CHAPTER 7

INSTRUMENTATION AND CONTROL SYSTEMS

TABLE OF CONTENTS

CHAPTER 7

INSTRUMENTATION AND CONTROL SYSTEMS

TABLE OF CONTENTS

Section **Title** **Page**

CHAPTER 7

INSTRUMENTATION AND CONTROL SYSTEMS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
ALARA	as low as reasonably achievable
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOV	air operated valve
APL	actuation and priority logic
BIST	built-in self-test
CAAS	criticality accident alarm system
CAMS	continuous air monitoring system
cc	cubic centimeter
CCF	common cause failure
CDA	critical digital asset
CDBEM	carbon delay bed effluent monitor
Ci	curie
CM	communication modules
COTS	commercial off-the-shelf
cps	counts per second

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
CRC	cyclic redundancy checks
CTB	calibration and test bus
DC	direct current
EIM	equipment interface module
EMI	electromagnetic interference
ESFAS	engineered safety features actuation system
FAT	factory acceptance test
FCHS	facility chilled water system
FCR	facility control room
FDCS	facility data and communications system
FDWS	facility demineralized water system
FHWS	facility heating water system
FNHS	facility nitrogen handling system
FPGA	field programmable gate array
HIPS	highly integrated protection system
HRS	hardware requirements specification

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
HSI	human system interfaces
HVAC	heating, ventilation, and air conditioning
HVPS	high voltage power supply
HWM	hardwired module
I&C	instrumentation and control
IDE	integrated development environment
IDN	isolated development network
IEEE	Institute of Electrical and Electronic Engineers
IF	irradiation facility
ISG	interim staff guidance
ISM	input submodule
ITS	impurity treatment subsystem
IU	irradiation unit
IXP	iodine and xenon purification
μCi	microcurie
M	subcritical multiplication factor

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
MEPS	molybdenum extraction and purification system
MI-CM	monitoring and indication communication module
MIB	monitoring and indication bus
MIPS	molybdenum isotope product packaging system
MWS	maintenance workstation
N2PS	nitrogen purge system
NDAS	neutron driver assembly system
NFDS	neutron flux detection system
NIST	National Institute of Standards and Technology
NPSS	normal electrical power supply system
NVM	nonvolatile memory
OOS	out of service
PCLS	primary closed loop cooling system
PICS	process integrated control system
PLDS	programmable logic design specification

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
PLRS	programmable logic requirements specification
PTDA	partial trip determination actuation
PVVS	process vessel vent system
QA	quality assurance
RAMS	radiation area monitoring system
RCA	radiologically controlled area
RDS	radioactive drain system
RFI	radio-frequency interference
RLWI	radioactive liquid waste immobilization
RLWS	radioactive liquid waste storage
RPCS	radioisotope process facility cooling system
RPF	radioisotope production facility
RVZ1	radiological ventilation zone 1
RVZ2	radiological ventilation zone 2
RVZ3	radiological ventilation zone 3

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
SASS	subcritical assembly support structure
SBM	scheduling and bypass modules
SCAS	subcritical assembly system
SDB1	safety data bus 1
SDB2	safety data bus 2
SDB3	safety data bus 3
SDE	secure development environment
SFM	safety function module
SGS	standby generator system
SOV	solenoid operated valve
SRM	stack release monitor
SRMS	stack release monitoring system
SVM	scheduling and voting module
SyRS	system requirements specification
TID	total integrated dose
TOGS	TSV off-gas system

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
TPS	tritium purification system
TRPS	target solution vessel reactivity protection system
TSPS	target solution preparation system
TSSS	target solution storage system
TSV	target solution vessel
UPSS	uninterruptible electrical power supply system
URSS	uranium receipt and storage system
V&V	verification & validation
VAC/ITS	vacuum/impurity treatment subsystem
VTS	vacuum transfer system

CHAPTER 7 – INSTRUMENTATION AND CONTROL SYSTEMS

7.1 SUMMARY DESCRIPTION

The instrumentation and control (I&C) systems provide the capability to monitor and control the SHINE facility systems manually and automatically during normal conditions and maintain the facility in a safe condition under accident conditions.

This chapter describes the design of the I&C systems, including classification, functional requirements and architecture, and demonstrates the systems' capabilities to perform safety and nonsafety-related functions. The scope of the information provided in this chapter includes systems that are safety-related as defined by SHINE's Quality Assurance Program Description and nonsafety-related I&C systems that perform specific regulatory required functions.

Section 7.1 provides an introduction and overview of I&C systems, which include safety-related and nonsafety-related systems. Systems and topics addressed in this chapter include:

- the process integrated control system (PICS)
- the target solution vessel (TSV) reactivity protection system (TRPS)
- the engineered safety feature actuation system (ESFAS)
- the highly integrated protection system (HIPS) underlying TRPS and ESFAS
- facility control room control consoles and displays
- radiation monitoring, including
    - safety-related process radiation monitors considered part of the ESFAS, TRPS, and tritium purification system (TPS)
    - nonsafety-related process radiation monitors included as part of other facility processes
    - the radiation area monitoring system (RAMS)
    - the continuous air monitoring system (CAMS)
    - the stack release monitoring system (SRMS)
    - the criticality accident alarm system (CAAS)
- the neutron flux detection system (NFDS)

The architectural design of I&C systems is based on providing clear interconnection interfaces of facility I&C structures, systems, and components. Each irradiation unit (IU) has an independent safety-related TRPS and NFDS. A single nonsafety-related PICS provides the nonsafety functions of the IUs and facility level nonsafety-related functions. An ESFAS is provided for safety-related functions that are common to the entire facility. The CAAS, RAMS, CAMS, and SRMS provide their functions at a facility level separate from the irradiation units.

A simplified block diagram of the overall I&C system architecture is provided in Figure 7.1-1.

7.1.1 PROCESS INTEGRATED CONTROL SYSTEM

The PICS is a nonsafety-related distributed digital control system that provides monitoring and control of the various processes throughout the SHINE facility. The PICS includes system controls, both automated and manual, and human system interfaces (HSIs) necessary to provide the operator interaction with the necessary process control mechanism. The HSIs are provided in the facility control room (FCR) and are described in Section 7.6.

The principal functions of the PICS are to control and monitor facility systems and components. This includes systems and components within the irradiation facility (IF). PICS also interfaces with the systems and components in the radioisotope production facility (RPF).

The functions of the PICS enable the operator to perform irradiation cycles, transfer target solution to and from the IU as well as throughout the RPF, and interface with the TPS, processes in the supercell, waste handling operations, and the auxiliary systems.

The PICS is further described in Section 7.3.

7.1.2 TARGET SOLUTION VESSEL REACTIVITY PROTECTION SYSTEM

The purpose of the TRPS is to monitor process variables and provide automatic initiating signals in response to off-normal conditions, providing protection against unsafe IU operation during the IU filling, irradiation, and post-irradiation modes of operation. Each IU has its own TRPS, configured as shown in Figure 7.1-2. The major safety function of the TRPS is to monitor variables associated with the IU and trip the neutron driver and actuate the engineered safety features when specified setpoints, based on analytical limits, are reached or exceeded.

The TRPS maintains the modes of operation of the IU and creates the necessary interlocks and permissives on each safety function needed for the different modes. Modes are transitioned sequentially using an operator input.

The TRPS also transmits status and information signals to the nonsafety-related maintenance workstation (MWS) and to the PICS for display in the FCR, trending, and historian purposes.

The TRPS is built utilizing the HIPS as described in Subsection 7.1.4. HIPS is a field programmable gate array (FPGA)-based system. The TRPS incorporates the fundamental I&C principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth as used by the HIPS platform.

The TRPS includes the following safety-related (except where noted otherwise) components:

- three divisions of input modules, signal conditioning, and trip determination
- two divisions of power distribution panels
- power supplies for sensors and TRPS components
- two nonsafety-related MWSs
- two divisions of voting and actuation equipment
- manual input switches

The boundary of the TRPS extends from the terminations of the cabling at the output of the sensors to the terminations of the cabling to each actuation component of the TRPS.

The TRPS is further described in Section 7.4.

7.1.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

The purpose of the ESFAS is to monitor process variables and provide automatic initiating signals in response to off-normal conditions, providing protection against unsafe conditions in the SHINE facility. The ESFAS is a plant level control system not specific to any operating unit or process, configured as shown in Figure 7.1-3. The two major safety functions of the ESFAS are to provide:

- sense and command functions necessary to maintain the facility confinement strategy and
- process actuation functions as required by the safety analysis.

The ESFAS also transmits status and information signals to the nonsafety-related MWS and to the PICS for display in the FCR, trending, and historian purposes.

The ESFAS, like the TRPS, is also built using the HIPS platform as described in Subsection 7.1.4. The ESFAS incorporates the fundamental I&C principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth as used by the HIPS platform.

The ESFAS includes the following safety-related components (except where noted otherwise):

- three divisions of input modules, signal conditioning, and trip determination
- two divisions of power distribution panels
- power supplies for sensors and ESFAS components
- two nonsafety-related MWSs
- two divisions of voting and actuation equipment
- manual input switches

The boundary of the ESFAS extends from the terminations of the cabling at the output of the sensors to the terminations of the cabling to each actuation component of the ESFAS.

The ESFAS is further described in Section 7.5.

7.1.4 HIGHLY INTEGRATED PROTECTION SYSTEM DESIGN

The HIPS is used for both the TRPS and ESFAS as shown in Figure 7.1-2 and Figure 7.1-3. This subsection describes the design characteristics of the HIPS.

The safety function module (SFM) receives sensor inputs to the HIPS platform at the signal conditioning circuitry to measure variables important to the safe operation of the IU. The SFM performs three main functions with the sensor inputs:

- Signal conditioning
- Trip determination
- Communication to the TRPS communication modules

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

The trip determination receives sensor input values in a digital format from the signal conditioning block. The trip determination performs the comparison of the sensor inputs to setpoints programmed into the FPGA and makes a trip determination based on the output of the comparison. The output of the trip determination is transmitted as trip or no-trip to the voting logic in the communication modules.

The SFM also provides monitoring and indication bus (MIB) functionality and calibration and test bus (CTB) functionality. The MIB is responsible for obtaining variables, parameters, trip determination results, status, and diagnostic information from each of the core logic paths. The CTB allows for the MWS to update the tunable parameters (i.e., setpoints) in the nonvolatile memory when the SFM is taken out of service (OOS).

The SFM has three core logic paths that are separated at the output of the signal condition circuitry. The three core logic paths each perform trip determination and send the results to the three safety data buses (SDB1, SDB2, and SDB3). In two of the three divisions, SFMs send the data via the chassis backplane directly to the scheduling and voting module (SVM) associated with the respective safety data bus where the two-out-of-three voting occurs. The third division sends the data to scheduling and bypass modules (SBMs) local to that division, which collects the data and transmits the collected data to each of the SVMs to complete the two-out-of-three voting inputs. Both the SBM and SVM are the master of the respective safety data bus to the SFMs. Transmission from the third division's SBM to the SVMs is point-to-point one-way communication.

The results of the two-out-of-three voting are transmitted through the chassis backplane in a round robin fashion to each of the equipment interface modules (EIMs). There the EIMs combine the input from the three SVMs associated with the three different safety data buses in a two-out-of-three vote to determine if a protective function requiring deenergizing the output of that EIM is necessary.

All status and diagnostic information from each of the individual module types is provided to the MIB. The monitoring and indication communication module (MI-CM) is the bus master for all communications on the MIB. The MI-CM provides status and diagnostic information from all modules through isolated, transmit-only communication ports to nonsafety-related equipment.

Each SFM has an associated trip/bypass switch connected to a hardwired module (HWM) that isolates the signal and places the trip or bypass information on the backplane where it is routed to either the SBMs or SVMs where it is used. Each SFM also has an OOS switch installed on its front plate. When the OOS switch on the SFM is activated, the SBM forces the safety function into either trip or bypass, depending on the position of the trip/bypass switch, and takes the channel OOS. It also provides the appropriate alarm output information.

Manual switches in the FCR, as well as any other discrete signal inputs from other systems, are received via the hardwired module. A manual switch for each safety function is provided. The manual switch is directly input into the actuation and priority logic (APL) in the EIM downstream of all programmable logic.

The priority on the different control signals provided to the logic from within the HIPS platform is defined by the APL. There are five different command signals that the APL accepts:

- Automated trip signal passed down from the SFM
- Manual trip signal from the FCR
- Enable nonsafety enabled

- Enable nonsafety disabled
- Manual controls from the PICS

Discrete logic is used for the APL for actuation of components based on the prioritization design. PICS is only allowed control by the APL logic if the enable nonsafety enable permissive signal is active and no manual or automated protective functions are present.

The circuitry of the APL is designed so that, when an actuation signal is received, either through the safety data path or manually through the HWM, the APL ensures the action carries through until completion. Upon a reset of the sense and command features, the APL continues to hold the actuated components on the requested position until deliberate operator action is taken to change the component's state.

7.1.5 CONTROL CONSOLE AND DISPLAYS

The operator workstations and main control board are provided as the HSI subset of components for the FCR. These components are included as part of the PICS and are classified as nonsafety-related.

The two operator workstations provide operators with interactive displays to perform daily activities for the SHINE facility. The displays at the operator workstation are capable of being changed to the appropriate screen applicable to the activities that the operator is performing during day-to-day operations of the SHINE facility.

The main control board, located in front of the two operator workstations, includes both digital displays and limited manual interfaces.

The main control board provides the operator with multiple digital displays, configured to continuously display variables important to safety-related system status for individual IUs and the balance of the production facility. The displays on the main control board are used to support manual actuation of safety-related systems and to verify correct operation of the safety-related systems in the event of an actuation.

The main control board provides operator interfaces for:

- manual actuation of the TRPS and ESFAS protective functions,
- the enable nonsafety function, which allows PICS control of the APL output state (i.e., deenergized or energized), and
- the facility operating permissive key, which is used to place the SHINE facility into a secure state.

The supervisor workstation is located at the rear of the facility control room and acts as an extension of the operator workstations. The supervisor workstation is equipped with equipment display screens that allow the supervisor to monitor system status, but not control facility components.

Facility controls are designed and located using consideration of human factors engineering principles. The SHINE Human Factors Engineering Program is used to facilitate the safe, efficient, and reliable performance of operations, maintenance, tests, inspections, and surveillance tasks, and to ensure the implementation of operator interfaces, indicators, and controls are standardized across vendors.

These systems are further described in Section 7.6.

7.1.6 RADIATION MONITORING

Radiation monitoring is used to monitor radiation levels within the SHINE facility, to provide alarms for personnel within the facility and the control room, to provide actuation signals to safety-related control systems, and to monitor airborne effluent streams from the facility.

Safety-related process radiation monitoring is performed by ESFAS, TRPS and TPS radiation monitors. These monitors provide input into the safety-related controls to provide input for safety actuations and interlocks, and provide indication and alarm signals to the FCR.

Nonsafety-related process radiation monitors are used in select facility processes to provide status information and diagnose off-normal process conditions.

Area radiation monitoring and local alarms within the general areas of the facility radiologically controlled area (RCA) are provided by the RAMS. This nonsafety-related system also provides signals to the FCR to inform operators of abnormal conditions within the facility.

Airborne contamination monitoring within general areas of the facility RCA is performed by the CAMS. The CAMS units are nonsafety-related devices that provide local alarms and provide signals to the FCR to inform operators of the occurrence and approximate location of abnormal conditions.

Normal airborne facility effluents are directed into a single facility stack and are monitored by the stack release monitor. An alternate safety-related vent path for the nitrogen purge system is monitored by the carbon delay bed effluent monitor. These nonsafety-related effluent monitors provide control room indication and alarm. The SHINE facility does not have a normal liquid effluent path from the RCA, and as such no liquid effluent monitoring system is provided.

Criticality accident monitoring and alarm is provided by the facility CAAS. The CAAS provides alarms both locally and within the FCR.

These systems are further described in Section 7.7.

7.1.7 NEUTRON FLUX DETECTION SYSTEM

The NFDS is used for monitoring the reactivity and power of the subcritical assembly system in the IU. The NFDS is a safety-related system with redundant channels of neutron flux detectors. The NFDS detects and provides remote indication of the neutron flux levels during TSV filling and irradiation to determine the multiplication factor and power levels, respectively. The NFDS provides safety-related outputs to the TRPS used for trip determination. The NFDS also provides nonsafety-related outputs to the PICS, which are used for monitoring of conditions within the IU.

Three watertight fission chamber NFDS detectors are provided for each IU, located in the light water pool surrounding the subcritical assembly support structure (SASS).

Three NFDS divisions, designated as Division A, Division B, and Division C, serve each IU cell. The NFDS divisions are powered from safety-related power feeds, and the equipment associated with each NFDS division maintains electrical and physical separation with the other divisions for the same IU cell.

The NFDS is further described in Section 7.8.

Figure 7.1-1 – Instrumentation and Control System Architecture

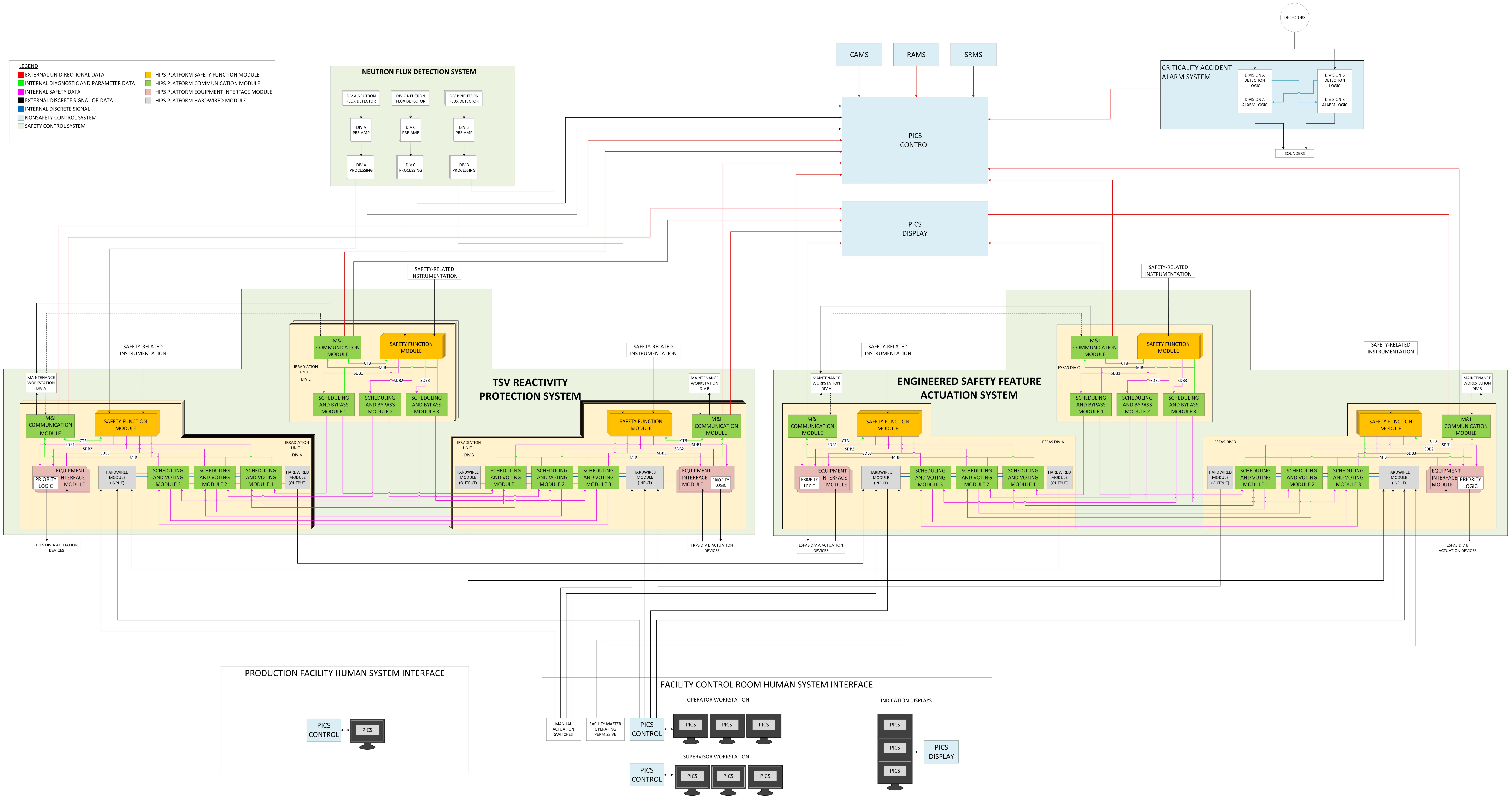

LEGEND
🟥 EXTERNAL UNIDIRECTIONAL DATA
🟩 INTERNAL DIAGNOSTIC AND PARAMETER DATA
🟪 INTERNAL SAFETY DATA
⬛ EXTERNAL DISCRETE SIGNAL OR DATA
🟦 INTERNAL DISCRETE SIGNAL
□ NONSAFETY CONTROL SYSTEM
□ SAFETY CONTROL SYSTEM
🟨 HIPS PLATFORM SAFETY FUNCTION MODULE
🟩 HIPS PLATFORM COMMUNICATION MODULE
▨ HIPS PLATFORM EQUIPMENT INTERFACE MODULE
▨ HIPS PLATFORM HARDWIRED MODULE
NEUTRON FLUX DETECTION SYSTEM
DIV A NEUTRON FLUX DETECTOR
DIV C NEUTRON FLUX DETECTOR
DIV B NEUTRON FLUX DETECTOR
DIV A PRE-AMP
DIV C PRE-AMP
DIV B PRE-AMP
DIV A PROCESSING
DIV C PROCESSING
DIV B PROCESSING
CAMS
RAMS
SRMS
PICS CONTROL
PICS DISPLAY
DETECTORS
CRITICALITY ACCIDENT ALARM SYSTEM
DIVISION A DETECTION LOGIC
DIVISION B DETECTION LOGIC
DIVISION A ALARM LOGIC
DIVISION B ALARM LOGIC
SOUNDERS
SAFETY-RELATED INSTRUMENTATION
TSV REACTIVITY PROTECTION SYSTEM
MAINTENANCE WORKSTATION DIV A
MAINTENANCE WORKSTATION DIV B
M&I COMMUNICATION MODULE
SAFETY FUNCTION MODULE
CTB
SDB1
SDB2
SDB3
MIB
IRRADIATION UNIT 1 DIV A
IRRADIATION UNIT 1 DIV C
IRRADIATION UNIT 1 DIV B
SCHEDULING AND BYPASS MODULE 1
SCHEDULING AND BYPASS MODULE 2
SCHEDULING AND BYPASS MODULE 3
EQUIPMENT INTERFACE MODULE
PRIORITY LOGIC
HARDWIRED MODULE (INPUT)
HARDWIRED MODULE (OUTPUT)
SCHEDULING AND VOTING MODULE 1
SCHEDULING AND VOTING MODULE 2
SCHEDULING AND VOTING MODULE 3
TRPS DIV A ACTUATION DEVICES
TRPS DIV B ACTUATION DEVICES
ENGINEERED SAFETY FEATURE ACTUATION SYSTEM
ESFAS DIV A
ESFAS DIV C
ESFAS DIV B
ESFAS DIV A ACTUATION DEVICES
ESFAS DIV B ACTUATION DEVICES
PRODUCTION FACILITY HUMAN SYSTEM INTERFACE
PICS CONTROL
PICS
FACILITY CONTROL ROOM HUMAN SYSTEM INTERFACE
MANUAL ACTUATION SWITCHES
FACILITY MASTER OPERATING PERMISSIVE
OPERATOR WORKSTATION
SUPERVISOR WORKSTATION
INDICATION DISPLAYS
PICS CONTROL
PICS DISPLAY
PICS

