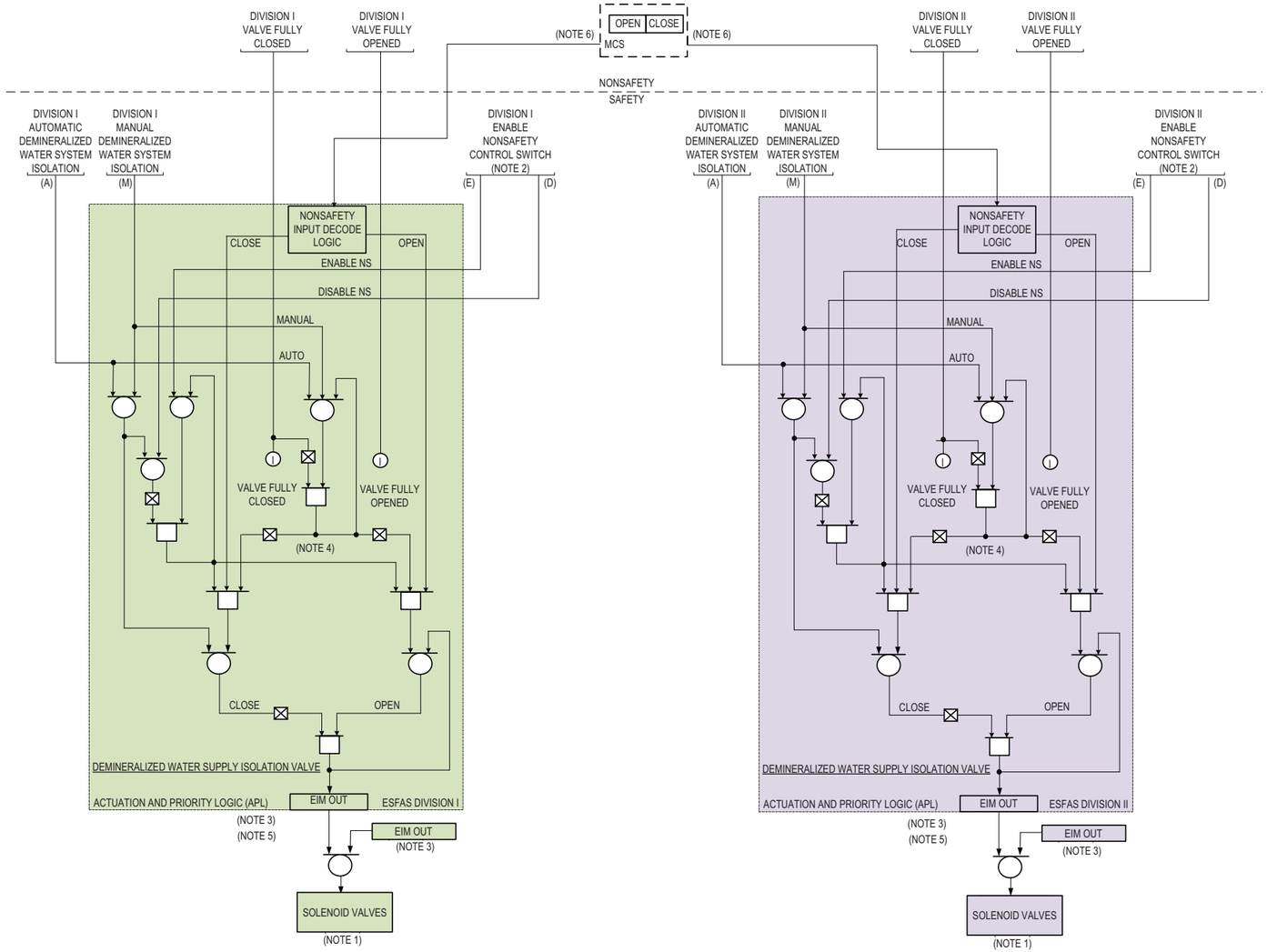
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

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



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 SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

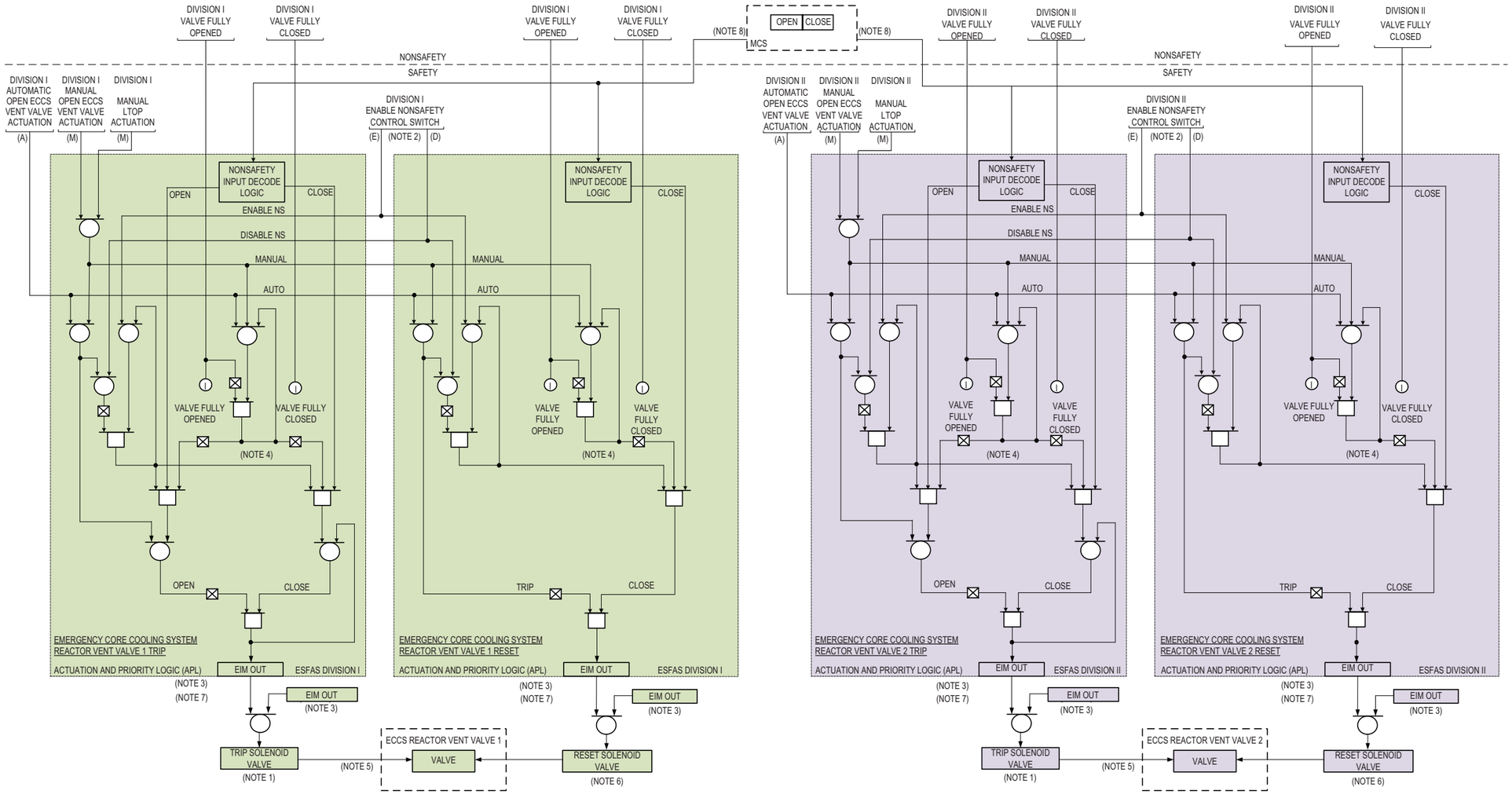
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTUATION. 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 7.1-1aa: Emergency Core Cooling System Reactor Vent Valve 1 & 2 Actuation



NOTE 1: THE ECCS VENT VALVE IS CLOSED WITH THE TRIP SOLENOID VALVE ENERGIZED BY REDUNDANT EIMS; THE TRIP SOLENOID IS DE-ENERGIZED TO OPEN THE ECCS VENT VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFTEY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL 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.

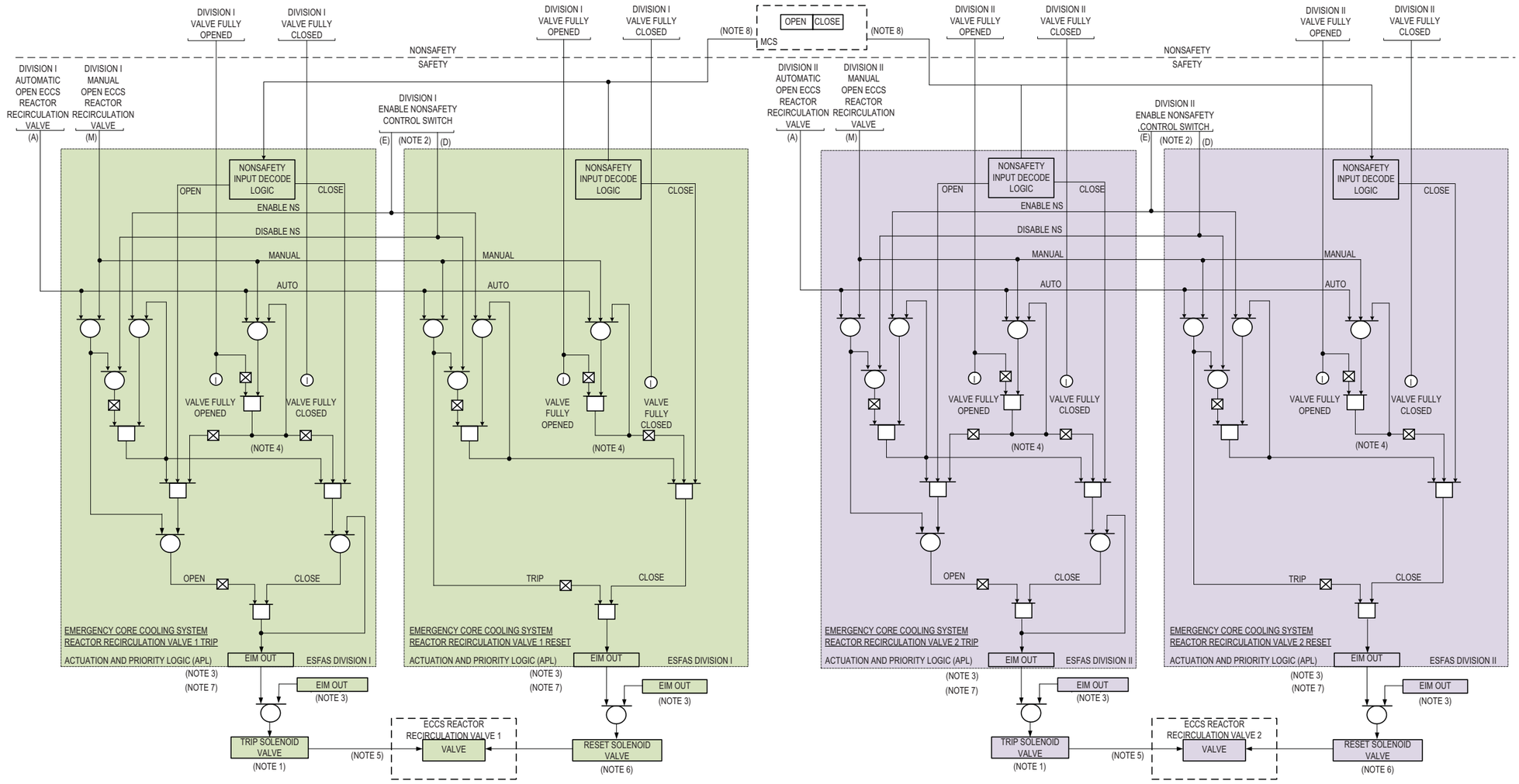
NOTE 5: THE ECCS VENT VALVE DESIGN INCLUDES AN ARMING VALVE. THE ARMING VENT VALVE IMPLEMENTS THE INADVERTENT ACTUATION BLOCK (IAB) FUNCTION THAT DELAYS OPENING OF THE ECCS VENT VALVE WHEN THE TRIP SOLENOID DE-ENERGIZES UNTIL RPV TO CNV DIFFERENTIAL PRESSURE IS BELOW THE ARMING VENT VALVE SET PRESSURE.

NOTE 6: THE ECCS RESET SOLENOID VALVE IS NORMALLY DE-ENERGIZED (CLOSED). THE RESET SOLENOID MUST BE ENERGIZED (OPENED) TO CLOSE THE ECCS VALVE. THIS PROVIDES A PATH FOR CVCS MAKEUP TO THE MAIN VALVE CONTROL CHAMBER UNTIL RPV PRESSURE IS SUFFICIENT TO OVERCOME THE SPRING FORCE HOLDING THE VALVE OPEN.

NOTE 7: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 8: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

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



NOTE 1: THE ECCS RECIRCULATION VALVE IS CLOSED WITH THE TRIP SOLENOID VALVE ENERGIZED BY REDUNDANT EIMS; THE TRIP SOLENOID IS DE-ENERGIZED TO OPEN THE ECCS RECIRCULATION 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 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.

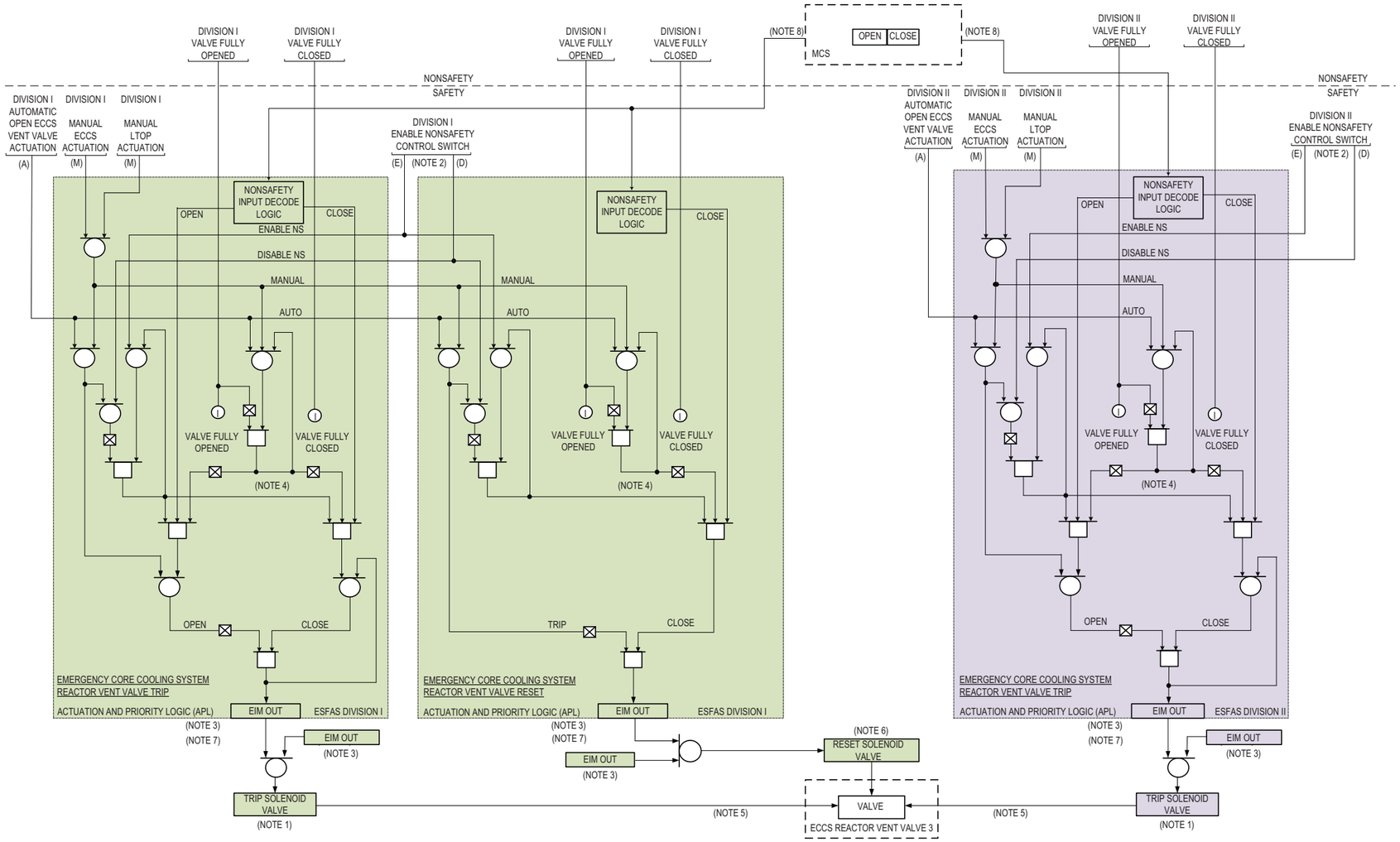
NOTE 5: THE ECCS RECIRCULATION VALVE DESIGN INCLUDES AN ARMING VALVE. THE ARMING VALVE IMPLEMENTS THE INADVERTENT ACTUATION BLOCK (IAB) FUNCTION THAT DELAYS OPENING OF THE ECCS RECIRCULATION VALVE WHEN THE TRIP SOLENOID DE-ENERGIZES UNTIL RPV TO CNV DIFFERENTIAL PRESSURE IS BELOW THE ARMING VALVE SET PRESSURE.

NOTE 6: THE ECCS RESET SOLENOID VALVE IS NORMALLY DE-ENERGIZED (CLOSED). THE RESET SOLENOID MUST BE ENERGIZED (CLOSED) TO OPEN THE ECCS RECIRCULATION VALVE. THIS PROVIDES A PATH FOR CVCS MAKEUP TO THE MAIN VALVE CONTROL CHAMBER UNTIL RPV PRESSURE IS SUFFICIENT TO OVERCOME THE SPRING FORCE HOLDING THE VALVE OPEN.

NOTE 7: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 8: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ac: Emergency Core Cooling System Reactor Vent Valve 3 Actuation



NOTE 1: THE ECCS VENT VALVE IS CLOSED WITH THE TRIP SOLENOID VALVE ENERGIZED BY REDUNDANT EIMS; THE TRIP SOLENOID IS DE-ENERGIZED TO OPEN THE ECCS VENT 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 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.

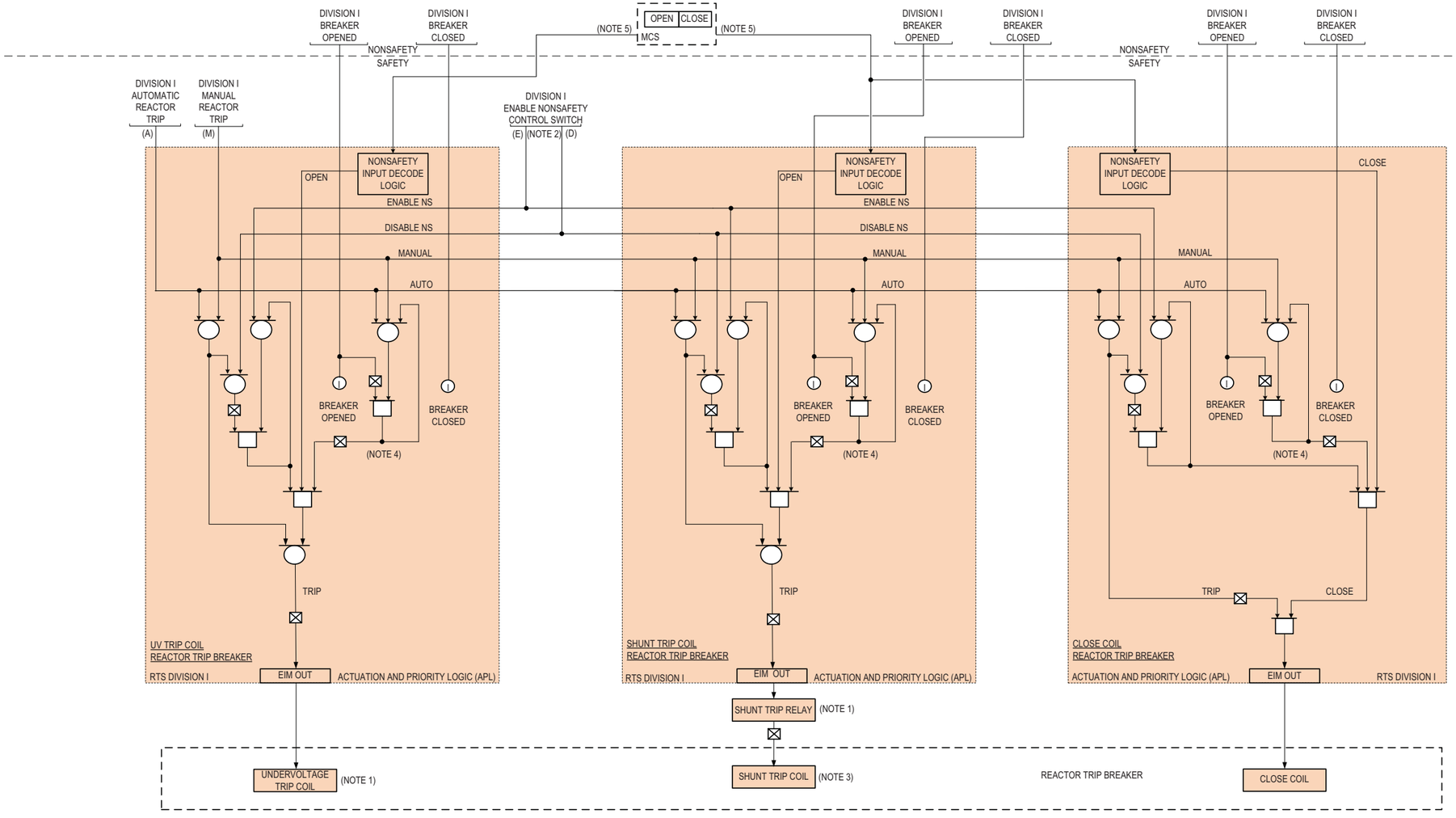
NOTE 5: THE ECCS VENT VALVE DESIGN INCLUDES AN ARMING VALVE. THE ARMING VALVE IMPLEMENTS THE INADVERTENT ACTUATION BLOCK (IAB) FUNCTION THAT DELAYS OPENING OF THE ECCS VENT VALVE WHEN THE TRIP SOLENOID DE-ENERGIZES UNTIL RPV TO CNV DIFFERENTIAL PRESSURE IS BELOW THE ARMING VALVE SET PRESSURE.

NOTE 6: THE ECCS RESET SOLENOID VALVE IS NORMALLY DE-ENERGIZED (CLOSED). THE RESET SOLENOID MUST BE ENERGIZED (CLOSED) TO OPEN THE ECCS VENT VALVE. THIS PROVIDES A PATH FOR CVCS MAKEUP TO THE MAIN VALVE CONTROL CHAMBER UNTIL RPV PRESSURE IS SUFFICIENT TO OVERCOME THE SPRING FORCE HOLDING THE VALVE OPEN.