Figure 7.1-2 – Target Solution Vessel Reactivity Protection System Architecture

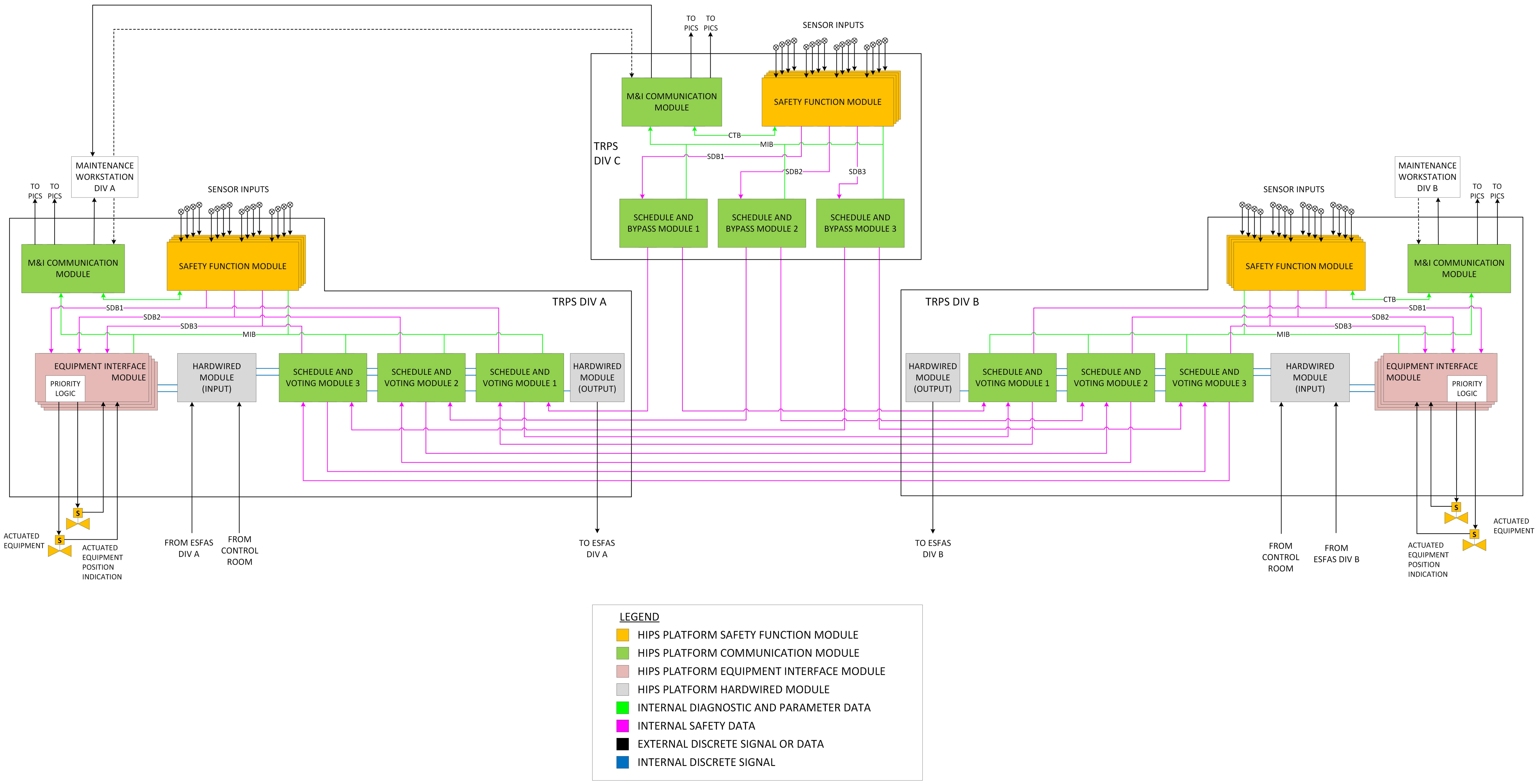
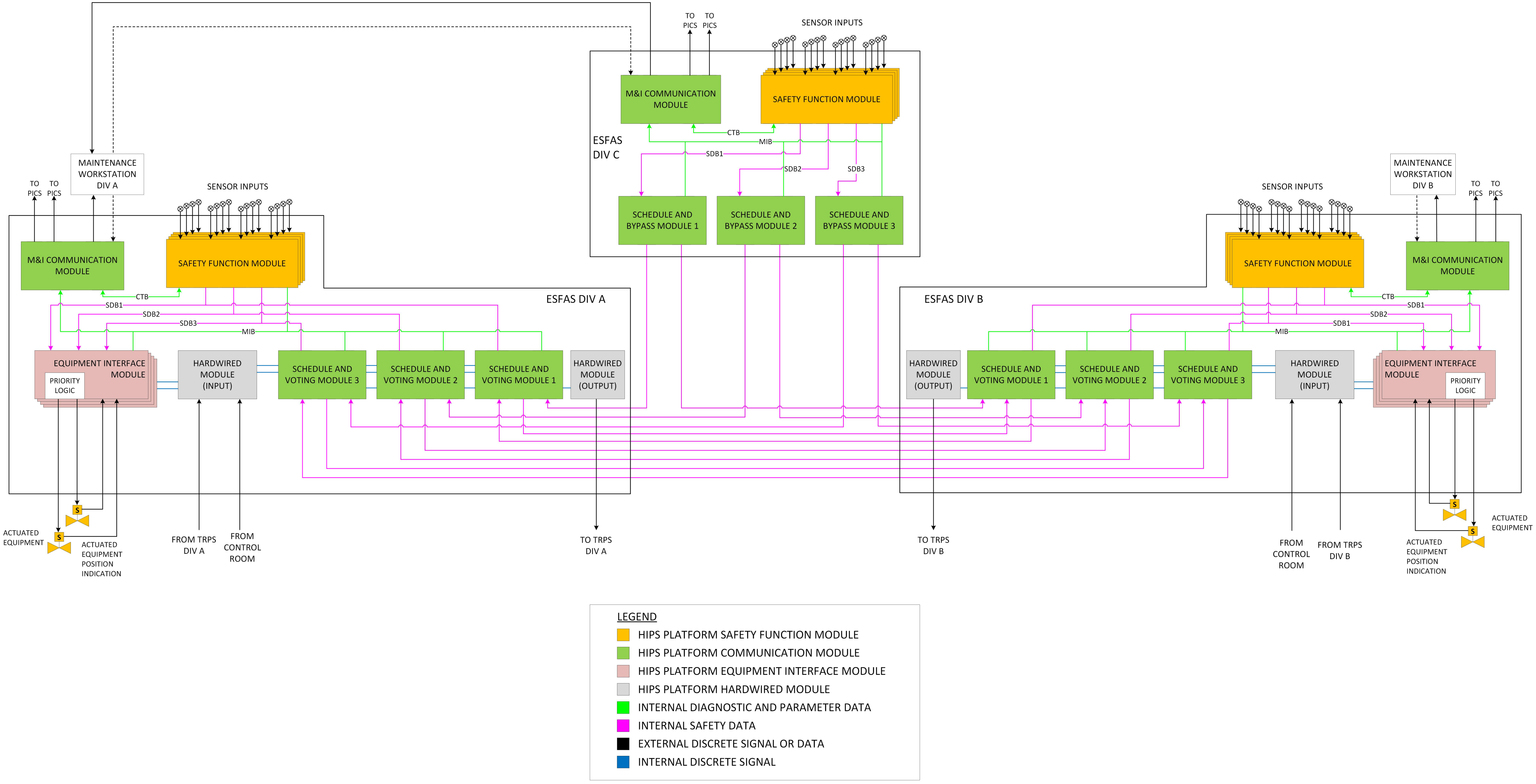

TO PICS
TO PICS
SENSOR INPUTS
M&I COMMUNICATION MODULE
SAFETY FUNCTION MODULE
CTB
MIB
SDB1
SDB2
SDB3
TRPS DIV C
SCHEDULE AND BYPASS MODULE 1
SCHEDULE AND BYPASS MODULE 2
SCHEDULE AND BYPASS MODULE 3
MAINTENANCE WORKSTATION DIV A
MAINTENANCE WORKSTATION DIV B
TRPS DIV A
TRPS DIV B
EQUIPMENT INTERFACE MODULE
PRIORITY LOGIC
HARDWIRED MODULE (INPUT)
HARDWIRED MODULE (OUTPUT)
SCHEDULE AND VOTING MODULE 1
SCHEDULE AND VOTING MODULE 2
SCHEDULE AND VOTING MODULE 3
S
ACTUATED EQUIPMENT
ACTUATED EQUIPMENT POSITION INDICATION
FROM ESFAS DIV A
FROM CONTROL ROOM
TO ESFAS DIV A
TO ESFAS DIV B
FROM ESFAS DIV B
LEGEND
🟧 HIPS PLATFORM SAFETY FUNCTION MODULE
🟩 HIPS PLATFORM COMMUNICATION MODULE
🟥 HIPS PLATFORM EQUIPMENT INTERFACE MODULE
⬜ HIPS PLATFORM HARDWIRED MODULE
🟩 INTERNAL DIAGNOSTIC AND PARAMETER DATA
🟪 INTERNAL SAFETY DATA
⬛ EXTERNAL DISCRETE SIGNAL OR DATA
🟦 INTERNAL DISCRETE SIGNAL

Figure 7.1-3 – Engineered Safety Feature Actuation System Architecture


TO PICS
TO PICS
SENSOR INPUTS
M&I COMMUNICATION MODULE
SAFETY FUNCTION MODULE
CTB
MIB
SDB1
SDB2
SDB3
ESFAS DIV C
SCHEDULE AND BYPASS MODULE 1
SCHEDULE AND BYPASS MODULE 2
SCHEDULE AND BYPASS MODULE 3
MAINTENANCE WORKSTATION DIV A
TO PICS
TO PICS
SENSOR INPUTS
M&I COMMUNICATION MODULE
SAFETY FUNCTION MODULE
CTB
SDB1
SDB2
SDB3
MIB
ESFAS DIV A
EQUIPMENT INTERFACE MODULE
PRIORITY LOGIC
HARDWIRED MODULE (INPUT)
SCHEDULE AND VOTING MODULE 3
SCHEDULE AND VOTING MODULE 2
SCHEDULE AND VOTING MODULE 1
HARDWIRED MODULE (OUTPUT)
S
S
ACTUATED EQUIPMENT
ACTUATED EQUIPMENT POSITION INDICATION
FROM TRPS DIV A
FROM CONTROL ROOM
TO TRPS DIV A
MAINTENANCE WORKSTATION DIV B
TO PICS
TO PICS
SENSOR INPUTS
SAFETY FUNCTION MODULE
M&I COMMUNICATION MODULE
CTB
SDB1
SDB2
SDB1
MIB
ESFAS DIV B
HARDWIRED MODULE (OUTPUT)
SCHEDULE AND VOTING MODULE 1
SCHEDULE AND VOTING MODULE 2
SCHEDULE AND VOTING MODULE 3
HARDWIRED MODULE (INPUT)
EQUIPMENT INTERFACE MODULE
PRIORITY LOGIC
S
S
ACTUATED EQUIPMENT
ACTUATED EQUIPMENT POSITION INDICATION
TO TRPS DIV B
FROM CONTROL ROOM
FROM TRPS DIV B
LEGEND
HIPS PLATFORM SAFETY FUNCTION MODULE
HIPS PLATFORM COMMUNICATION MODULE
HIPS PLATFORM EQUIPMENT INTERFACE MODULE
HIPS PLATFORM HARDWIRED MODULE
INTERNAL DIAGNOSTIC AND PARAMETER DATA
INTERNAL SAFETY DATA
EXTERNAL DISCRETE SIGNAL OR DATA
INTERNAL DISCRETE SIGNAL

7.2 DESIGN OF INSTRUMENTATION AND CONTROL SYSTEMS

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

- independence
- redundancy
- predictability and repeatability
- diversity

The design criteria of the I&C systems were derived from the criteria in 10 CFR 50, Appendix A, and 10 CFR 70.64(a), as described in Table 3.1-3, as well as the draft interim staff guidance (ISG) for Chapter 7 of NUREG-1537. The criteria were applied in a graded approach to each I&C system.

7.2.1 DESIGN CRITERIA

The SHINE design criteria are described in Section 3.1. Table 3.1-1 and Table 3.1-2 show how the criteria are applied to each I&C system. Additional design criteria for individual systems and subsystems are provided in Sections 7.3 through 7.8. Codes and standards used in the design of each I&C system are also identified in Sections 7.3 through 7.8.

7.2.2 DESIGN BASES

The design bases for safety-related I&C systems (i.e., target solution vessel [TSV] reactivity protection system [TRPS], engineered safety features actuation system [ESFAS], and neutron flux detection system [NFDS]) were derived using a graded approach from the criteria identified in the draft ISG for NUREG-1537 as they applied to the four fundamental design principles and are described in this subsection.

Modes of operation, safety functions, permissive conditions, monitored variables and their ranges, conditions for manual control, and any other special design bases requirements specific to each of the I&C systems are described in Sections 7.3 through 7.8.

Environmental and radiological parameters for I&C components located in different areas of the facility are provided in Tables 7.2-1 through 7.2-6 and are referred to in Sections 7.3 through 7.8.

Environmental parameters inside the main production facility are maintained by the facility heating, ventilation, and air conditioning (HVAC) systems, which are described in Section 9a2.1.

7.2.2.1 Independence

The physical, electrical, communications, and functional independence attributes are discussed in this subsection.

7.2.2.1.1 Physical Separation

The TRPS and ESFAS structures, systems and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident. Division independence is maintained throughout both systems, 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 for circuits. Separation of wiring is achieved using separate wireways and cable trays for each of Division A, Division B and Division C. Division A and C of the TRPS and ESFAS are located on the opposite side of the facility control room from where Division B is located. Safety-related equipment for different divisions is located in separate fire areas when practicable. Exceptions include components for all three divisions are located in the facility control room, in individual irradiation unit (IU) and TSV off-gas system (TOGS) cells, and in other locations where end devices are installed.

The NFDS divisions are physically separate. The NFDS detectors are installed 120 degrees equidistant around the subcritical assembly structure in relation to the target solution vessel and the cabling is routed in physically separate cable trays and raceways.

7.2.2.1.2 Electrical Isolation

The electrical isolation devices that are used as a safety system boundary are considered part of the safety-related system (i.e., TRPS and ESFAS). The electrical 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 minimum performance requirements.

Electrical isolation between the safety-related and nonsafety-related systems is provided by the following devices:

- Nonsafety-related inputs. The equipment interface module (EIM) provides isolation via galvanic isolation between the nonsafety inputs (e.g., actuation component position indication feedback) and the safety system. The isolation is a passive safety-related feature that does not rely on power to provide the required protection.
- Safety-related to nonsafety-related communication interface. Communication with nonsafety-related systems is provided through transmit-only or receive-only ports, which provide isolation through unidirectional communication links. The monitoring and indication communication module (MI-CM) provides isolation from the safety systems (TRPS or ESFAS) to the nonsafety systems (the process integrated control system [PICS] and the maintenance workstation [MWS]) via communication ports configured as one-way transmit only on the device. A single data port on the MI-CM is configured as receive-only, and can receive information from the MWS through a temporary cable that is connected during maintenance activities.
- Hardwired inputs into the safety-related systems. The hardwired module (HWM) receives signals from the manual switches in the facility control room, discrete hardwired signals from the PICS, and from the safety function module (SFM) trip/bypass switches. The HWM is constructed only from discrete logic components. The HWM provides direct current (DC)-to-DC and galvanic isolation between the TRPS and ESFAS and any input to the HWM.

7.2.2.1.3 Communications Independence

The TRPS and ESFAS each use five separate and independent serial communication bus structures:

- Safety data bus 1 (SDB1)
- Safety data bus 2 (SDB2)
- Safety data bus 3 (SDB3)
- Monitoring and indication bus (MIB)
- Calibration and test bus (CTB)

The communication buses are used for intradivisional communication via a backplane. Each backplane is specific to either the TRPS or ESFAS. The backplane contains point-to-point copper signal traces that are the signal paths for SDB1, SDB2, SDB3, MIB, and CTB. Each bus is separate, asynchronous, and can be active simultaneously and operate independently. The buses use a master-slave protocol, using simple, different RS-485 virtual point-to-point or point-to-multipoint communication.

With exception of the interdivisional voting, the communication within the TRPS and ESFAS division is independent and does not rely on communication from outside the respective division to perform a safety function. The SFM performs independent signal conditioning and trip determination, and provides the result to either the scheduling and voting module (SVM) in Division A and B or the scheduling and bypass module (SBM) in Division C (used for two-out-of-three votes, when provided).

The safety function is processed through three redundant communication modules (CMs) to provide error detection and fault tolerance of the safety function. Data communications going out of or into the highly integrated protection system (HIPS) chassis use one-way isolated communication ports on the CMs. The CMs are part of the safety-related HIPS platform and are considered safety-related modules, isolated from nonsafety-related equipment.

TRPS or ESFAS communication to nonsafety systems is provided by one-way, isolated data communication paths from the MIB. The communication from the TRPS or ESFAS to the PICS or MWS is through a MI-CM in each division. The MWS provides communication to the ESFAS or TRPS using a temporary cable. This communication is only allowed when the SFM is taken out of service by placing the out of service switch on the face plate of the SFM in the "out of service" position.

The NFDS is an analog system with no digital communications. Communication independence with the NFDS is maintained by implementing separate hardwired connections to the TRPS and PICS.

7.2.2.1.4 Functional Independence

The SFMs in ESFAS and TRPS are responsible for both signal conditioning and trip determination from input signals. The trip determination portions of each SFM receive process input values from the signal conditioning portions of that SFM. Each independent SFM is dedicated to implementing one safety function or a limited group of functions. This results in the gate-level implementation of each group of safety functions being different from other safety functions performed on a separate SFM. A removal of one SFM only affects the safety function group that is implemented by that SFM and no other SFM. This design attribute supports functional independence.

The built-in self-test (BIST) feature in the field programmable gate array (FPGA) logic is separate and independent of the FPGA safety function logic; thus, the programming of the FPGA safety function logic is not made more complex by the inclusion of the diagnostic and self-test FPGA logic.

7.2.2.2 Redundancy

Redundancy is used to ensure that the safety-related I&C systems can perform the required safety functions during a design basis event. Redundancy features of the safety-related I&C systems are also used to improve system reliability.

7.2.2.2.1 Redundancy in the Target Solution Vessel Reactivity Protection System and Engineered Safety Feature Actuation System

The safety I&C system platform design includes redundancy in the areas of power, module, communication, equipment interface, and platform. These features ensure that no single failure results in loss of the protection function, and removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

The SFM is designed with three redundant signal paths and begins the communication paths for a two-out-of-three comparison. This internal redundancy provides for easy fault detection, giving higher reliability from spurious actuation without increasing the complexity of the design.

Redundancy within the safety I&C system platform architecture is achieved by employing two or three divisions of sensors, detectors, and trip determination, and two divisions of trip and actuation circuitry. Three divisions of sensors, detectors and trip determination are selected for functions where spurious actuation may significantly impact overall facility operation or for operational convenience; two divisions are used for other functions. Using multiple divisions of sensors and detectors and trip and actuation determination is one of the mechanisms employed to satisfy single-failure criteria and improve system availability.

Coincidence voting on functions with three divisions of trip determination is implemented so that a single failure of an input process signal will not prevent a trip or actuation from occurring when required. In addition, a single failure of an input process signal with three divisions of trip determination will not cause spurious actuation or inadvertent trips or actuations when they are not required. Figures 7.1-2 and 7.1-3 show typical signal data flow paths in the HIPS platform.

The following features are provided to improve the reliability of the systems:

- The equipment chassis provide for redundant auctioneered DC power feeds to supply both the general logic design and the FPGA core supply power requirements. Fuses are used to protect the modules from cases of severe overcurrent and board failures.
- The safety I&C system platform provides triple redundant communication paths. These redundant paths provide fault tolerance and the ability to replace a CM on line without causing a trip or actuation. From the output of the input submodule to the EIM voting, the three redundant safety data signal paths remain independent and redundant.
- The safety I&C system platform provides redundant EIMs. These parallel EIMs allow for more thorough testing and equipment removal, thus providing a higher reliability of the field components from spurious actuation.

7.2.2.2.2 Redundancy in the Neutron Flux Detection System

Redundancy within the NFDS platform is achieved by utilizing three divisions of detectors, amplifiers and process circuits.

7.2.2.3 Predictability and Repeatability

The behavior of the functions within the FPGA of each module is deterministic. Deterministic behavior allows implementation of a simple communication protocol using a predefined message structure with fixed time intervals. This simple, periodic communication scheme is used throughout the architecture. Communication between modules within a chassis is implemented through an RS-485 physical layer. The configurable transmit-only or receive-only ports on a CM use a point-to-point physical layer. Communication between modules is done asynchronously, which simplifies implementation by avoiding complex syncing techniques.

Process input values are communicated using a deterministic path and are provided to a specific SFM. Input values are converted to engineering units to determine what safety function or group of safety functions is implemented on that specific SFM. The SFMs make a trip determination using the engineering units. A trip determination is based on a predetermined set point and provides a trip or no-trip demand signal to each actuation division through an isolated transmit-only serial data path.

The I&C safety system platform uses a virtual point-to-point connection of the trip decision to the voting level of the architecture. It also uses the point-to-multipoint arrangement achieved within a master-relay-to-slave-relay connection.

Each SVM of the two actuation divisions receives inputs from the trip determination portions of the SFMs through isolated receive-only serial data paths. The trip determinations are combined in the voting logic so that two or more trip inputs from the trip determination modules produce an actuation output demand signal, which is sent to dedicated actuation and priority logic (APL) circuits to actuate the appropriate equipment associated with that division. Manual trip and actuation capability also provide a direct trip or actuation of equipment, as well as input to the automatic portion of the system, to ensure the sequence is maintained.

Continuous self-test and calibration checks are performed on the analog input submodule analog to digital converters. These tests verify the calibration of the analog portion and that the input submodule is working. The continuous calibration check verifies that the analog to digital converter is within the desired accuracy and that it has not drifted out of calibration. These features support the predictable and repeatable platform design.

The FPGA functions on the EIM consist of deterministic-state machines. The EIM uses discrete logic for the actuation and priority logic, high-drive switching outputs, hard-wired signals, and equipment feedback circuitry. This architecture performs manual actuations downstream of any programmable logic. The EIM is a slave module to the three SVMs and the MI-CM. The EIM uses the FPGA device to implement the logic circuits for automatic trip signal voting, handling of the indication and diagnostic information, and bus communication logic. The EIM is equipped with eight high-drive switching outputs. The high-drive output is implemented as a redundant output, where a single failure in one of the driving components is automatically detected and mitigated without affecting the output operation.

The HIPS platform design requires each task to be performed under well-defined and deterministic timing. Figure 7.2-1 shows the timing of transferring a division's partial trip determination actuation (PTDA) from the SFM to the EIM. The timing diagram is focused on the programmable logic portion. The blue line indicates that t1 and t2 are asynchronous. The diagram includes the analog input delay on the left and the analog output delay on the right side. These analog delays are dependent on the application and are simply added to the overall timing calculation. The diagram also shows the logic delays of the modules that are included in the transaction times. These logic delays are very small compared to the communications timing; as such, they are added as an element in the worst-case timing calculation.

To meet a response time performance requirement of 500 ms, a HIPS platform-based system must acquire the input signal that represents the start of a response time performance requirement, perform logic processing associated with the response time performance requirement, and generate an output signal that represents the end of a response time performance requirement. These HIPS platform response time components exclude (1) the earlier plant process delays through the sensor input to the platform, and (2) the latter delays through a final actuating device to affect the plant process. The required response times for the TRPS and ESFAS, which cover the analog delays, logic delays, and times t1 and t2 of Figure 7.2-1, are provided in Sections 7.4 and 7.5, respectively.

7.2.2.4 Diversity

The HIPS platform provides functional diversity with the use of different protection logic on each SFM in order to implement the unique safety function(s) assigned to that SFM. As a result, programmable logic design for an SFM is unique when compared to the protection logic for any other SFM. A failure of an SFM would be limited to the safety functions of that SFM and would not prevent other SFMs from performing their safety functions.

7.2.2.5 Simplicity

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

Simplicity has been considered throughout the development of the TRPS, ESFAS, and NFDS systems. The I&C system architecture is consistent with proven safety systems designs used for nuclear production facilities.

The HIPS technology used for the TRPS and ESFAS is based on only four core modules. The use of FPGA technology allows for modules to perform a broader range of unique functions yet utilize the same core components. Increased flexibility with core components provides simplified maintainability. The quantity of spare parts can be reduced to blank modules that are programmed and configured as needed.

Functions within the FPGA of each module are implemented with finite state machines in order to achieve deterministic behavior. The HIPS platform does not rely on complex system/platform controllers. Dedicating SFMs to a function or group of functions based on its input provides inherent function segmentation creating simpler and separate SFMs that can be more easily tested. This segmentation also helps limit module failures to a subset of safety functions.

The physical layer of a CM used for intradivisional communication is a multidrop topology; however, the flexibility afforded by FPGAs allows implementation of a simple virtual point-to-point communication protocol. Autonomous modules allow for simpler component testing, implementation, and integration.

Use of fundamentally different FPGA architectures provides a simple and verifiable approach to equipment and design diversity. By simply implementing safety functions on an SFM based on its inputs, safety functions have been segmented to provide functional diversity. The discrete and programmable logic circuits on an EIM provide a clear distinction between those portions that are and are not vulnerable to a software common cause failure (CCF). These diversity attributes simplify the TRPS and ESFAS systems design by not having to install a separate diverse actuation system to address software CCF concerns.

Implementation of triple redundant communication within a division of a HIPS platform increases the number of components (e.g., additional communication modules) but provides simpler maintenance and self-testing. A single communication path would be vulnerable to undetectable failures. Failure of a data path or CM with triple redundant communication is simpler in comparison. A single failure does not cause all safety functions of that division to be inoperable.

Functions within the FPGA of each module are implemented with finite state machines in order to achieve deterministic behavior. Deterministic behavior allows implementation of a simple communication protocol using a predefined message structure with fixed time intervals. This simple periodic communication scheme is used throughout the architecture. Communication between SFMs and CMs is implemented through a simple and well-established RS-485 physical layer. The configurable transmit-only or receive-only ports on a communication module use a point-to-point physical layer. Communication between modules is done asynchronously which simplifies implementation by avoiding complex syncing techniques.

The NFDS is an analog system with no digital communications.

7.2.3 SYSTEM DESCRIPTION

In the SHINE facility, instrumentation and controls are composed of the following systems:

- PICS
- TRPS
- ESFAS
- facility control room control consoles and displays
- radiation monitoring, including
  - the radiation area monitoring system (RAMS)
  - the continuous air monitoring system (CAMS)
  - safety-related process radiation monitoring considered part of the ESFAS and tritium purification system (TPS)
  - nonsafety-related process radiation monitoring included within individual process systems
  - the stack release monitoring system (SRMS)
  - the criticality accident alarm system (CAAS)
- NFDS

A simplified block diagram of the overall I&C system architecture is provided in Figure 7.1-1.

Detailed descriptions of the above systems, including equipment and major components, control and protection system development processes, and operational, support and operator interface requirements are provided in Sections 7.3 through 7.8.

SHINE uses a documented methodology for establishing and calibrating setpoints for safety-related I&C functions. A combination of statistical and algebraic methods is used to combine instrument uncertainties to determine the total instrument loop uncertainty for each setpoint. The methodology considers both random and non-random uncertainties, and considers process measurement and miscellaneous effects uncertainties, sensor uncertainties, and protection system processing uncertainties. The methodology is used to ensure an adequate margin exists between analytical limits and instrument setpoints so that protective actions are initiated before safety limits are exceeded.

7.2.4 SYSTEM PERFORMANCE ANALYSIS

This section includes performance analysis information related to the HIPS platform, which is used for both the TRPS and ESFAS safety-related control system. Information specific to the TRPS and ESFAS is contained in Sections 7.4 and 7.5, respectively. Performance analysis information related to other I&C systems is contained in Sections 7.3, 7.6, 7.7 and 7.8.

Diagnostic and maintenance features provided by the HIPS platform features include the use of BIST, cyclic redundancy checks (CRC), periodic surveillance testing, and other tests in each type of module, as appropriate, to verify normal operation.

In-chassis calibration of the defined setpoints and tunable parameters can be performed for the SFM. Other modules are only capable of maintenance changes when taken out of the chassis. The calibration uses the MWS as the primary interface. The CMs do not require calibration. There are no setpoints and tunable parameters in the CM that need monitoring. Calibration of the SFM involves the analog input submodules. The discrete input submodule does not require calibration.

The HIPS platform has end-to-end self-testing that covers each module from sensor input to the output switching logic (except for the discrete circuitry of the APL). The individual self-tests on the different components of the HIPS platform evaluate whether the entire platform is functioning correctly. The APL (which contains discrete logic) periodic surveillance testing, as required in the technical specifications, determines if the APL is functioning correctly. In the overlap method, the modules check if each module is functioning correctly, and the error checking on the communication buses verifies that the transfer of data is correct.

The surveillance testing on analog and temperature input submodule (ISM) types uses the MWS as the primary test interface. Self-testing for an SFM with a discrete ISM is sufficient for checking the performance of the submodule, since there are no calibration requirements. The self-testing for a discrete input submodule verifies pins for "stuck low," "stuck high," "shorts," or "open."

Self-testing performed by the SFM includes the following:

- SFM BIST including startup and operational testing of the FPGA and nonvolatile memory (NVM)
- SFM FPGA voltage checks during startup and operation
- SFM monitors work-cycle performance

- SFM ISM analog and temperature signal self-testing and auto calibration
- SFM ISM discrete input self-testing

Self-testing performed by the EIM includes the following:

- EIM BIST including startup and operational testing of the FPGA and NVMs
- EIM FPGA voltage checks during startup and operation
- EIM monitors work-cycle performance
- the data message error checking
- discrete input operation self-testing
- high-drive output self-testing
- two-out-of-three voting logic for the three safety data bus inputs

The CMs do not require surveillance testing. Self-testing of the logic is incorporated into the BIST feature provided by the FPGA the logic is built into. The data message error checking also detects any failures that may occur in the CM.

The BIST feature in the FPGA logic is separate and independent of the FPGA safety function logic; thus, the programming of the safety function FPGA logic is not made more complex by the inclusion of the diagnostic and self-test FPGA logic.

FPGAs on the SFM and EIM use the BIST feature provided by the FPGA. The BIST in a static random-access memory-based FPGA is used for checking the functionality of the NVM and the FPGAs included on each module. The BIST checks both the NVM and the FPGA upon startup and continuously during normal operation. NVM and FPGA self-test errors during startup result in vital faults. The BIST in a one-time programmable or flash-based FPGA does not check the logic configuration because the logic in this type of FPGA is a fixed configuration. Once this configuration is established, it remains fixed when the FPGA is powered or when it is not powered.

The communication integrity self-testing performed on the SDBs (i.e., redundancy failure detection, synchronization/timing failure detection, CRC failure detection, and protocol failure) detects communication errors caused by an upstream module, communication data links, or communication processing with the module itself.

Verification of the integrity of the communicated information between modules by CRC check is another type of test provided by the HIPS platform. This capability includes a high degree of fault detection on the HIPS bus, since the data that is sampled on the bus must match the calculated value and must be there at the correct time of the HIPS bus transaction to be declared valid.

Verification of the integrity of the NVM memory by CRC check is another type of self-test provided by the HIPS platform. This capability during startup and operation includes an automatic check to ensure that NVM has not been changed or corrupted.

The performance of the core logic within the SFM FPGA, as well as the SDB communications buses, can be monitored by reviewing the results of the periodic injection of a PTDA test signal into one core logic within the SFM FPGA in a round robin fashion. The effects of the PTDA can be observed by reviewing actuation status data information transmitted out of the HIPS platform using the MIB. The test injection can be used to confirm that the core logic and the SDBs are functioning correctly from the SFM output through the two-out-of-three triple modular redundant voting in the EIM. The periodic injection of the PTDA test signal has no adverse impact on the safety function of the division, since the other two core logics and SDBs not being tested remain fully functional and can process PTDA decisions made in the SFM logic.

The HIPS platform has design features that directly support methods to perform cross-checking between redundant safety-system channel sensors or between sensor channels that bear a known relationship to each other. The HIPS platform design features use coincidence logic support implementation of application-specific diagnostic logic and confirmation of continued execution with the use of the MWS.

HIPS modules include light emitting diodes that are used to determine the state of the module latches, the operational state of the module, and the presence of any faults. The HIPS platform self-testing features and the associated front panel light emitting diodes allow for the timely identification of certain malfunctions within the HIPS equipment.

7.2.5 ACCESS CONTROL AND CYBER SECURITY

The safety-related control systems, TRPS and ESFAS, are implemented using the HIPS platform. Access control and cyber security requirements described in this section, which consist of the secure development and operating environment, are applied to these safety-related control systems. Access control and cyber security requirements for the nonsafety-related PICS are described in Section 7.3.

7.2.5.1 Secure Development Operating Environment

The developmental process for the TRPS and ESFAS has been delegated to SHINE's safety-related control system vendor. The process addresses the potential cyber security vulnerabilities (physical and electronic) in the developmental phases of the software and the controls to prevent unauthorized physical and electronic access. The secure development controls are applied from developing the requirements of the software, designing the software, integrating the hardware and software, and testing the system. The development controls include physical access controls at the development facility, personnel access controls that limit access to the TRPS and ESFAS design information to authorized individuals, and the use of an isolated development network (IDN).

The HIPS platform contains design features that reduce the susceptibility to inadvertent access to both hardware and software and undesirable behavior from connected systems. These platform features support the establishment and use of a secure operational environment and protective measures to maintain it.

Specific requirements are defined for the TRPS and ESFAS that provide and maintain a secure operational environment during the defined modes of operation. A requirements traceability matrix is used throughout the development process. Bi-directional traceability is independently verified to ensure that requirements are implemented (forward tracing) and that no unwanted or unnecessary code has been introduced (backward tracing).

7.2.5.2 Cyber Security Design Features

The TRPS and ESFAS are designed using a defensive system architecture, as shown in Figure 7.1-1.

The defensive system architecture has the following characteristics:

- Communication outside of the TRPS and ESFAS system while in service is through one-way isolated communication ports over point-to point cables.
- Communication ports that are for communication outside of a HIPS chassis implement the one-way communication with hardware.
- Communication from an MWS to a HIPS chassis is only allowed when the affected module is placed out of service by activating the out of service (OOS) switch using a temporary cable that is attached from the MWS to a HIPS chassis.
- No capability for remote access to the safety system is included with the HIPS platform design.

7.2.5.3 Access Control

The TRPS and ESFAS have additional access control features:

- TRPS and ESFAS require a physical key at the main control board to prevent unauthorized use of the TRPS and ESFAS.
- TRPS and ESFAS rack mounted equipment are installed within cabinets that can be locked so access can be administratively controlled.
- FPGAs on any of the HIPS modules cannot be modified (for static random-access memory type) or replaced (for one-time programmable or flash types) while installed in the HIPS chassis.
- Capability to modify modules installed in the HIPS chassis is limited to setpoints and tunable parameters that may require periodic modification.

Each division of TRPS and ESFAS systems has a nonsafety-related MWS for the purpose of online monitoring and offline maintenance and calibration. The HIPS platform MWS supports online monitoring through one-way isolated communication ports. The MWS is used to update setpoints and tunable parameters in the HIPS chassis when the safety function is out of service. Physical and logical controls are put in place to prevent modifications to a safety channel when it is being relied upon to perform a safety function. A temporary cable and OOS switch are required to be activated before any changes can be made to an SFM. When the safety function is removed from service, either in bypass or trip, an indication is provided by the HIPS platform that can be used to drive an alarm in the facility control room to inform the operator. Adjustments to parameters are performed in accordance with facility technical specifications, including any that establish the minimum number of redundant safety channels that must remain operable for the applicable operating mode and conditions.

7.2.6 SOFTWARE REQUIREMENTS DEVELOPMENT

The TRPS and ESFAS are designed and implemented using a programmable logic-based I&C platform that is based on fundamental safety-related I&C design principles of independence, redundancy, predictability and repeatability, and diversity, and was developed specifically to provide a simple and reliable solution for safety-related applications. These design principles help contribute to simplicity in both the functionality of the system and in its implementation.

The TRPS and ESFAS are implemented on a logic-based platform that does not utilize traditional software or microprocessors for operation. It is composed of logic implemented using discrete components and FPGA technology. The platform design was developed to support meeting the guidelines and the requirements of NRC Regulatory Guides and Institute of Electrical and Electronics Engineers (IEEE) standards applicable to safety-related applications. The HIPS platform has been reviewed and approved by the NRC for use in safety-related applications for commercial nuclear power plants (NuScale, 2017).

The development of the TRPS and ESFAS have been delegated to SHINE's safety-related control system vendor. Any modifications to the TRPS or ESFAS logic required to be implemented after initial development activities are complete are also delegated to the vendor.

The TRPS and ESFAS are developed using the vendor's Project Management Plan, which describes a planned and systematic approach to design, implement, test, and deliver the TRPS and ESFAS. The approach defines the technical and managerial processes necessary to develop high-quality products that satisfy the specified requirements.

The TRPS and ESFAS are developed in accordance with the vendor's Project Quality Assurance Plan, which defines the techniques, procedures, and methodologies used to develop and implement the TRPS and ESFAS.

7.2.6.1 Key Responsibilities

SHINE is responsible for providing oversight of the vendor, verifying deliverables are developed in accordance with approved quality and procurement documents, and maintaining the vendor as an approved supplier on the SHINE approved supplier list.

The vendor is responsible for developing and delivering the TRPS and ESFAS control systems in accordance with the processes identified in this section.

The key responsibilities for the TRPS and ESFAS activities are identified in the vendor's Project Management Plan and project implementing procedures.

7.2.6.2 Programmable Logic Lifecycle Process

The TRPS and ESFAS programmable logic lifecycle process shown in Figure 7.2-2 provides an overview of the programmable logic development process from planning through installation. The programmable logic lifecycle process is implemented through the vendor system design control procedure. The procedure defines the minimum system design control tasks from the planning phase through the shipment phase.

Design interfaces are established during the design development process, and during the design review and approval process. Design interfaces are controlled in accordance with the Project Management Plan.

7.2.6.2.1 Planning Phase

SHINE procurement and technical documents (e.g., specifications, drawings, input/output database, etc.) are inputs to the planning phase. These documents are reviewed by the vendor to identify design input documents containing TRPS and ESFAS requirements. The design input documents are formally received from SHINE and controlled by version and date. Design output documents and data required by SHINE are identified and scheduled for development.

A system requirements specification (SyRS) that defines the system design requirements detail is generated. The SyRS is generated in accordance with the vendor system requirements specification development procedure. A system design description is generated to define the system design details.

Planning documents for the implementation of the programmable logic lifecycle process are developed:

- Project Configuration Management Plan
- Project Verification and Validation (V&V) Plan
- Project Equipment Qualification Plan
- Project Test Plan
- Project Security Plan
- Project Integration Plan

Planning phase documents are verified and processed in accordance with the vendor design document and data control procedures.

7.2.6.2.2 Requirements Phase

A hardware requirements specification (HRS) is generated by the vendor to define the system hardware requirements detail. The HRS is generated in accordance with the vendor hardware requirements specification development procedure.

A programmable logic requirements specification (PLRS) is generated to translate the conformed design specification into project-specific programmable logic requirements. The PLRS is generated in accordance with the vendor programmable logic requirements specification development procedure.

The PLRS is reviewed in accordance with the vendor verification process procedure.

Programmable logic lifecycle activities from this point forward are performed within a secure development environment (SDE) using an IDN. Exceptions for the use of an SDE and IDN may be specified by management in accordance with contract requirements and/or regulatory requirements, as defined in the vendor SDE and IDN Security Plan.

The PLRS defines what the programmable logic should do, but not how the programmable logic meets the requirements. The complete description of the functions to be performed by the programmable logic are included in the PLRS.

When the programmable logic requirements are expressed by a requirement specification model, the model elements are categorized as either:

- Model elements that represent programmable logic requirements including derived requirements, or
- Model elements that do not represent programmable logic requirements.

The requirement specification model is developed to define the programmable logic functionality in accordance with the vendor model-based development procedure and reviewed in accordance with the vendor verification process procedure.

7.2.6.2.3 Design Phase

The input documents to the design phase are the SyRS, HRS, and PLRS.

A hardware design specification is generated to define the system hardware design details. The hardware design specification is generated in accordance with the vendor hardware design specification development procedure.

A programmable logic design specification (PLDS) is generated to translate the PLRS into:

- A description of the functional requirements
- A description of the system or component architecture
- A description of the control logic, data structures, input/output formats, interface descriptions, and algorithms

The PLDS is generated in accordance with the vendor programmable logic design specification development procedure and reviewed in accordance with the vendor verification process procedure.

In the case when a programmable logic design specification is expressed by a design specification model, model elements that do not represent programmable logic requirements or architecture and are not input to a subsequent development activity may be included in a model (for example, comment elements). These elements will not be implemented in the executable code and therefore need to be clearly identified. Model elements are categorized as described in the vendor model-based development procedure as either:

- Model elements that represent programmable logic design, including derived requirements or architecture, or
- Model elements that do not represent programmable logic design or architecture.

Design specification models are developed in accordance with the vendor model-based development procedure and are traceable, verifiable, and consistent.