NOTE 7: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 8: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

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



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

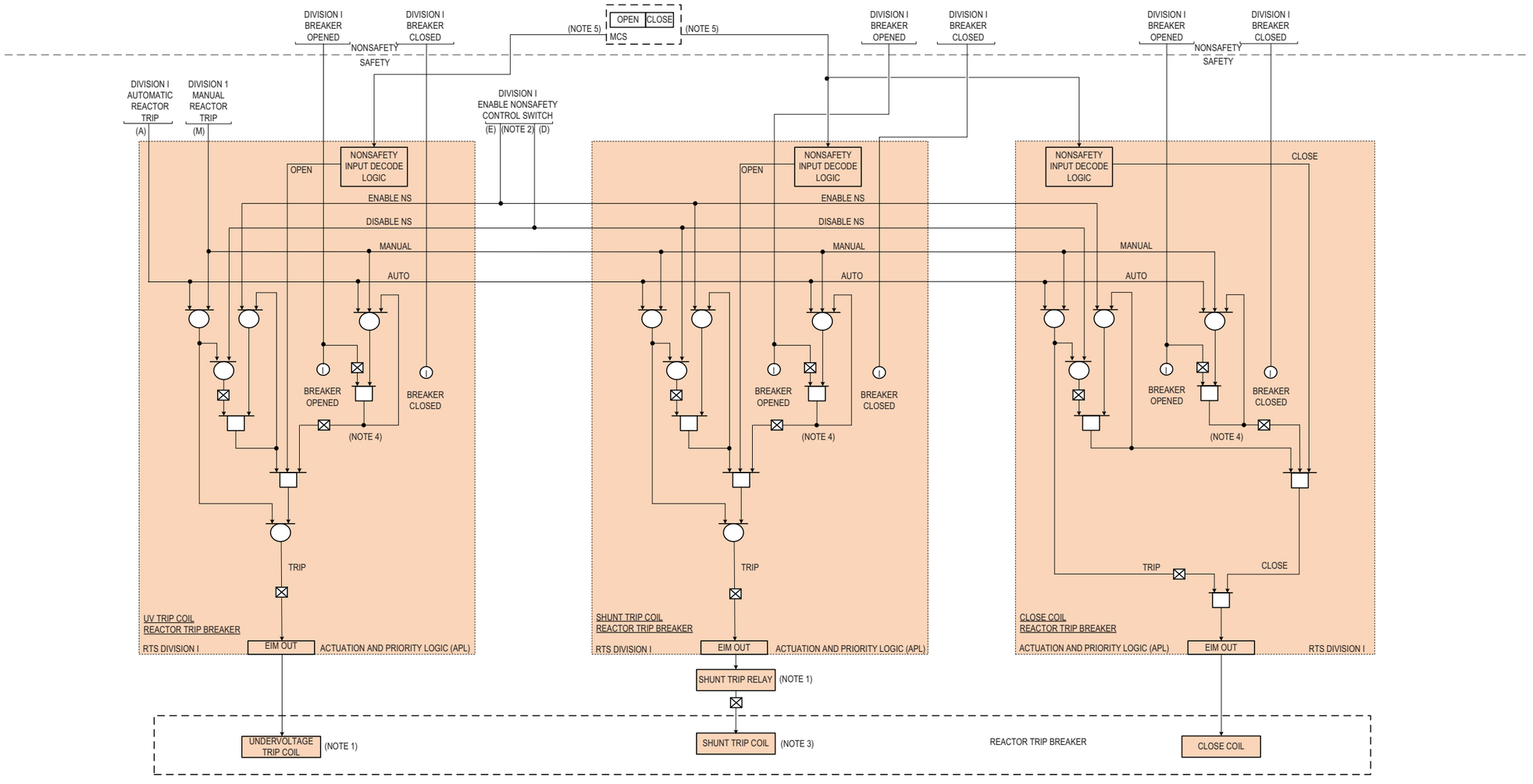
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

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 7.1-1ae: Reactor Trip Breaker Division I B



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

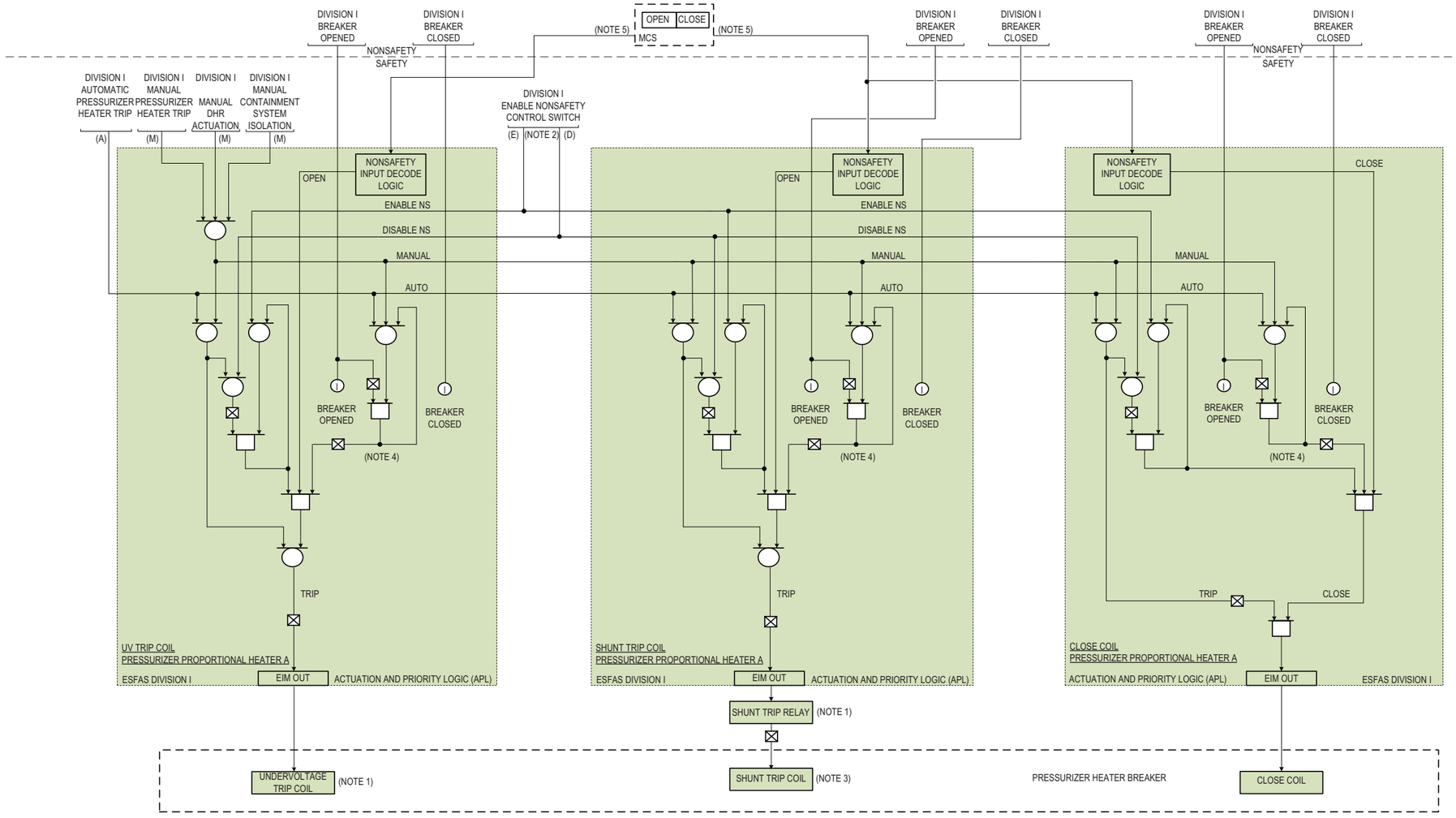
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

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 Trip Breaker Proportional Heater A



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

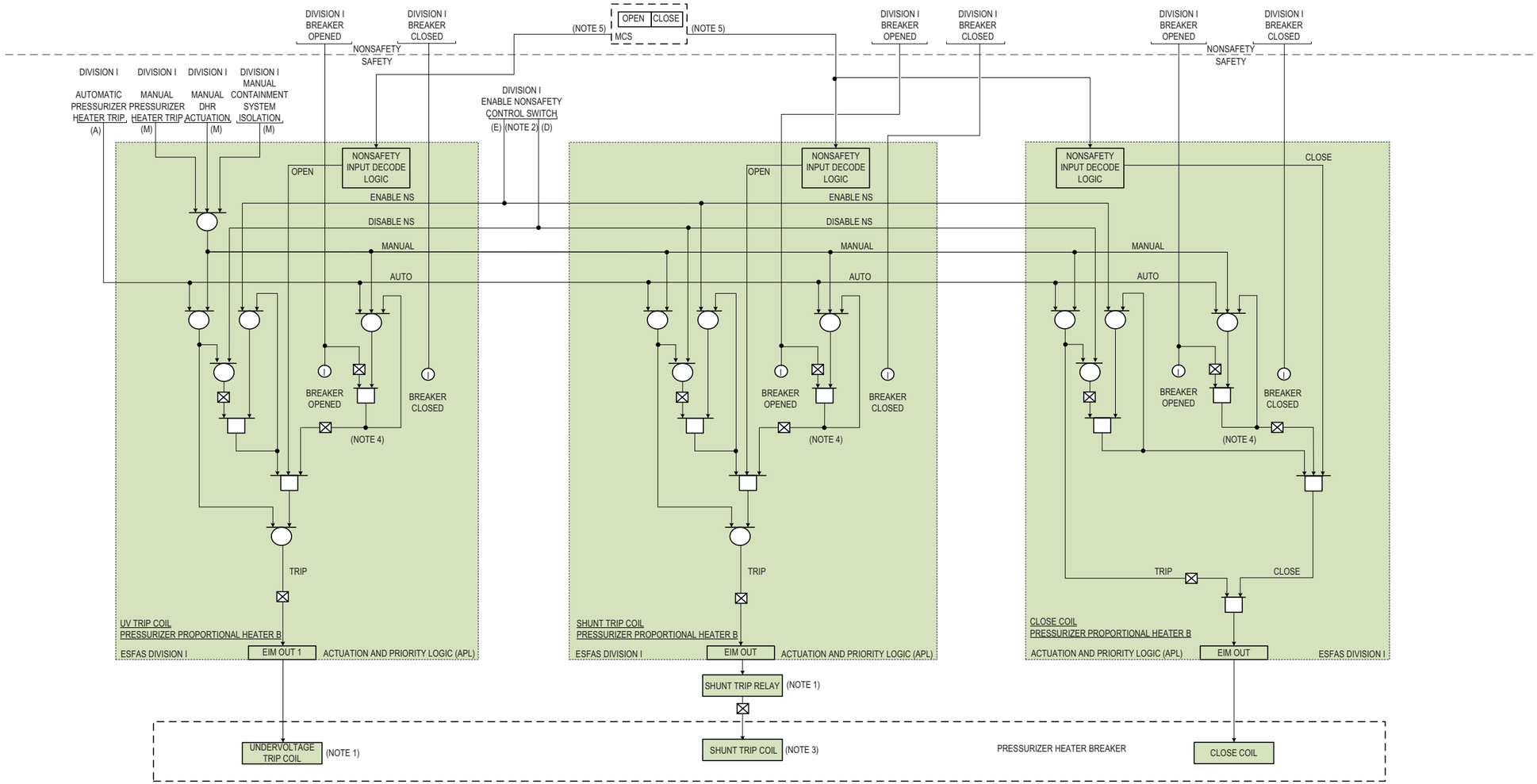
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

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 7.1-1ag: Pressurizer Heater Trip Breaker Proportional Heater B



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

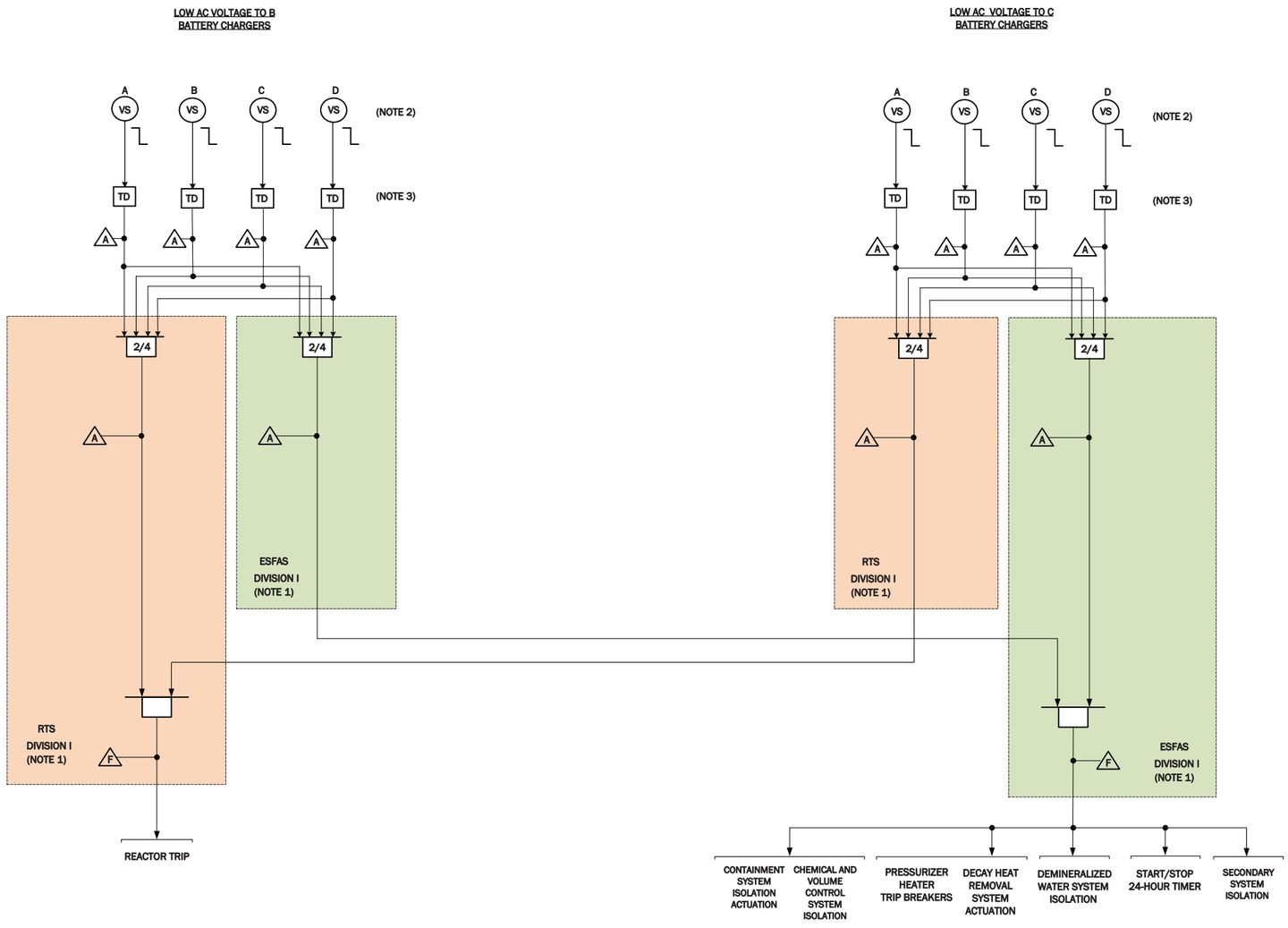
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

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

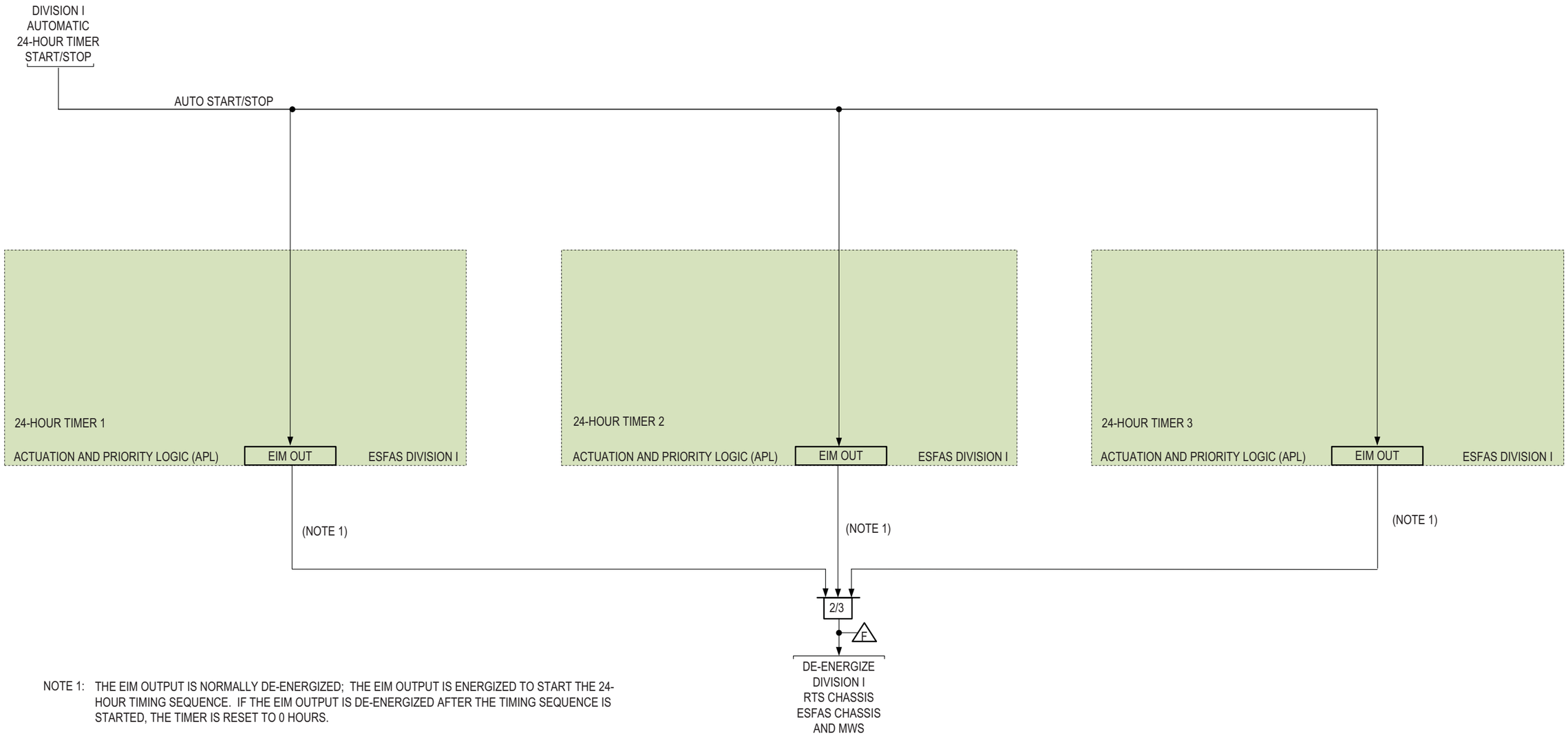


NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

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

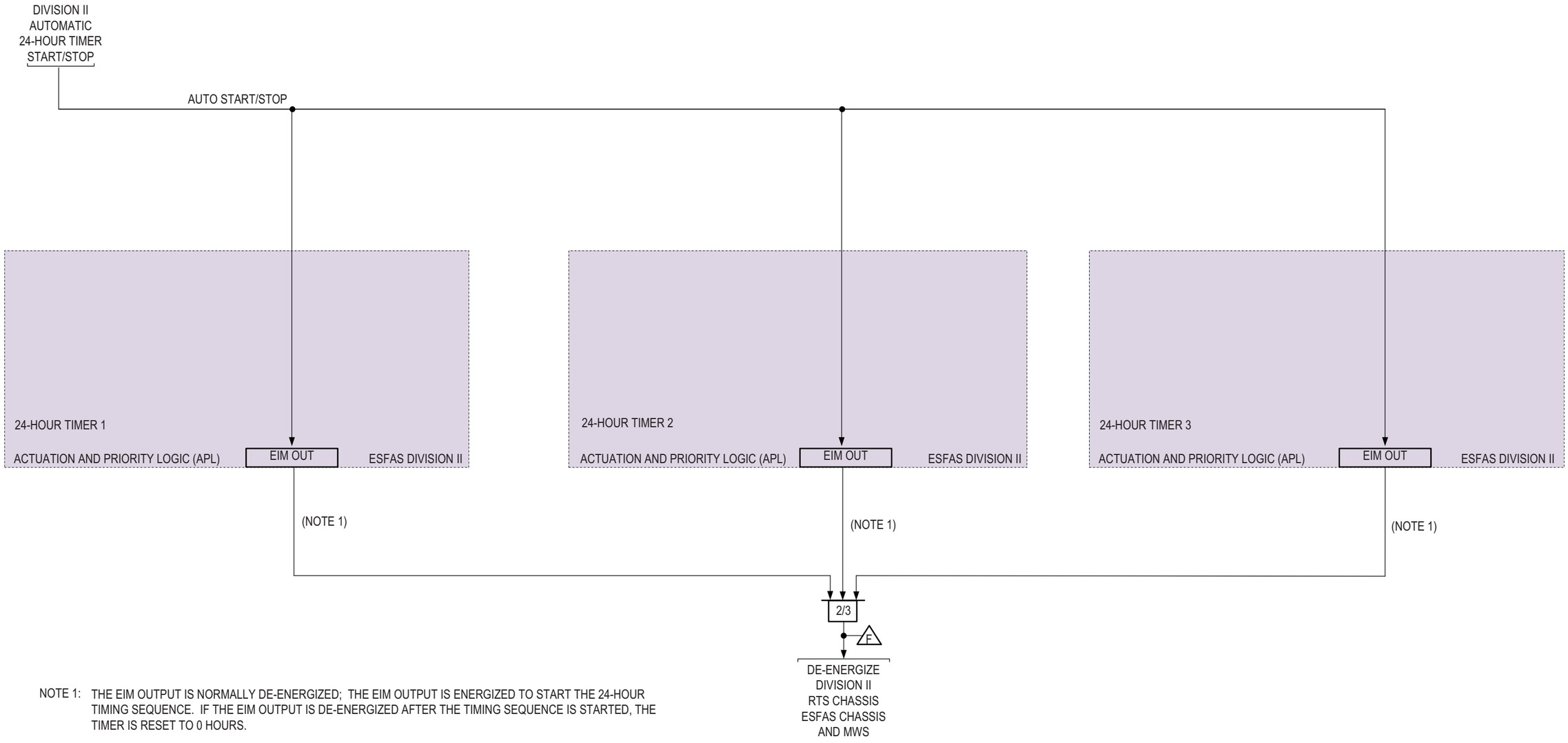
NOTE 3: THE TIME DELAY (TD) IS ADDED TO DELAY THE START OF THE TIMING SEQUENCE TO PREVENT ACTUATION OF TRIP LOGIC ON MOMENTARY AC BUS VOLTAGE TRANSIENTS. THE TIME DELAY ALSO DELAYS THE RESET OF THE TIMING SEQUENCE TO PREVENT PREMATURE RESET OF TRIP LOGIC ON MOMENTARY AC BUS VOLTAGE TRANSIENTS.

Figure 7.1-1ai: Loss of AC Power to ELVS 24 Hour Timers Division I



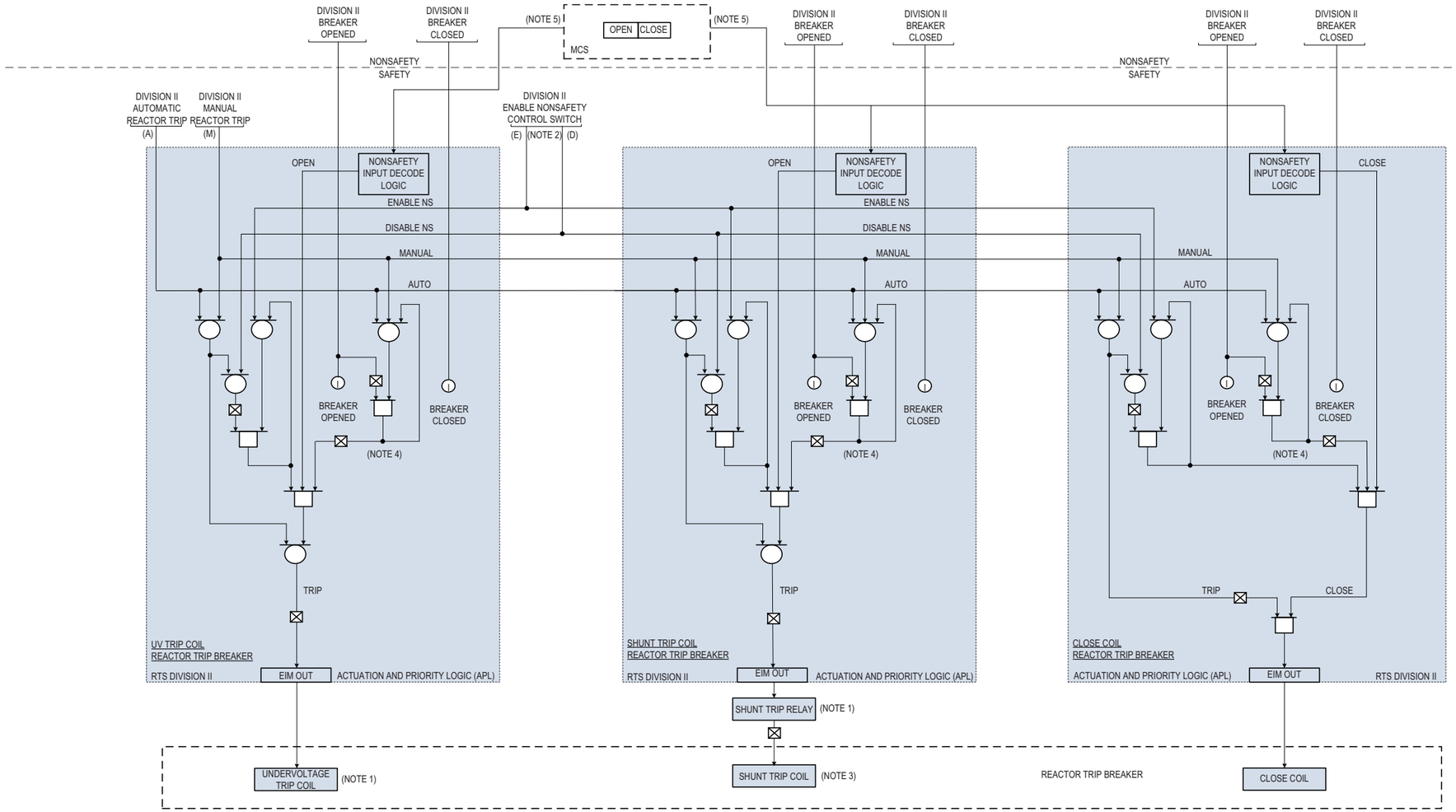
NOTE 1: THE EIM OUTPUT IS NORMALLY DE-ENERGIZED; THE EIM OUTPUT IS ENERGIZED TO START THE 24-HOUR TIMING SEQUENCE. IF THE EIM OUTPUT IS DE-ENERGIZED AFTER THE TIMING SEQUENCE IS STARTED, THE TIMER IS RESET TO 0 HOURS.

Figure 7.1-1aj: Loss of AC Power to ELVS 24 Hour Timers Division II



NOTE 1: THE EIM OUTPUT IS NORMALLY DE-ENERGIZED; THE EIM OUTPUT IS ENERGIZED TO START THE 24-HOUR TIMING SEQUENCE. IF THE EIM OUTPUT IS DE-ENERGIZED AFTER THE TIMING SEQUENCE IS STARTED, THE TIMER IS RESET TO 0 HOURS.