Independent design review is performed to verify that the system design meets TRPS and ESFAS requirements in accordance with the vendor verification process procedure. Design tests are performed to validate that the system design meets TRPS and ESFAS requirements in accordance with the vendor test control procedure.

7.2.6.2.4 Implementation Phase

The input documents to the implementation phase are the completed tasks and approved documents from the development phase. Although implementation phase activities may proceed, the outputs from the implementation phase are not approved until the development phase documents are approved.

The HIPS platform hardware and programmable logic components are integrated into the project during this phase to provide the target hardware and incorporate the HIPS platform programmable logic that has been previously designed, developed, tested, qualified and implemented.

The implementation phase ends at the completion of the programmable logic design, development, and verification. Exit to the test phase occurs when the completed programmable logic is ready for validation on target hardware.

The implementation phase V&V summary report documents the implementation phase exit. If control point exit criteria are not met, a conditional release can be issued in accordance with the vendor conditional release procedure prior to beginning test phase activities.

Approved documents ready for V&V are placed into configuration management prior to implementation phase exit.

7.2.6.2.5 Test Phase

The test phase is the validation phase. Outputs from this phase, which are requirements of the project but may not serve as inputs to the shipment phase, are completed prior to test phase exit.

Verification that test phase tasks are complete and output documents are approved serves as the control point to transition the project from the test phase to the shipment phase. The test phase V&V summary report documents the test phase exit. Proceeding beyond the control point before control point exit criteria are met adds risk to the successful completion of the project. If control point exit criteria are not met, a conditional release may be issued in accordance with the vendor conditional release procedure prior to the shipment phase.

Approved documents are placed into configuration management prior to test phase exit.

7.2.6.2.6 Shipment Phase and Installation

The shipment phase prepares the system for shipment and ships the system to SHINE. Output documents from this phase are completed prior to shipment phase exit.

The shipment phase V&V summary report is completed. The final V&V report documents the completed project V&V activities.

Shipment phase documents are verified to be complete and approved prior to transitioning the project from the shipment phase.

Approved documents are placed into configuration management prior to shipment phase exit.

Systems are installed and site acceptance tests are performed in accordance with written plans and instructions prepared and controlled under the installer's quality assurance program. SHINE is responsible for providing oversight of the installer and maintaining the installer as an approved supplier on the SHINE approved supplier list.

7.2.6.3 Programmable Logic Regression Analysis

Initial release of a PLRS or PLDS does not require regression analysis. Subsequent releases of PLRS or PLDS require regression analysis to determine the required independent verification and validation activities to perform. Regression analysis is performed if changes are made to previously tested programmable logic to determine the impact to all parts of the system. This regression analysis occurs prior to the execution of tests. Any tests based on the identified changes and impact analysis to detect any possible errors due to the recent changes are rerun. When the programmable logic requirements are expressed by a requirement specification model or programmable logic design is expressed by a design specification model, the regression analysis is performed in accordance with vendor model-based development procedure.

7.2.6.4 Project Requirements Traceability Matrix

A TRPS and ESFAS requirements traceability matrix is developed by the vendor during each of the project phases. These traceability matrices are used for the traceability analysis tasks in each respective phase. The TRPS and ESFAS requirements traceability matrices are developed in accordance with the vendor traceability matrix development procedure.

When using model-based development, identification of requirements in accordance with the method defined in the vendor traceability matrix development procedure and vendor modeling standards document are used for bi-directional traceability between model elements and requirements external to the model.

7.2.6.5 Verification and Validation

SHINE has delegated verification and validation activities related to the safety-related control system development to the vendor. The TRPS and ESFAS vendor Project Verification and Validation Plan is designed to detect and report errors that may have been introduced during the system development process. The programmable logic verification process verifies that:

- System requirements allocated to programmable logic have been developed into programmable logic requirements that satisfy those system requirements.
- Programmable logic requirements have been developed into logic architecture and design that satisfy the programmable logic requirements.
- Logic architecture and design have been developed into code that satisfies the logic architecture and design.
- Developed code satisfies the requirements and provides confidence that there is no unintended functionality.
- Developed code is robust such that it can respond properly to abnormal inputs and conditions.
- Methods used to perform this verification are technically correct and complete for the specified programmable logic integrity level.

IEEE Standard 1012-2004 (IEEE, 2004a), Standard for Software Verification and Validation, Section 4, provides guidance on selection of criticality levels for software based on its intended use and application. The software and hardware developed for the TRPS and ESFAS are classified as Software Integrity Level 2. The vendor Project Verification and Validation Plan for the TRPS and ESFAS system development was tailored and adapted for FPGA technology from the guidance in IEEE Standard 1012-2004 (IEEE, 2004a). The V&V activities for the TRPS and ESFAS are commensurate with the expectations for a Software Integrity Level 2 classification.

The V&V activities are performed using an internal verification and validation team from within the design organization as defined in IEEE Standard 1012-2004 (IEEE, 2004a), Annex C.4.4. It is recommended, but not required, that the personnel performing the V&V activities are not the same personnel involved directly in the design. The V&V team is independent of the design team with both teams in the same reporting structure. This organization structure was selected taking into consideration the Software Integrity Level 2 classification of the project scope and the size of the vendor organization.

For the lifecycle phases described in IEEE Standard 1012-2004 (IEEE, 2004a), the lifecycle phases applicable to the vendor work scope are the management and development phases. The V&V development phase activities follow the TRPS and ESFAS development lifecycle as described in Subsection 7.2.6.2.

The V&V team is responsible for determining the extent to which a V&V task is repeated when its input or procedure is changed. Design changes are subject to design control measures commensurate with those applied to the original design per the vendor system design control procedure.

V&V personnel review each design output at the end of its life cycle phase, prior to approving the deliverable. Revision control is performed in accordance with the TRPS and ESFAS Project Configuration Management Plan.

Data and document reviews are performed in accordance with the vendor verification process procedure and testing activities are performed in accordance with the vendor test control procedure.

The TRPS and ESFAS requirements traceability matrices are used to generate comprehensive validation test procedure(s) that ensure that each requirement is adequately tested and meets the TRPS and ESFAS requirements. Test procedure(s) are generated by V&V personnel.

7.2.6.5.1 Management Phase V&V

The V&V effort performs the following V&V tasks for management of V&V:

- Project Verification and Validation Plan Generation
- Baseline Change Assessment
- Management Review of V&V
- Management and Technical Review Support
- Interface with Organizational and Supporting Processes

7.2.6.5.2 Planning Phase V&V

Verification of the programmable logic planning process is conducted to ensure that the project plans and procedures comply with the requirements and guidelines of the development standards and regulatory requirements, and that means are provided to execute the plans.

The objectives of the planning phase verification are to:

- Determine that the V&V methods enable the objectives of the development standards and regulatory guidelines.
- Verify that the development processes can be applied consistently.
- Verify that each development process produces evidence that its outputs can be traced to their activity and inputs, showing the degree of independence of the activity, the environment, and the methods used.

7.2.6.5.3 Requirements Phase V&V

The requirements phase reviews and analysis activities detect and report requirements errors that may have been introduced during the requirements process. These reviews and analysis activities confirm that the programmable logic requirements satisfy the following objectives:

- Compliance with system requirements
- Accuracy and consistency
- Compatibility with the target hardware
- Testability
- Conformance to applicable standards and procedures
- Traceability

7.2.6.5.4 Design Phase V&V

The design phase review and analysis activities detect and report design errors that may have been introduced during the programmable logic design process. These reviews and analysis activities confirm that the programmable logic design satisfies the following objectives:

- Compliance with programmable logic requirements
- Accuracy and consistency
- Compatibility with the target hardware
- Testability
- Conformance to applicable standards and procedures
- Traceability

Verification of the design can be divided into two types: functional verification and timing verification. Functional verification only considers whether the logic functions of the design meet the requirements and can be done by simulation or formal proof. Timing verification considers whether the design meets the timing constraints and can be performed using dynamic timing simulation or static timing analysis.

White-box testing techniques are used for analyzing application programmable logic during verification activities.

7.2.6.5.5 Implementation Phase V&V

The implementation phase review and analysis activities detect and report errors that may have been introduced during the coding process. Primary concerns include correctness of the code with respect to programmable logic requirements, design, and conformance to coding standards. These reviews and analysis are confined to the code and confirm that the code satisfies these objectives:

- Compliance with programmable logic design
- Compliance with the programmable logic architecture
- Testability
- Conformance to standards
- Traceability
- Accuracy and consistency

Verification of the design can be divided into two types: functional verification and timing verification. Functional verification only considers whether the logic functions of the design meet the requirements and can be done by simulation or formal proof. Timing verification considers whether the design meets the timing constraints and can be performed using dynamic timing simulation or static timing analysis.

White-box testing techniques are used for analyzing application programmable logic during verification activities.

7.2.6.5.6 Test Phase V&V

The purpose of the test phase V&V is to uncover errors that may have been introduced during the development processes. Testing objectives include the development and execution of test cases and procedures to verify the following:

- Code complies with the PLRS
- Code complies with the PLDS
- Code is robust
- Code complies with the target hardware

Black-box testing techniques are used to execute functional checks on the system components during system testing.

7.2.6.6 Configuration Management

7.2.6.6.1 Development Phase Configuration Management

Configuration management of the development of safety-related control systems has been delegated to the vendor and is applied to data and documentation used to produce, verify, test, and show compliance with the programmable logic used in the TRPS and ESFAS. The programmable logic configuration management process is described in this subsection.

Configuration identification is the first activity of configuration management. Configuration identification identifies items to be controlled, establishes identification schemes for the items and their versions, and establishes the tools and methods to be used in acquiring and managing controlled items. Configuration identification provides a starting point for other configuration management activities. Configuration identification provides the ability to:

- Identify the components of the system throughout the development process, and
- Trace between the programmable logic and its development process data.

Each configuration item is uniquely identified. The identification method includes a naming convention with version numbers or letters. The configuration identification facilitates storage, retrieval, tracking, reproduction, and distribution of configuration items. The following configuration items are identified and are placed under configuration management:

- Design input documents
- Design output documents
- System requirements specifications
- System design specifications

- System hardware design specifications
- Programmable logic requirements documents
- Programmable logic requirements models
- Programmable logic design models
- Programmable logic hardware description language code
- Verification and validation data and documents
- Programmable logic development environment
- Change requests including customer deviation / exception requests and interim change notices
- Third-party vendor supplied documents
- Third-party vendor supplied software

The TRPS and ESFAS vendor Configuration Management Plan specifies a numbering scheme for project data and documents.

The integrated development environment (IDE) tool is used to store and manage configuration items. Configuration items such as data, requirements, models, code files, reports, and tests are stored and placed under source control in the IDE tool. The IDE tool is used to perform the following configuration management activities:

- Review changes in modified files
- Run impact analysis
- Run project integrity checks
- Commit modified files into source control
- Discard modifications made to committed files
- Retrieve configuration items from source control
- Revert to a previous version of a file
- View and report configuration item source control information

Configuration baselines are established at various points in the project. A baseline is the programmable logic and its data at a point in time. The baseline serves as a basis for further development. Once a baseline is established, changes can only be made through the change control process described in the TRPS and ESFAS Configuration Management Plan.

Baselines are established after each development phase, at the completion of the formal review by the V&V team. The following baselines are established:

- Requirements Baseline
- Design Baseline
- Implementation Baseline
- Test Baseline

Baselining is performed by committing phase configuration items into source control and listing the configuration item in the master configuration list, as specified in the vendor system design control procedure. The project file contains and manages programmable logic configuration items in one project folder structure allowing committing of all project phase configuration items using one project file in the IDE tool.

A baselined configuration item is traceable to the baselined configuration item from which it was developed.

A baselined configuration item is traceable to either the output it identifies or to the process with which it is associated. The traceability of baselined configuration items is recorded in the TRPS and ESFAS requirements traceability matrix.

Any proposed change to a baselined configuration item is subject to the change control and review requirements in the TRPS and ESFAS Configuration Management Plan. The change in status is flagged in the IDE tool and the file is baselined after the change control and review requirements are satisfied.

Once the configuration item is baselined, only authorized personnel can change the configuration item. Changes to baselined configuration items are planned, documented, approved, and tracked in accordance with a change control process.

The IDE tool records each change to baselined configuration items, including who made the change, and can discard changes that have been implemented or revert to any previous baseline after the changed configuration item has been baselined.

The archival and retrieval process involves the storage of data so that it can be accessed by authorized personnel. Project documents and records are retained and filed in the system integration document package and are stored in dual remote storage locations to preclude loss caused by natural disasters. The archival and retrieval process ensures:

- Accuracy and completeness
- Protection from unauthorized change
- Quality of storage media and protection from disaster
- Accuracy of retrieval and duplication

Programmable logic code load controls include approved load procedures, load verification, and part marking verification.

The programmable logic development environment includes the tools, methods, procedures, programming languages, and hardware used to develop, verify, control, and produce the programmable logic. The tools identification data, including version numbers, are listed in the Master Configuration List.

The code generation tools version is automatically included in the code files. The tool version used to develop the programmable logic is verified as the version on the master configuration list.

Changes to the development environment are subject to change control.

Configuration reviews are required for configuration items prior to shipment. The configuration audits include both document configuration items and programmable logic components.

Configuration status accounting involves recording and reporting information that is needed to effectively manage the programmable logic configuration items development, verification, and validation processes. Reports are generated to inform managers, developers, and SHINE about the project status. Configuration status accounting reports provide consistent, reliable, and timely status information that enhances communication, avoids duplication, and prevents repeat mistakes. The configuration status accounting reports provide the following information:

- Status of data items including configuration identification
- Status of change requests and test anomaly reports
- Status of released data and files
- List of baselined contents and differences from previous baseline

Configuration status accounting reports include the master configuration list, model development reports, and change request and test anomaly reports.

The master configuration list identifies hardware part numbers and the programmable logic code associated with the hardware. Before loading the code onto the hardware, the identification of the programmable logic code and the hardware is performed to ensure compatibility.

No commercial off-the-shelf (COTS) vendor supplied documents or software are edited by the safety-related control system vendor project team. The document versions and software versions are recorded upon receipt in the master configuration list and should not change. Therefore, neither configuration change procedures nor baselining apply to COTS documents or software.

A purchase order issued by the safety-related control system vendor to a third-party vendor for a COTS program or technical calculations typically contains:

- a description of the major components of the software design, as they relate to the software requirements,
- a technical description of the software with respect to the theoretical basis, mathematical model, control flow, data flow, control logic and data structure,
- a description of the allowable or prescribed ranges for inputs and outputs, and
- the design described in a manner that can be translated into code.

The purchase order requires the vendor to provide a software design description and evidence of verification and validation.

The third-party vendor software and documentation are verified for sufficiency such that a person who is technically qualified in the subject is able to understand the third-party vendor deliverables and verify the adequacy of the results without recourse to the originator.

7.2.6.6.2 Post-Installation Phase Configuration Management

Configuration management of any post-installation changes or modifications required to the safety-related control systems has been delegated to the vendor. Processes equivalent to those used for initial development, described in Subsection 7.2.6.6.1, are followed. SHINE maintains oversight of the vendor, authorization of changes, control of the scope of changes, and evaluation of the change against the requirements of the SHINE facility license.

7.2.6.7 Independent Testing

Development, review, and release of V&V generated test documents and execution of tests is performed by the vendor in accordance with the TRPS and ESFAS Test Plan and Verification and Validation Plan. V&V personnel are responsible for hardware and software test setup.

The test schedule is developed to ensure project deliverables satisfy the system technical and regulatory requirements. The test tasks include the following:

- Test plan development
- Pre-Factory Acceptance Test (FAT) procedures development
- FAT procedures development
- TRPS and ESFAS requirements traceability matrix update
- Test equipment setup
- Pre-FAT test procedures execution
- Report pre-FAT results and update FAT documents
- FAT procedures execution
- Report FAT results
- Test phase V&V summary report development

The test documentation includes the following:

- Project test plan
- Test procedures
- Test scripts and test input stimulus files
- Test reports
- Test anomaly reports
- Test phase summary report

Testing is performed to ensure satisfactory hardware have been developed in accordance with the SyRS. Measurement and test equipment calibration is performed before a testing activity and traceable to National Institute of Standards and Technology (NIST) standards. Measures are taken to establish that tools, gauges, instruments, and other measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy within acceptable limits. Testing activities include both pre-FAT and FAT.

The pre-FAT ensures that the FAT procedures are developed properly and the TRPS and ESFAS protection systems components conform to the SyRS in an operating integrated system environment. The pre-FAT informally executes the FAT procedures to determine their suitability, correctness, completeness, and efficiency of the test procedures.

The FAT validates the system hardware conforms to the system requirements as defined in the SyRS and documented in the TRPS and ESFAS requirements traceability matrix.

The FAT is performed on each protection system and includes integration tests and system tests. It consists of a documented series of inspections, power-on tests, and calibration verification steps to confirm that the system hardware conforms to the approved requirements and design documents and is in overall proper working order. It also verifies that the test configuration is correct and the required test equipment is properly calibrated.

The FAT integration test cases and procedures perform the following:

- Test programmable logic interfaces and basic programmable logic operations, and
- Test interface characteristics defined in the requirements specifications and design description such as protocols, sequences, and timing.

The FAT system test cases and procedures perform the following:

- Test system functions as defined in the SyRS
- Test voting functions
- Test trip or protective outputs
- Test system operation in all modes as defined in the SyRS

Normal and robustness test cases are prepared in the test procedures to demonstrate that design outputs conform to requirements.

The acceptance criteria for each testable requirement are specified in the applicable test case. The acceptance criteria are specified by either qualitative (pass/fail) or quantitative (numerical) acceptance criteria. When an acceptance criterion is numerical, the minimum and maximum values are specified.

Any testable attribute that does not meet the stated acceptance criteria is documented on a Test Anomaly Report. This includes both programmable logic anomalies and hardware deficiencies. The Test Anomaly Report identifies the resolution of the stated problem and describes any retesting requirements.

The results of the FAT are summarized in the FAT summary report and are incorporated into a separate test phase summary report, which is generated at the end of the test phase. The FAT summary report also incorporates other reports including test anomaly reports (used to document deficiencies found during testing) and change requests as attachments.

The FAT summary report documents the review of the test results with the following criteria:

1. Complete: Test cases and steps have been executed.
2. Acceptable: Results are within the expected results.
3. Anomalies resolved: Test anomaly reports have been resolved.
4. Changes implemented and tested: Change requests submitted during testing have been performed in accordance with the TRPS and ESFAS Configuration Management Plan and are implemented and tested.

There is no process risk associated with either the TRPS and ESFAS test plan or implementation of the related FAT. The FAT is conducted using simulated inputs, using either measurement and test equipment generated signals or computer-based test systems. The outputs are not connected to any plant process equipment, but are connected to displays, measurement and test equipment, or computer-based indication and data collection equipment. No equipment is operated outside of design parameters; therefore, there is no expectation of equipment failure. The only risks associated with the TRPS and ESFAS test plan are schedule compliance and satisfaction of test acceptance criteria.

7.2.6.8 Project Risk Management

The vendor TRPS and ESFAS Project Management Plan describes the risk management activities for the project. The risk management approach consists of five activities:

1. Risk identification
2. Risk analysis

3. Risk mitigation planning
4. Risk mitigation implementation
5. Risk tracking and control

Risk identification activities occur throughout the project lifecycle. Identified risks are documented in a safety-related control system vendor project risk register, which includes a description of the risk, areas of concern, likelihood, mitigating actions, and possible consequences. The project risk register may also describe the impacts to stakeholders, assumptions, constraints, relationship to other project risks, possible alternatives, as well as impacts to the project budget, schedule, or deliverables.

Each identified risk is analyzed to determine the type and the extent of the impacts should the risk situation or event occur. The analysis considers several relevant factors and includes any assumptions made, constraints, and sensitivity of the risk item.

Risk mitigation planning involves developing plans for mitigation and/or contingency actions for a specific risk. The risk mitigation plans address topics such as:

- Identification of mitigation and contingency actions for funding, schedule, staff or resources
- Identification of actions to be taken to reduce the likelihood or consequences of impact on the project
- Determination of the planned response based on a cost/benefit analysis
- Assignment of responsibility for each mitigation and contingency action

Risk tracking, monitoring, and control assesses how the project risk profile is changing throughout the project lifecycle, as well the effectiveness of any mitigation/contingency plans that have been executed. When changes to the risk occur, the process to identify, analyze, and plan is repeated. Existing risk mitigation plans are modified to change the approach if the desired effect is not being achieved.

Table 7.2-1 – Design Radiation Environments

Location	Normal	Transient
Radioisotope production facility (RPF) general area	1.0E+3 Rad TID, 5 mR/hr	100 mR/hr
Irradiation facility (IF) general area	1.0E+3 Rad TID, 5 mR/hr	50 mR/hr
Tritium purification system (TPS) room, glovebox and exhaust duct	50 Rad TID, 0.25 mR/hr	5 mR/hr
Irradiation unit (IU) cell above the light water pool	1.8E+8 Rad TID, 1E+3 R/hr	1E+3 R/hr
IU cell near dump tank and flux detectors (in light water pool)	1.8E+10 Rad TID, 1E+5 R/hr	1E+5 R/hr
Inside the target solution vessel (TSV) off-gas system (TOGS) instrument box	5.4E+8 Rad TID, 3E+3 R/hr	3E+3 R/hr
Inside the TOGS cell, outside instrument box	1.2E+10 Rad TID, 7E+4 R/hr	7E+4 R/hr
Inside the cooling room	1.8E+4 Rad TID, 100 mR/hr	100 R/hr

Note: (1) Total integrated dose (TID) is calculated over a 20-year timeframe.

(2) Design radiation environments lower than those listed may be defined for specific locations using additional analysis or localized shielding.