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



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

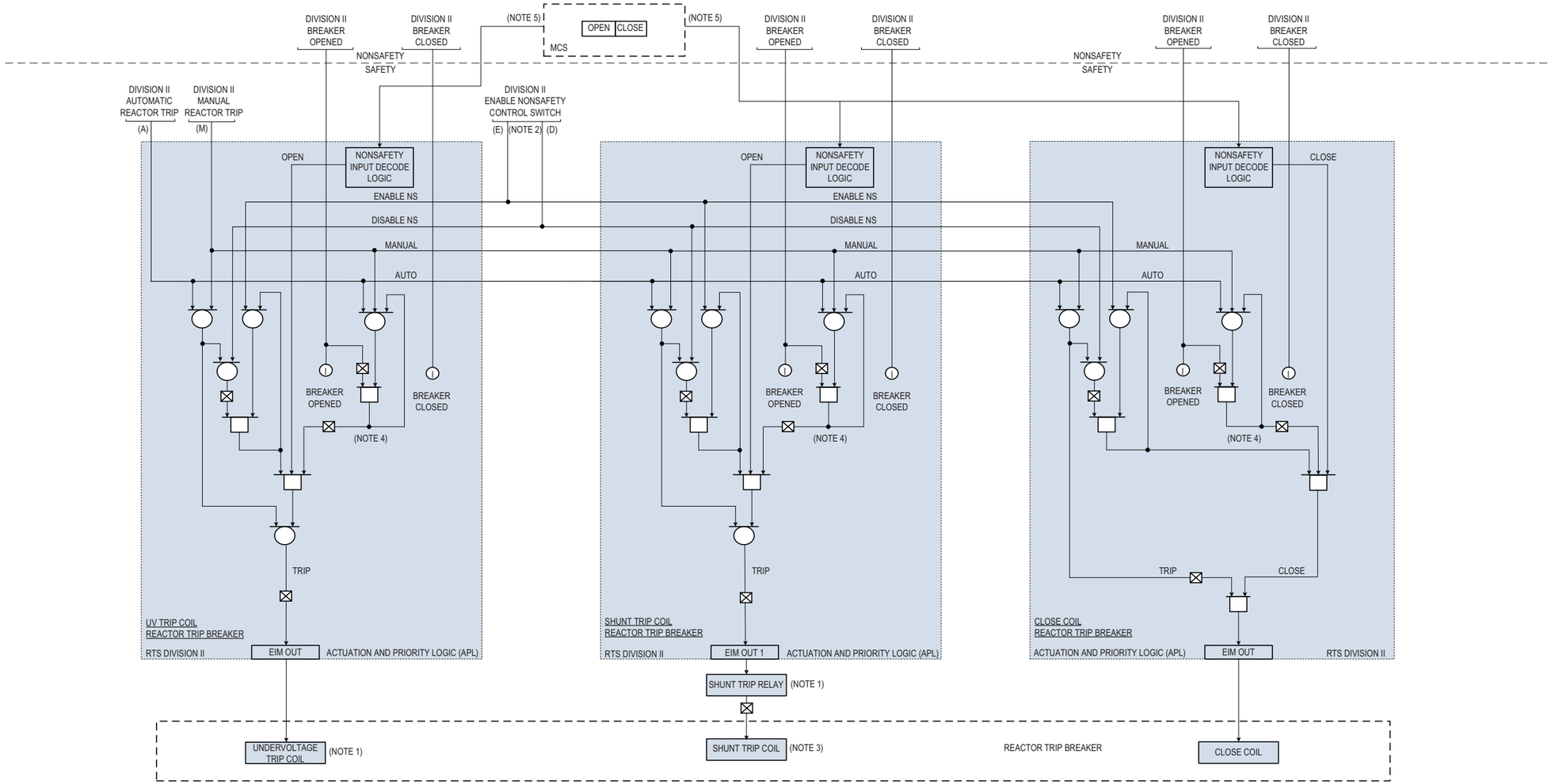
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

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 7.1-1al: Reactor Trip Breaker Division II B



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

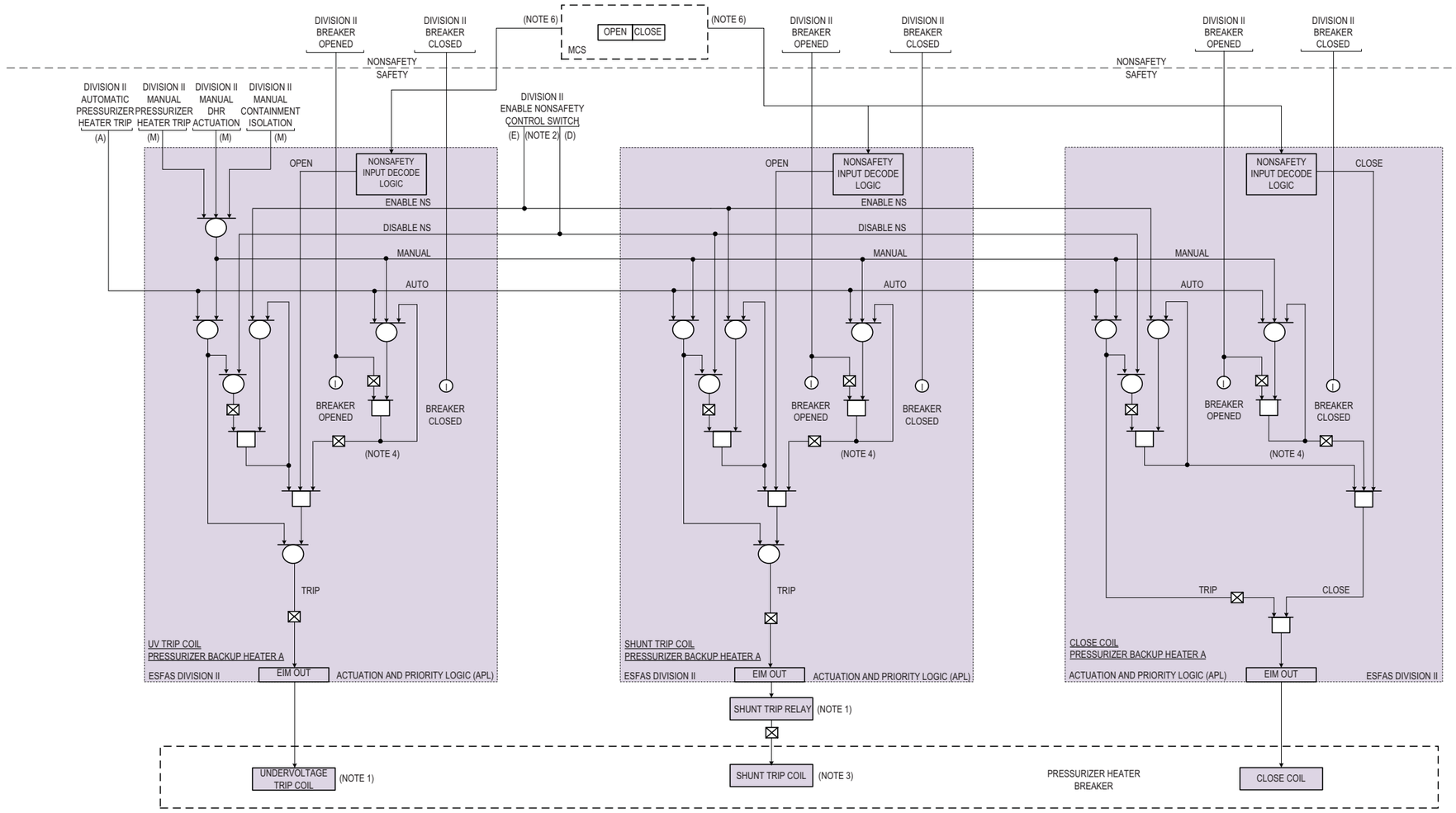
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

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 7.1-1am: 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.

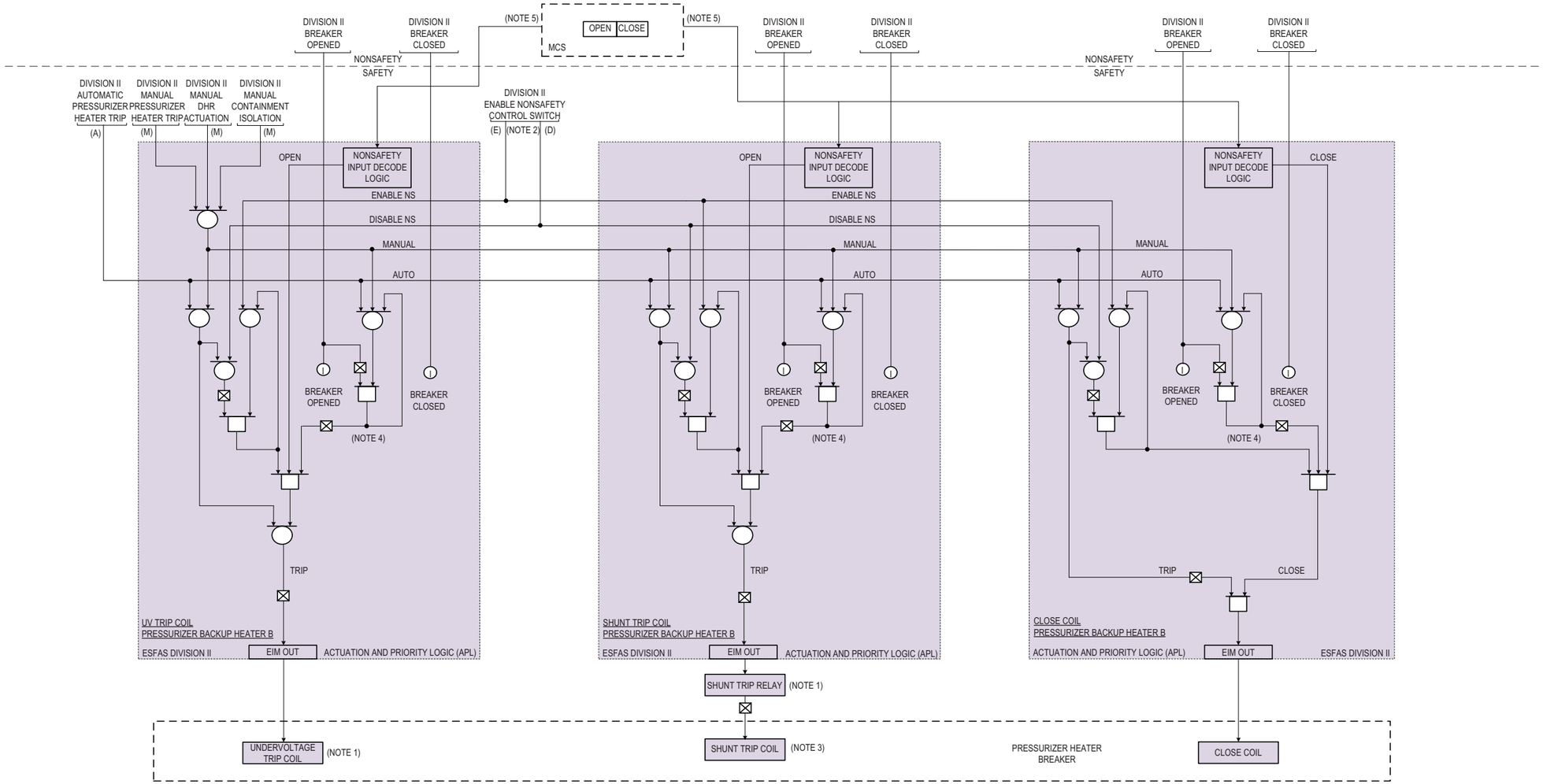
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

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 7.1-1an: Pressurizer Heater Trip Breaker Backup Heater B



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.

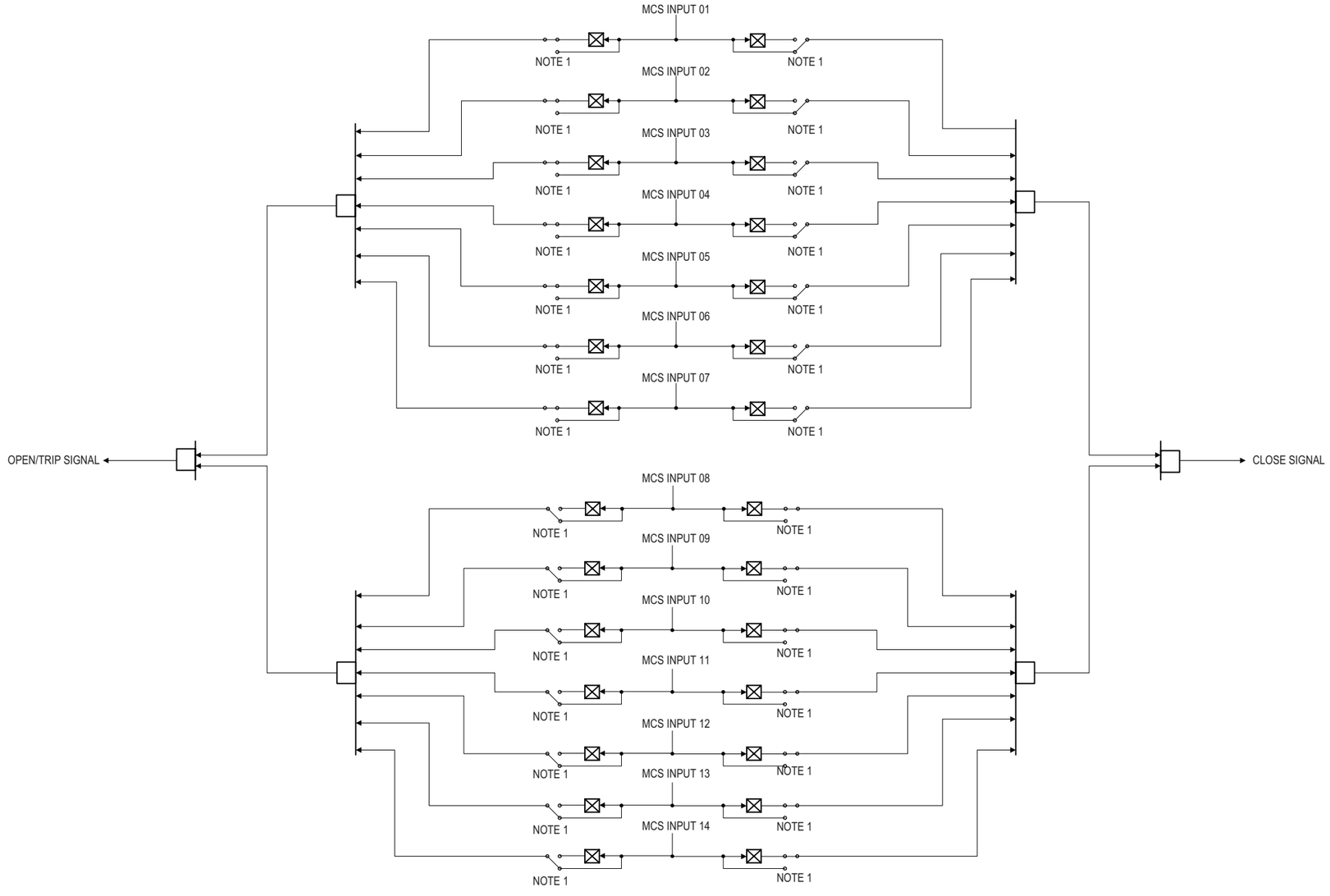
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

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.

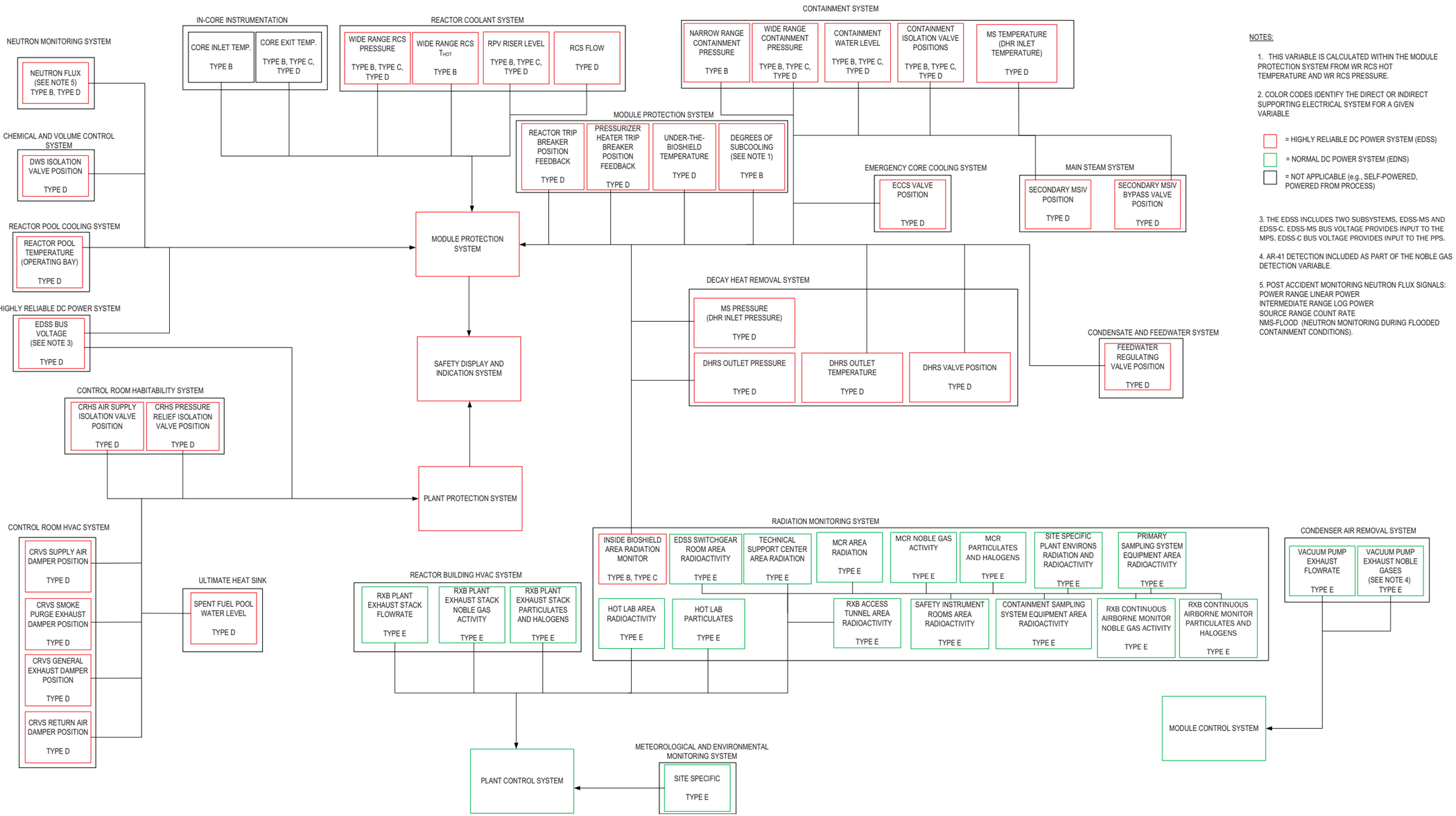
NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ao: 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. THIS VARIABLE IS CALCULATED WITHIN THE MODULE PROTECTION SYSTEM FROM WR RCS HOT TEMPERATURE AND WR RCS PRESSURE.

2. COLOR CODES IDENTIFY THE DIRECT OR INDIRECT SUPPORTING ELECTRICAL SYSTEM FOR A GIVEN VARIABLE

   = HIGHLY RELIABLE DC POWER SYSTEM (EDSS)

   = NORMAL DC POWER SYSTEM (EDNS)

   = NOT APPLICABLE (e.g., SELF-POWERED, POWERED FROM PROCESS)

3. THE EDSS INCLUDES TWO SUBSYSTEMS, EDSS-MS AND EDSS-C. EDSS-MS BUS VOLTAGE PROVIDES INPUT TO THE MPS. EDSS-C BUS VOLTAGE PROVIDES INPUT TO THE PPS.

4. AR-41 DETECTION INCLUDED AS PART OF THE NOBLE GAS DETECTION VARIABLE.

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).

Figure 7.1-3a: 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 OOS SWITCH ON THE SFM IS IN THE OPERATE POSITION, THE TRIP DETERMINATION RESULT OF THE SAFETY FUNCTION ALGORITHM IS SENT TO THE SBM.

IF THE OOS SWITCH IS IN THE OUT OF SERVICE POSITION, THE POSITION OF THE TRIP/BYPASS SWITCH DETERMINES WHAT IS SENT TO THE EIM. IF THE TRIP/BYPASS SWITCH IS IN BYPASS, ALL SAFETY FUNCTIONS FOR THAT SFM ARE FORCED TO NOT TRIP OR NOT ACTUATE. IF THE TRIP/BYPASS SWITCH IS IN THE TRIP POSITION, THEN ALL SAFETY FUNCTIONS FOR THAT SFM ARE FORCED TO TRIP AND ACTUATE.

IF THE SFM FAILS TO COMMUNICATE CORRECTLY TO THE SBM OR IS REMOVED, THE POSITION OF THE TRIP/BYPASS SWITCH WILL DETERMINE THE COMMANDS SENT TO THE EIM FOR THE SAFETY FUNCTION ON THAT SFM. (ASSOCIATED LOGIC IS SHOWN BELOW)

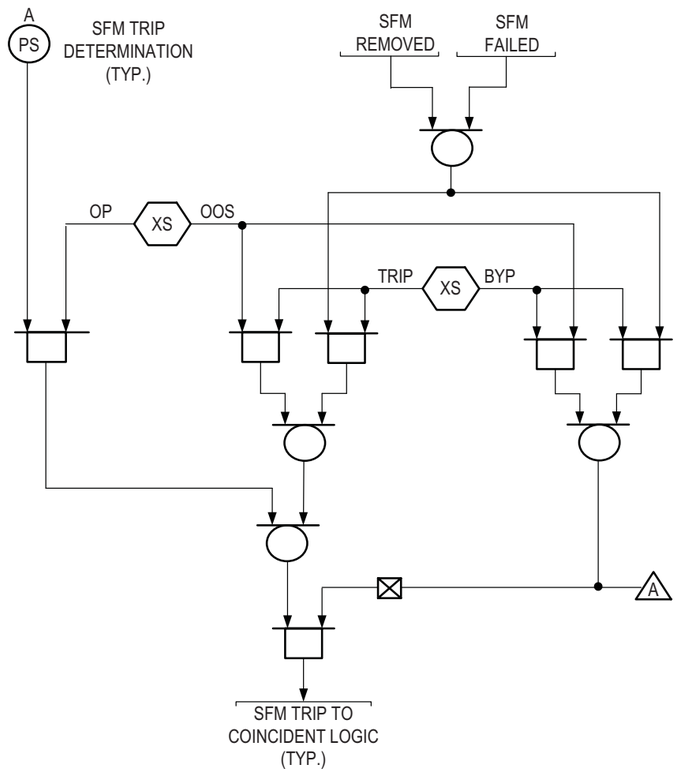
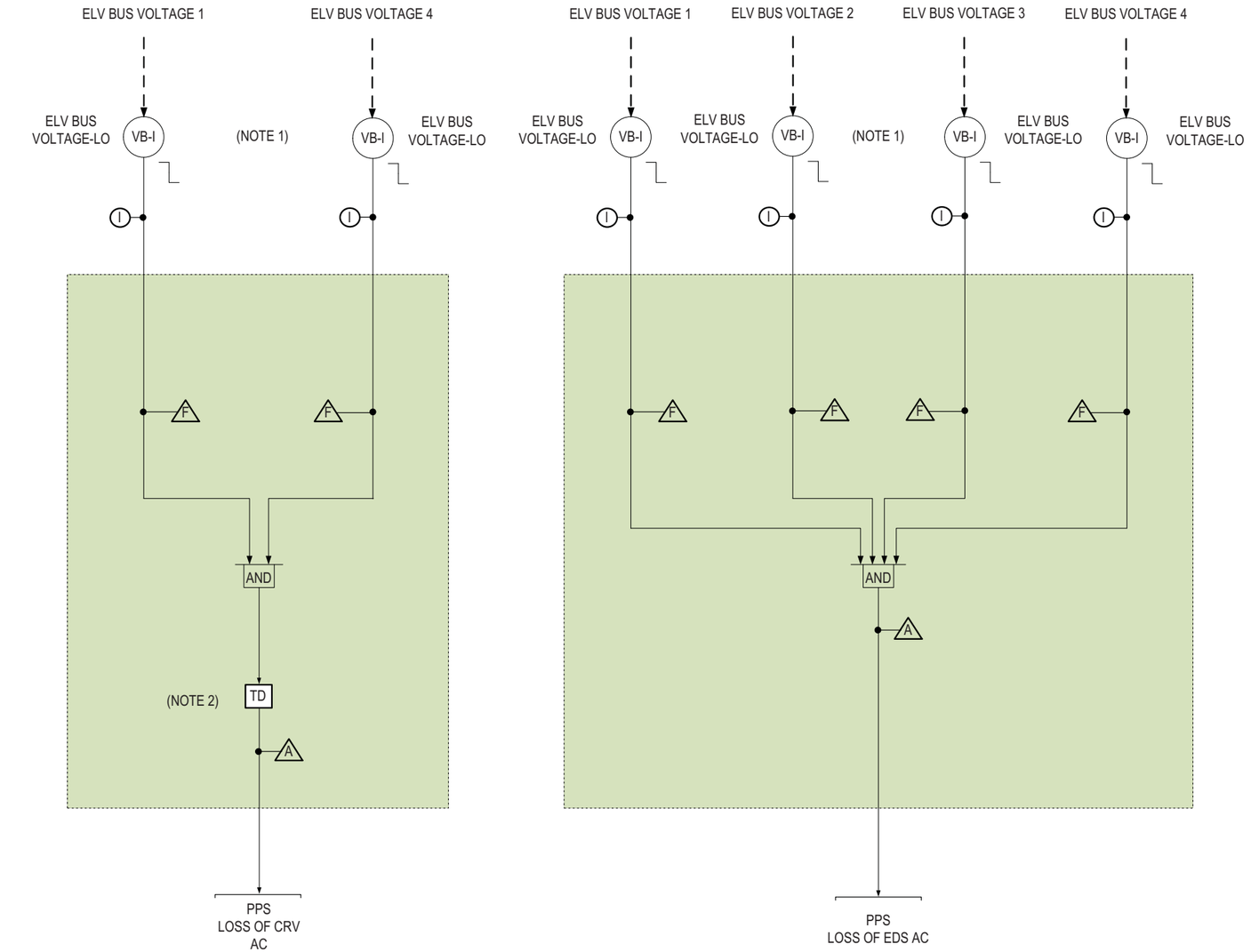
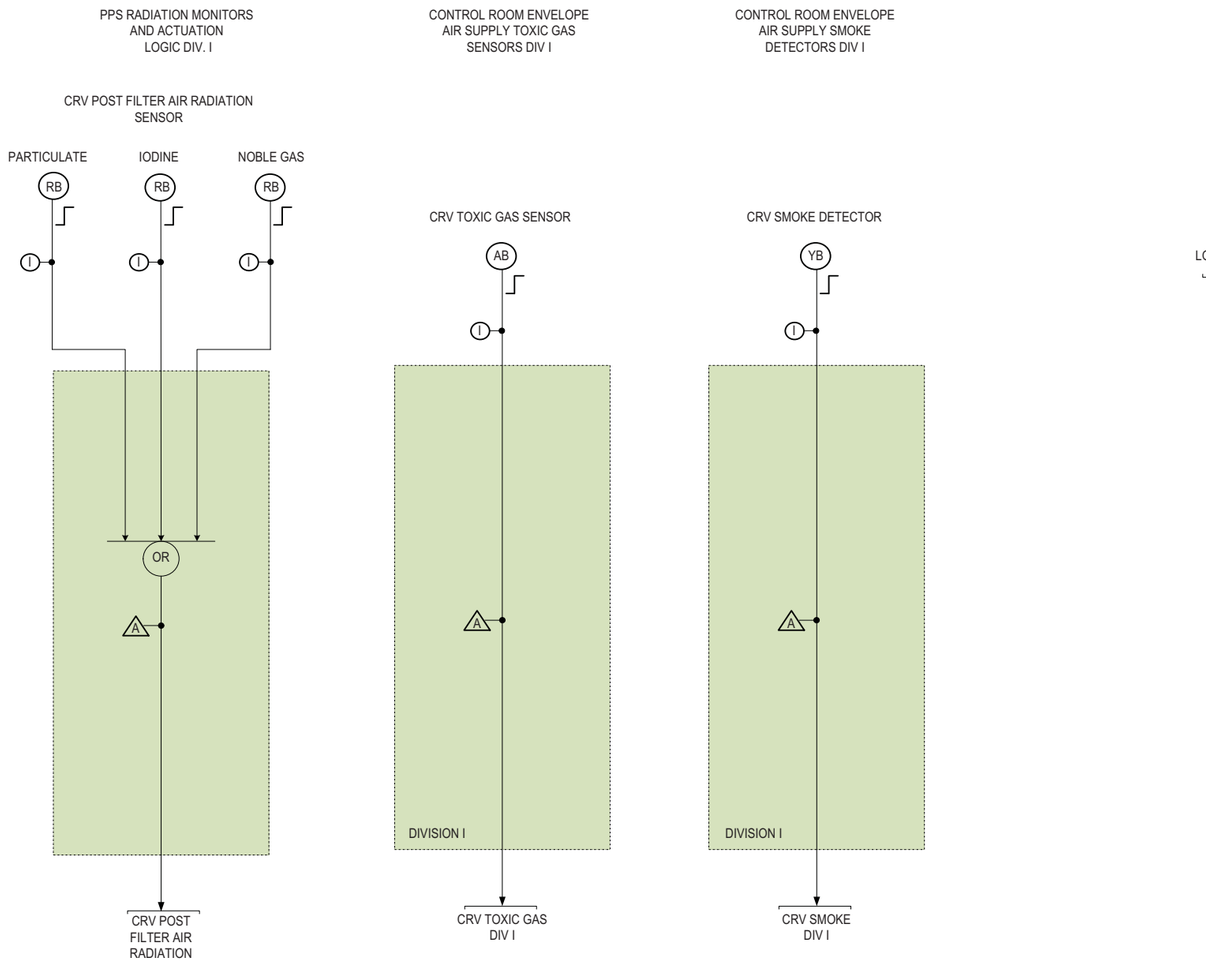


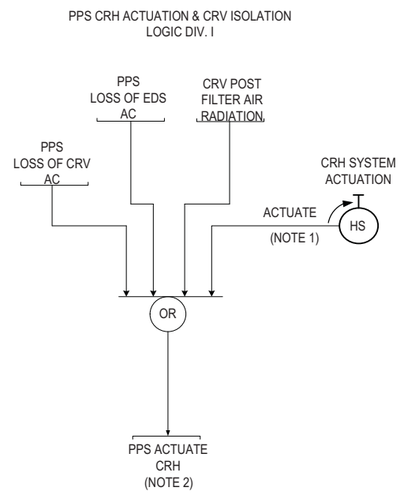
Figure 7.1-3b: Plant Protection System Loss of Normal Control Room HVAC System AC and Loss of Highly Reliable DC Power System AC

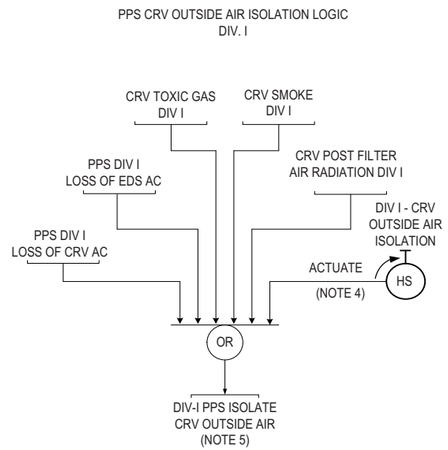


NOTE 1: ONLY ONE DIVISION IS SHOWN. OTHER DIVISION IS SIMILAR.
NOTE 2: THERE IS A 10 MIN. TIME DELAY ASSOCIATED WITH LOSS OF CRV AC POWER.