Table 7.2-2 – Facility Control Room Design Environmental Parameters

Parameter	Normal	Transient
Temperature	60ºF to 80ºF	40ºF to 120ºF
Pressure	Ambient	Ambient
Relative Humidity	10 percent to 80 percent (non-condensing)	10 percent to 95 percent (non-condensing)

Table 7.2-3 – RPF and IF General Area Design Environmental Parameters

Parameter	Normal	Transient
Temperature	65ºF to 85ºF	40ºF to 120ºF
Pressure	Ambient	Ambient
Relative Humidity	10 percent to 80 percent (non-condensing)	10 percent to 95 percent (non-condensing)

Table 7.2-4 – IU Cell Interior Design Environmental Parameters

Parameter	Normal	Transient
Temperature	40ºF to 104ºF	40ºF to 120ºF
Pressure	Ambient	14 psia to 19 psia
Relative Humidity	10 percent to 100 percent (condensing)	10 percent to 100 percent (condensing)

Table 7.2-5 – TOGS Cell Interior Design Environmental Parameters

Parameter	Normal	Transient
Temperature	40ºF to 104ºF	40ºF to 120ºF
Pressure	Ambient	14 psia to 19 psia
Relative Humidity	10 percent to 100 percent (condensing)	10 percent to 100 percent (condensing)

Table 7.2-6 – Primary Cooling Room Interior Design Environmental Parameters

Parameter	Normal	Transient
Temperature	40ºF to 120ºF	40ºF to 120ºF
Pressure	Ambient	Ambient
Relative Humidity	10 percent to 80 percent (non-condensing)	10 percent to 95 percent (non-condensing)

Figure 7.2-1 – HIPS Platform Timing

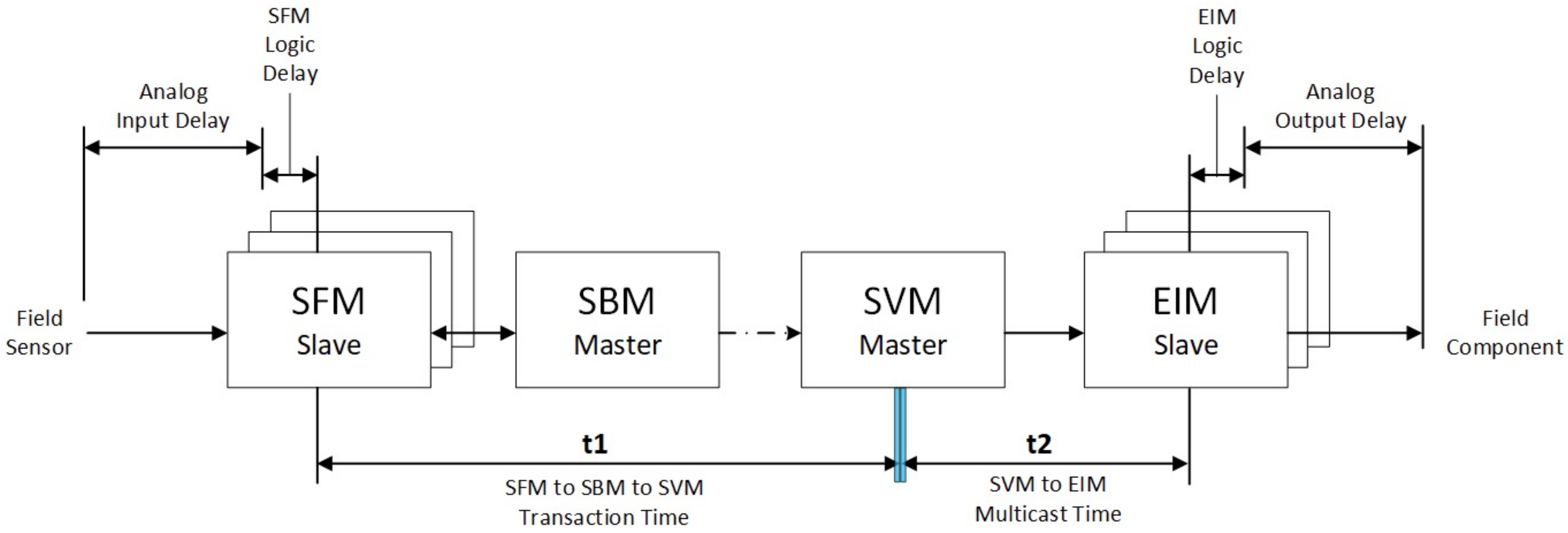
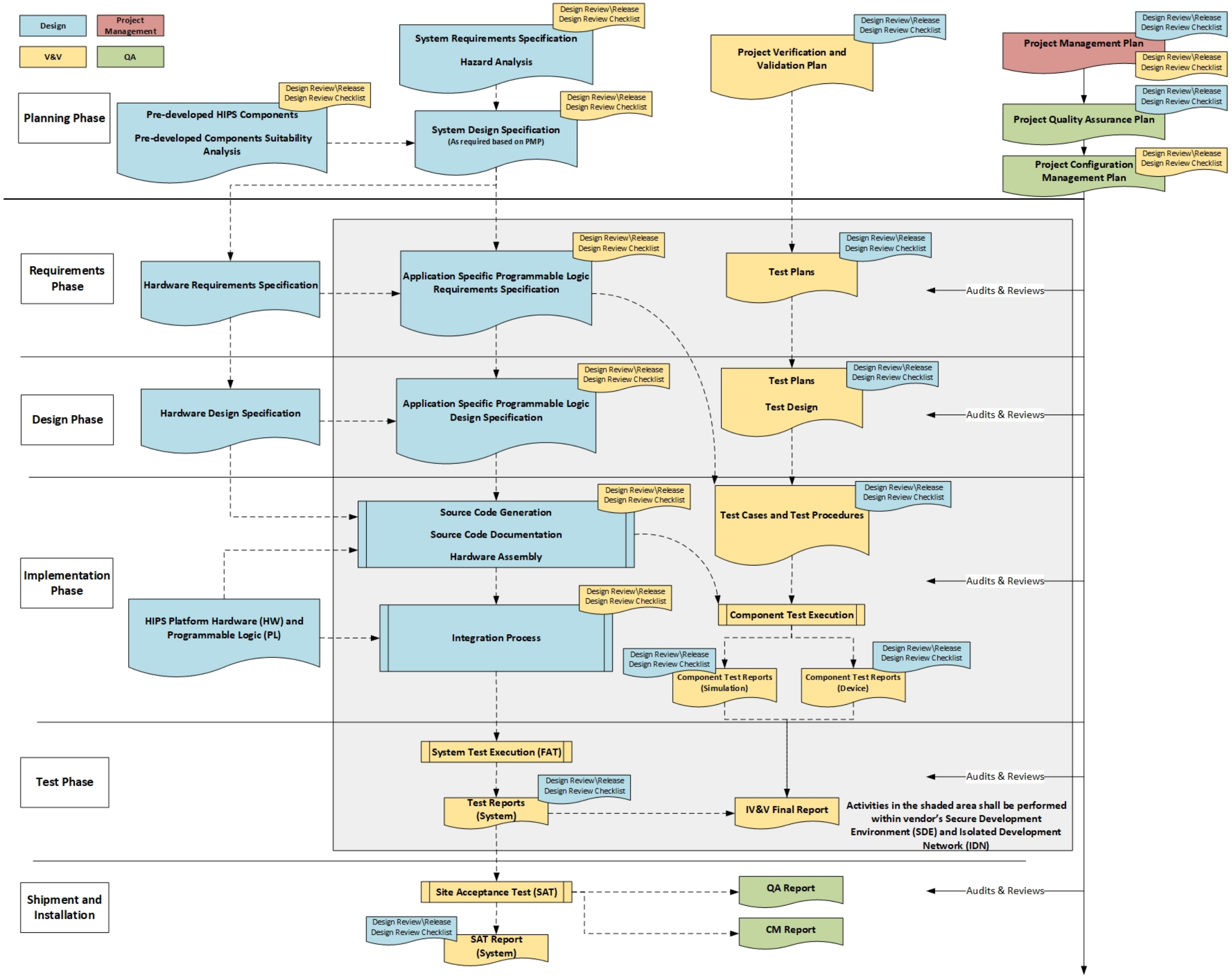


Figure 7.2-2 – TRPS and ESFAS Programmable Logic Lifecycle Process


Design
Project Management
V&V
QA
Planning Phase
Requirements Phase
Design Phase
Implementation Phase
Test Phase
Shipment and Installation
System Requirements Specification
Hazard Analysis
Design Review\Release Design Review Checklist
Project Verification and Validation Plan
Project Management Plan
Project Quality Assurance Plan
Project Configuration Management Plan
Pre-developed HIPS Components
Pre-developed Components Suitability Analysis
System Design Specification
(As required based on PMP)
Hardware Requirements Specification
Application Specific Programmable Logic Requirements Specification
Test Plans
Audits & Reviews
Hardware Design Specification
Application Specific Programmable Logic Design Specification
Test Plans
Test Design
Source Code Generation
Source Code Documentation
Hardware Assembly
Test Cases and Test Procedures
HIPS Platform Hardware (HW) and Programmable Logic (PL)
Integration Process
Component Test Execution
Component Test Reports (Simulation)
Component Test Reports (Device)
System Test Execution (FAT)
Test Reports (System)
IV&V Final Report
Activities in the shaded area shall be performed within vendor's Secure Development Environment (SDE) and Isolated Development Network (IDN)
Site Acceptance Test (SAT)
SAT Report (System)
QA Report
CM Report

7.3 PROCESS INTEGRATED CONTROL SYSTEM

The process integrated control system (PICS) is a nonsafety-related digital control system that performs various functions throughout the SHINE facility. PICS functions include signal conditioning, system controls, interlocks, and monitoring of the process variables and system status.

7.3.1 DESIGN CRITERIA

Table 3.1-1 shows the SHINE design criteria applicable to the PICS. The SHINE design criteria are described in Section 3.1.

Additional criteria applicable to the PICS are as follows:

7.3.1.1 Access Control

PICS Criterion 1 - The PICS design shall incorporate design or administrative controls to prevent/limit unauthorized physical and electronic access to critical digital assets (CDAs) during the operational phase, including the transition from development to operations. CDAs are defined as digital systems and devices that are used to perform or support, among other things, physical security and access control, safety-related functions, and reactivity control.

7.3.1.2 Software Requirements Development

PICS Criterion 2 - A structured process, which is commensurate with the risk associated with its failure or malfunction and the potential for the failures challenging safety systems, shall be used in developing software for the PICS.

PICS Criterion 3 - The PICS software development life cycle process requirements shall be described and documented in appropriate plans which shall address verification and validation (V&V) and configuration control activities.

PICS Criterion 4 - The configuration control process shall assure that the required PICS hardware and software are installed in the appropriate system configuration and ensure that the correct version of the software/firmware is installed in the correct hardware components.

7.3.1.3 Fail Safe

PICS Criterion 5 - The PICS shall assume a defined safe state with loss of electrical power to the PICS.

7.3.1.4 Effects of Control System Operation/Failures

PICS Criterion 6 - The PICS shall be designed so that it cannot fail or operate in a mode that could prevent the target solution vessel (TSV) reactivity protection system (TRPS) or engineered safety features actuation system (ESFAS) from performing their designated functions.

7.3.1.5 Operational Bypass

PICS Criterion 7 - Bypasses of PICS interlocks, including provisions for testing, shall be under the direct control of a control room operator and shall be indicated on control room displays.

7.3.1.6 Surveillance

PICS Criterion 8 - Subsystems of and equipment in the PICS shall be designed to allow testing, calibration, and inspection to ensure functionality.

PICS Criterion 9 - Testing, calibration, and inspections of the PICS shall be sufficient to confirm that surveillance test and self-test features address failure detection, self-test capabilities, and actions taken upon failure detection.

7.3.2 DESIGN BASIS

The PICS is designed to allow the operator to perform irradiation cycles, transfer target solution to and from the irradiation unit (IU) as well as through the production facility, and interface with the tritium purification system (TPS), supercell, waste handling, and auxiliary systems.

The modes of operation for the functions of the PICS that interface with individual IUs correspond to the mode of that IU (see Subsection 7.3.3). Portions of the PICS that monitor or control common or facility-wide systems are not mode-dependent.

The PICS control cabinets are located in the non-radiologically controlled areas of the main production facility and PICS components are in various plant areas with varying environmental conditions. The PICS is designed for the normal environmental and radiological conditions provided in Tables 7.2-1 through 7.2-6.

7.3.3 DESCRIPTION

The PICS is a collection of instrumentation and control equipment located throughout the facility to support monitoring, indication, and control of various systems. Decentralized implementation of the PICS functions allows subsets of the system to perform functions independent of each other. A portion of the PICS supports the main control board and operator workstations in the facility control room by receiving operator commands and collecting and transmitting facility information to the operators, as described in Section 7.6. A summary of the PICS facility system interfaces is provided in Figure 7.3-1.

7.3.3.1 Irradiation Unit Systems

The PICS is used to monitor parameters and perform manual and automatic actions during each of the operational modes of a subcritical assembly system (SCAS):

Mode 0 - Solution Removed: No target solution in the SCAS
Mode 1 - Startup: Filling the TSV
Mode 2 - Irradiation: Operating mode (neutron driver active)
Mode 3 - Post-Irradiation: TSV dump valves open
Mode 4 - Transfer to RPF: Dump tank drain valve opens to permit solution transfer

The systems associated with SCAS modes of operation include the SCAS itself, the neutron driver assembly system (NDAS), the TSV off-gas system (TOGS), the primary closed loop cooling system (PCLS), and the neutron flux detection system (NFDS).

Mode 0 - Solution Removed

In Mode 0, the PICS provides the capability to control equipment needed to transition an irradiation unit into Mode 1, including closing the TSV fill valves and dump valves and starting the TOGS blowers as needed to meet mode transition criteria. The PICS also provides monitoring and controls of the common TPS, which is integrated with the modes of operation for each IU cell.

Mode 1 - Startup Mode

After the operator transitions the IU to Mode 1 using the operating mode input to TRPS, the PICS is used to open the TSV fill valves and operate the vacuum transfer system to add target solution to the TSV from the associated TSV hold tank. The PICS also provides a defense-in-depth interlock to prevent the TSV fill valves from opening if one or more TOGS blowers is not running, separate from the TRPS Mode 0 to Mode 1 transition criteria.

The TSV is filled incrementally. The TSV fill increment is determined by 1/M calculations. The operator may use the PICS as a check to calculate the next required fill volume based on the 1/M calculation. The PICS also provides defense-in-depth time limits and interlocks to control the maximum volumetric step addition during the 1/M fill process to prevent challenging the TRPS Fill Stop actuation function described in Section 7.4.

Mode 2 - Irradiation

When the TSV fill has been completed, PICS is used to close the TSV fill valves to meet Mode 2 transition criteria. The PICS provides an interlock with the source range channel of the NFDS to prevent TSV irradiation without sufficient neutron counts on the detectors, and when that permissive is met, PICS is used to close the neutron driver breakers to enable the target solution in the TSV to be irradiated. The PICS interfaces with the NDAS control system to start or stop the driver, and is used to control the introduction of tritium into the NDAS target from the TPS.

During irradiation, PICS is used to monitor neutron flux levels, concentrations of radiolytic gases generated, NDAS performance parameters, and other parameters associated with the irradiation process.

Mode 3 - Post-Irradiation

The neutron driver breakers are opened by the PICS, ending the irradiation period and satisfying the mode transition criteria, allowing the operator to transition from Mode 2 to Mode 3. When transitioning from Mode 2 to Mode 3 during normal operations, the PICS uses the mode transition signal from the TRPS to automatically open the TSV dump valves to drain the target solution to the dump tank. While in Mode 3, the PICS is used to monitor TOGS and SCAS operational parameters while the solution is held for decay.

Mode 4 - Transfer to RPF

After the operator transitions the IU to Mode 4, the PICS is used to open the TSV dump tank drain isolation valve allowing the target solution to be vacuum lifted out of the IU cell, pumped through an extraction column, and drained to a target solution hold tank. The PICS is used to select the flow path for the transfer to the desired extraction cell and to operate the vacuum transfer system (VTS) which accomplishes the lift.

When the solution has been removed from the dump tank, the operator uses PICS to verify that low-high TSV dump tank level is inactive, meeting the Mode 4 to Mode 0 transition criteria.

7.3.3.2 Process Systems

The PICS provides the automated and manual control of systems used to prepare target solution, transfer target solution between locations within the facility, extract and purify isotopes of interest, and manage radioactive waste.

Target Solution Preparation

Target solution preparation activities are performed by the target solution preparation system (TSPS) and uranium receipt and storage system (URSS) and are described in more detail in Section 4b.4. PICS provides monitoring and alarming functions for parameters associated with the TSPS preparation and dissolution tanks, including alarms to alert the operators of potential overflow of the TSPS dissolution tank into the TSPS glovebox. PICS is also used to monitor parameters and provide alarms associated with TSPS and URSS glovebox operation.

Target Solution Transfer

Target solution transfer activities occur throughout the facility in order to remove irradiated solution from the TSV dump tank, extract isotopes, and return target solution to an IU. These activities are accomplished by the VTS and target solution staging system (TSSS), described in more detail in Sections 9b.2 and 4b.4, respectively. PICS provides level information associated with VTS and TSSS process tanks and position indication information for process control valves to facilitate automatic and manual control of solution transfers between tanks.

Isotope Extraction and Purification

Isotope extraction and purification activities are performed by the molybdenum extraction and purification system (MEPS), molybdenum isotope product packaging system (MIPS), and iodine and xenon purification and packaging (IXP) system, which are described in Section 4b.3. The PICS is used to transfer irradiated target solution from the TSV dump tank to the extraction process, as described above. The PICS is also used to monitor parameters associated with the extraction and purification processes, including reagent additions and tank levels. Process system control valves are operated by the PICS.

Radioactive Liquid Drains

Drains from vaults, trenches, and other areas where uranium-bearing solutions may be present are part of the radioactive drain system (RDS), described in Subsection 9b.7.2. PICS is used to provide indication of leakage in individual vaults and the presence of liquid in the RDS sump tanks to alert the operator of abnormal situations.

Radioactive Liquid Waste

Radioactive liquid waste is stored in the radioactive liquid waste storage system (RLWS) and immobilized in the radioactive liquid waste immobilization system (RLWI). These systems are described in detail in Section 9b.7. The PICS is used to monitor tank levels and temperatures, control the operation of system valves, and provide functionality to support administrative controls related to the transfer of radioactive liquid waste between tanks using the VTS.

PICS is also used to support the RLWI process by providing control of RLWI pumps and controlling the waste drum operation through the waste solidification skid, including drum fill and mixing operations.

7.3.3.3 Other Facility Systems

The PICS provides the automated control and operator interface to manually control aspects of the facility auxiliary and electrical systems.

Electrical

The PICS is used to monitor and provide alarms for parameters related to the facility electrical systems, including the uninterruptible electrical power supply system (UPSS), the normal electrical power supply system (NPSS), and the standby generator system (SGS). The PICS also provides the manual ability to open or close motorized breakers. Electrical systems are discussed in Chapter 8.

The PICS remains operational upon a loss of off-site power for a minimum of 10 minutes (see Subsection 7.3.4). The PICS provides automatic and manual control of the SGS, including the automatic function to start and load the SGS after a loss of off-site power event.

The PICS also provides the automatic function of disconnecting the on-site electric power systems from the utility on loss of phase, phase reversal, undervoltage, and overvoltage.

Ventilation, Heating and Cooling

Facility heating, ventilation, and air conditioning (HVAC) systems are described in Section 9a2.1 and facility cooling systems are described in Chapter 5. The PICS is used to interface with the main production facility ventilation local digital control systems to operate the supply, exhaust, and recirculation systems in normal operating modes. The PICS monitors temperatures and differential pressure on ventilation systems, and other operational parameters related to the radioisotope process facility cooling system (RPCS), facility heating water system (FHWS), and facility chilled water system (FCHS).

Balance of Plant

The PICS provides select monitoring and control capabilities for other balance of plant systems in the main production facility, including, but not limited to, the facility nitrogen handling system (FNHS) and the facility demineralized water system (FDWS).

Seismic Monitoring

The PICS contains a seismic monitoring system, which includes instrumentation, control cabinets, and a dedicated computer for monitoring seismic activity in the safety-related portion of the facility. The seismic monitoring system provides event recording time histories for seismic events and provides indication of a seismic event to the PICS for alarm in the facility control room. Data may be retrieved from the seismic monitoring system by either the dedicated computer or via the operator workstation in the facility control room.

7.3.3.4 Safety-Related Control and Indication Systems

The PICS contains no safety-related controls and has no safety-related functions, however, the safety-related TRPS, ESFAS, NFDS and safety-related radiation monitors provide nonsafety-related system status and measured process variable values to the PICS for viewing, recording, and trending. The PICS is also used to transmit discrete hardwired signals to the TRPS and ESFAS for deliberate operator action to return the TRPS or ESFAS to a normal operating state.

7.3.4 OPERATION AND PERFORMANCE

The PICS is designed to operate under normal facility conditions and anticipated transients to ensure adequate safety for the facility.

The design of the PICS allows operators to remove main control board or operator workstation displays from service without impacting the operation of the remaining portions of the PICS.

The PICS includes local battery supplies sufficient to allow the PICS to continue to operate for at least 10 minutes after a loss of external power. The 10-minute design supports starting and loading the defense-in-depth SGS within five minutes following a loss of off-site power event (see Section 8a2.2).

Components controlled by the PICS assume a defined safe state on loss of electrical power.

7.3.5 ACCESS CONTROL AND CYBER SECURITY

The PICS does not use the secure development and operating environment implemented for the safety-related control systems described in Section 7.2.5, but rather incorporates features commensurate with the risk and magnitude of the harm that would result from unauthorized and inappropriate access, use disclosure, disruption, or destruction of this nonsafety-related control system.