Figure 7.1-3c: Plant Protection System Radiation Monitors and Actuation Logic







NOTE 1: MANUAL ACTUATE INITIATES CRH AND CRV ISOLATION AT THE COMPONENT LEVEL THROUGH THE EIM APL LOGIC. MANUAL ACTUATE SWITCHES ARE LOCATED IN THE MCR.

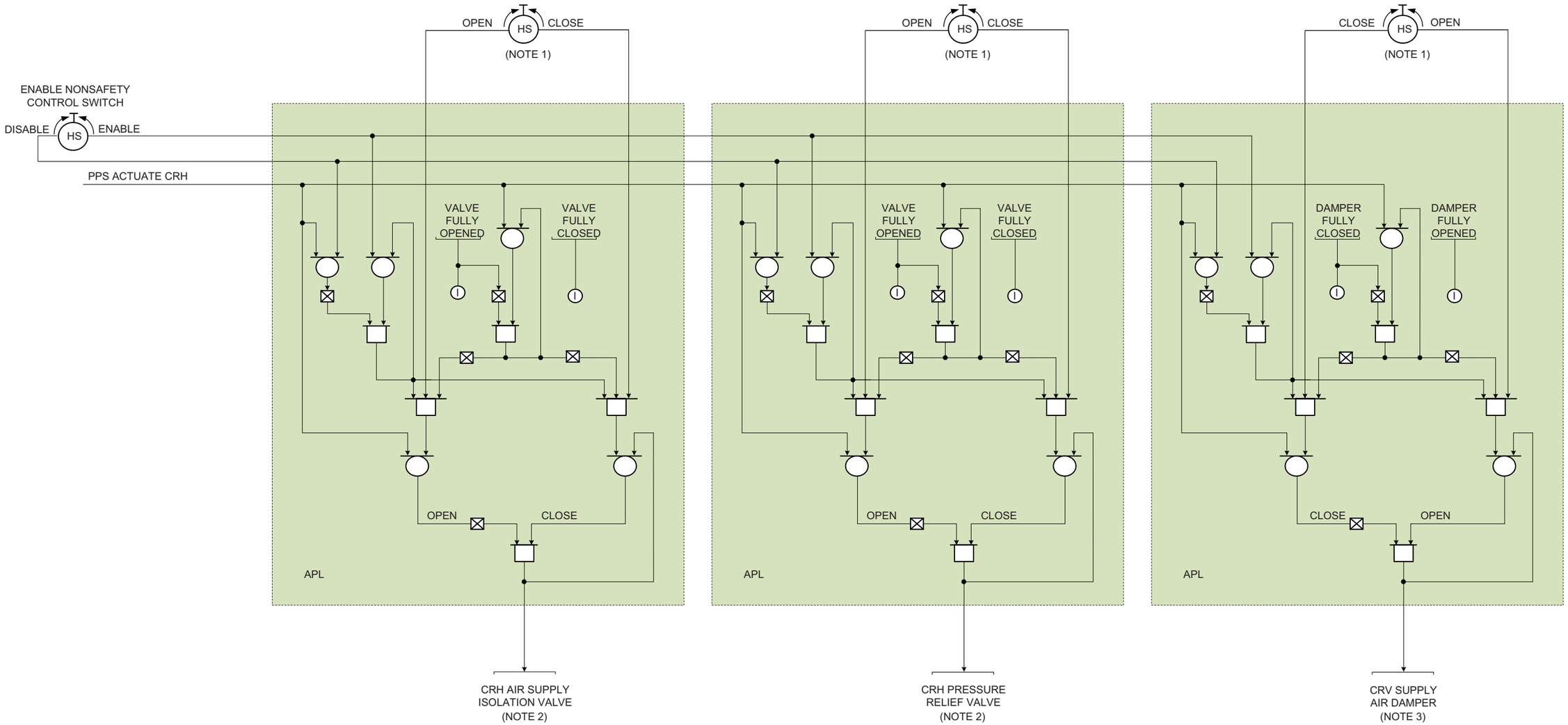
NOTE 2: PPS ACTUATE CRH, WHEN ACTIVE, INITIATES CRH AND ISOLATES THE CRE BY CLOSING ASSOCIATED DAMPERS.

NOTE 3: ONLY ONE DIVISION IS SHOWN. OTHER DIVISION WILL BE SIMILAR.

NOTE 4: MANUAL ACTUATE INITIATES CRV OUTSIDE AIR ISOLATION AT THE COMPONENT LEVEL THROUGH THE EIM APL LOGIC. MANUAL ACTUATE SWITCHES ARE LOCATED IN THE MCR.

NOTE 5: PPS ISOLATE CRV OUTSIDE AIR, WHEN ACTIVE, ISOLATES THE CRV OUTSIDE AIR INTAKE BY CLOSING ASSOCIATED DAMPERS.

Figure 7.1-3d: Plant Protection System Actuation Logic (1 of 3)



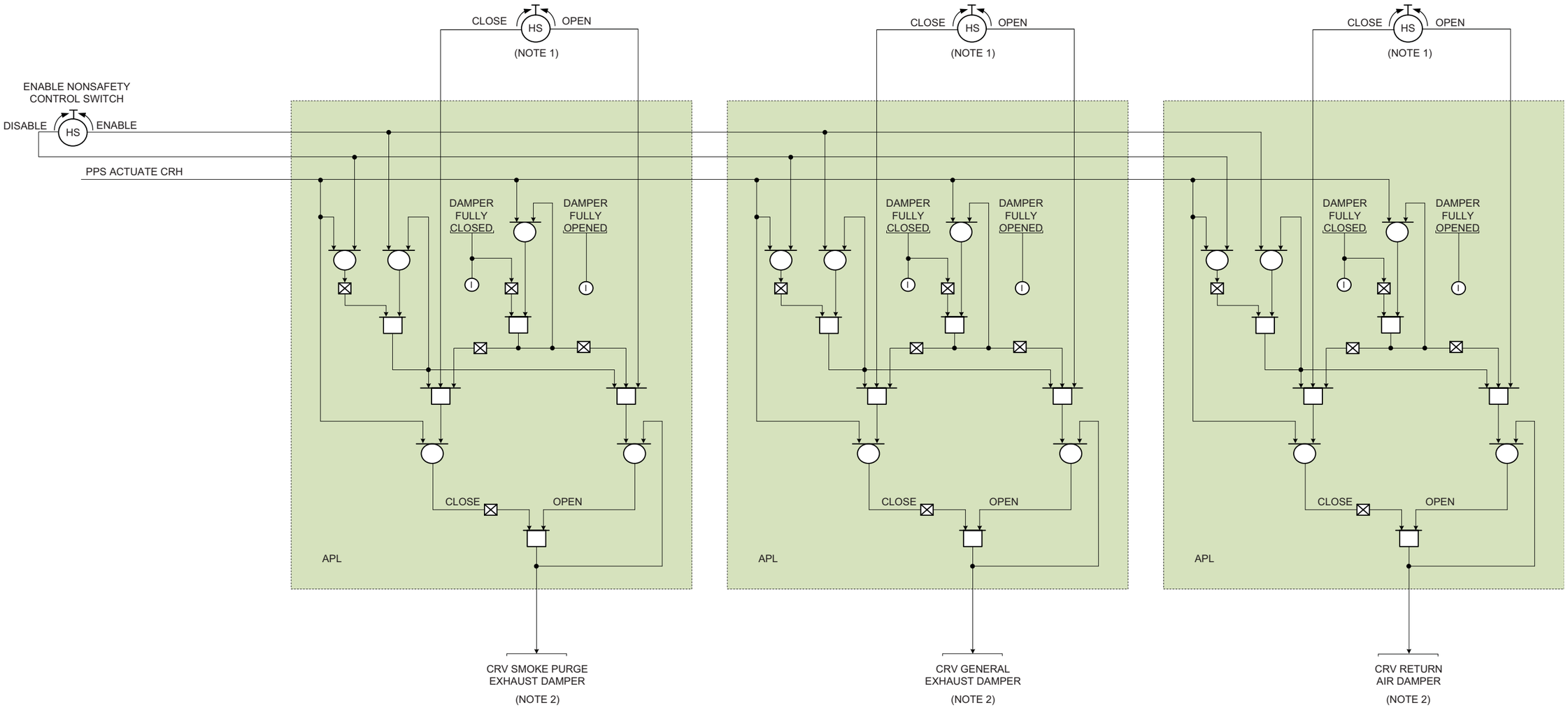
NOTE 1: MANUAL HAND SWITCH IS USED TO REPRESENT INPUTS FROM PCS.

NOTE 2: SOLENOID NORMALLY ENERGIZED TO CLOSE VALVE; DE-ENERGIZED TO OPEN VALVE.

NOTE 3: PPS DAMPER OUTPUT IS CLOSED TO ENABLE DAMPER OPERATION (NORMAL) AND DAMPER OUTPUT IS OPEN TO CLOSE DAMPER (ACTUATED).

NOTE 4: ONLY ONE DIVISION IS SHOWN. OTHER DIVISION IS SIMILAR.

Figure 7.1-3e: Plant Protection System Actuation Logic (2 of 3)

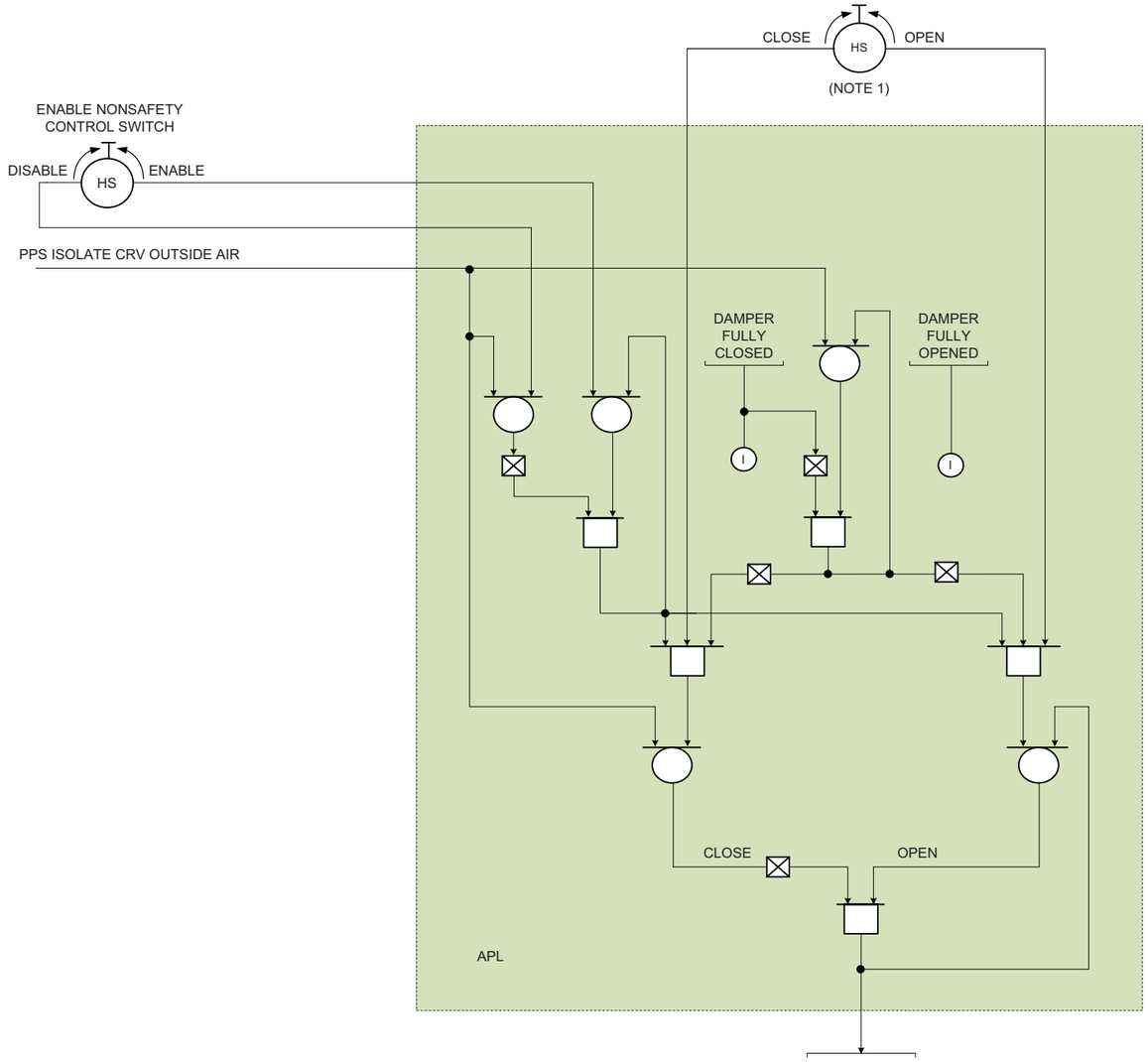


NOTE 1: MANUAL HAND SWITCH IS USED TO REPRESENT INPUTS FROM PCS.

NOTE 2: PPS DAMPER OUTPUT IS CLOSED TO ENABLE DAMPER OPERATION (NORMAL) AND DAMPER OUTPUT IS OPEN TO CLOSE DAMPER (ACTUATED).

NOTE 3: ONLY ONE DIVISION IS SHOWN. OTHER DIVISION IS SIMILAR.

Figure 7.1-3f: Plant Protection System Actuation Logic (3 of 3)



NOTE 1: MANUAL HAND SWITCH IS USED TO REPRESENT INPUTS FROM PCS.

NOTE 2: PPS DAMPER OUTPUT IS CLOSED TO ENABLE DAMPER OPERATION (NORMAL) AND DAMPER OUTPUT IS OPEN TO CLOSE DAMPER (ACTUATED).

NOTE 3: ONLY ONE DIVISION IS SHOWN. OTHER DIVISION IS SIMILAR.

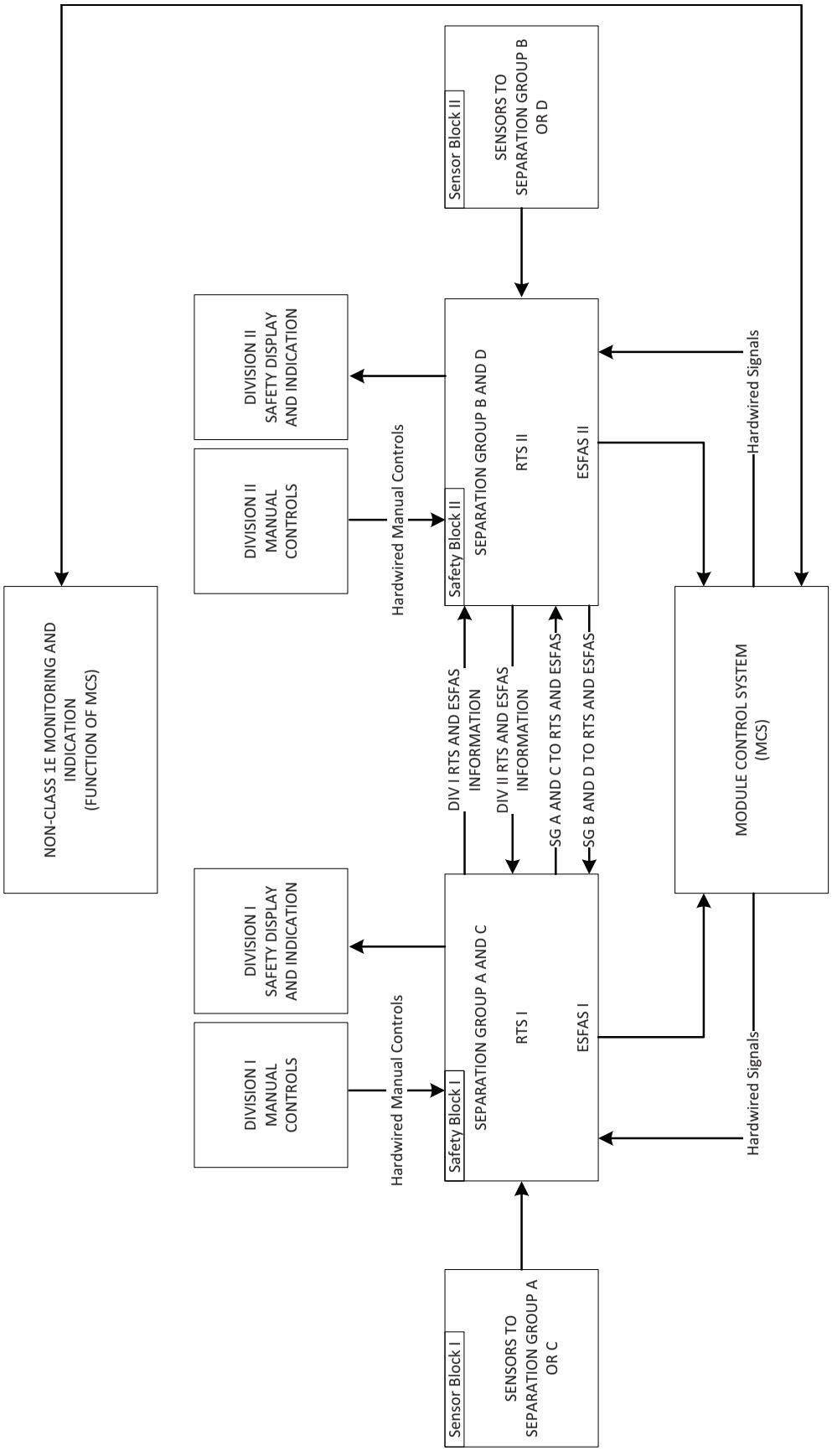


Figure 7.1-4: Blocks Selected for Defense-in-Depth Analysis

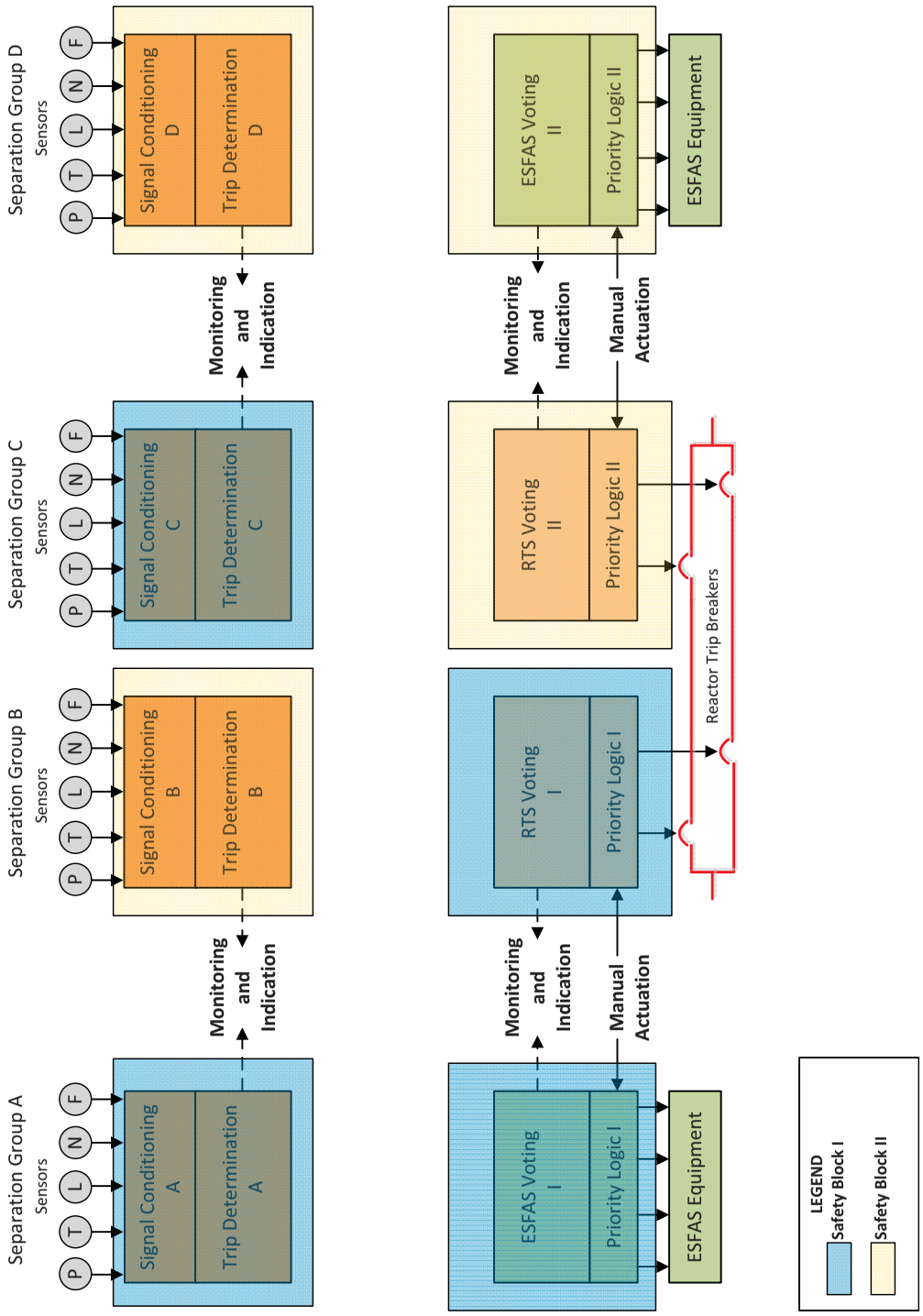


Figure 7.1-5: Blocks Selected for Defense-in-Depth Analysis

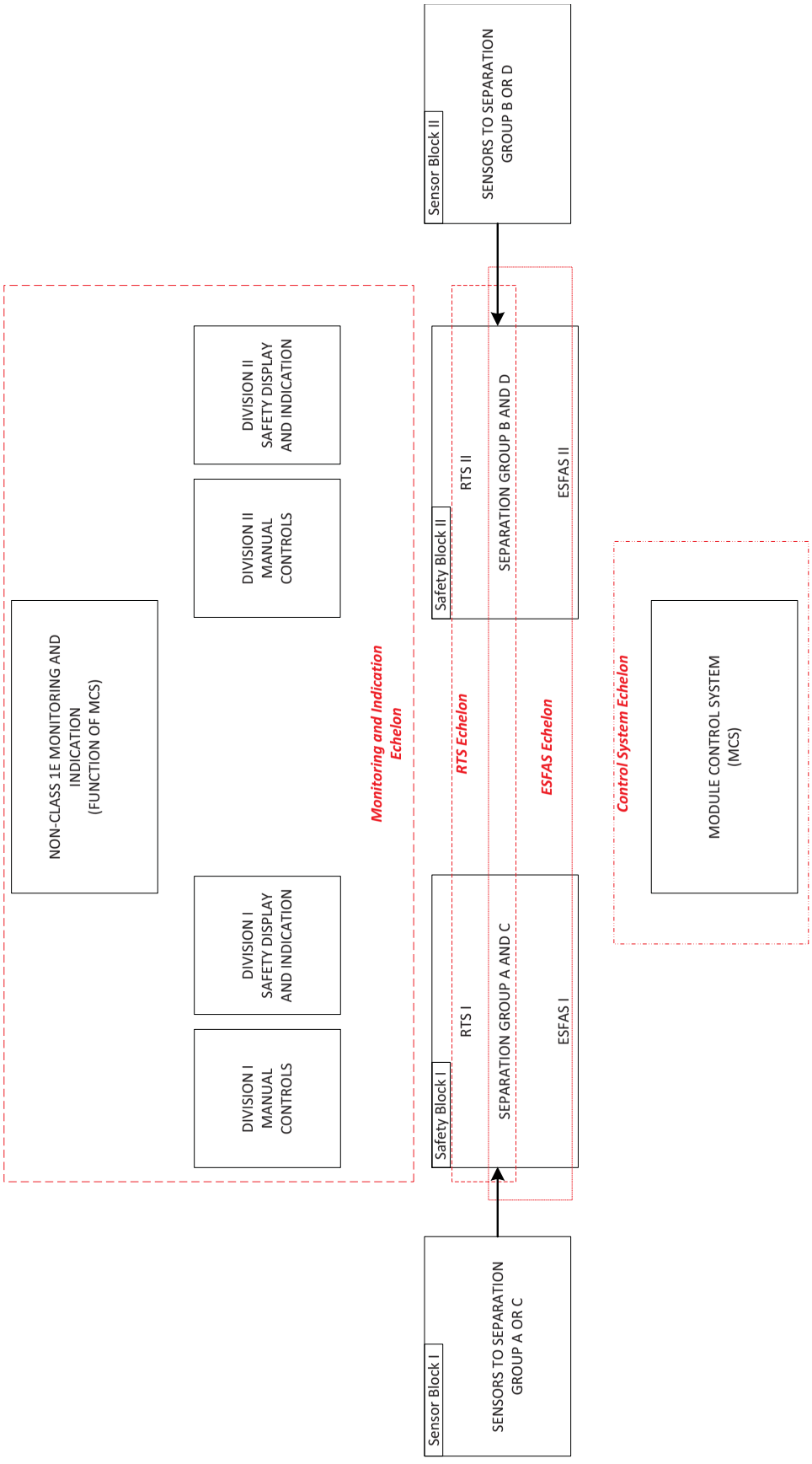


Figure 7.1-6: Four Echelons of Defense within Chosen Blocks

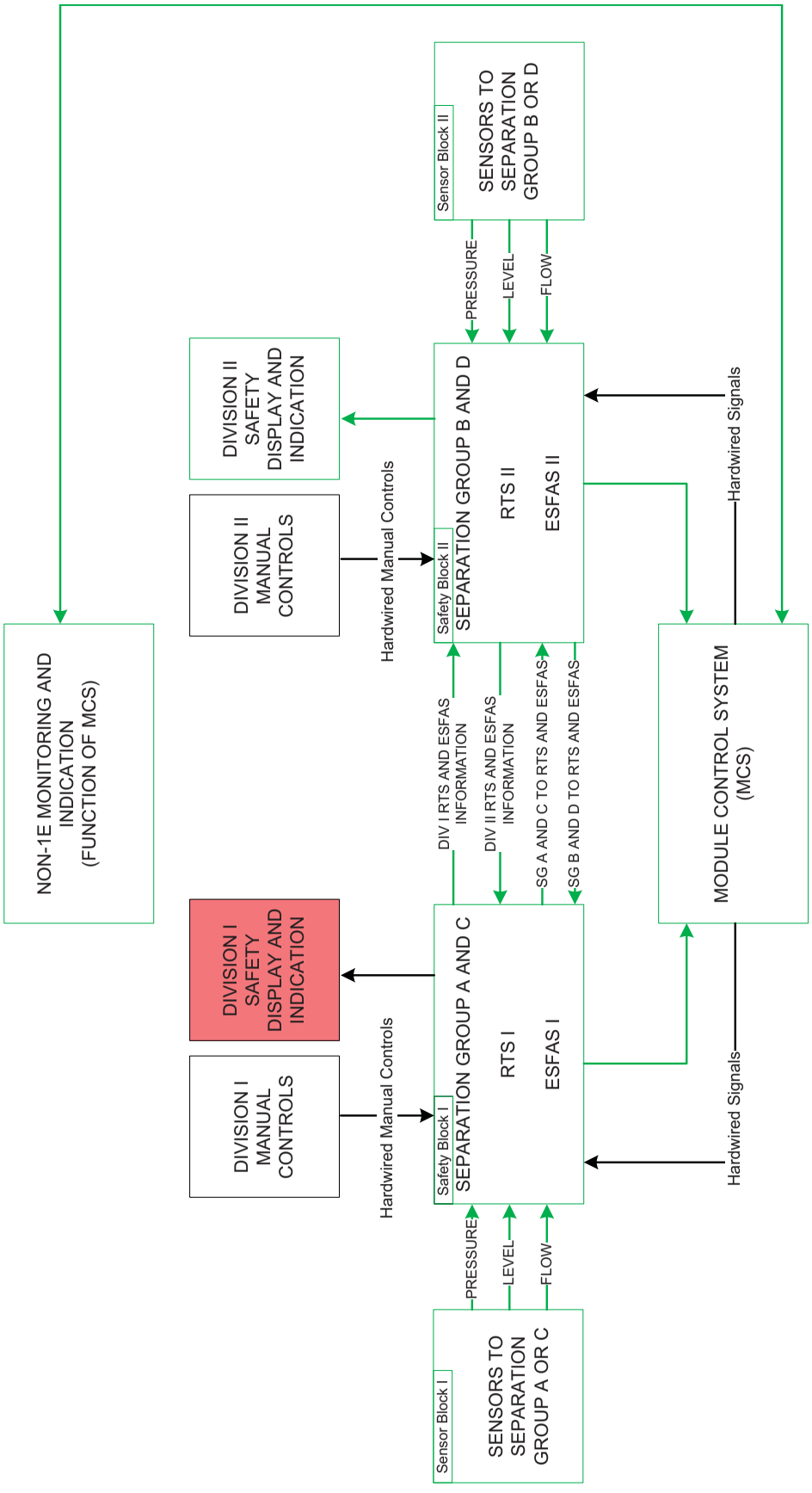


Figure 7.1-7: Common Cause Failure of Division I Safety Display and Indication System