The PICS does not allow remote access. Remote access is defined as the ability to access the components of the operator workstations, main control board, PICS display cabinet, and other PICS controllers and cabinets from a location with less physical security.

The PICS includes the capability to disable, through software or physical disconnection, unneeded networks, communication ports and removable media drives or provide engineered barriers.

The PICS does not use any wireless interface capabilities for control functions.

The PICS provides information to the facility data and communications system (FDCS) networks and equipment via a one-way data diode, such that no inputs can be provided to the PICS from off-site sources.

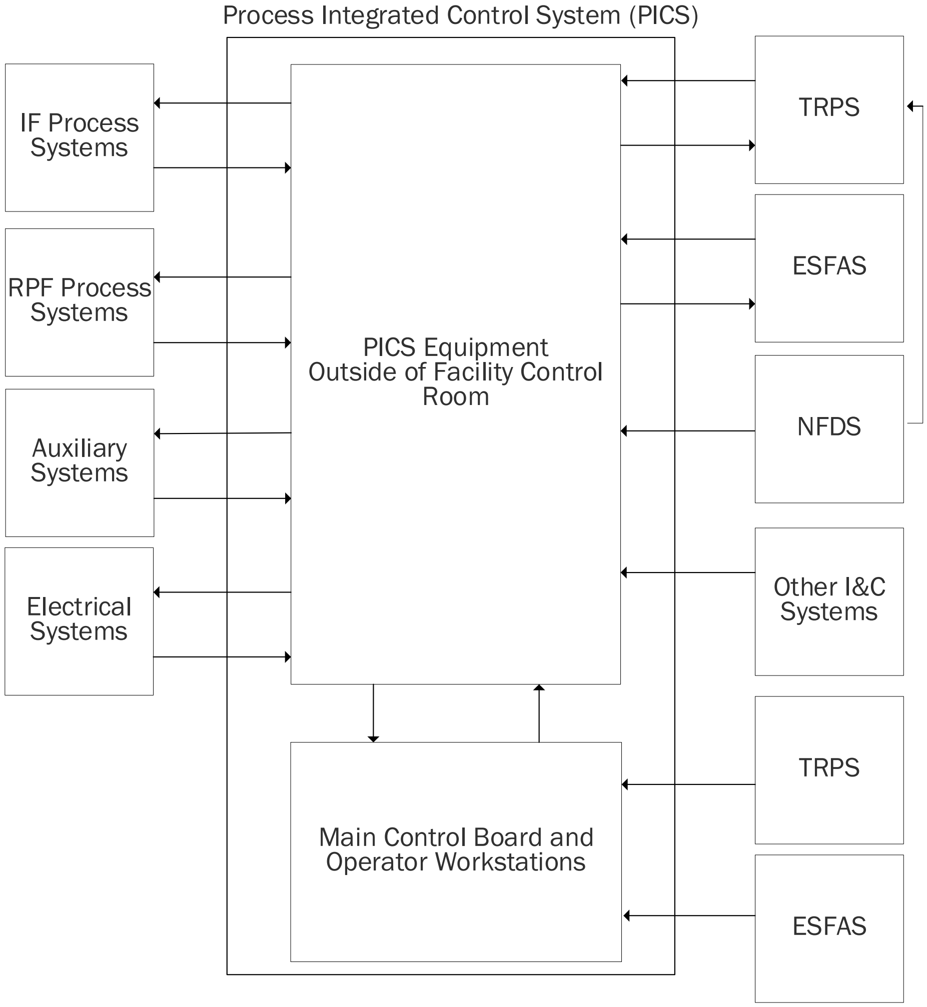
7.3.6 SOFTWARE DEVELOPMENT

The PICS is developed under a structured process commensurate with the risk associated with its failure or malfunction. The process includes the definition of functional requirements, a documented development and implementation process, and a plan for verification of software outputs.

7.3.7 TECHNICAL SPECIFICATIONS

Certain material in this section provides information that is used in the technical specifications. This includes limiting conditions for operation, setpoints, design features, and means for accomplishing surveillances. In addition, significant material is also applicable to, and may be referenced by, the bases that are described in the technical specifications.

Figure 7.3-1 – Process Integrated Control System Interfaces


Process Integrated Control System (PICS)
IF Process Systems
RPF Process Systems
Auxiliary Systems
Electrical Systems
PICS Equipment Outside of Facility Control Room
Main Control Board and Operator Workstations
TRPS
ESFAS
NFDS
Other I&C Systems
TRPS
ESFAS

7.4 TARGET SOLUTION VESSEL REACTIVITY PROTECTION SYSTEM

7.4.1 SYSTEM DESCRIPTION

The target solution vessel (TSV) reactivity protection system (TRPS) performs various design basis safety functions for accelerator-based irradiation processes taking place within each irradiation unit (IU) cell of the SHINE production facility. While operating, the TRPS performs various detection, logic processing, control, and actuation functions associated with the SHINE irradiation process. The TRPS includes input/output capabilities necessary to interface with various indications and control components located within the facility control room. The TRPS also provides nonsafety-related system status and measured process variable values to the facility process integrated control system (PICS) for viewing, recording, and trending.

The TRPS monitors variables important to the safety functions of the irradiation process during each operating mode of the IU to perform one or more of the following safety functions:

- IU Cell Safety Actuation
- IU Cell Nitrogen Purge
- IU Cell TPS Actuation
- Driver Dropout

The TRPS also performs the nonsafety defense-in-depth Fill Stop function.

The TRPS monitors the IU cell from filling of the TSV through irradiation of the target solution, dumping of the target solution, and transfer of the target solution to the radioisotope production facility (RPF). All advances to the modes of operation throughout the irradiation process are manually initiated by the operator and the TRPS implements the required mode-specific system interlocks and bypasses; however, the TRPS does not automatically determine the mode of operation. If at any point during the irradiation process a monitored variable indicating unsafe conditions exceeds its setpoint, the TRPS automatically places the IU into a safe state. The TRPS logic diagrams are shown in Figure 7.4-1.

The TRPS uses redundant and independent sensors through three divisions to complete the logical decisions necessary to initiate the required protective trips and actuations. When a TRPS input channel exceeds a predetermined limit, the trip determinations from each division of the TRPS are sent to voting logic where a two-out-of-three coincident logic vote is performed to initiate a trip or actuation. The general architecture of the TRPS is shown in Figure 7.1-2.

When a TRPS output is in its normal, energized state, it does not control the position of the actuation component. Instead, the TRPS and the PICS are arranged in a series configuration for the PICS to control the component normally, and deenergizing the output of the TRPS forces the component to its safe state via the physical design of the valve or breaker. The only exception to this control configuration is for the nitrogen purge system inerting gas valves, TSV off-gas system (TOGS) radioisotope process facility cooling system (RPCS) supply and return isolation valves, TOGS nitrogen vent isolation valves, and the radiological ventilation IU cell dampers. For these components, the TRPS assumes normal control, and PICS only has control of the component when appropriate permissives are active.

7.4.2 DESIGN CRITERIA

The SHINE design criteria are described in Section 3.1. Table 3.1-1 shows the SHINE design criteria applicable to the TRPS. Additional system-specific design criteria for the TRPS are described in this section.

7.4.2.1 Access Control

TRPS Criterion 1 – The TRPS shall require a key or combination authentication input at the control console to prevent unauthorized use of the TRPS.

TRPS Criterion 2 – Developmental phases for TRPS software shall address the potential cyber security vulnerabilities (physical and electronic) to prevent unauthorized physical and electronic access.

TRPS Criterion 3 – The TRPS design shall incorporate design or administrative controls to prevent/limit unauthorized physical and electronic access to critical digital assets (CDAs) during the operational phase, including the transition from development to operations. CDAs are defined as digital systems and devices that are used to perform or support, among other things, physical security and access control, safety-related functions, and reactivity control.

7.4.2.2 Software Requirements Development

TRPS Criterion 4 – The functional characteristics of the TRPS software requirements specifications shall be properly and precisely described for each software requirement.

TRPS Criterion 5 – Development of TRPS software shall follow a formally defined life cycle process and address potential security vulnerabilities in each phase of the life cycle.

TRPS Criterion 6 – TRPS development life cycle phase-specific security requirements shall be commensurate with the risk and magnitude of the harm that would result from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the TRPS.

TRPS Criterion 7 – TRPS software development life cycle process requirements shall be described and documented in appropriate plans which shall address safety analysis, verification and validation (V&V), and configuration control activities.

TRPS Criterion 8 – Tasks for validating and verifying the TRPS software development activities shall be carried out in their entirety. Independent V&V shall be performed by individuals or groups with appropriate technical competence in an organization separate from the development and program management organizations. Successful completion of V&V tasks for each software life cycle activity group shall be documented.

TRPS Criterion 9 – The TRPS software life cycle configuration control program shall trace software development from software requirement specification to implementation and address any impacts on TRPS safety, control console, or display instruments.

TRPS Criterion 10 – The TRPS configuration control program shall assure that the required TRPS hardware and software are installed in the appropriate system configuration and ensure that the correct version of the software/firmware is installed in the correct hardware components.

TRPS Criterion 11 – Validation testing shall test all portions of TRPS programmable logic necessary to accomplish its safety functions and shall exercise those portions whose operation or failure could impair safety functions during testing.

TRPS Criterion 12 – The TRPS software development life cycle shall include a software risk management program which addresses vulnerabilities throughout the software life cycle.

TRPS Criterion 13 – TRPS equipment not designed under SHINE approved quality assurance (QA) program shall be accepted under the SHINE commercial-grade dedication program.

7.4.2.3 General Instrumentation and Control Requirements

TRPS Criterion 14 – The TRPS safety function shall perform and remain functional during normal operation and during and following a design basis event.

TRPS Criterion 15 – Manual controls of TRPS actuation components shall be implemented downstream of the digital I&C portions of the safety system.

7.4.2.4 Single Failure

TRPS Criterion 16 – The TRPS shall be designed to perform its protective functions after experiencing a single random active failure in nonsafety control systems or in the TRPS, and such failure shall not prevent the TRPS and credited passive redundant control components from performing its intended functions or prevent safe shutdown of an IU cell.

TRPS Criterion 17 – The TRPS shall be designed such that no single failure can cause the failure of more than one redundant component.

7.4.2.5 Independence

TRPS Criterion 18 – Interconnections among TRPS safety divisions shall not adversely affect the functions of the TRPS.

TRPS Criterion 19 – A logical or software malfunction of any interfacing non-safety systems shall not affect the functions of the TRPS.

TRPS Criterion 20 – The TRPS shall be designed with physical, electrical, and communications independence of the TRPS both between the TRPS channels and between the TRPS and nonsafety-related systems to ensure that the safety functions required during and following any design basis event can be accomplished.

TRPS Criterion 21 – Physical separation and electrical isolation shall be used to maintain the independence of TRPS circuits and equipment among redundant safety divisions or with nonsafety systems so that the safety functions required during and following any design basis event can be accomplished.

TRPS Criterion 22 – The TRPS shall be designed such that no communication – within a single safety channel, between safety channels, and between safety and nonsafety systems – adversely affects the performance of required safety functions.

TRPS Criterion 23 – TRPS data communications protocols shall meet the performance requirements of all supported systems.

TRPS Criterion 24 – The timing of TRPS data communications shall be deterministic.

TRPS Criterion 25 – TRPS communications protocols shall conform to validated protocol specifications by formally generated test procedures and test data vectors and verify that the implementations themselves were constructed using a formal design process that ensures consistency between the product and the validated specification.

TRPS Criterion 26 – The TRPS shall be designed such that no unexpected performance deficits exist that could adversely affect the TRPS architecture.

7.4.2.6 Prioritization of Functions

TRPS Criterion 27 – TRPS devices that receive signals from safety and nonsafety sources shall prioritize the signal from the safety system.

7.4.2.7 Fail Safe

TRPS Criterion 28 – The TRPS shall be designed to assume a safe state on loss of electrical power.

7.4.2.8 Setpoints

TRPS Criterion 29 – Setpoints for an actuation of the TRPS shall be based on a documented analysis methodology that identifies assumptions and accounts for uncertainties, such as environmental allowances and measurement computational errors associated with each element of the instrument channel. The setpoint analysis parameters and assumptions shall be consistent with the safety analysis, system design basis, technical specifications, and facility design, and expected maintenance practices.

TRPS Criterion 30 – Adequate margin shall exist between setpoints and safety limits so that the TRPS initiates protective actions before safety limits are exceeded.

TRPS Criterion 31 – Where it is necessary to provide multiple setpoints for adequate protection based on particular modes of operation or sets of operating conditions, the TRPS shall provide positive means of ensuring that the more restrictive setpoint is used when required.

TRPS Criterion 32 – The sensitivity of each TRPS sensor channel shall be commensurate with the precision and accuracy to which knowledge of the variable measured is required for the protective function.

7.4.2.9 Operational Bypass, Permissives and Interlocks

TRPS Criterion 33 – Permissive conditions for each TRPS operating or maintenance bypass capability shall be documented.

TRPS Criterion 34 – TRPS interlocks shall ensure that operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required.

TRPS Criterion 35 – TRPS provisions shall exist to prevent activation of an operating bypass unless applicable permissive conditions exist.

TRPS Criterion 36 – Bypass capability shall not be provided for the mechanisms to manually initiate TRPS safety.

TRPS Criterion 37 – If provisions for maintenance or operating bypasses are provided, the TRPS design shall retain the capability to accomplish its safety function while a bypass is in effect.

TRPS Criterion 38 – Whenever permissive conditions for bypassing a train or channel in the TRPS are not met, a feature in the TRPS shall physically prevent or facilitate administrative controls to prevent the unauthorized use of bypasses.

TRPS Criterion 39 – All TRPS operating bypasses, either manually or automatically initiated, shall be automatically removed when the facility moves to an operating regime where the protective action would be required if an accident occurred.

TRPS Criterion 40 – If operating conditions change so that an active operating bypass is no longer permissible, the TRPS shall automatically accomplish one of the following actions:

- Remove the appropriate active operating bypass(es).
- Restore conditions so that permissive conditions once again exist.
- Initiate the appropriate safety function(s).

TRPS Criterion 41 – Portions of TRPS execute features with a degree of redundancy of one shall be designed so that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.

TRPS Criterion 42 – Provisions shall exist to allow the operations staff to confirm that a bypassed TRPS safety function has been properly returned to service.

7.4.2.10 Completion of Protective Actions

TRPS Criterion 43 – The TRPS design shall ensure that once initiated, the safety actions will continue until the protective function is completed.

TRPS Criterion 44 – Only deliberate operator action shall be permitted to reset the TRPS or its components following manual or automatic actuation.

TRPS Criterion 45 – Mechanisms for deliberate operator intervention in the TRPS status or its functions shall not be capable of preventing the initiation of TRPS.

7.4.2.11 Equipment Qualification

TRPS Criterion 46 – The effects of electromagnetic interference/radio-frequency interference (EMI/RFI) and power surges (such as high-energy faults and lightning) on the TRPS, including field programmable gate array (FPGA)-based digital portions, shall be adequately addressed.

7.4.2.12 Surveillance

TRPS Criterion 47 – Equipment in the TRPS (from the input circuitry to output actuation circuitry) shall be designed to allow testing, calibration, and inspection to ensure operability. If testing is required or can be performed as an option during operation, the TRPS shall retain the capability to accomplish its safety function while under test.

TRPS Criterion 48 – Testing, calibration, and inspections of the TRPS shall be sufficient to show that once performed, they confirm that surveillance test and self-test features address failure detection, self-test features, and actions taken upon failure detection.

TRPS Criterion 49 – The design of the TRPS and the justification for test intervals shall be consistent with the surveillance testing intervals as part of the facility technical specifications.

7.4.2.13 Classification and Identification

TRPS Criterion 50 – TRPS equipment shall be distinctly identified to indicate its safety classification and to associate equipment according to divisional or channel assignments.

7.4.2.14 Human Factors

TRPS Criterion 51 – Human factors shall be considered at the initial stages and throughout the TRPS design process to ensure that the functions allocated in whole or in part to the operator(s) can be successfully accomplished to meet TRPS design goals.

TRPS Criterion 52 – The TRPS shall include readily available means for manual initiation of each protective function at the system level.

TRPS Criterion 53 – The TRPS shall be designed to provide the information necessary to support annunciation of the channel initiating a protective action to the operator and requiring manual operator reset when all conditions to resume operation are met and satisfied.

7.4.2.15 Quality

TRPS Criterion 54 – The quality of the components and modules in the TRPS shall be commensurate with the importance of the safety function to be performed.

TRPS Criterion 55 – Controls over the design, fabrication, installation, and modification of the TRPS shall conform to the guidance of ANSI/ANS 15.8-1995, Quality Assurance Program Requirements for Research Reactors (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5, Quality Assurance Program Requirements for Research and Test Reactors (USNRC, 2010).

7.4.3 DESIGN BASIS

The TRPS is used to initiate protective actions of the IU in response to monitored variables exceeding predetermined limits. Modes of operation are used within the TRPS to set interlocks on the applicable variables for each operating mode in the IU and to create permissives for allowing the operator to perform certain actions with the safety-related TRPS components.

7.4.3.1 Mode Transition

IU operating modes are described in Subsection 7.3.3.1.

Each mode transition in the TRPS is initiated manually through the PICS, except for transition to Mode 3 via an IU Cell Safety Actuation or use of the control key to deactivate the facility master operating permissive. Before an operator is able to transition to a different mode, the transition criteria conditions must be met. Figure 7.4-2 shows a state diagram of the mode transitions.

Mode 0 to Mode 1 Transition Criteria

The TRPS permissives prevent transitioning from Mode 0 to Mode 1 until the TSV dump valves and TSV fill isolation valves have been confirmed to be closed and TOGS mainstream flow is at or above the low flow limit. Normal control of actuation component positions when going from Mode 0 to Mode 1 is manual and independent from TRPS mode transition.

Mode 0 to Mode 3 Transition Criteria

Transition from Mode 0 to Mode 3 is initiated automatically by TRPS or manually by an operator via manual actuation or the facility master operating permissive. Initiation of this transition generates an IU Cell Safety Actuation.

Mode 1 to Mode 2 Transition Criteria

The TRPS permissives prevent transitioning from Mode 1 to Mode 2 until the TSV fill isolation valves indicate fully closed. Normal control of actuation component positions when going from Mode 1 to Mode 2 is manual and independent from TRPS mode transition.

Mode 1 to Mode 3 Transition Criteria

Transition from Mode 1 to Mode 3 is initiated automatically by TRPS or manually by an operator via manual actuation or the facility master operating permissive. Initiation of this transition generates IU Cell Safety Actuation.

Mode 2 to Mode 3 Transition Criteria

The TRPS permissives prevent transitioning from Mode 2 to Mode 3 until the neutron driver assembly system (NDAS) high voltage power supply (HVPS) breakers have been confirmed opened. Normal control of the HVPS breakers from closed to open is manual and independent from TRPS mode transition. Normal transition of the dump valves to the open position is automated by PICS upon receipt of a mode transition signal from TRPS to PICS signifying that the TRPS has entered Mode 3.

Transition from Mode 2 to Mode 3 may also be initiated automatically by TRPS or manually by an operator via manual actuation or the facility master operating permissive. Initiation of this transition generates an IU Cell Safety Actuation.

Mode 3 to Mode 4 Transition Criteria

Transition of the TRPS from Mode 3 to Mode 4 is prevented if an automated IU Cell Safety Actuation is present. Normal control of actuation components is manual and independent from TRPS mode transition.

Mode 3 to Secure State Transition Criteria

Transition from Mode 3 to the secure state is initiated manually by an operator via disengaging the facility master operating permissive. While operating in the secure state, transition to another mode of operation is not allowed.

Mode 4 to Mode 0 Transition Criteria

The TRPS permissives prevent the transition from Mode 4 to Mode 0 until the TSV dump tank level is below the low-high dump tank level setpoint. There is no requirement for normal control of the actuation components to transition from Mode 4 to Mode 0.

Mode 4 to Mode 3 Transition Criteria

Transition from Mode 4 to Mode 3 is initiated automatically by TRPS or manually by an operator via manual actuation or the facility master operating permissive. Initiation of this transition generates an IU Cell Safety Actuation.

Secure State to Mode 3 Transition Criteria

Transition from the secure state to Mode 3 is initiated manually by an operator via engaging the facility master operating permissive. Initiation of this transition permits a transition to another mode of operation.

7.4.3.2 Safety Functions

7.4.3.2.1 IU Cell Safety Actuation

An IU Cell Safety Actuation is initiated in response to high neutron flux levels or when other process variables indicate abnormal conditions. An IU Cell Safety Actuation shuts down the irradiation process and isolates the primary system boundary and primary confinement boundary.

An IU Cell Safety Actuation causes a transition of the TRPS to Mode 3 operation, isolation of the primary system boundary, and isolation of the primary confinement boundary via transition of each of the following components to their deenergized state.

Mode 3 Transition Components

- TSV dump valves
- NDAS HVPS breakers

Primary System Boundary Components

- TSV fill isolation valves
- TSV dump tank drain isolation valve
- TOGS gas supply isolation valves
- TOGS vacuum tank isolation valves
- Vacuum transfer system (VTS) lower lift tank target solution valve(s)

The VTS lower lift tank target solution valves are redundant to the TSV dump tank drain isolation valve for an IU Cell Safety Actuation.