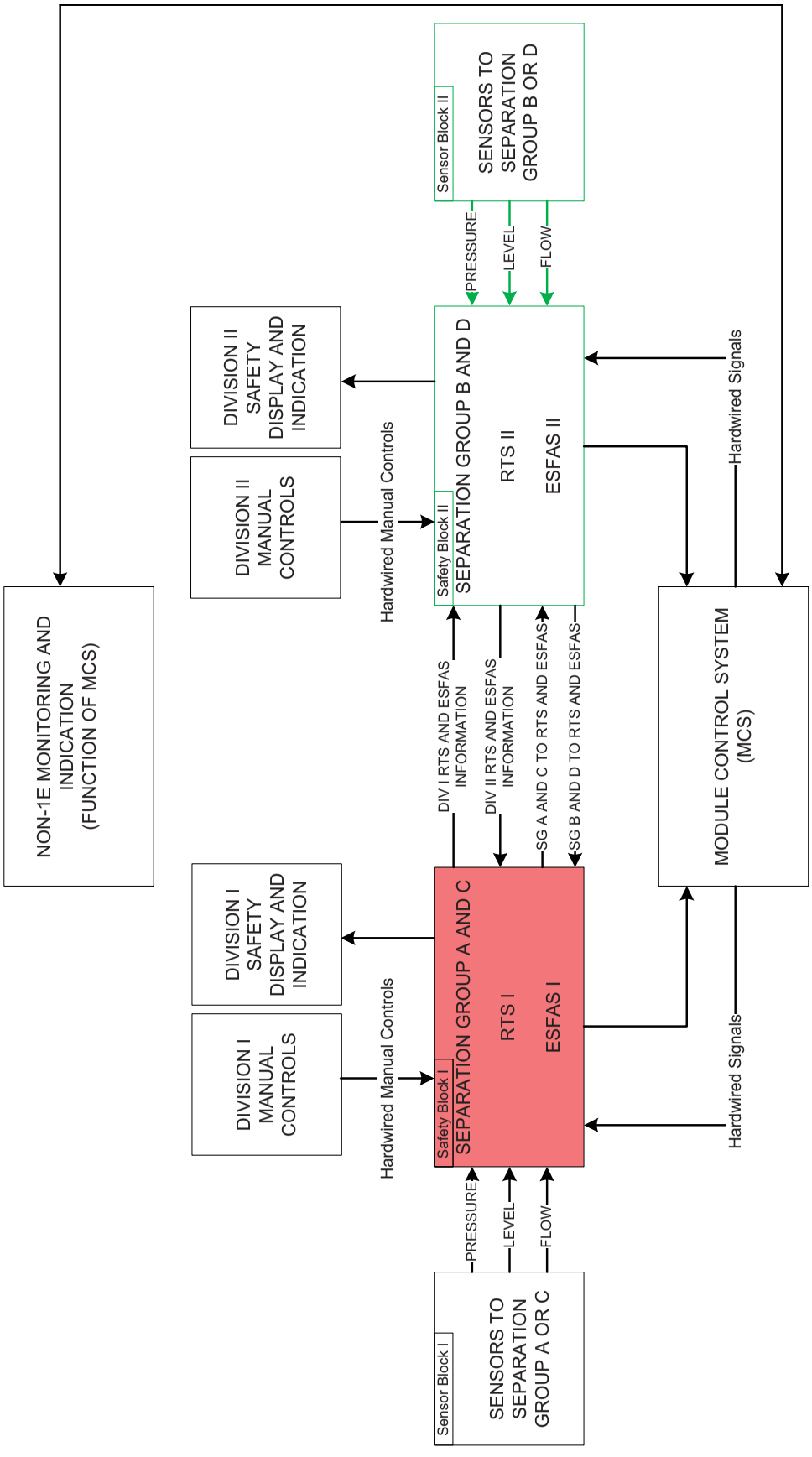


Figure 7.1-8: Common Cause Failure of Safety Block I with Correct Indication

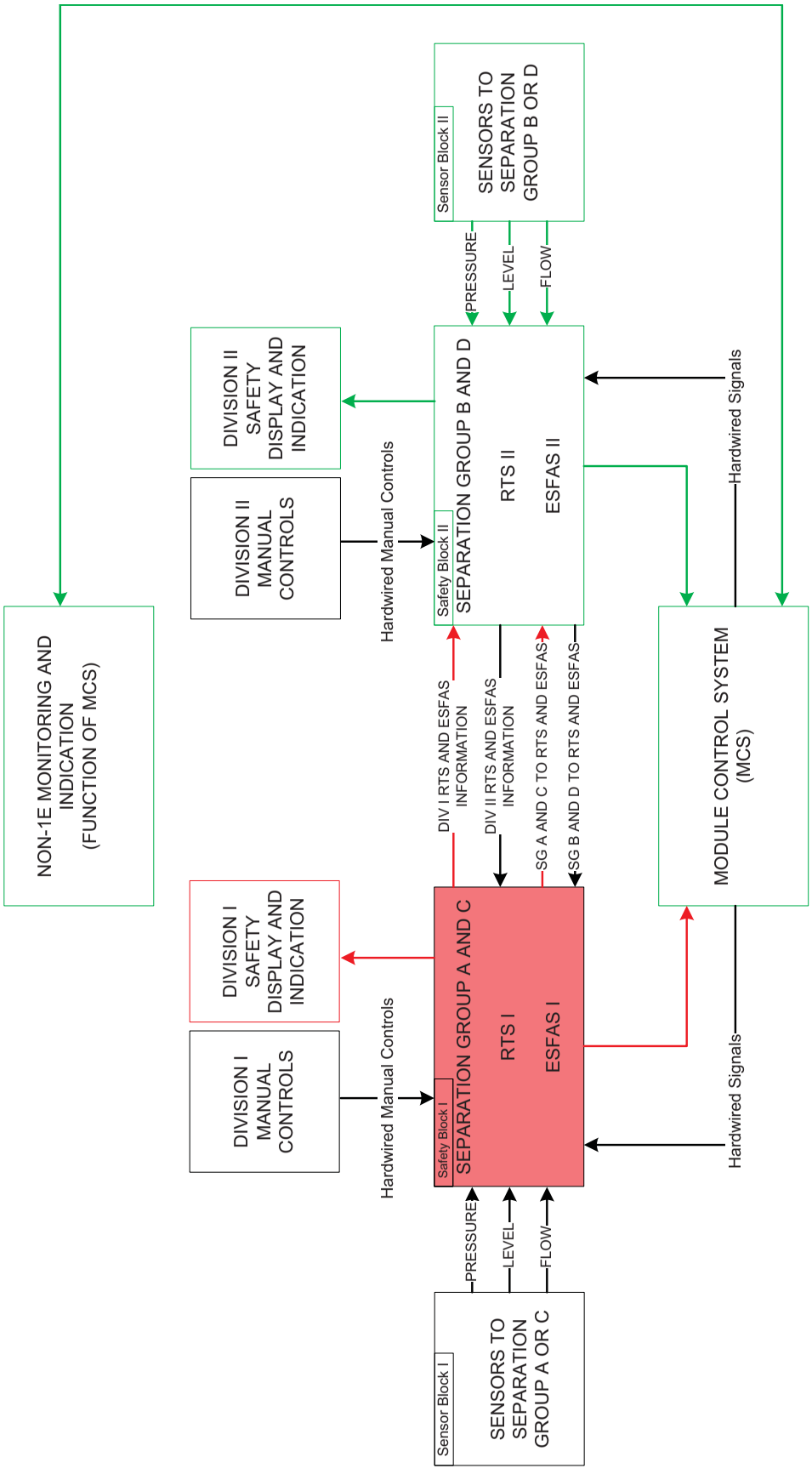


Figure 7.1-9: Common Cause Failure of Safety Block I with False Indication

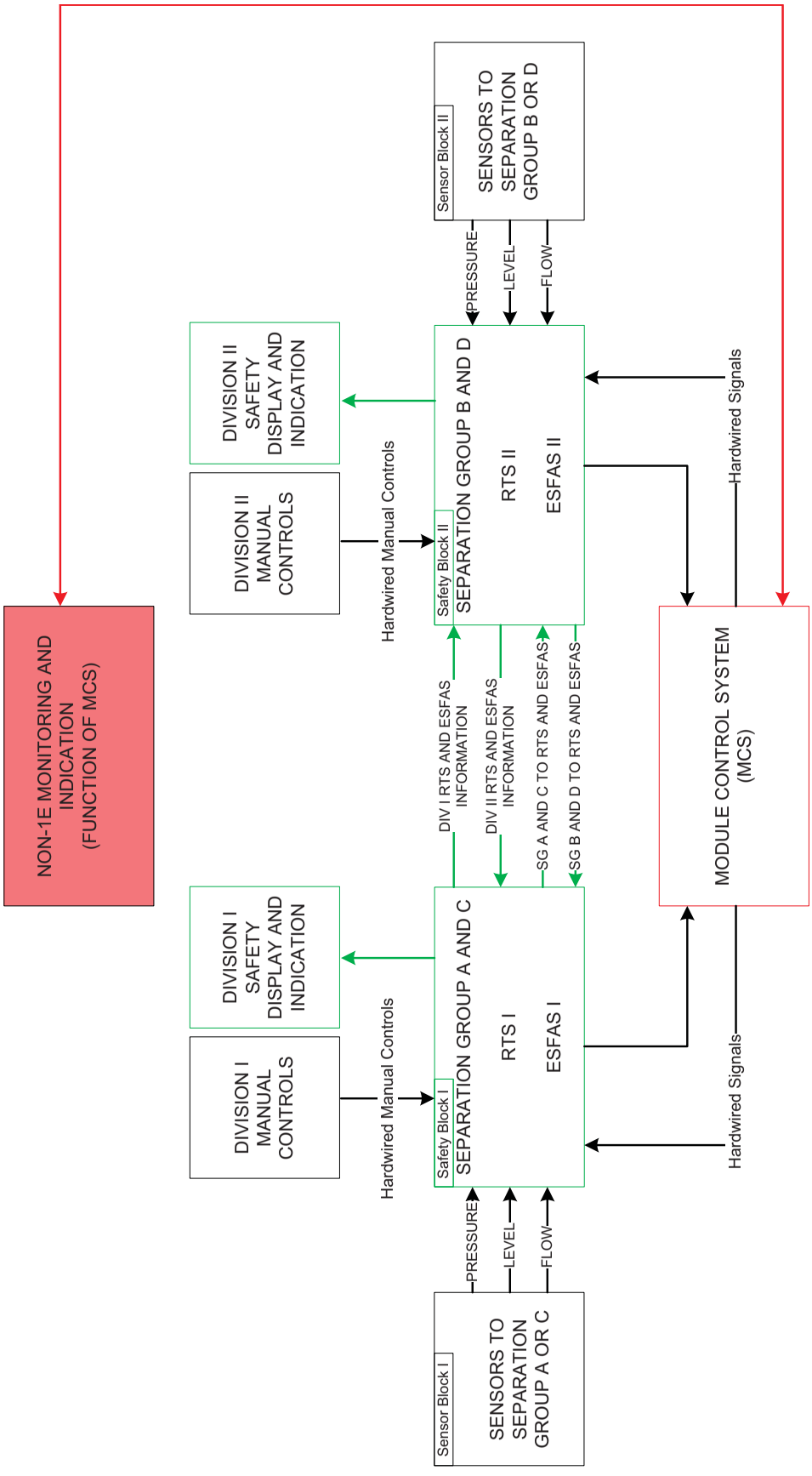


Figure 7.1-10: Common Cause Failure of Non-Class 1E Monitoring and Indication

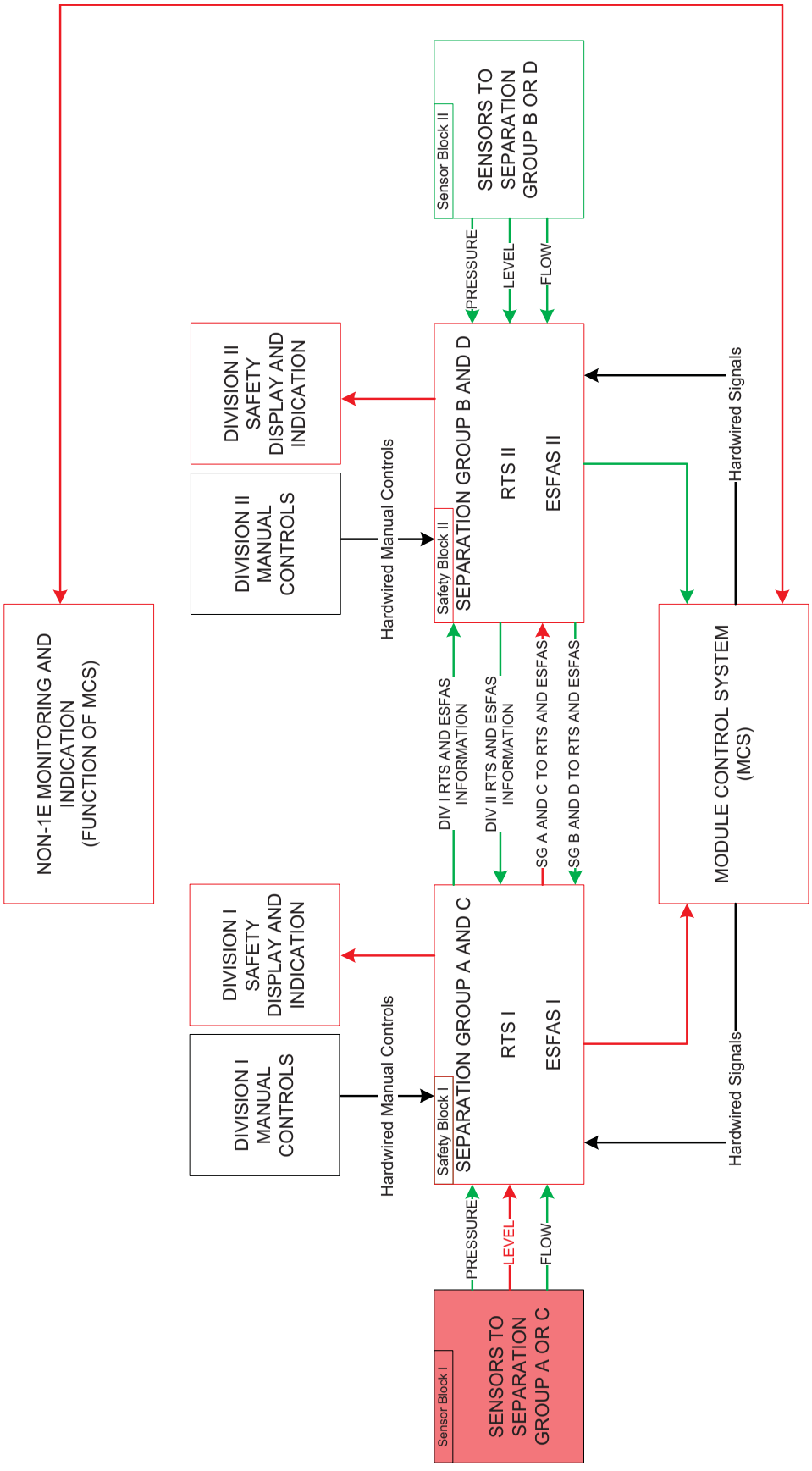


Figure 7.1-11: Digital-Based Common Cause Failure of Level Function Type in Sensor Block I

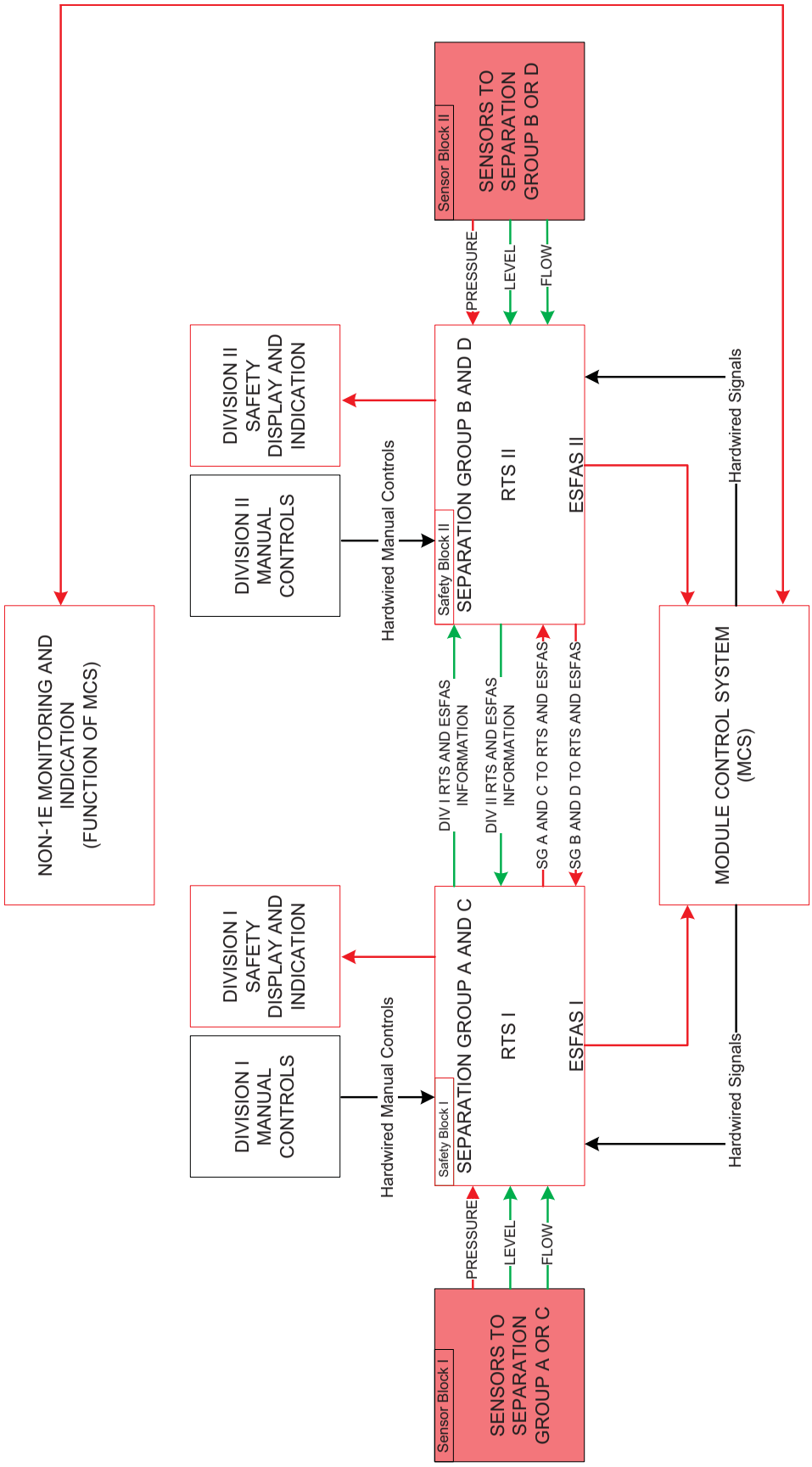


Figure 7.1-12: Digital-Based Common Cause Failure of Pressure Measuring System Function Type in Sensor Block I and II

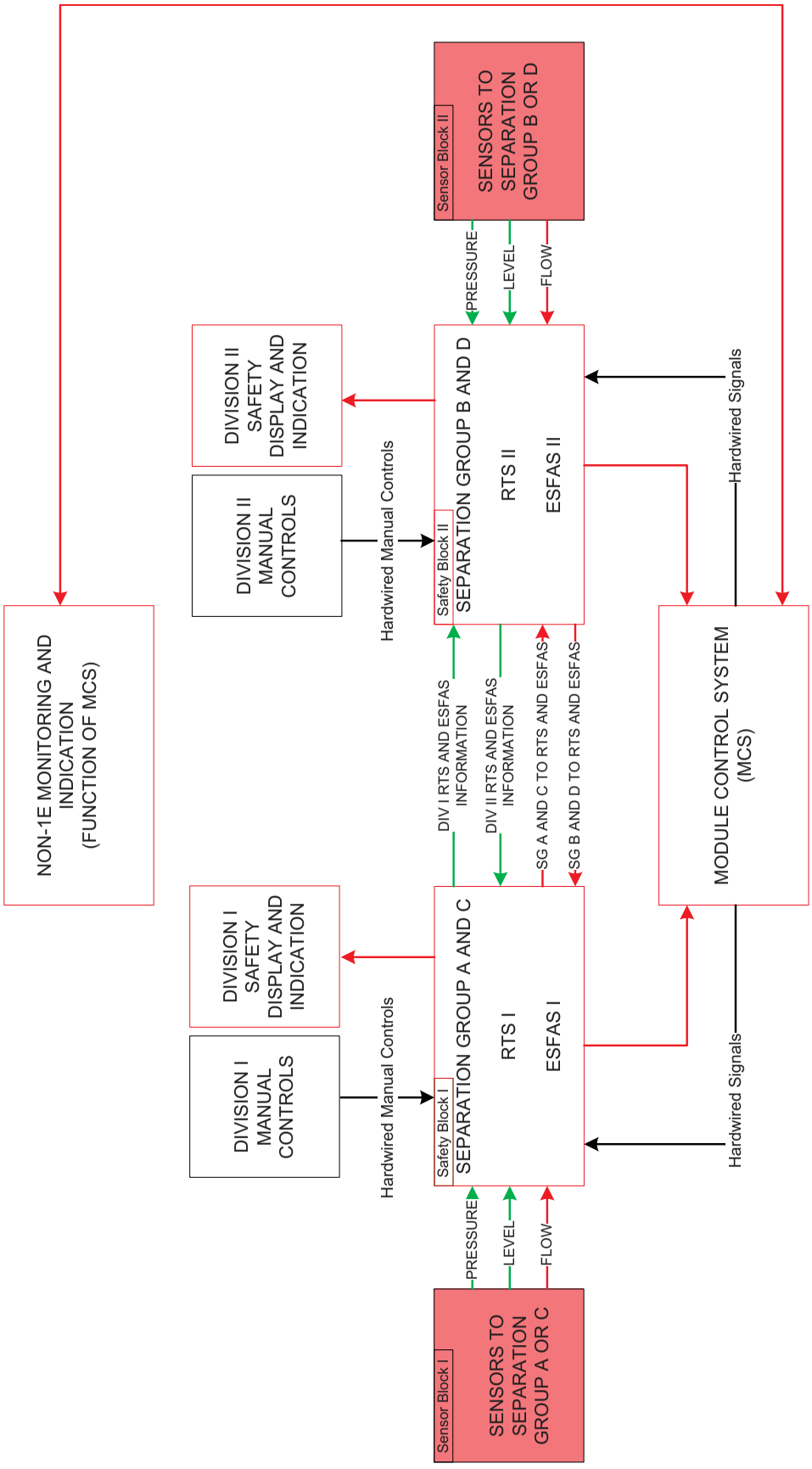


Figure 7.1-13: Digital-Based Common Cause Failure of Flow Function Type in Sensor Block I and II

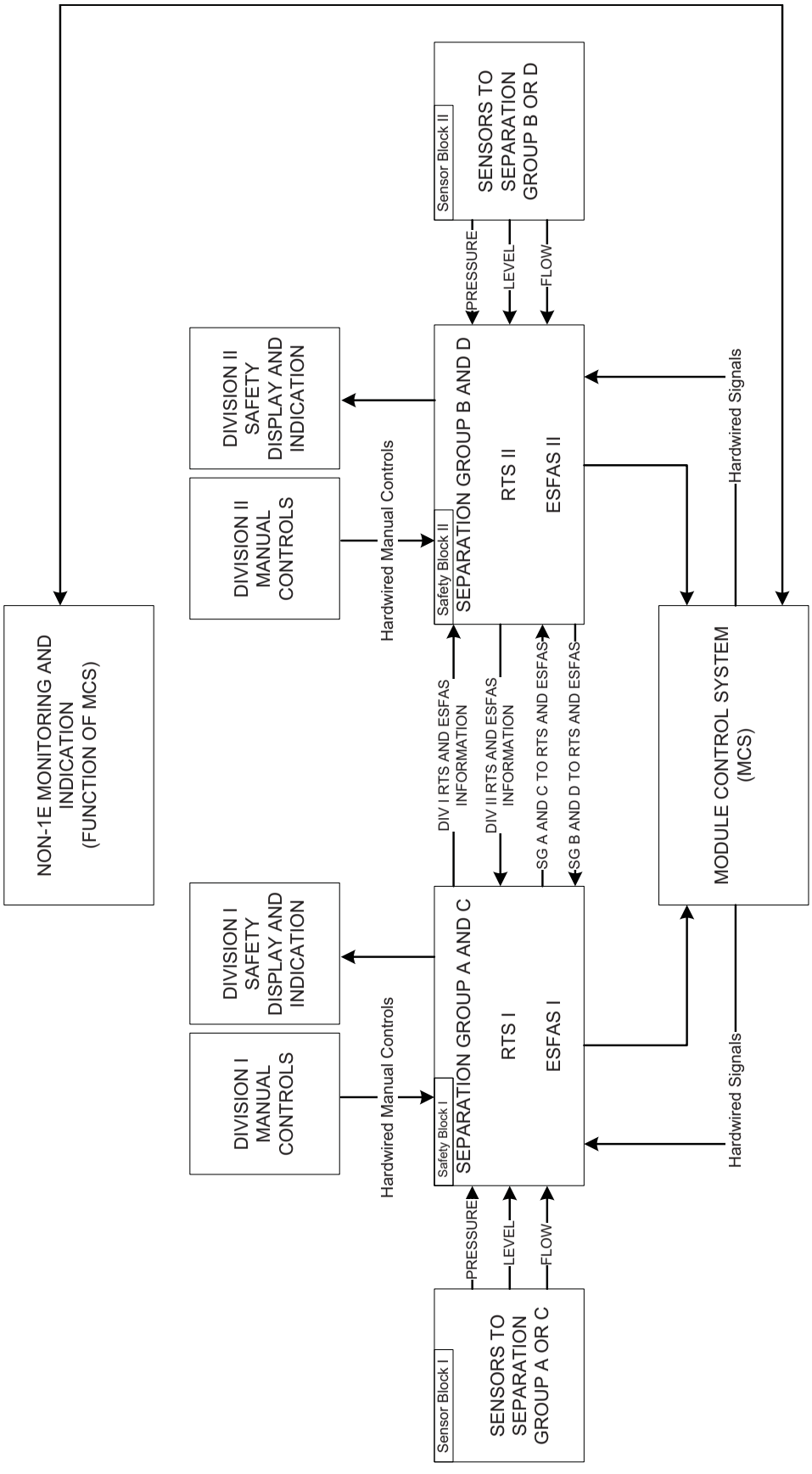


Figure 7.1-14: Direction of Information and Signals between Analysis Blocks

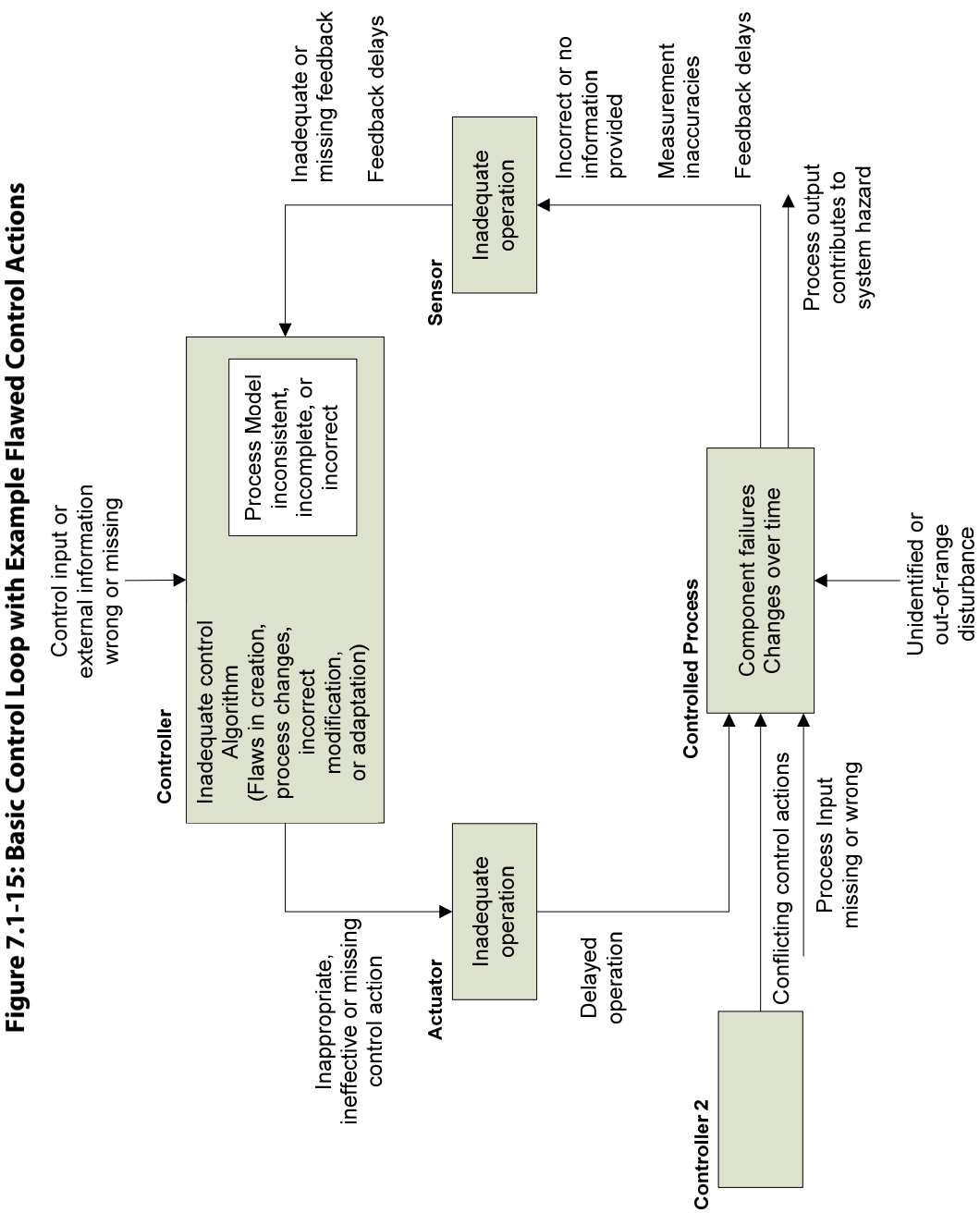


Figure 7.1-15: Basic Control Loop with Example Flawed Control Actions

Figure 7.1-16: Example Module Protection System High Level Control Structure

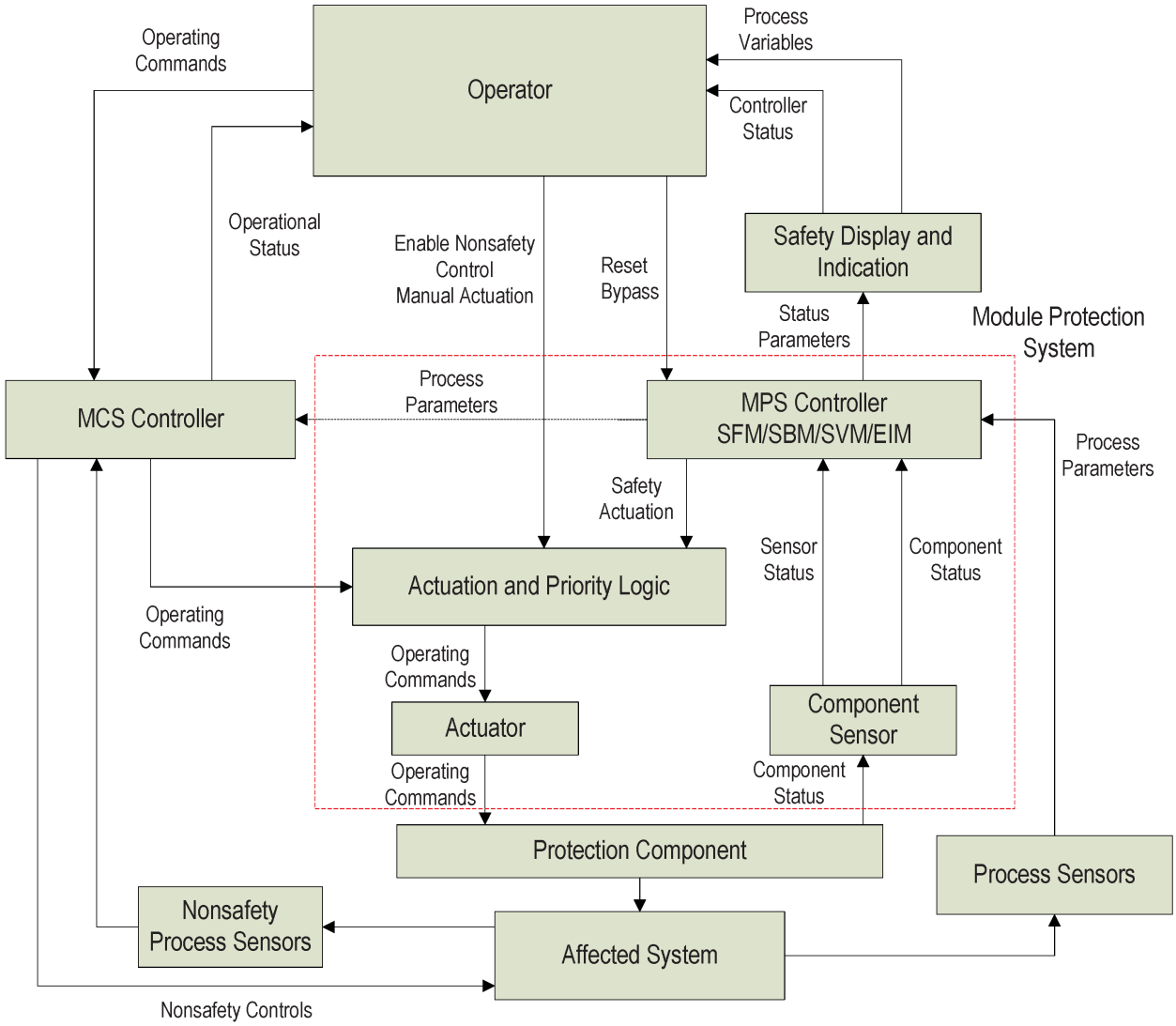


Figure 7.1-17: Example Neutron Monitoring System High Level Control Structure

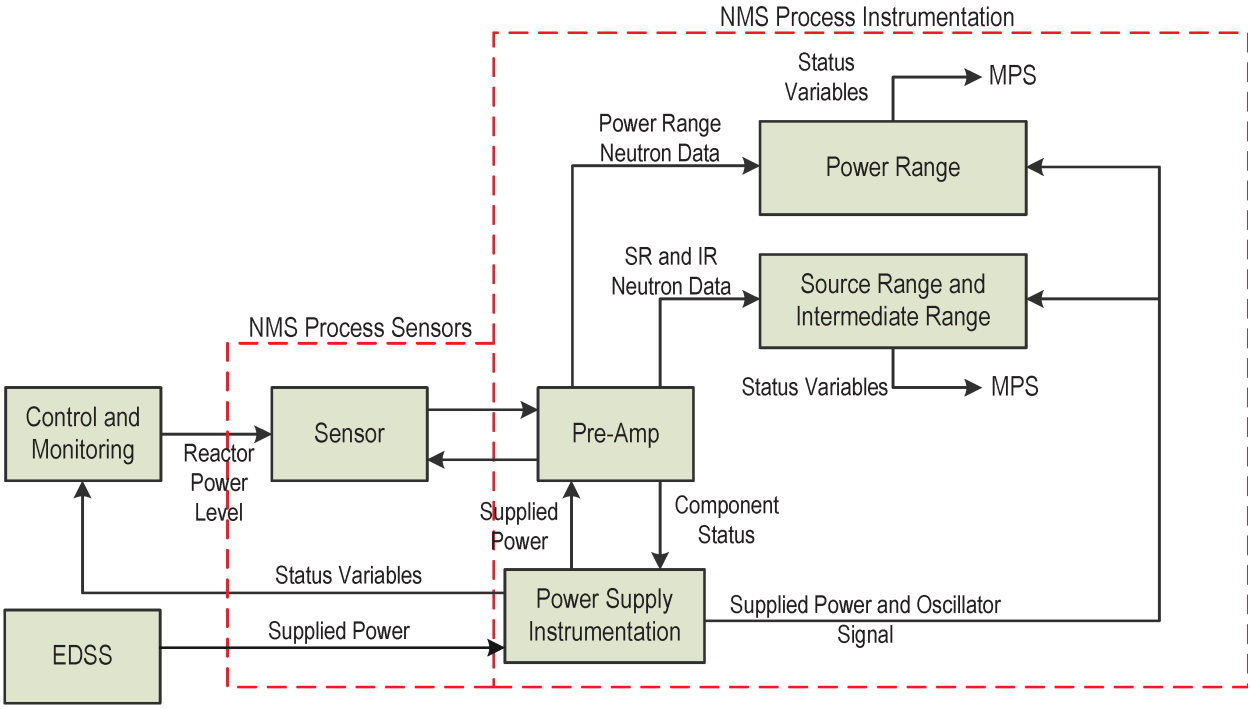


Figure 7.1-18: Safety Function Module Low-Level Logic Structure

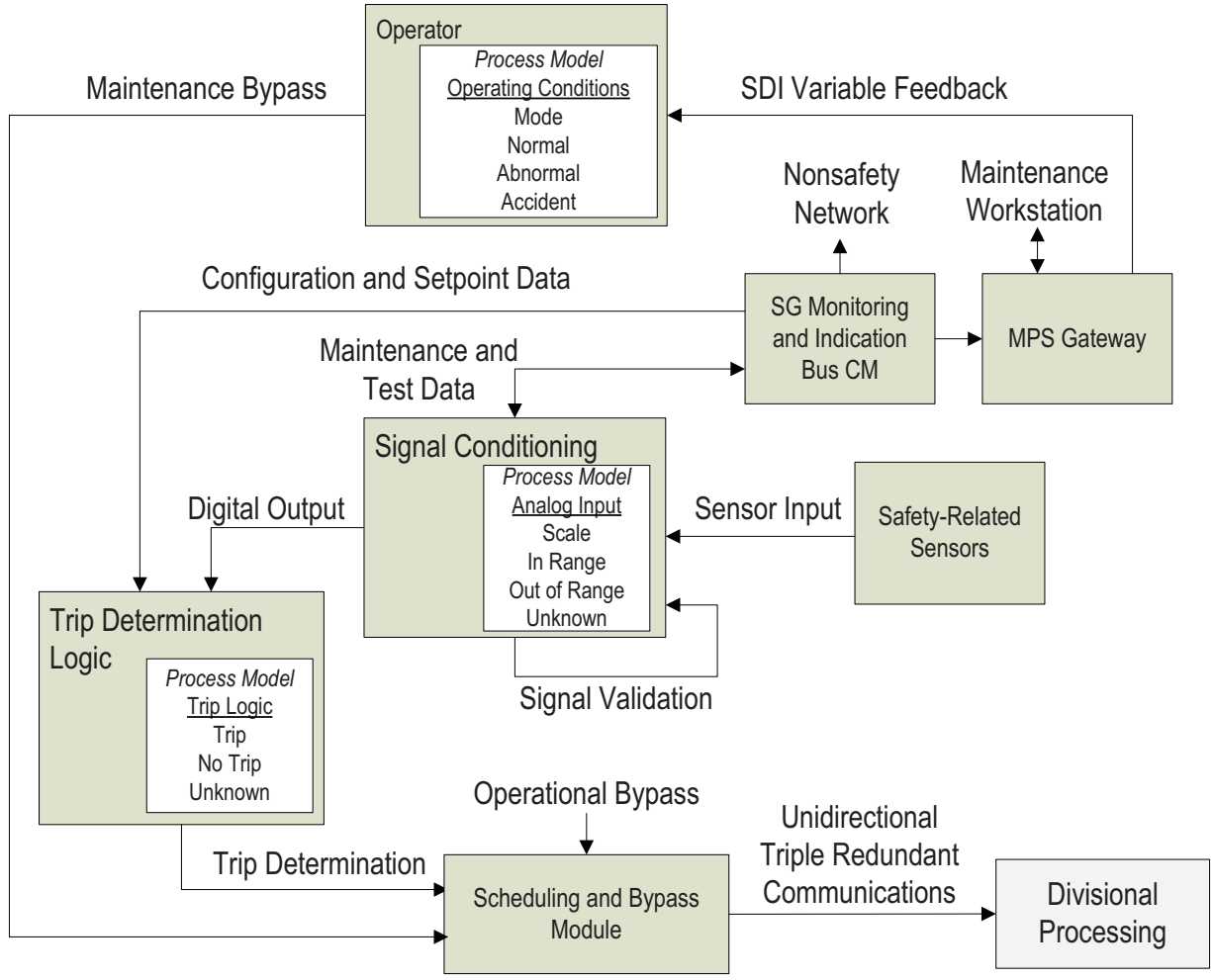
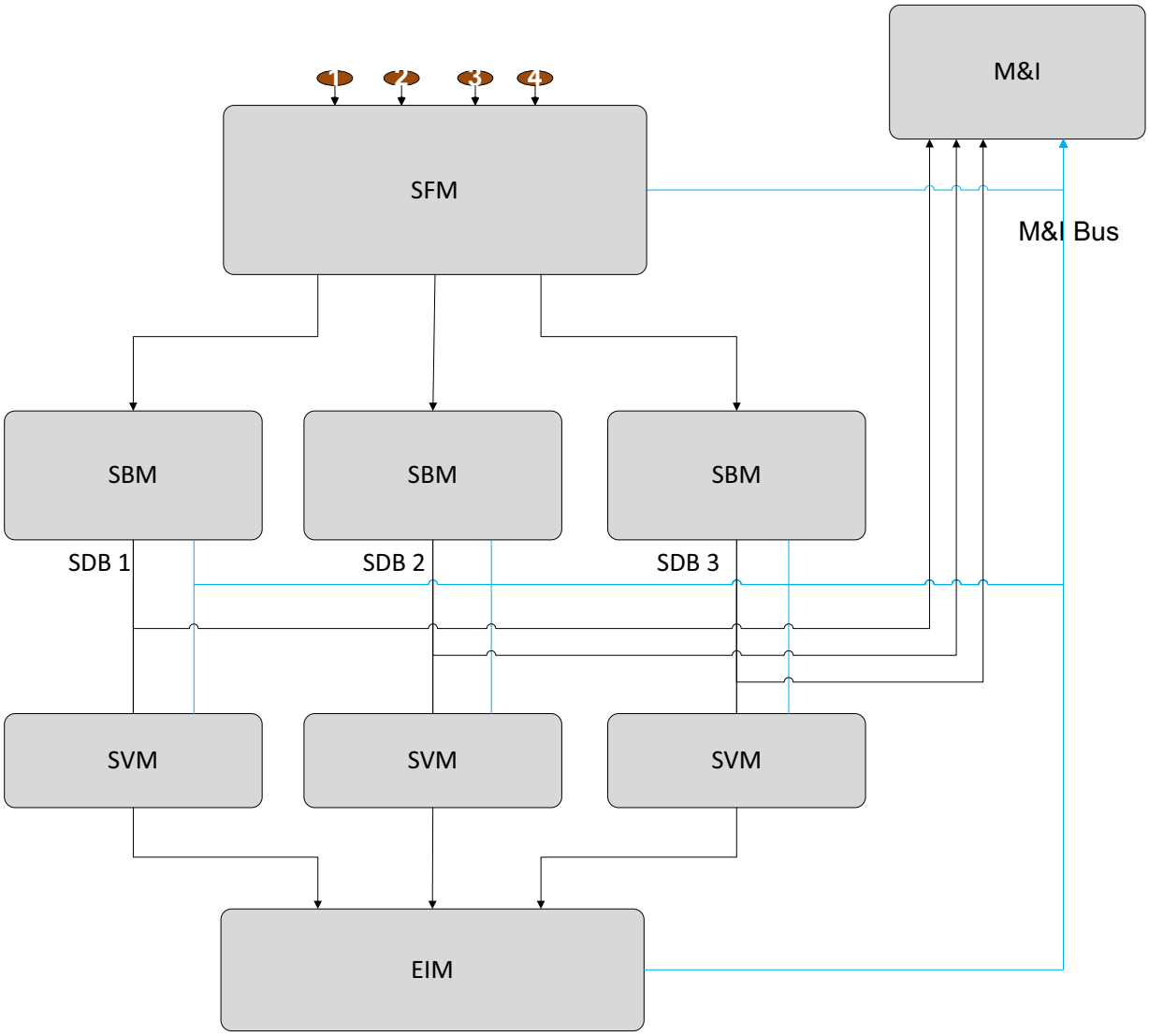


Figure 7.1-19: Basic Module Protection System Configuration



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 7.2-11), 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 7.2-13).

Specific features that are incorporated in the NuScale 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 between sense and command features and other systems
- multi-unit 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 risk-significant I&C systems is described in NuScale topical report, "Quality Assurance Program Description for the NuScale Power Reactor," NP-TR-1010-859-NP, Revision 4 (Reference 7.2-30). The QAP complies with NQA-1-2008 (Reference 7.2-2) and NQA-1a-2009 Addenda (Reference 7.2-3), Requirement 3, Sections 100 through 900 and the standards for computer software in NQA-1-2008 and NQA-1a-2009 Addenda, Part II, Subpart 2.7.

The information in this section satisfies the application specific information requirements in topical report NuScale Power, LLC, TR-1015-18653-P-A, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.2-25) listed in Table 7.0-2 for

application specific action item (ASAI) numbers 4, 16, 47, 49, 50, and 51. The following regulatory guidance applies to the QAP for digital I&C systems:

- Regulatory Guide 1.28, Revision 4, endorses ASME NQA-1-2008 and the ASME NQA-1a-2009 Addenda, "Addenda to ASME NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications," and states that these standards provide an adequate basis for complying with the requirements of 10 CFR Part 50 Appendix B.

Because the approved NuScale QAP is based on ASME NQA-1-2008 and the ASME NQA-1a-2009 Addenda, it satisfies the regulatory requirements in RG 1.28.

The overall QAP is supplemented by four NuScale process plans:

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

The NuScale 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 NuScale Quality Management Plan and the NuScale 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 NuScale Digital I&C Software Quality Assurance Plan and the NuScale 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 NuScale 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 NuScale 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, Revision 3. The plan follows the guidelines of IEEE Std 730-2002, "IEEE Standard for Software Quality Assurance Plans" (Reference 7.2-14).

The NuScale Digital I&C Software Quality Assurance Plan applies to digital I&C software classified as software integrity levels (SILs) 4 and 3 in accordance with the NuScale Software Classification Procedure. The NuScale Digital I&C Software Quality Assurance Plan may be applied to digital I&C software classified at less than SIL 3, by applying the approach defined in the Digital I&C Software Verification and Validation Plan and Software Management Plan which ensures nonsafety-related software or logic meets applicable quality requirements.

Software development and QA controls are applied to the following safety-related and nonsafety-related 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)
- general I&C structures, systems, and components that contain embedded digital devices

The NuScale Digital I&C Software Quality Assurance Program applies equally in the application of different FPGA technologies within the MPS; the program activities do not

differentiate between different FPGA technologies. The NuScale classification process allocates systems to one of the four SILs. Safety-related systems are classified as SIL4. The development process implementing procedures define the requirements applied to the various SIL levels.

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 device logic for physical security protection, as delineated within 10 CFR 73.55

The following regulations apply to the QAP for digital I&C safety systems.

- 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). Section 5.3 requires that components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates. It also requires that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QAP.
- 10 CFR 50.54(jj) and 50.55(i) require, in part, that systems and components subject to the codes and standards in 10 CFR 50.55a be designed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. 10 CFR 50.54(jj) and 10 CFR 50.55(i) do not apply to design certification applicants, and 10 CFR 50.55a(a)(1) has been modified to remove quality requirements.
- 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 1, requires, in part, that systems and components be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
- Appendix B to 10 CFR Part 50 establishes QA requirements for the design, manufacture, construction, and operation of safety-related structures, systems, and components.
- Regulatory Guide 1.152, Revision 3 endorses the quality guidance for digital I&C safety systems in IEEE Std 7-4.3.2-2003 (Section 5.3) as an acceptable method for satisfying the NRC regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants. RG 1.152 does not endorse Annexes B - F of IEEE Std 7-4.3.2-2003.
- IEEE Std 7-4.3.2-2003 Section 5.3 specifies additional requirements that are necessary to meet the IEEE Std 603-1991 quality requirements for digital I&C for the following topics:
  - software development (Section 5.3.1)
  - use of software tools (Section 5.3.2)
  - verification and validation (Sections 5.3.3 and 5.3.4)
  - configuration management (Section 5.3.5)
  - risk management (Section 5.3.6)
  - qualification of existing commercial computers (Section 5.4.2)

The life cycle process defined in the NuScale 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 NuScale QAP and NuScale 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 NuScale Digital I&C Software Quality Assurance Plan requires that the NuScale Digital I&C Software Management Plan address quality metrics, as required by IEEE Std 7-4.3.2-2003 Section 5.3.1.1; however, NuScale is maintaining flexibility for the definition of specific metrics until a vendor is selected to implement the digital I&C designs. This approach enables NuScale to adjust the metrics based on the technology and vendor selections. It also allows for adoption of established metrics used by the vendor.

The NuScale Digital I&C Software Quality Assurance Plan incorporates tool requirements from IEEE Std 7-4.3.2-2003. The NuScale 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 NuScale Digital I&C Software Verification and Validation Plan is based on IEEE Std 1012-2004 (Reference 7.2-19), as endorsed by RG 1.168 Revision 2. The V&V program for safety-related software (i.e., SIL 4) is implemented by a V&V team that is independent from the design development team. The NuScale Digital I&C Software Verification and Validation Plan conforms to IEEE Std 1012-2004 with adaptations, as allowed by the standard, and exceptions:

Adaptations

- V&V activities are adapted to NuScale life cycle and Complex Logic Device technology (i.e., field programmable gate arrays (FPGA)). In the application of different FPGA technologies within the MPS, the V&V activities are the same; they do not differentiate between different FPGA technologies.
- V&V tasks are adapted to Complex Logic Device technology.