Primary Confinement Boundary Components

- Primary closed loop cooling system (PCLS) supply isolation valve
- PCLS return isolation valves
- TPS target chamber supply isolation valves
- TPS deuterium supply isolation valves
- TPS target chamber exhaust isolation valves
- TPS neutron driver evacuation isolation valves
- Radiological ventilation zone 1 exhaust subsystem (RVZ1e) IU cell ventilation dampers
- TOGS RPCS supply isolation valves
- TOGS RPCS return isolation valve
- Radiological ventilation zone 1 recirculation subsystem (RVZ1r) RPCS supply isolation valve
- RVZ1r RPCS return isolation valve

The TRPS initiates an IU Cell Safety Actuation based on the following variables:

- High source range neutron flux signal
- High wide range neutron flux
- High time-averaged neutron flux
- High RVZ1e IU cell radiation
- Low TOGS oxygen concentration
- Low TOGS mainstream flow (Train A)
- Low TOGS mainstream flow (Train B)
- Low TOGS dump tank flow
- High TOGS condenser demister outlet temperature (Train A)
- High TOGS condenser demister outlet temperature (Train B)
- Low PCLS flow (180 second delay)
- High PCLS temperature (180 second delay)
- Low PCLS temperature
- Low-high TSV dump tank level signal
- High-high TSV dump tank level signal
- TSV fill isolation valves not fully closed
- Facility master operating permissive

7.4.3.2.2 IU Cell Nitrogen Purge

An IU Cell Nitrogen Purge is initiated when monitored variables indicate a loss of hydrogen recombination capability in the IU. An IU Cell Nitrogen Purge results in purging the primary system boundary with nitrogen.

An IU Cell Nitrogen Purge consists of an automatically or manually initiated transition of each of the following components to their deenergized state and providing a signal to the engineered safety features actuation system (ESFAS) to initiate an ESFAS IU Cell Nitrogen Purge (see Section 7.5).

- Nitrogen purge system (N2PS) inerting gas isolation valves
- TOGS nitrogen vent isolation valves
- TOGS RPCS supply isolation valves
- TOGS RPCS return isolation valve

The TRPS initiates an IU Cell Nitrogen Purge based on the following variables:

- Low-high TSV dump tank level
- High-high TSV dump tank level
- Low TOGS oxygen concentration
- Low TOGS mainstream flow (Train A)
- Low TOGS mainstream flow (Train B)
- Low TOGS dump tank flow
- High TOGS upstream condenser demister outlet temperature (Train A)
- High TOGS upstream condenser demister outlet temperature (Train B)
- ESFAS loss of external power

7.4.3.2.3 IU Cell TPS Actuation

An IU Cell TPS Actuation is initiated when monitored variables indicate a release of tritium in a TPS glovebox. An IU Cell TPS Actuation results in isolating the TPS lines into and out of the IU cell, isolating the RVZ1 exhaust out of the IU cell, and deenergizing the neutron driver.

An IU Cell TPS Actuation consists of an automatically or manually initiated transition of each of the following components to their deenergized state and initiating a Driver Dropout (see Section 7.4.3.2.4):

- TPS target chamber supply isolation valves
- TPS deuterium supply isolation valves
- TPS target chamber exhaust isolation valves
- TPS neutron driver evacuation isolation valves
- RVZ1e IU cell ventilation dampers

The TRPS initiates an IU Cell TPS Actuation based on the following variables:

- ESFAS IU Cell TPS Actuation
- ESFAS TPS Process Vent Actuation

7.4.3.2.4 Driver Dropout

A Driver Dropout responds to monitored variables that indicate a loss of neutron driver output or a loss of cooling to allow the SCAS to recover from NDAS or PCLS transients. A Driver Dropout functions differently depending on whether it was initiated based on loss of neutron driver output or loss of cooling.

The TRPS initiates a Driver Dropout based on:

- Low power range neutron flux
- Low PCLS flow
- High PCLS temperature
- IU Cell TPS Actuation

The TRPS initiates a loss of neutron driver Driver Dropout on low power range neutron flux by opening the NDAS HVPS breakers with a timed delay. Driver Dropout on low power range neutron flux is bypassed until the power range neutron flux has reached the power range driver dropout permissive. After the bypass of Driver Dropout on low power range neutron flux has been removed, it remains removed until a mode transition or both HVPS breakers are open. The TRPS implements a timed delay of [ ]$^{\text{PROP/ECI}}$ from the time the low power range neutron flux signal is initiated, indicating that the neutron flux has exceeded its lower limits, to when the TRPS output to the HVPS breakers is deenergized. If fewer than two-out-of-three low power range neutron flux actuation signals are present before the timer has expired, then the low power range neutron flux timer resets. This delay allows the neutron driver to be restarted or to restart automatically within analyzed conditions.

The TRPS initiates a loss of cooling Driver Dropout on low PCLS cooling water flow or high PCLS cooling water supply temperature to open the NDAS HVPS breakers without a timed delay. This shuts down the neutron driver to prevent overheating of the target solution, while allowing the target solution to remain within the TSV. The breakers are then interlocked open until the PCLS flow and temperature are in the allowable range. If PCLS flow and temperature are not in the allowable range within 180 seconds, an IU Cell Safety Actuation is initiated, as described in Subsection 7.4.3.2.1.

7.4.3.2.5 Fill Stop

The nonsafety-related Fill Stop function aids in controlling the rate of fill of the TSV. If Fill Stop parameters are not met, then the Fill Stop deenergizes the TSV fill isolation valves blocking the fill path into the TSV.

During Mode 1, after neutron flux detection system (NFDS) source range neutron flux has reached or exceeded 40 percent of the maximum 95 percent fill flux, if the TSV fill isolation valve fully closed position indication becomes inactive, then a [ ]$^{\text{PROP/ECI}}$ timer is initiated. If the TSV fill isolation valve fully closed position indication is not active before the end of the [ ]$^{\text{PROP/ECI}}$ duration, then the TRPS initiates a Fill Stop. If the TSV fill isolation valve fully closed position indication is active prior to the end of the [ ]$^{\text{PROP/ECI}}$ duration, then the [ ]$^{\text{PROP/ECI}}$ timer resets.

During Mode 1, after NFDS source range neutron flux has reached or exceeded 40 percent of the maximum 95 percent fill flux, if the TSV fill isolation valve fully closed position indication becomes active, a 5-minute timer is initiated. If the TSV fill isolation valve fully closed position indication becomes inactive prior to the duration of the 5-minute timer ending, then the TRPS initiates a Fill Stop.

The Fill Stop parameters ensure that target solution can only be added to the TSV for a maximum of [ ]$^{\text{PROP/ECI}}$ and that a 5-minute delay occurs between fill steps.

7.4.3.3 Target Solution Vessel Reactivity Protection System Monitored Variables

Table 7.4-1 identifies the specific variables that provide input into the TRPS and includes the instrument range for covering normal and accident conditions, the accuracy for each variable, and the analytical limit.

7.4.3.4 Operating Conditions

The TRPS control and logic functions are located inside of the facility control room, where the environment is mild and not exposed to the irradiation process. However, cables providing signals to and from the TRPS are routed through the radiologically controlled area (RCA) and into the IUs, where those cables are exposed to harsher environments. Many of the sensors providing information to the TRPS are connected to the primary system boundary, so the cable routing to these sensors is exposed to the operating environment of the irradiation process.

During normal operation, the TRPS equipment will operate in the applicable normal radiation environments identified in Table 7.2-1 for up to 20 years, replaced at a frequency sufficient such that the radiation qualification of the affected components is not exceeded.

The environmental conditions present anywhere a component within the boundary of the TRPS may reside are outlined in Table 7.2-2 through Table 7.2-6. The facility heating, ventilation, and air conditioning (HVAC) systems are relied upon to maintain the temperature and humidity parameters in these areas. The facility HVAC systems are described in Section 9a2.1.

7.4.4 DESIGN ATTRIBUTES

7.4.4.1 Access Control

Access control is detailed in Subsection 7.2.5.

7.4.4.2 Software Requirements Development

Software requirements development is detailed in Subsection 7.2.6.

7.4.4.3 General Instrumentation and Control Design

The TRPS is powered from the uninterruptible electrical power supply system (UPSS), which provides a reliable source of power to maintain the TRPS functional during normal operation and during and following a design basis event. The UPSS is designed to provide power to the TRPS for two hours after a loss of off-site power. The UPSS is described in Section 8a2.2.

The actuation and priority logic (APL) portions within an equipment interface module (EIM) support the implementation of different actuation methods. The APL is implemented using discrete components and is not vulnerable to a software common cause failure (CCF). Having the capability for hardwired signals into each EIM supports the capability for additional and diverse actuation means from automated actuation. As an example, a division of APL circuits may receive inputs automatically from the programmable logic portion of the TRPS, inputs from manual controls in the facility control room, and input signals from a nonsafety control system. Both the manual controls and nonsafety control system inputs come individually into the APL and are downstream of the programmable logic portion of the TRPS architecture as shown in Figure 7.1-2.

7.4.4.4 Single Failure

The TRPS consists of three divisions of input processing and trip determination and two divisions of actuation logic (see Figure 7.1-2), arranged such that no single failure within the TRPS results in the loss of the protective function, and no single failure in a single measurement channel can generate an unnecessary safety actuation.

The only nonsafety inputs into the TRPS are those from the PICS for control, the discrete mode input, and monitoring and indication only variables. The nonsafety control signals from the PICS are implemented through a hardwired parallel interface that requires the PICS to send a binary address associated to the output state of the EIM along with a mirrored complement address. The mirrored complement address prevents any single incorrectly presented bit from addressing the wrong EIM output state. To prevent the PICS from inadvertently presenting a valid address, the TRPS contains a safety-related enable nonsafety switch that controls when the hardwired parallel interface within the APL is active, thus controlling when the PICS inputs are allowed to pass through the input circuitry and for use in the priority logic within the APL. When the enable nonsafety switch is not active, the nonsafety-related control signal is ignored. If the enable nonsafety is active, and no automatic or manual safety actuation command is present, the nonsafety-related control signal can control the TRPS output. The hardwired module (HWM) provides isolation for the nonsafety-related signal path.

The discrete mode input has a unique input for each of Division A and Division B. The HWM provides isolation of the signal path into the TRPS. As a discrete input, the three failure modes that are addressed are stuck high, stuck low, or oscillating. Because the TRPS only clocks in a new mode on the rising edge of the mode input, an input stuck low or high would maintain the TRPS in the same mode and continue monitoring the variables important to the safe operation of that mode. If the mode input began oscillating continuously between a logic high and low, the TRPS would only allow the mode to change if permissive conditions for the current mode are met. If the permissive conditions place the IU into a state that within the transitioned mode are outside of the predetermined operating limits, then the TRPS would initiate an IU Cell Safety Actuation and transition to and maintain Mode 3, ignoring any further input from the discrete mode input.

Each input variable to the TRPS for monitoring and indication only is processed on independent input submodules that are unique to that input. If the variable is not used for a safety function (i.e., no trip determination is performed with the variable), then the variable is not connected to the safety data buses and is only placed onto the monitoring and indication bus. The monitoring and indication bus is used by the monitoring and indication communication module (MI-CM) without interacting with any of the safety data paths.

7.4.4.5 Independence

See Subsection 7.2.2 for independence applied to the TRPS.

7.4.4.6 Prioritization of Functions

The APL (which is constructed of discrete components and part of the EIM) is designed to provide priority to safety-related signals over nonsafety-related signals. Division A and Division B priority logic of the TRPS prioritizes the following TRPS inputs, with the first input listed having the highest priority and each successive input in the list having a lower priority than the previous.

1) Automatic Safety Actuation, Manual Safety Actuation
2) PICS nonsafety control signals

7.4.4.7 Fail Safe

Safety actuations result in deenergizing one or more control outputs, and the controlled components are designed such that they go to their safe state when deenergized. On a loss of power to the TRPS, the TRPS deenergizes actuation components to the positions defined below:

<u>Mode 3 Transition Components</u>

- NDAS HVPS breakers
  - Open
- TSV dump valves
  - Open

<u>Primary System Boundary Components</u>

- TSV fill isolation valves
  - Closed
- TSV dump tank drain isolation valve
  - Closed
- TOGS gas supply isolation valves
  - Closed
- TOGS vacuum tank isolation valves
  - Closed
- VTS lower lift tank target solution valves
  - Closed

<u>Primary Confinement Components</u>

- N2PS inerting gas isolation valves
  - Open
- TOGS nitrogen vent isolation valves
  - Open
- TOGS RPCS supply isolation valves
  - Closed
- TOGS RPCS return isolation valve
  - Closed

- RVZ1e IU cell ventilation dampers
  - Closed
- RVZ1r RPCS supply isolation valve
  - Closed
- RVZ1r RPCS return isolation valve
  - Closed
- PCLS supply isolation valve
- ClosedPCLS return isolation valves
  - Closed
- TPS target chamber supply isolation valves
  - Closed
- TPS deuterium supply isolation valves
  - Closed
- TPS target chamber exhaust isolation valves
  - Closed
- TPS neutron driver evacuation isolation valves
  - Closed

7.4.4.8 Setpoints

Setpoints in the TRPS are based on a documented methodology that identifies each of the assumptions and accounts for the uncertainties in each instrument channel. The setpoint methodology is further described in Subsection 7.2.3.

7.4.4.9 Operational Bypass, Permissives, and Interlocks

Maintenance bypasses are described in Subsection 7.1.4.

Permissive conditions, bypasses, and interlocks are created in each mode of operation specific to that mode to allow the operator to progress the TRPS to the next mode of operation. The TRPS implements logic associated with each mode of operation to prevent an operator from activating a bypass through changing the IU cell mode out of sequential order. Each mode of operation is achieved through manual input from the operator when permissive conditions for the next mode in the sequence have been met. See the TRPS mode state diagram in the TRPS logic diagrams (Figure 7.4-1) for the transitional sequence of the TRPS. Below are the required conditions that must be satisfied before a transition to the following mode in the sequence can be initiated.

- The TRPS shall only transition from Mode 0 to Mode 1 if all TSV dump valve position indications and all TSV fill isolation valve indications indicate valves are fully closed and the TOGS mainstream flow is above the minimum flow rate.
- The TRPS shall only transition from Mode 1 to Mode 2 if the TSV fill isolation valve position indications indicate both valves are fully closed.
- The TRPS shall only transition from Mode 2 to Mode 3 if all HVPS breaker position indications indicate the breakers are open.
- The TRPS shall only transition from Mode 3 to Mode 4 if an IU Cell Safety Actuation is not present.
- The TRPS shall only transition from Mode 4 to Mode 0 if the TSV dump tank level is below the low-high TSV dump tank level.

In each mode of operation, the TRPS bypasses different actuation channels when the actuation channel is not needed for initiation of an IU Cell Safety Actuation, an IU Cell Nitrogen Purge, or Driver Dropout. The lists below identify each variable that is bypassed during the different modes of operation.

Safety actuations based on the following instrumentation channels are bypassed in Mode 0:

- Low power range neutron flux
- Low PCLS temperature
- High PCLS temperature
- Low PCLS flow
- Low TOGS mainstream flow
- Low TOGS dump tank flow
- High TOGS condenser demister outlet temperature
- ESFAS loss of external power

Safety actuations based on the following instrumentation channels are bypassed in Mode 1:

- Low power range neutron flux
- TSV fill isolation valve not fully closed

Safety actuations and interlocks based on the following instrumentation channels are bypassed in Mode 2:

- High source range neutron flux signal

The TRPS bypasses Driver Dropout on the low power range neutron flux signal until the power range neutron flux is above the driver dropout permissive setpoint. The bypass is reapplied if there has been a change in mode of operation or if both HVPS breaker position indications indicate in Mode 2 that they are open.

When the low power range neutron flux signal becomes active, a timer is started to create a [ ]$^{\text{PROP/ECI}}$ delay before a Driver Dropout is initiated. If fewer than two-out-of-three low power range neutron flux actuation signals are present before the timer has expired, then the low power range neutron flux timer resets.

Low PCLS flow and high PCLS temperature do not initiate an IU Cell Safety Actuation until after a time delay of 180 seconds from the start of the low PCLS flow or high PCLS temperature signal. If fewer than two-out-of-three Low PCLS flow or high PCLS temperature signals are present before the timer has expired, then the 180 second timer resets.

Safety actuations and interlocks based on the following instrumentation channels are bypassed in Mode 3:

- High source range neutron flux signal
- Low power range neutron flux
- High PCLS temperature
- Low PCLS temperature
- Low PCLS flow

- Low-high TSV dump tank level signal
- TSV fill isolation valve not fully closed

The TRPS includes the ability for the operator to transition the system from Mode 3 operation to a secure state of operation. While in the secure state, an interlock is maintained preventing the TRPS from transitioning to the next sequential mode. The control key, via use of a facility master operating permissive, is used to place the TRPS into and out of the secure state.

Safety actuations and interlocks based on the following instrumentation channels are bypassed in Mode 4:

- High source range neutron flux signal
- Low power range neutron flux
- High PCLS temperature
- Low PCLS temperature
- Low PCLS flow
- Low-high TSV dump tank level signal
- TSV fill isolation valve not fully closed

When the mode of operation changes, the bypasses are removed from the previous mode where they are no longer appropriate. The status of each bypass is provided to the operator through the monitoring and indication bus to the PICS, which allows the operator to confirm that a function has been bypassed or returned to service.

The manual actuation signals input from the operators in the facility control room are brought directly into the discrete actuation and priority logic. The manual actuation input into the priority logic does not have the ability to be bypassed and will always have equal priority to the automated actuation signal over any other signals that are present.

7.4.4.10 Completion of Protective Actions

The TRPS is designed so that once initiated, protective actions will continue to completion. Only deliberate operator action can be taken to reset the TRPS following a protective action. Figure 7.4-1 shows how the TRPS latches in a protective action and maintains the state of a protective action until operator input is initiated to reset the output of the TRPS.

The output of the TRPS is designed so that actuation through automatic or manual means of a safety function can only deenergize the output. If there is no signal present from the automatic safety actuation or manual safety actuation, then the output of the EIM remains in its current state. A safety-related enable nonsafety switch allows a facility operator, after the switch has been brought to enable, to control the output state of the TRPS with a hardwired binary control signal from the nonsafety-related controls. The enable nonsafety switch is classified as part of the safety system and is used to prevent spurious nonsafety-related control signals from adversely affecting safety-related components. If the enable nonsafety switch is active, and no automatic safety actuation or manual safety actuation signals are present, the operator is capable of energizing or deenergizing any EIM outputs using the nonsafety-related hardwired control signals. If the enable nonsafety switch is not active, the nonsafety-related hardwired control signals are ignored.

7.4.4.11 Equipment Qualification

TRPS rack mounted equipment is installed in a mild operating environment and is designed to meet the environmental conditions described in Subsection 7.4.3.4. Rack mounted TRPS equipment is tested to appropriate standards to show that the effects of EMI/RFI and power surges are adequately addressed. Appropriate grounding of the TRPS is performed in accordance with Section 5.2.1 of Institute of Electrical and Electronics Engineers (IEEE) Standard 1050-2004, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations (IEEE, 2004b).

7.4.4.12 Surveillance

The TRPS supports calibration and testing to ensure operability as described in Subsection 7.2.4.

7.4.4.13 Classification and Identification

Each division of the TRPS is uniquely labeled and identified in accordance with SHINE identification and classification procedures.

7.4.4.14 Human Factors

The TRPS provides manual safety actuation capability for the IU Cell Safety Actuation, the IU Cell Nitrogen Purge and Driver Dropout. To support the use of manual safety actuations, the TRPS associated with each IU cell includes isolated outputs for each safety-related instrument channel to provide monitoring and indication information to the PICS. To facilitate operator indication of mode control status, TRPS actuation function status, manual initiation and reset of protective actions, the TRPS, at the division level, includes isolated input/output for the following:

- Indication of TRPS variable values
- Indication of TRPS parameter values
- Indication of TRPS logic status
- Indication of TRPS equipment status
- Indication of TRPS actuation device status
- Indication of TRPS mode

7.4.4.15 Quality

The following codes and standards are applied to the TRPS design:

1) Section 8 of IEEE Standard 344-2013, IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations (IEEE, 2013); invoked as guidance to meet SHINE Design Criterion 2, Natural phenomena hazards.
2) IEEE Standard 379-2000, IEEE Standard Application of Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (IEEE, 2000); invoked to meet SHINE Design Criterion 15, Protection system reliability and testability.
3) IEEE Standard 384-2008, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (IEEE, 2008); invoked for separation of safety-related and nonsafety-related cables and raceways, as described in Subsection 8a2.1.3 and Subsection 8a2.1.5.

4) IEEE Standard 1023-2004, IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities (IEEE, 2004c); invoked as a guidance to support implementation of human factors into the design of I&C systems.
5) Section 5.2.1 of IEEE Standard 1050-2004, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations (IEEE, 2004b); invoked as guidance to support electromagnetic compatibility qualification for digital I&C equipment.
6) Regulatory Guide 1.152, Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (USNRC, 2011); invoked to demonstrate secure development and operating environment.
7) The guidance of ANSI/ANS 15.8-1995, Quality Assurance Program Requirements for Research Reactors (R2013) (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5, Quality Assurance Program Requirements for Research and Test Reactors (USNRC, 2010), is applied as part of the SHINE Quality Assurance Program for complying with the programmatic requirements of 10 CFR 50.34(b)(6)(ii).

7.4.5 OPERATION AND PERFORMANCE

7.4.5.1 High Source Range Neutron Flux

The high source range neutron flux signal protects against an insertion of excess reactivity during the filling process. The TRPS bypasses safety actuations based on the high source range neutron flux signal when filling activities cannot be in progress (i.e., Mode 2 and Mode 3), because the fill isolation valves are closed. The signal is transmitted as a discrete input to the TRPS from the NFDS through three independent and redundant channels, one for each division of TRPS. When two-out-of-three or more high source range neutron flux signals are active, an IU Cell Safety Actuation is initiated.