Exceptions

- Documentation requirement details in Sections 6 and 7 of the standard that conflict with NuScale standard documentation practices or QAP requirements or are inconsistent with the platform neutral strategy (where flexibility is retained to adopt established vendor documentation formats).

The NuScale Digital I&C Software Verification and Validation Plan, with the noted exceptions, satisfies the requirements of IEEE Std 7-4.3.2-2003 Sections 5.3.3 and 5.3.4.

The NuScale Digital I&C Software Configuration Management Plan conforms to IEEE Std 828-2005 "IEEE Standard for Software Configuration Management Plans" (Reference 7.2-15), as endorsed by RG 1.169 Revision 1. The NuScale 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 NuScale process plans (the NuScale Digital I&C Software Development Plan, the Digital I&C Software Management Plan, and the NuScale 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 NuScale Digital I&C Software Development Plan and the NuScale 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 NuScale Digital I&C Quality Assurance Plan provides a framework for commercial grade dedication. The NuScale 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 7.2-5) for the commercial grade dedication of digital I&C equipment. RG 1.152 notes 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 NuScale Digital Safety System SDOE Plan is a NuScale process plan that defines security controls for the phases of the NuScale 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, Revision 3.

NuScale has taken the following general approach to using the software-based RGs and associated IEEE standards:

- adapted 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 between different FPGA technologies.
- capture 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
- specify 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

1) Regulatory Guide 1.173, Revision 1 endorses IEEE Std 1074-2006 "IEEE Standard for Developing a Software Project Life Cycle Process" (Reference 7.2-22) The NuScale digital I&C safety system development life cycle is implemented in the following NuScale process plans:

    - NuScale Digital Safety Systems Project Plan
    - NuScale Digital I&C Software Management Plan

- NuScale Digital I&C Software Development Plan
- NuScale Digital I&C Software Quality Assurance Plan
- NuScale Digital I&C Software Verification and Validation Plan
- NuScale Digital I&C Software Master Test Plan
- NuScale Digital I&C Software Requirements Management Plan
- NuScale Digital I&C Software Configuration Management Plan
- NuScale Digital I&C Software Integration Plan
- NuScale Digital I&C Software Safety Plan
- NuScale Digital I&C Software Installation Plan
- NuScale 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 NuScale 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, Revision 1.

2) Regulatory Guide 1.172, Revision 1 endorses IEEE Std 830-1998, "IEEE Recommended Practice for Software Requirements Specifications" (Reference 7.2-17) as an acceptable approach for the preparation of software requirements specifications. The NuScale 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, Revision 1 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 7.2-16) 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.

3) Regulatory Guide 1.171, Revision 1 endorses IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing" (Reference 7.2-18) as an acceptable approach for performing unit testing of safety system software. The NuScale 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, Revision 1, and IEEE Std 1008-1987 with the following exceptions:

   - adjustment of testing methods to reflect the use of Complex Logic Device-related testing tools
   - adjustment of specification documents to reflect the use of Complex Logic Device test tools (i.e., to produce test documents)
   - exceptions to IEEE Std 829-2008 for software test documentation, as discussed below

4) Regulatory Guide 1.170, Revision 1 endorses IEEE Std 829-2008 as an acceptable approach for safety system software test documentation. The NuScale Digital I&C Software Master Test Plan specifies the requirements for software test documentation, consistent with the technical guidance in RG 1.170, Revision 1, and IEEE Std 829-2008 with the exception of documentation requirement details of the standard that conflict with NuScale standard engineering documentation practices or QAP requirements.

5) Regulatory Guide 1.169, Revision 1 endorses IEEE Std 828-2005 as an acceptable approach for safety system software configuration management. The NuScale Digital I&C Software Configuration Management Plan specifies the requirements for software configuration management, consistent with the guidance in RG 1.169, Revision 1 and IEEE Std 828-2005. The NuScale Digital I&C Software Configuration Management Plan conforms to complies with the requirements in IEEE Std 828-2005, as endorsed by RG 1.169, Revision 1.

6) Regulatory Guide 1.168, Revision 2 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 7.2-20) as an acceptable approach for carrying out software reviews, inspections, walkthroughs, and audits typically used in association with software QA activities. The NuScale Software Verification and Validation Plan is based on IEEE Std 1012-2004, as endorsed by RG 1.168 Revision 2. The V&V program for safety-related software (i.e., SIL 4) is implemented by a V&V team that is independent from the design development team. The NuScale Digital I&C Software Verification and Validation Plan conforms to IEEE Std 1012-2004 with adaptations and exceptions as follows:

   Adaptations

   - V&V activities 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 between different FPGA technologies.
   - V&V tasks adapted to Complex Logic Device technology

   Exceptions

   - Consistent with the guidance in RG 1.170, Revision 1, exceptions are taken for documentation requirement details in Sections 6 and 7 of IEEE Std 1012-2004 that conflict with NuScale standard documentation practices or are inconsistent with the platform neutral strategy (where flexibility is retained to adopt established vendor documentation formats). In all cases, the approved NuScale QAP (see Section 17.5) takes precedence.

   NuScale performs software reviews, inspections, walkthroughs, and audits as part of software design, V&V, and quality assurance activities. These activities are performed and documented in accordance with methods defined in NuScale procedures and QA program requirements. NuScale takes exception to the methods and documentation requirement specified in IEEE Std 1028-2008, since these details conflict with NuScale standard documentation practices or QA program requirements or are inconsistent with the platform neutral strategy (where flexibility is retained to adopt established

vendor methods and documentation formats for these activities). NuScale does not conform to the requirements in IEEE Std 1028-2008.

7.2.1.1 I&C Safety System Development Process

The I&C safety system development process is structured to follow a life cycle that includes a top-down iterative requirement and specification development, design implementation, and a bottoms-up V&V effort at each level of integration. The life cycle allows iteration of requirements, design, and implementation based on the nature and evaluations of the safety critical aspects of the system design. The system development approach allows prototyping activities and in-process QA efforts to be executed integral to the system and software development stages.

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 validation and verification
- configuration management

The NuScale 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 verification and validation methods, activities, and oversight for development of the I&C safety systems, which is both 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 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 requirement specification (ERS) development.

Basic design activities are performed in accordance with the NuScale 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 final 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 NuScale 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 NuScale Digital I&C Software Quality Assurance Plan, NuScale Digital I&C Software Verification and Validation Plan, NuScale Digital Safety System Safety Plan, NuScale Digital Safety System SDOE Plan, and preliminary hazard analyses are final products of this phase.

The NuScale 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 NuScale 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. This includes guidance for the generation of software V&V plans specific to individual software products.

The NuScale Digital Safety System 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 NuScale Digital Safety System Safety 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 NuScale Digital Safety System 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 any other logic that could adversely impact the integrity or reliability of the digital safety system. The NuScale Digital Safety System 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 should facilitate bi-directional 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 NuScale 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 per the NuScale Digital Safety Systems Safety Plan. The system hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale Digital I&C Software Quality Assurance Plan with the results documented in the system protoype 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 ERSs are 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 hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale Digital I&C Software Quality Assurance Plan with the results documented in the equipment requirements specification phase.

The NuScale Digital I&C Software Integration Plan, NuScale Digital I&C Software Configuration Management Plan, NuScale Digital l&C Software Master Test Plan and NuScale Software Installation Plan are also products of this phase.

The NuScale Digital I&C Software Integration Plan is a NuScale process plan that documents the integration and testing of all software items, hardware, manual processes, and other system interfaces that constitute the I&C system, consistent with the architectural design.

The NuScale Digital I&C Software Configuration Management Plan is a NuScale process plan that documents the process for providing the identification and configuration baselines for system and software items.

The NuScale Digital l&C Software Master Test Plan is a NuScale process plan that provides guidance for test planning and management for system and software testing for digital safety systems.

The NuScale Digital l&C Software Integration and Installation Plans together are the NuScale process plans that 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 NuScale Quality Assurance Plan.

Detailed system design includes hardware development and an iterative software development process which are described in the NuScale Digital I&C Software Development Plan.

The life cycle phase entry and exit criteria are defined in the NuScale 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 hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 NuScale Digital I&C Software Development Plan, NuScale Digital I&C Software Verification and Validation Plan, NuScale Digital I&C Software Master Test Plan, and NuScale Digital I&C Software Training Plan. The system hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 vendor and by NuScale
- determining the integrity level of the software to be developed
- establishing the exact requirements in the NuScale 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, etc.)
- 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 NuScale Digital I&C Software Verification and Validation Plan defines the activities, expectations, processes, and base level of rigor for V&V which is to be performed for SIL 1 through 4 software systems.

The NuScale 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 NuScale 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 requirement specification (HRS). The system hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 Requirement Specification with the Interface Requirements Specification.

The independent V&V team develops the Acceptance and System Test Plans for SIL 3 and 4 software systems during this phase.

The Digital I&C Software Requirement Specification is analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management according to the NuScale Digital I&C Software Configuration Management Plan. The Digital I&C Software Requirement Specification is also used as input to the ongoing I&C system safety analyses per the NuScale Digital I&C Software Safety Plan. Additional outputs of this phase include a SDOE assessment, criticality assessment update, RTM update, interface requirements specification, and a software safety analysis. The system hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 HRS in accordance with the Hardware Development Plan. The system hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 NuScale Digital I&C Software Quality Assurance Plan. The Software Design Description is developed based on the Software Requirement 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 (IDDs), and the acceptance, system, integration, and component test design documents. The Software Design Description and IDDs are analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management according to the NuScale Digital I&C Software Configuration Management Plan. The Software Design Description is also used as input to the ongoing I&C system safety analyses per the NuScale Digital I&C Software Safety Plan. Additional outputs of this phase include a SDOE assessment, criticality assessment update, RTM update, and a software safety analysis. The system hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 NuScale Digital I&C Software Master Test Plan.

7.2.1.1.2.3 System Implementation Phase

Software Implementation

The NuScale 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 requirements into hardware description language. The functions described in the Software Design Description are developed in the software development environment utilizing applicable coding standards (e.g., Hardware Description Language Specifications and Conventions Guideline). Analysis is performed on the software to identify potential hazards in accordance with the NuScale Digital I&C Software Safety Plan.

This phase includes the generation, testing, and assessment of the developed software including development of component, integration, system, factory and site acceptance 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 NuScale Digital I&C Software V&V Plan, and the NuScale Digital I&C Software Master Test Plan.

Additional outputs of this phase include a SDOE assessment, criticality assessment update, RTM update, and a software safety analysis update. The system hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale Digital I&C Software Quality Assurance Plan with the results documented in the software implementation phase.

Software Configuration

During the software configuration phase, the software is implemented on system hardware and tested in accordance with the NuScale Digital I&C Software Verification and Validation Plan and the Software Master Test Plan. The system hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 software integrity levels 3 and 4 software systems.

During this phase, the software is integrated with any software from previous iterations and logic integration testing is performed in accordance with the test procedures according to the NuScale Digital I&C Master Test Plan. 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 hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 NuScale 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 hazards analysis is reviewed when any 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 hazards analysis or if new hazards are identified according to the NuScale 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 NuScale 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 NuScale 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 between 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 concepts phase with the Preliminary Hazards 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 pursuant to the hazards analysis V&V tasks as specified in the NuScale Digital I&C Software Verification and Validation Plan. Anomalies identified during the V&V process are documented in a V&V anomaly report and reported to the software development team. All anomalies must be satisfactorily resolved prior to issuing a V&V task report pursant to the NuScale Digital I&C Verification and Validation Plan.

The Software Safety Analysis Report constitutes a configuration item and is placed under configuration management, for which change control is documented pursuant to the NuScale Digital I&C Software Configuration Management Plan.

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 (see 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 documentation and system design documentation and/or Digital I&C System Requirements Specification 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 3 and 4, an independent V&V team performs a V&V of the digital I&C System Requirements Specification in accordance with the NuScale Digital I&C Software Verification and Validation Plan. For SIL 1 and 2, an independent verifier within the engineering 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. All anomalies must be satisfactorily resolved prior to issuing a V&V task report pursant to the NuScale Digital I&C Verification and Validation Plan.

The digital I&C System Requirements Specification is baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan.

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 per the NuScale Digital Safety System Safety Plan.

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. Bi-directional traceability is established between the ERS and the system design documentation. The ERS is used as input to the ongoing system safety analyses per the NuScale Digital I&C Software Safety Plan.

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 Device logic within the digital I&C system. In this NuScale development process, a software or Complex Logic Device logic product is the highest element in the software hierarchy. Software or Complex Logic Device 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 Device logic.

For SIL 3 and 4 software, an independent V&V team performs a V&V of the Software Requirements Specification in accordance with the NuScale Digital I&C Software Verification and Validation Plan. For SIL 1 and 2 software, an independent verifier within the engineering 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. All anomalies must be satisfactorily resolved prior to issuing a V&V task report pursant to the NuScale Digital I&C Verification and Validation Plan.

The Software Requirements Specification is baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan.

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 Device 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 Device logic), and testing. The software or Complex Logic Device 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 IDD 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 between 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).

The NuScale Digital I&C Software Development Plan requires that 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 may 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.

The NuScale Digital Safety System SDOE Plan requires that vulnerability assessments be 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 NuScale 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 NuScale Digital Safety System 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 operating environments.

For commercial off-the-shelf software, previously developed software or complex programmable logic classified as SIL 4, the NuScale 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 secure development and operational environment design requirements and does not adversely affect system reliability.

The NuScale Digital I&C Software Quality Assurance Plan and the NuScale 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 Complex Logic Device logic coverage analyzers). The NuScale Digital I&C Software Configuration Management Plan governs the process for controlling code change requests and modifications.

The completed Software Requirements Specification is used as input to the ongoing software safety analysis activity for SIL 3 and 4 software or Complex Logic Device logic.

For SIL 3 and 4, an independent V&V team performs a V&V of the Digital I&C Software Design Description in accordance with the NuScale Digital I&C Software Verification and Validation Plan. For SIL 1 and 2 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. All anomalies must be satisfactorily resolved prior to issuing a V&V task report pursant to the NuScale Digital I&C Verification and Validation Plan.

The Software Design Description is baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan.

7.2.1.2.7 Software Implementation

The NuScale 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 NuScale Software Coding and Hardware Description Language Coding Guidelines. 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 Device logic:

- reliability
- robustness
- traceability
- maintainability

The software code or Complex Logic Device logic is designed to facilitate analysis, testing and readability.

For SIL 3 and 4 software, an independent V&V team performs a V&V of the software or Complex Logic Device logic in accordance with the NuScale Digital I&C Software Verification and Validation Plan. For SIL 1 and 2 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. All anomalies must be satisfactorily resolved prior to issuing a V&V task report pursant to the NuScale Digital I&C Verification and Validation Plan.

The software or Complex Logic Device logic is baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan.

The NuScale 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 (FAT) and SAT cases
- component test procedure
- integration test procedure
- system test procedure
- component test report

For SIL 3 and 4 software or Complex Logic Device logic, a test engineer from within an independent V&V team performs component level testing. For SIL 1 and 2 software or Complex Logic Device logic, a test engineer from within the engineering team performs the testing.

Complex Logic Device 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

For SIL 3 and 4 software or Complex Logic Device logic, in order to maintain the required technical, managerial, and financial independence from the developer of the test documentation (i.e., a test engineer within the V&V team), an independent verifier within the engineering team performs V&V of the test documents and records the same on corresponding V&V task reports pursuant to the NuScale Digital I&C Software Verification and Validation Plan.

The test documents are baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan.

7.2.1.2.8 Software Integration and Testing

The NuScale 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 (FAT) and site acceptance test (SAT) test procedures
- integration test report
- system test report
- FAT report

For SIL 3 and 4 software or Complex Logic Device 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 Device 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 any inconsistencies between the software or Complex Logic Device logic and the hardware.
- documents system test results and analyzes test results to verify that digital I&C system requirements from the 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 of the NuScale Digital I&C Software Safety Plan.

For SIL 3 and 4 software or Complex Logic Device logic, an engineer from the engineering team performs V&V of the test documents developed by the V&V team and documents the results on corresponding V&V task reports pursuant to the NuScale Digital I&C Software Verification and Validation Plan. For SIL 1 and 2 software or Complex Logic Device logic, an independent verifier within the engineering 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 in accordance with the NuScale Digital I&C Software Configuration Management Plan.

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 3 and 4 software or Complex Logic Device logic, a team performs V&V of the installation package and documents the results on corresponding V&V task reports pursuant to the NuScale Digital I&C Software Verification and Validation Plan. For SIL 1 and 2 software or Complex Logic Device logic, an independent verifier within the engineering team does the V&V and documents the results.

The installation package is baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan.

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 NuScale Digital I&C Software Master Test Plan governs the generation of the Site Acceptance Test Report.

For SIL 3 and 4 software or Complex Logic Device 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 1 and 2 software or Complex Logic Device logic, the engineering team SAT demonstrates that the installed system performs the safety function described in the system design basis.

The SAT report is baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan. 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: A COL applicant that references the NuScale Power Plant design certification is responsible for the implementation of the life cycle processes for the operation phase for the instrumentation and controls systems, as defined in Institute of Electrical and Electronics Engineers (IEEE) Std 1074-2006 and IEEE Std 1012-2004.

7.2.1.2.11 Instrumentation System Maintenance

COL Item 7.2-2: A COL applicant that references the NuScale Power Plant design certification is responsible for the implementation of the life cycle processes for the maintenance phase for the instrumentation and controls systems, as defined in Institute of Electrical and Electronics Engineers (IEEE) Std 1074-2006 and IEEE Std 1012-2004.

7.2.1.2.12 Instrumentation System Retirement

COL Item 7.2-3: The NuScale Digital instrumentation and controls (I&C) Software Configuration Management Plan provides guidance for the retirement and removal of a software product from use. A COL applicant that references the NuScale Power Plant design certification is responsible for the implementation of the life cycle processes for the retirement phase for the instrumentation and controls systems, as defined in Institute of Electrical and Electronics Engineers (IEEE) Std 1074-2006 and IEEE Std 1012-2004. The NuScale 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 l&C Software Quality Assurance Plan
- Digital l&C Software Verification and Validation Plan
- Digital l&C Software Master Test Plan
- Digital l&C Software Configuration Management Plan
- Digital I&C Software Requirements Management Plan
- NuScale Digital I&C Software Integration Plan
- NuScale Digital I&C Software Installation Plan
- NuScale 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 NuScale Digital I&C Software Quality Assurance Plan and Software Management Plan address the aspects of risk management and development tools.

The NuScale 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 hazards analysis, and SDOE vulnerability assessments by the Independent V&V design engineering teams respectively
- Coordination of risk analysis by the independent V&V test engineer with generation or update of the project risk register by the project manager
- Development of software and CLD logic by the design engineering team

- Development of test documentation and performance of testing by independent V&V test engineers for SIL 3 and 4 software and complex logic device logic.
- Management of the configuration of software and CLD logic and its documentation by Configuration Management
- Independent Verification and Validation of configuration of SIL 3 and 4 software and CLD logic Quality reviews and audits by the Quality Assurance organization

The NuScale Digital I&C Software Verification and Validation Plan address the aspects of quality metrics. For additional details regarding risk management, quality metrics, and the control of software tools, see the discussion of RG 1.28, Revision 4, RG 1.152, Revision 3, and IEEE Std 7-4.3.2-2003 in Section 7.2.1.

7.2.1.4 Software Quality Assurance Processes

For software QA, see the discussion of RG 1.28, Revision 4, RG 1.152, Revision 3, and IEEE Std 7-4.3.2-2003 in Section 7.2.1.

7.2.1.5 Software Verification and Validation Processes

For the software V&V process, see the discussion of RG 1.152, Revision 3, and IEEE Std 7-4.3.2-2003 in Section 7.2.1.

For software audits, see the discussion of RG 1.168, Revision 2, IEEE Std 1012-2004, and IEEE Std 1028-2008 in Section 7.2.1.

7.2.1.6 Software Configuration Management Processes

For the software configuration management process, see the discussion of RG 1.152, Revision 3, and IEEE Std 7-4.3.2-2003 in Section 7.2.1, as well as the discussion of RG 1.169, Revision 1, and IEEE Std 828-2005 in Section 7.2.1.

7.2.2 Equipment Qualification

The safety I&C SSC are designed to perform their safety-related functional requirements over the range of environmental conditions postulated for the area in which the components are located and during the time period when this performance is required.

The NuScale 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, Revision 1.

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 17, 18, and 23.

7.2.2.1 Instrumentation and Controls Qualification

MPS and Neutron Monitoring System-Excore Equipment Operating Environment

MPS 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 which is a harsh environment. The MPS and NMS-excore equipment rooms 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 7.2-7) 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 7.2-8) 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 on the 75'-0" and 86'-0" elevations (Figures 1.2-14 and Figure 1.2-15, respectively) which is a Seismic Category I, reinforced concrete structure. 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 detectors.

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 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. The Reactor Building and the Control Building (at and below elevation 120’-0”) are Seismic Category I, reinforced concrete structures, except as noted in Section 1.2.2.2. See Section 3.2 for more 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 (see 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. 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. MPS and NMS-excore cables are required to pass the flame test as required in IEEE Std 1202-2006 (Reference 7.2-28) 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 7.2-10) as endorsed by RG 1.75, Rev 3. 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. See 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 MPS rooms and cabinets. Refer to Section 9.5.1 for more detail on the fire protection methods employed in the NuScale Power Plant 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 trip 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 MPS equipment rooms within the reactor building. The operators then relocate to the remote shutdown station (RSS) to monitor plant conditions. Following shutdown and initiation of passive cooling, the NuScale 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 NuScale Power Module (NPM) in the RSS that when repositioned isolate the MPS manual actuation switches, override switches and enable nonsafety control switches for each NPM's MPS in the MCR to prevent spurious actuation of equipment due to fire damage.

MPS and NMS Equipment EMI and RFI 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 (EMI) and radio frequency interference (RFI) 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 EMI and RFI, surge withstand capabilities, and operating envelopes are elements of the total package that is needed to ensure electromagnetic compatibility within a NuScale Power Plant.

For compliance to RG 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants," NuScale applies the guidance for EMI and RFI protection from IEEE Std 1050-1996 "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations" (Reference 7.2-21) to the design of I&C systems. IEEE Std 665-1995, "IEEE Guide for Generating Station Grounding" (Reference 7.2-12) and IEEE Std C62.23-1995 "IEEE Application Guide for Surge Protection of Electric Generating Plants" (Reference 7.2-6) provide guidance and do not contain specific mandatory design requirements.

Instrument Sensing Lines

The safety-related sensors associated with the NuScale reactor design are described in NuScale Power, LLC, TR-0316-22048 "Nuclear Steam Supply Systems Advanced Sensor Technical Report," (Reference 7.2-26). The sensors that utilize instrument sensing lines are pressurizer pressure narrow range, reactor coolant system 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-67.02.01-1999 "Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants" (Reference 7.2-24), as endorsed by RG 1.151. More detailed information is provided in technical report TR-0316-22048 on sensor functions, sensor requirements, sensor design, sensor installation, sensor maintenance, and sensor qualification.

7.2.3 Reliability, Integrity, and Completion of Protective Action

This section discusses the reliability and integrity of the NuScale I&C systems, and the ability to complete a protective action once initiated to accomplish the safety functions. The design of the NuScale 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 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 analog components. The FPGA logic elements are arranged in an array of open connections. This 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 NuScale 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. Due to 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 7.2-9) to satisfy the single failure criterion through the addition of redundancy (see Section 7.1.3), diversity (see Section 7.1.5) and testability (see Section 7.2.15). The MPS remains functional in the presence of a single failure. An MPS hazard analysis was also 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 in the runtime environment. 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 (see Section 7.1.8) was 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, see 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). The MWS is located close to the equipment to facilitate troubleshooting activities. 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 via 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 via 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 equipment interface module (EIM) outputs are designed to remove power to the final actuation devices causing them to go to a safe-state (e.g., reactor trip breakers open, ECCS valves open). This ensures 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 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 main control room.

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.

In all cases, the highest priority is given to the automatic and manual RTS and ESFAS actuation signals. As shown in Figure 7.1-1k through 7.1-1an, these actuation signals have equal, highest priority; they are differentiated only 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. In all cases, 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 all 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 which 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, Revision 1. 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 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 either automatically or manually block certain protective actions that otherwise prevent mode changes during plant operation (e.g., plant startup). 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 NuScale 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 were evaluated, as described in Section 7.1.3. The operating bypass switches are momentary-contact switches and will normally be 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

MPS variables are monitored by four redundant channels which actuate the protective functions utilizing 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 SFM 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) which 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 MPS equipment rooms. The switches are connected to the HWM in the SFM chassis (See Figure 7.0-4).

If the SFM is not out of service, the SBM transmits the safety function algorithm result that was 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 reactor trip breakers can be tested at power because of the breaker configuration by opening one breaker at a time. This allows for reactor trip breaker testing without the need for a maintenance bypass associated with the reactor trip breakers. Most of the ESFAS components are not tested at power since 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 reactor trip breakers 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 (See Figure 7.0-6). During testing of the trip actuation logic, the trip signals to the undervoltage trip mechanism of the reactor trip breakers are not actuated. The MPS is designed to permit overlapping online testing of MPS logic and reactor trip breakers.

The part of MPS that is not tested at power is the actuation priority logic circuit on the EIM. This includes 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. Due to 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, revision 1. The MPS equipment status information is automatically sent to the MCS and SDIS. The MCS and SDIS will provide the operator with continuous indication 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.

Information on displaying system bypass status information is provided in Section 7.2.13.

7.2.5 Interlocks

Interlocks ensure the reactor trip and engineered safety feature 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 the requirments of 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 I&C interlocks used to maintain the ESFAS variables within the ranges of values specified in the safety analyses 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.

NMS 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 emergency core cooling system (ECCS) valves contain an inadvertent actuation block feature which minimizes the probability of a spurious opening of an ECCS valve at operating pressure (see Section 6.3). In the unlikely event of an inadvertent signal

from MPS to actuate the ECCS valves at nominal plant pressure, the valves will not open until a sufficiently low differential pressure between the reactor pressure vessel and the containment vessel is reached. This allows the operator to respond to the inadvertent signal without the opening of the ECCS valves and the resulting plant transient.

Plant conditions during a valid ECCS actuation per the nominal trip setpoint should allow the ECCS valves 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 will not occur until the inadvertent actuation block has allowed the ECCS valves to fully 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 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. All but one MPS variable identified and used for safety-related functions is derived from process signals that are direct measurements of the process variables credited in the plant safety analysis (see Chapter 15). The exception is steam superheat, that is a variable calculated from steam pressure and steam temperature. 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 are provided in the TR-0316-22048.

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 which 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 listed in Table 7.0-2 for ASAI number 44.

NuScale Power, LLC, TR-616-49121 "NuScale Instrument Setpoint Methodology Technical Report," (Reference 7.2-27) 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 TR-616-49121.

The methodology described has been 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-67.04.01-2006, "Setpoints for Nuclear Safety-Related Instrumentation," (Reference 7.2-29) and addresses the regulatory issues identified in U.S. Nuclear Regulatory Commission Regulatory Issue Summary 2006-17. Table 1.9-2 addresses the partial conformance with Regulatory Guide 1.105, revision 3 that endorses ISA-S67.04-1994, "Setpoints for Nuclear Safety-Related Instrumentation," (Reference 7.2-23).

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. The detailed setpoint calculation processes for the MPS are described in TR-616-49121 and may change according to the plant-specific instrument accuracy and uncertainty data. 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 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 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 module protection system (MPS) or neutron monitoring system (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 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 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 safety function modules, scheduling and bypass modules, scheduling and voting modules, 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 safety function modules, scheduling and bypass modules, scheduling and voting modules, 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 via the actuation priority logic function within the equipment interface module. 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 highly reliable DC power system (EDSS) 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 reactor trip breakers and pressurizer heater breakers. The shunt trip coil and relays of the reactor trip breakers and the pressurizer heater trip breakers do not affect the MPS in accomplishing its safety functions. Each breaker utilizes 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 post-accident monitoring (PAM) only mode. The 24-hour timers and associated components of the MPS are used to ensure a 72-hour EDSS-MS battery capacity by shedding loads on EDSS 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 (EIM). When plant conditions require MPS to initiate the 24-hour timers, MPS also initiates a reactor trip, decay heat removal system actuation, demineralized water supply isolation, and containment isolation using separate EIMs. 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 Type B, Type C, and Type D variable 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 EDSS 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, Revision 3 and RG 1.152, Revision 3.

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 11, 22, 31, 32, 33, 53, 54, and 58.

7.2.9.1 Control of Access

The NuScale 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, Revision 3 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 platform development process is outlined in the NuScale Digital Safety System Project Plan and the Digital I&C Software Quality Assurance Plan that provide detailed information on the life cycle processes (see Section 7.2.1).

As documented in the Digital Safety System Project Plan (see 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, Revision 1 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 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 any 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 planning, requirements, design, and implementation, and test phases of a typical software life cycle.

During the detailed design process element, 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.

When the system ownership transfers from NuScale or the vendor to the licensee, the system transitions from a secure development environment to a secure operational environment. The licensee is required to develop procedures to describe the

requirements of their secure operational environment, a cyber-security plan, along with the system configuration management plans and procedures.

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.

Additional physical and logical controls also prevent modifications to a MPS safety channel when being relied upon to perform a safety function. Protection from a faulted MWS when not in use is provided through a qualified physical hardware disconnect and a qualified safety-related isolation device. 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 which 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 (DIMs) are located in the MCR.

The communication interfaces for each MPS separation group have uni-directional 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 utilized 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 uni-directional 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 (see 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 4 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 to systems within the Security Level 4 domain.

The NMS 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 MPS 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 utilizes 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. Any non-divisional cable within such cabinets is appropriately marked to distinguish it from the divisional cables. The method used for identification is readily distinguished between different divisions of Class 1E systems, between Class 1E and non- Class 1E systems, and between 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, Revision 3 (see Section 7.2.1).

MPS 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 NuScale Digital I&C Software Configuration Management Plan describes the following related to identification with digital I&C systems (see Section 7.2.1):

- identification of the program version as well as a means to identify the version after the software has been compiled and loaded onto a computer or the FPGA programming has been 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 rapidly 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 may be placed in bypass or trip depending on the technical specifications. This permits continued operation while still meeting the single-failure criterion. For SFMs, SBMs, SVMs, 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 reactor trip breaker 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 TR-1015-18653-P-A.

The normal configuration of MPS is designed with one-way communication from the MPS 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 a 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 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 MPS room can be connected and updated at one time. Because there are two separate MPS 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. This is administratively controlled.

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 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 via isolated, one-way communication paths (see 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. This reduces the number of penetrations into critical pressure boundaries, such as the reactor pressure vessel and steam lines. Isolated output signals maintain MPS channel independence (see 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.

MPS 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 utilized. 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, MCS will use the median value of all four inputs. If one of the inputs is "bad" due to 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 utilization.

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 has been bypassed for maintenance, or if the channel has failed (i.e. 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 will use 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-Unit Stations

This section describes the multi-unit station design of the NuScale Power Plant. 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 listed in Table 7.0-2 for ASAI number 35.

The NuScale Power Plant may include up to twelve 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. DBEs occurring in one module do not impair the ability of the I&C systems in another module from performing their required safety functions. See Chapter 21 for more details on multi-module effects on safety systems.

The electrical power provided by the module-specific EDSS is not shared between NPMs. The common portion of EDSS provides electrical power to shared plant SSC (see Section 8.3). Class 1E isolation is provided between the EDSS and MPS, and the isolation devices are classified as part of the safety system. Cross-tie capabilities between NPMs are not provided in the EDSS design.

The NuScale Power Plant is designed to monitor and control up to 12 NPMs from a single control room by utilizing human factors engineering (HFE) and increased automation to optimize staffing levels and reduce human errors. The operator staffing requirements associated with multi-module operations are described in Section 18.5. There is no sharing of safety-related I&C SSC between modules. PPS, PCS, and SDIS, which are all 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 EDSS (see Section 8.3.2.1). There are no interfaces or connections between the PPS or PCS to any NPMs' MPS or NMS. The SDIS is isolated from the MPS through the MPS gateways, as described in Section 7.1.2. The multi-module effects of the PCS and PPS are discussed in Chapter 21. The SDIS has been analyzed such that no credible failure of the SDIS can cause

a loss of multiple NuScale Power Module display functions. The SDIS human system interface is designed in accordance with human system interface design principles that conform to NUREG-0711 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 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 engineered safety features 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, Revision 1.

The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A listed in Table 7.0-2 for ASAIs 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 has been 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 7.1-1ao.

7.2.12.2 Manual Control

The MPS conforms to RG 1.62, Revision 1, 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 over pressure protection

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 will override the nonsafety signal and is prioritized within the actuation priority logic. For beyond DBEs 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 CFDS, RCS injection, and pressurizer spray containment isolation valves if an automatic containment system isolation actuation signal or a CVCS isolation actuation signal is present with the exception of the High Pressurizer Level CVCS isolation actuation signal.
- The manual override switches will generate an alarm when activated.

See the MPS functional logic diagrams (Figure 7.1-1j through Figure 7.1-1ao). The manual controls are controlled administratively through approved plant procedures.

No manually controlled actions are assumed in the NuScale Power Plant 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 497-2002 "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," (Reference 7.2-31). The MPS provides outputs of monitored variables to two redundant divisions of the MCR 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 and relocate to the RSS. 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 MPS 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 in the RSS, see 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, for the normal status and the bypassed and inoperable status of safety systems, and for satisfying applicable requirements of 10 CFR 50.34(f).

The design of the SDIS conforms to IEEE Std 603-1991, Section 5.8, and the guidance in RG 1.97, Revision 4 with exceptions 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 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 may be used to support manual initiation of protective actions, but the SDIS does not directly initiate protective actions.

MCR displays are developed following the guidance contained in NUREG-0700 as described in the NuScale Power Human-System Interface Design Results Summary Report (Reference 18.7-2). 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. There are two separate SDIS display panels, both panels independently display the same variables. This provides the operators in the MCR the ability to cross check data from independent divisions, independent sensors, on independent displays.

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 post-accident monitoring 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. PPS uses the PCS in conjunction with the SDIS.

MPS 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 that was used to identify the controls, alarms, and displays needed in the MCR to manage the plant safety functions and remote shutdown capability are detailed in Section 18.7.2.

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 NuScale Power Plant 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 497-2002. The SDIS meets the display criteria of IEEE Std 497-2002. 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 Type B, C and D 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. All 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 Remote Shutdown Station

The RSS is described in Section 7.1.1.2.3. There is an identical set of MCS and PCS displays located in the RSS provided for the operator to monitor the plant operation if evacuation of the MCR is required. SDIS displays are not provided in the RSS as there is no manual control of safety-related equipment allowed from the RSS.

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. See Section 7.2.4 for 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 were 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 defined in the Human System Interface Design Results Summary Report (Reference 18.7-2).

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 RSS. The MCS and PCS operator workstations are separate and independent from the control processors such that a failure of the control processors will 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 and RSS 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 which provides the operator the ability to understand and diagnose major plant upsets.

7.2.13.6 Three Mile Island Action Items

Control room indication is provided to measure, record, and readout containment pressure, containment water level, and noble gas effluents at the potential accident release points to satisfy the requirements of 10 CFR 50.34(f)(2)(xix) as well as the

following variables that are used to identify inadequate core cooling to satisfy the requirements of 10 CFR 50.34(f)(2)(xviii):

- core exit temperatures
- wide range reactor coolant system pressure
- degrees of subcooling
- wide range reactor coolant system hot temperature
- RPV water level
- containment water level

The bypassed and operable status indication of safety interlocks is automatically provided in the control room as described in Section 7.2.13.6 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.

Consistent with 10 CFR 50.34(f)(2)(xvii)(C) and 10 CFR 50.44(c)(4), The PSS containment sampling system includes oxygen and hydrogen analyzers to monitor the containment environment. These monitors are nonsafety-related instruments that continuously monitor oxygen and hydrogen concentrations in containment during operation and are capable of monitoring during beyond design-basis conditions. The analyzers are designed to be functional, reliable, and will meet design criteria discussed in Regulatory Position C.2 of RG 1.7. The hydrogen analyzer output signal is sent to the MCS, which can provide readout in the main control room. Additionally, local indication is also provided as a backup display/indication in event that information from MCS cannot be displayed in the control room post-accident.

Consistent with 10 CFR 50.34(f)(2)(xvii)(E), the PCS displays and records in the MCR information on noble gas effluent release points for the NuScale plant.

As described in Table 1.9-5, the NuScale 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 will cause the boundary device to reverse the direction of data flow. The MCS and PCS systems provide monitoring data via one-way communication interfaces to the plant network which provides data recording, trending, and historical retention that can be retrieved on the emergency operations facility stations and technical support center (TSC) engineering workstations.

Additionally, there is a link from the plant network to the NRC emergency response data system via dedicated communication servers that connect to the plant network and provide data communication of required plant data to offsite emergency response facilities.

The TSC engineering work stations are located on the 100' level of the Control Building and separated from the operator workstations, which are located in the MCR on the 76'-6" level in the control building. The TSC engineering work stations have fully licensed operating systems, all 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 and RSS 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 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 may be used for manual initiation of protective actions; however, there are no manual protective actions for which no automatic action exists. Alarms associated with MPS are designed to alert the operator of abnormal conditions that may lead to automatic reactor trip or engineered safety feature (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 all its sensors and equipment to the SDIS and the MCS for indication and alarms. The display instrumentation provides accurate, complete, and timely information which 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

MPS utilizes 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 7.1-1ao. 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. This aids in determining the course of action 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. Due to 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 for which automatic action does not exist. 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 which improves operator awareness and assists in making appropriate decisions.

Logic Status

PPS 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 in accordance with applicable technical specification limits. 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 any applicable technical specification limits, see Section 7.2.15. Additional self-diagnostics are implemented in PPS to provide device status rapidly 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. Due to the simplistic design of the NuScale Power Plant, 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 has gone 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.

The SDIS displays the availability of the equipment of the MPS, PPS and SDIS. With continuous self-diagnostics in the systems, the SDIS is able to immediately alert the operator when equipment is no longer available.

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 the Human-System Interface Design Results Summary Report (Reference 18.7-2).

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 described in the Human-System Interface Design Results Summary Report (Reference 18.7-2).

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 and the RSS.

The PCS operator workstation displays are located in the MCR, the radwaste building control room, and the RSS.

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, etc. has failed.

The operator workstation displays are designed as described in the Human-System Interface Design Results Summary Report (Reference 18.7-2).

Workstations in Locations outside of the MCR

The HSIs in the locations outside of the MCR (TSC, emergency operations facility, and the RSS) are all 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 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, Revision 0, RG 1.118, Revision 3, and RG 1.47, Revision 1.

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 14, 24, 25, 26, 32, 47, 49, 50, and 51.

7.2.15.1 System Calibration

The MPS and 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 (see Section 7.2.4). Any SFM in maintenance bypass will generate 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 monitoring and indication bus 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 I&C 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 7.2-32) as endorsed and modified by RG 1.118, Revision 3, and IEEE Std 603-1991 with supplemental guidance in RG 1.22, Revision 0, and RG 1.47, Revision 1.

The MPS and NMS allow SSC to be tested while retaining the capability to accomplish required safety functions. The MPS uses modules from the HIPS platform which 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 may 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. This includes the manual MCR switches and the nonsafety-related control 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 Type B, Type C and Type D post-accident monitoring 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 will 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 497-2002. The time periods during which SDIS and PPS may be bypassed or removed from service is administratively controlled.

While the MPS is in normal operation, self-tests run without affecting the performance of the safety function, including its response time.

MPS 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 will generate 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 via 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.

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 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 Not Used.

7.2-5 Electric Power Research Institute, "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," TR-106439, November 14, 1996.

7.2-6 Institute of Electrical and Electronics Engineers, "IEEE Application Guide for Surge Protection of Electric Generating Plants," IEEE Std C62.23-1995 (R2001), Piscataway, N.J.

7.2-7 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations," IEEE Std 323-2003, Piscataway, N.J.

7.2-8 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations." IEEE Std 323-1974, Piscataway, N.J.

7.2-9 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, N.J.

7.2-10 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," IEEE Std 384-1992 (R1998), Piscataway, N.J.

7.2-11 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603-1991, Piscataway, N.J.

7.2-12 Institute of Electrical and Electronics Engineers, "IEEE Guide for Generating Station Grounding," IEEE Std 665-1995 (R2001), Piscataway, N.J.

7.2-13 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, N.J.

7.2-14 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Quality Assurance Plans," IEEE Std 730-2002, Piscataway, N.J.

7.2-15 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Configuration Management Plans," IEEE Std 828-2005, Piscataway, N.J.

7.2-16 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software and System Test Documentation," IEEE Std 829-2008, Piscataway, N.J.

7.2-17 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Software Requirements Specifications," IEEE Std 830-1998, Piscataway, N.J.

7.2-18 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Unit Testing," IEEE Std 1008-1987 (R2009), Piscataway, N.J.

7.2-19 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Verification and Validation," IEEE Std 1012-2004, Piscataway, N.J.

7.2-20 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Reviews and Audits," IEEE Std 1028-2008, Piscataway, N.J.

7.2-21 Institute of Electrical and Electronics Engineers, "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations," IEEE Std 1050-1996, Piscataway, N.J.

7.2-22 Institute of Electrical and Electronics Engineers, "IEEE Standard for Developing a Software Project Life Cycle Process," IEEE Std 1074-2006, Piscataway, N.J.

7.2-23 International Society of Automation, "Setpoints for Nuclear Safety-Related Instrumentation," ISA-S67.04-1994, Research Triangle Park, North Carolina.

7.2-24 American National Standards Institute/International Society of Automation, "Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants," ANSI/ISA 67.02.01-1999, Research Triangle Park, North Carolina.

7.2-25 NuScale Power, LLC, "Design of the Highly Integrated Protection System Platform Topical Report," TR-1015-18653-P-A, Revision 2.

7.2-26 NuScale Power, LLC, "Nuclear Steam Supply Systems Advanced Sensor Technical Report," TR-0316-22048, Revision 0.

7.2-27 NuScale Power, LLC, "NuScale Instrument Setpoint Methodology Technical Report," TR-616-49121, Revision 0.

7.2-28 Institute of Electrical and Electronics Engineers, "Standard for Flame-Propagation Testing of Wire & Cable," IEEE Std 1202-2006, Piscataway, N.J.

7.2-29 International Society of Automation, "Setpoints for Nuclear Safety-Related Instrumentation," ISA-67.04.01-2006, Research Triangle Park, North Carolina.

7.2-30 NuScale Power, LLC, Topical Report, "Quality Assurance Program Description," NP-TR-1010-859-NP, Revision 4.

7.2-31 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," IEEE Std 497-2002, Piscataway, NJ.

7.2-32 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.

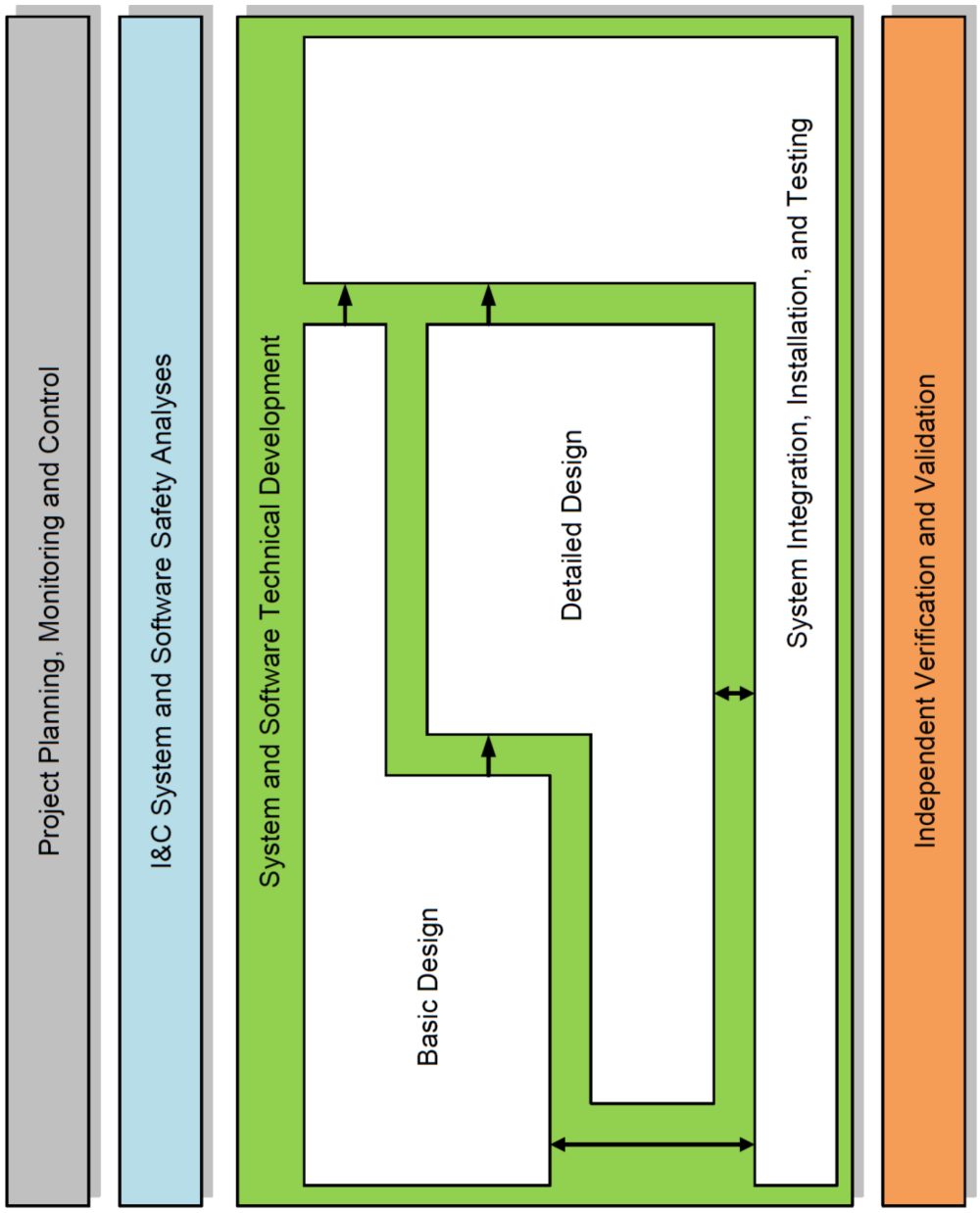


Figure 7.2-1: Instrumentation and Controls Safety System Development Processes

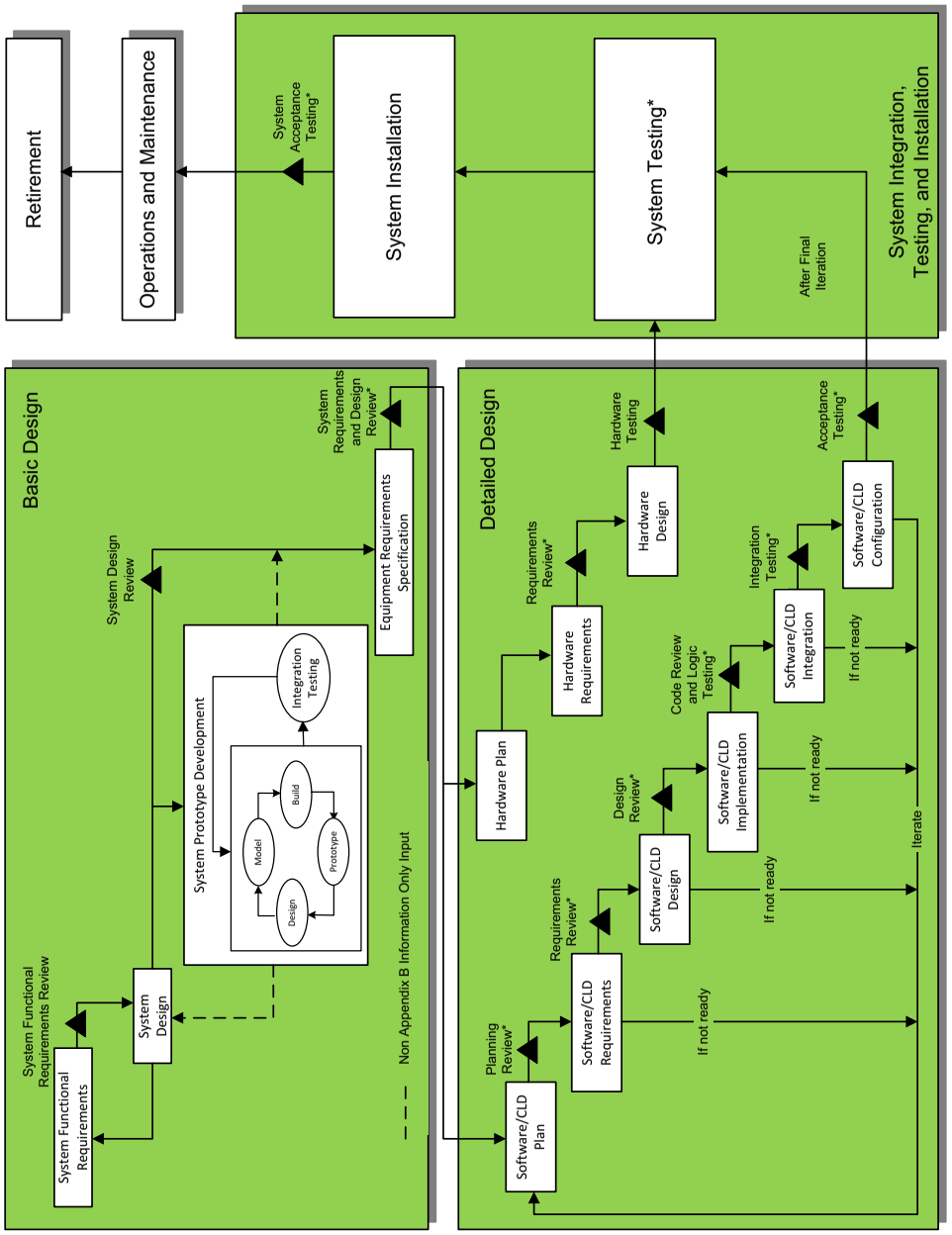


Figure 7.2-2: NuScale System and Software Technical Development Life Cycle Processes

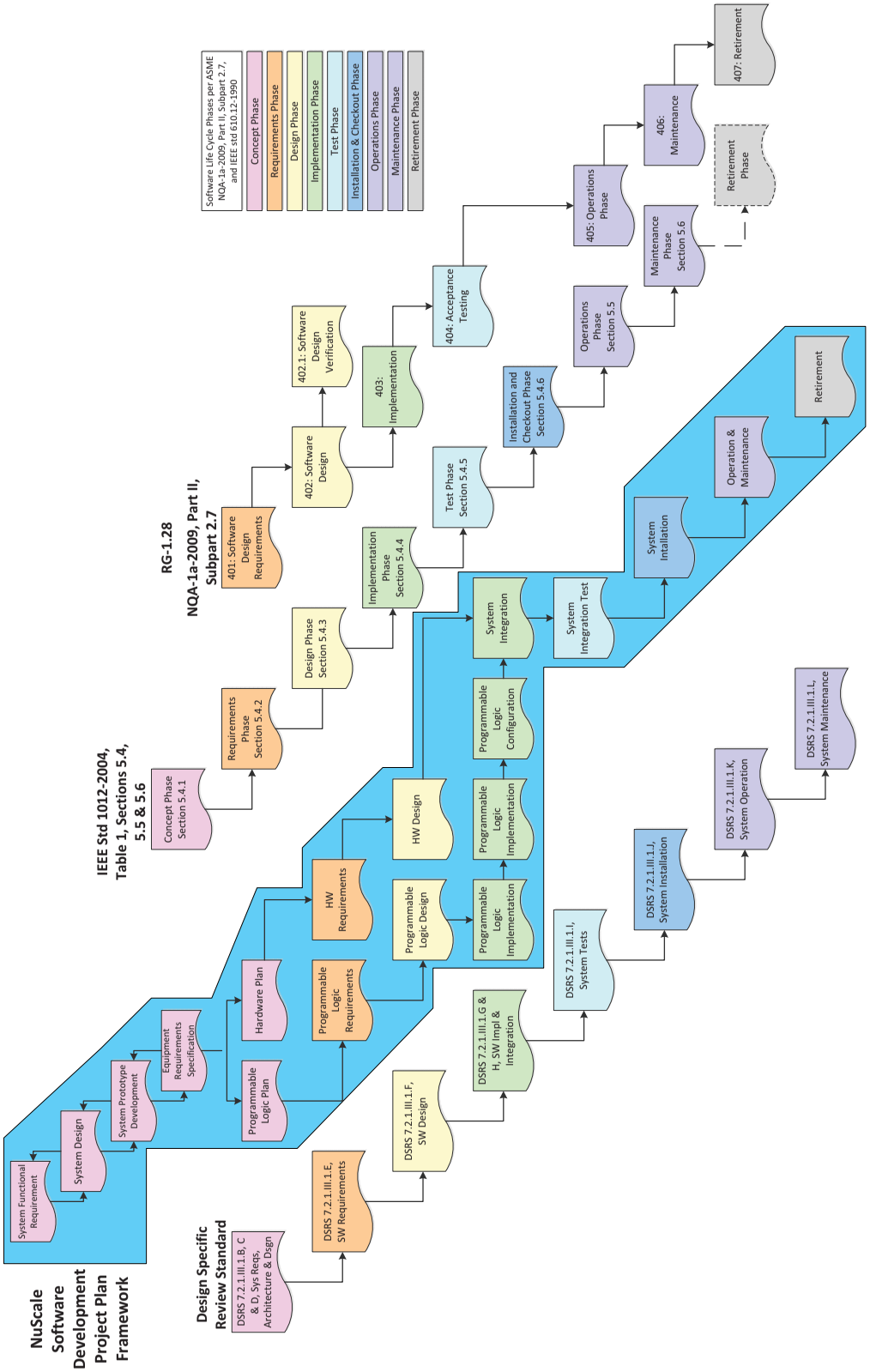


Figure 7.2-3: NuScale Software Lifecycle Comparisons