7.4.5.2 Low Power Range Neutron Flux

The low power range neutron flux signal protects against loss of the neutron beam followed by a restart of the neutron beam outside of analyzed conditions. The low power range neutron flux is only used during the irradiation process (Mode 2) and is bypassed in the other modes of operation. Safety actuations based on the low power range neutron flux are bypassed until the power range neutron flux has reached the power range driver dropout permissive. Once power range neutron flux levels have risen above the high setpoint, then the bypass on the low power range neutron flux is removed. The power range neutron flux is measured as an analog input to the TRPS from the NFDS through three independent and redundant channels, one for each division of TRPS. When two-out-of-three or more low power range neutron flux signals are active, a timer is started that must run to completion for a Driver Dropout to be initiated. If, while the timer is running, less than two-out-of-three low power range neutron flux actuation signals are active, the timer is reset and the TRPS continues operating under normal conditions.

7.4.5.3 High Time-Averaged Neutron Flux

The high time-averaged neutron flux signal protects against exceeding analyzed TSV power levels. The high time-averaged neutron flux averages the power range neutron flux over a set time period. The power range neutron flux is measured as an analog input to the TRPS from the NFDS through three independent and redundant channels, one for each division of TRPS. When two-out-of-three or more high time-averaged neutron flux signals are active, an IU Cell Safety Actuation is initiated.

7.4.5.4 High Wide Range Neutron Flux

The wide power range neutron flux signal protects against exceeding solution power density limits. The wide range neutron flux is measured as an analog input to the TRPS from the NFDS through three independent and redundant channels, one for each division of TRPS. When two-out-of-three or more high wide range neutron flux actuation signals are active, an IU Cell Safety Actuation is initiated.

7.4.5.5 High PCLS Temperature

The high PCLS temperature signal protects against a loss of cooling that could cause target solution heat-up. The PCLS temperature signal is measured with temperature interface on three different channels, one for each TRPS division. Safety actuations based on high PCLS temperature are not bypassed when target solution is present in the TSV (Mode 1 and Mode 2) and are bypassed in all other modes. When two-out-of-three or more PCLS temperature inputs exceed the allowable limit, a timer is started that must run to completion before initiating an IU Cell Safety Actuation. If, while the timer is running, less than two-out-of-three high PCLS temperature signals are active, the timer is reset and the TRPS continues operating under normal conditions. The timer is based on the acceptability of a complete loss of cooling for up to three minutes prior to transferring target solution to the TSV dump tank.

7.4.5.6 Low PCLS Temperature

The low PCLS temperature signal protects against an overcooling of the target solution that could cause an excess reactivity insertion. The PCLS temperature is measured with temperature interface on three different channels, one for each TRPS division. Safety actuations based on PCLS temperature are not bypassed during filling and irradiation of the target solution vessel (Mode 1 and Mode 2) and are bypassed in all other modes. When two-out-of-three or more PCLS temperature inputs drop below the allowable limit an IU Cell Safety Actuation is initiated.

7.4.5.7 Low PCLS Flow

The low PCLS flow signal protects against a loss of cooling that could cause target solution bulk boiling. The PCLS flow is measured with an analog interface on three different channels, one for each TRPS division. Safety actuation based on PCLS flow is not bypassed during filling and irradiation of the TSV (Mode 1 and Mode 2) and is bypassed in all other modes. When two-out-of-three or more PCLS flow inputs drop below the allowable limit, a timer is started that must run to completion before initiating an IU Cell Safety Actuation. If, while the timer is running, less than two-out-of-three low PCLS flow signals are active, the timer is reset and the TRPS continues operating under normal conditions. The timer is based on the acceptability of a complete loss of cooling for up to three minutes prior to transferring target solution to the TSV dump tank.

7.4.5.8 Low-High TSV Dump Tank Level

The low-high TSV dump tank level signal protects against a leak of liquid into the TSV dump tank, preventing the ability to transfer the entire batch of target solution from the TSV into the TSV dump tank. The low-high TSV dump tank level signal also results in a nitrogen purge of the

IU for an anticipatory loss of TSV dump tank headspace after target solution has been transferred to the TSV dump tank. The low-high TSV dump tank level signal is input as a discrete input from a level switch on three different channels, one for each TRPS division. Safety actuations based on the low-high TSV dump tank signal are bypassed during post irradiation when target solution is expected to be in the TSV dump tank (Mode 3 and Mode 4). The low-high TSV dump tank signal is used as a permissive condition to transition operational modes from transferring of the target solution to the RPF (Mode 4) to operating with no target solution in the IU (Mode 0). When two-out-of-three or more low-high TSV dump tank signals are active, an IU Cell Safety Actuation and an IU Cell Nitrogen Purge are initiated.

7.4.5.9 High-High TSV Dump Tank Level

The high-high TSV dump tank level signal protects against an overfill of the TSV dump tank (greater than the volume of target solution expected to be transferred from the TSV), compromising the ability of the TOGS to remove hydrogen from the TSV dump tank headspace. The high-high TSV dump tank level signal is input as a discrete input from a level switch on three different channels, one for each TRPS division. When two-out-of-three or more high-high TSV dump tank signals are active, an IU Cell Safety Actuation and an IU Cell Nitrogen Purge are initiated.

7.4.5.10 Low TOGS Oxygen Concentration

The low TOGS oxygen concentration signal protects against a deflagration in the primary system boundary caused by the inability to recombine hydrogen with oxygen. The TOGS oxygen signal is measured with an analog interface on three different channels, one for each division of TRPS. When two-out-of-three or more TOGS oxygen concentration inputs drop below the allowable limit, an IU Cell Safety Actuation and an IU Cell Nitrogen Purge are initiated.

7.4.5.11 Low TOGS Mainstream Flow

The low TOGS mainstream flow signal protects against a deflagration in the primary system boundary caused by the inability to sweep accumulated hydrogen through the TOGS hydrogen recombiners. The TOGS mainstream flow is measured with an analog interface on three different channels, one for each division of TRPS. Safety actuations based on the low TOGS mainstream flow are bypassed when no target solution is present in the IU. When two-out-of-three or more TOGS mainstream flow inputs drop below the allowable limit, an IU Cell Safety Actuation and an IU Cell Nitrogen Purge are initiated.

7.4.5.12 Low TOGS Dump Tank Flow

The low TOGS dump tank flow signal protects against a deflagration in the TSV dump tank caused by an inability to remove accumulated hydrogen from that tank. The TOGS dump tank flow is measured with an analog interface on three different channels, one for each division of TRPS. Safety actuations based on the low TOGS dump tank flow are bypassed when no target solution is present in the IU. When two-out-of-three or more TOGS dump tank flow inputs drop below the allowable limit, an IU Cell Safety Actuation and an IU Cell Nitrogen Purge are initiated.

7.4.5.13 High TOGS Condenser Demister Outlet Temperature

The high TOGS condenser demister outlet temperature signal protects against adverse effects on TOGS instrumentation and zeolite beds, causing them to fail to perform their safety functions. The TOGS condenser demister outlet temperature signal is measured with a temperature interface on three different channels, one for each TRPS division. When two-out-of-three or more TOGS condenser demister outlet temperature inputs exceed the allowable limit, an IU Cell Safety Actuation and an IU Cell Nitrogen Purge are initiated.

7.4.5.14 ESFAS Loss of External Power

The ESFAS loss of external power signal is an anticipatory protection against the impending loss of TOGS blowers and recombiners after the runtime of that equipment on the UPSS has been exceeded. TRPS does not receive the loss of external power signal from ESFAS until three minutes after the external power loss. The ESFAS loss of external power signal is measured with a discrete input signal on two different channels, one for each Division A and Division B of TRPS. When an ESFAS loss of external power signal is active, the division receiving the discrete signal initiates an IU Cell Nitrogen Purge.

7.4.5.15 High RVZ1e IU Cell Radiation

The high RVZ1 radiation signal protects against a breach in the primary system boundary. The RVZ1 radiation is measured with an analog interface on three different channels, one for each division of TRPS. When two-out-of-three or more RVZ1 radiation channels exceed the allowable limit, an IU Cell Safety Actuation is initiated.

7.4.5.16 TSV Fill Isolation Valves Open

A TSV fill isolation valve open signal protects against the inadvertent addition of target solution to the TSV. The TSV valve open position indication is measured with a discrete input on two different channels for each valve. When one-out-of-two or more TSV fill isolation valve open signals are active for both of the TSV fill isolation valves, an IU Cell Safety Actuation is initiated. IU Cell Safety Actuation on TSV valves open is only active when the IU cell is undergoing irradiation (Mode 2).

7.4.5.17 ESFAS IU Cell TPS Actuation

An ESFAS IU Cell TPS Actuation protects against release of tritium events in the TPS. The ESFAS IU Cell TPS Actuation is measured with a discrete input signal on two different channels, one for each Division A and Division B of TRPS. When an ESFAS IU Cell TPS Actuation is active, the division receiving the discrete signal initiates an IU Cell TPS Actuation.

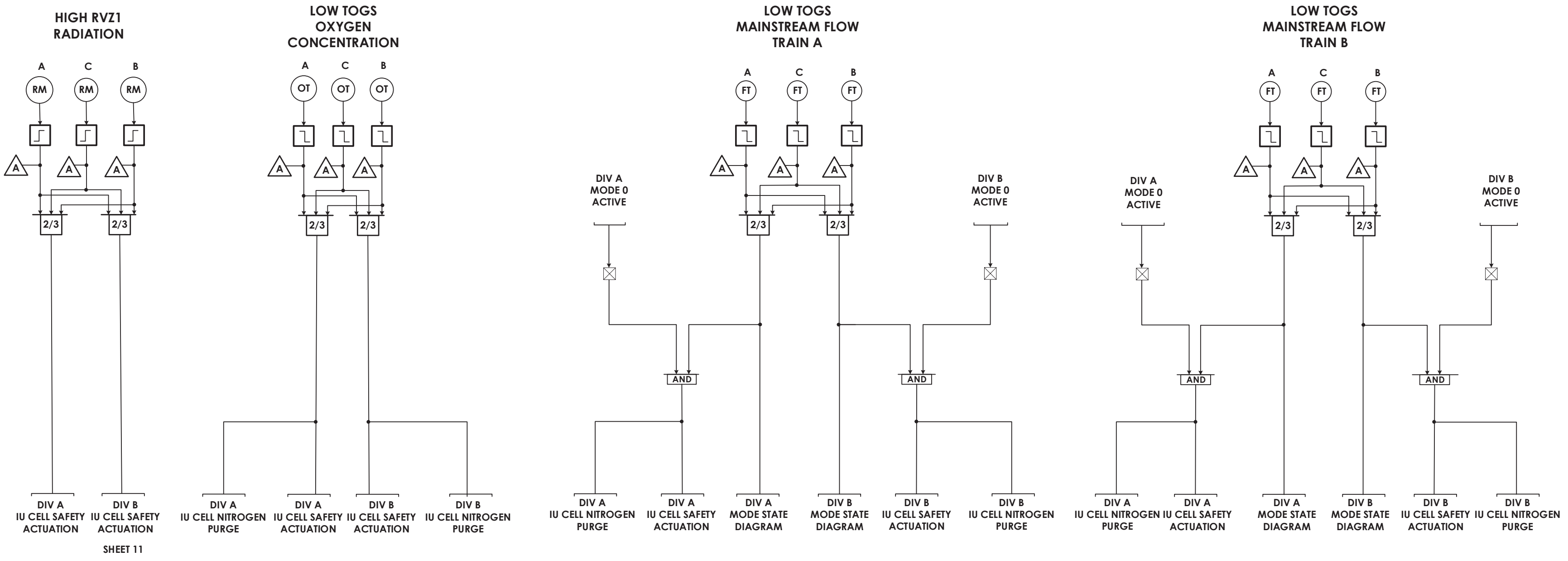
Table 7.4-1 – TRPS Monitored Variables (Sheet 1 of 2)

Variable	Analytical Limit	Logic	Range	Accuracy	Instrument Response Time
Source range neutron flux signal	1.5 times the nominal flux at 95 percent volume of the critical fill height	2/3↑	1 to 1.0E+05 cps	2 percent	450 milliseconds
Wide range neutron flux	240 percent	2/3↑	1.0E-8 to 250 percent	2 percent	450 milliseconds
Power range neutron flux	[ ]$^{\text{PROP/ECI}}$	2/3↓	0 to 125 percent	1 percent	1 second
	25 percent	2/3↑			
	104 percent	2/3↑			
RVZ1e IU cell radiation	5x background radiation	2/3↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
TOGS oxygen concentration	10 percent	2/3↓	0 to 25 percent	1 percent	120 seconds
TOGS mainstream flow	[ ]$^{\text{PROP/ECI}}$	2/3↓	[ ]$^{\text{PROP/ECI}}$	3 percent	0.5 seconds
TOGS dump tank flow	[ ]$^{\text{PROP/ECI}}$	2/3↓	[ ]$^{\text{PROP/ECI}}$	3 percent	0.5 seconds
TOGS upstream condenser demister outlet temperature	25°C	2/3↑	0 to 100°C	0.65 percent	10 seconds
Low-high TSV dump tank level signal	Active	2/3↑	Active/inactive	Discrete input signal	1.5 seconds
High-high TSV dump tank level signal	Active	2/3↑	Active/inactive	Discrete input signal	1.5 seconds
PCLS flow	[ ]$^{\text{PROP/ECI}}$	2/3↓	[ ]$^{\text{PROP/ECI}}$	1 percent	1 second
PCLS temperature	15°C	2/3↓	-1 to 121°C	1 percent	10 seconds
	25°C	2/3↑			

Table 7.4-1 – TRPS Monitored Variables
(Sheet 2 of 2)

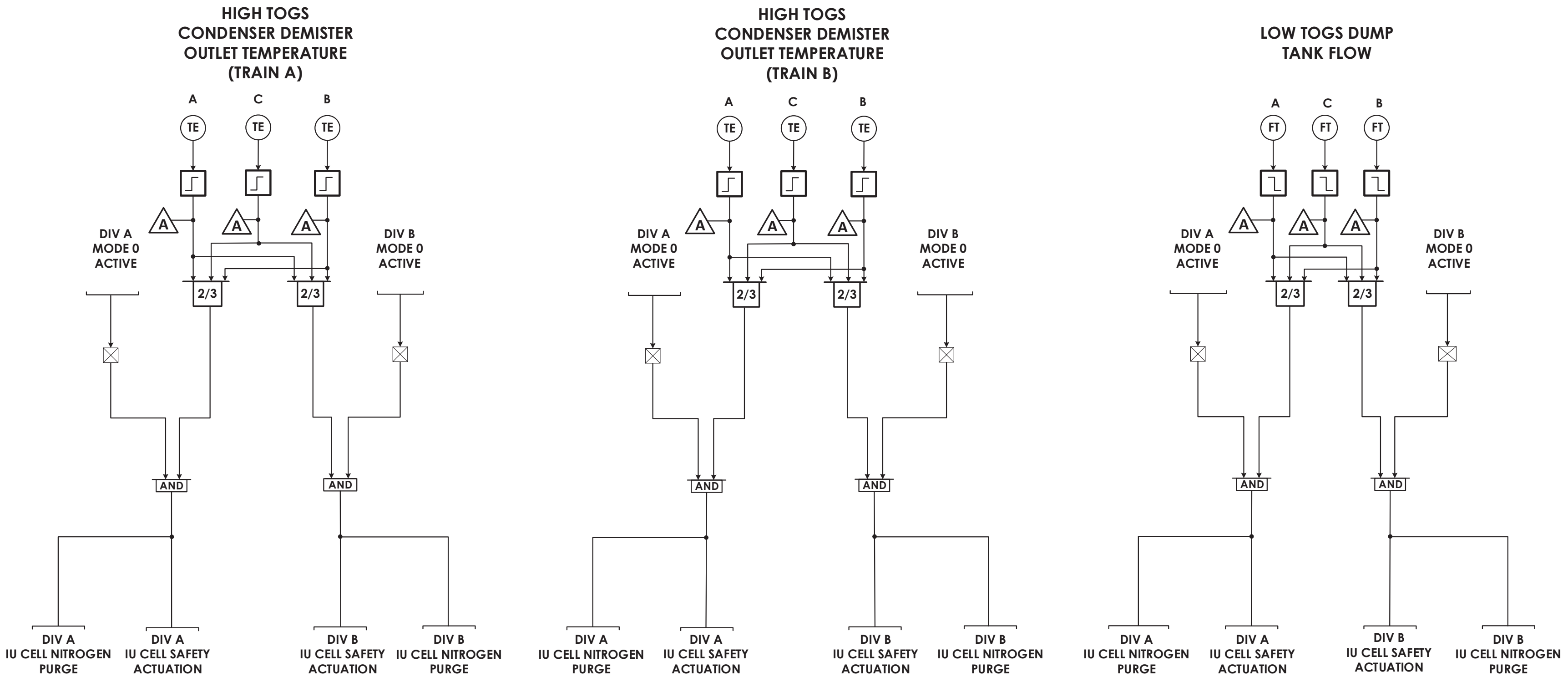
Variable	Analytical Limit	Logic	Range	Accuracy	Instrument Response Time
TSV fill valve close position indication	Inactive full close	1/2↑	Active/inactive	Discrete input signal	0.5 seconds
ESFAS loss of external power	Inactive	1/1↑	Active/inactive	Discrete input signal	0.5 seconds

Figure 7.4-1 – TRPS Logic Diagrams (Sheet 1 of 14)


HIGH RVZ1 RADIATION
A
C
B
RM
RM
RM
A
A
A
2/3
2/3
DIV A IU CELL SAFETY ACTUATION
DIV B IU CELL SAFETY ACTUATION
SHEET 11
LOW TOGS OXYGEN CONCENTRATION
A
C
B
OT
OT
OT
A
A
A
2/3
2/3
DIV A IU CELL NITROGEN PURGE
DIV A IU CELL SAFETY ACTUATION
DIV B IU CELL SAFETY ACTUATION
DIV B IU CELL NITROGEN PURGE
LOW TOGS MAINSTREAM FLOW TRAIN A
A
C
B
FT
FT
FT
A
A
A
DIV A MODE 0 ACTIVE
DIV B MODE 0 ACTIVE
2/3
2/3
AND
AND
DIV A IU CELL NITROGEN PURGE
DIV A IU CELL SAFETY ACTUATION
DIV A MODE STATE DIAGRAM
DIV B MODE STATE DIAGRAM
DIV B IU CELL SAFETY ACTUATION
DIV B IU CELL NITROGEN PURGE
LOW TOGS MAINSTREAM FLOW TRAIN B
A
C
B
FT
FT
FT
A
A
A
DIV A MODE 0 ACTIVE
DIV B MODE 0 ACTIVE
2/3
2/3
AND
AND
DIV A IU CELL NITROGEN PURGE
DIV A IU CELL SAFETY ACTUATION
DIV A MODE STATE DIAGRAM
DIV B MODE STATE DIAGRAM
DIV B IU CELL SAFETY ACTUATION
DIV B IU CELL NITROGEN PURGE

Trip Determination and Bypasses

Figure 7.4-1 – TRPS Logic Diagrams (Sheet 2 of 14)



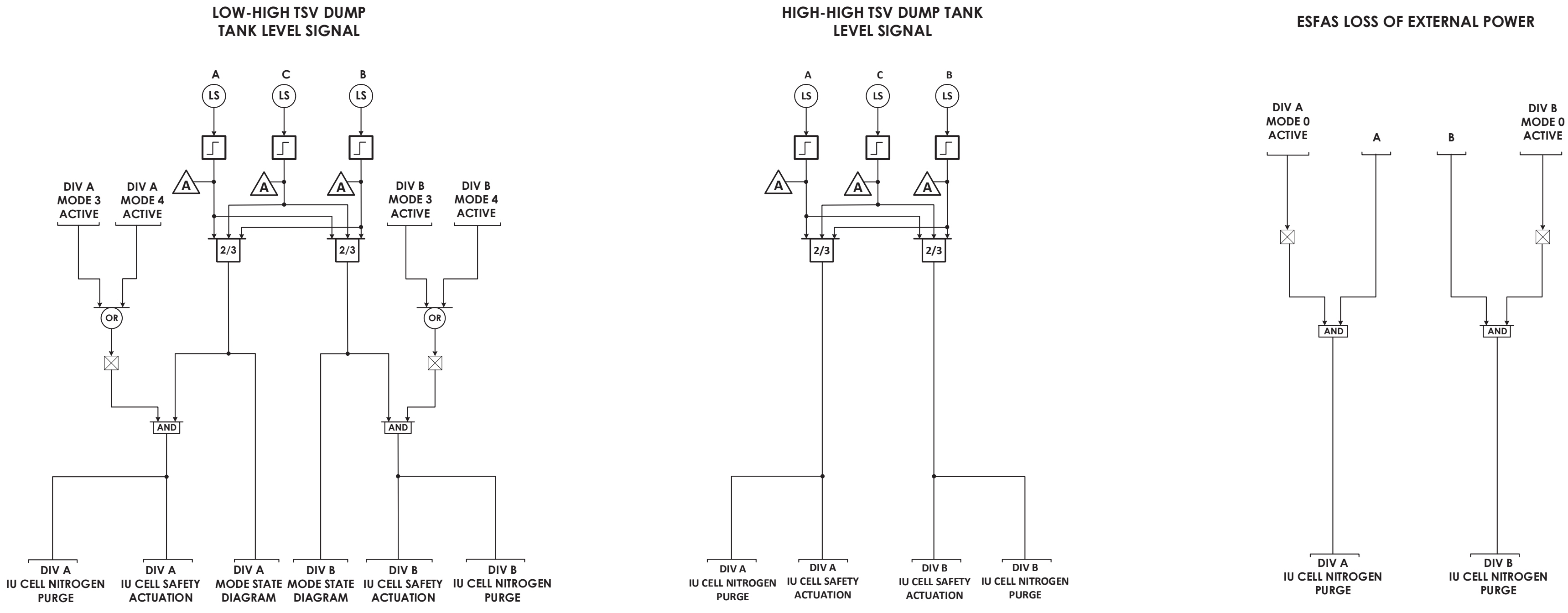
Trip Determination and Bypasses

Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 3 of 14)

Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 4 of 14)

**Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 5 of 14)**

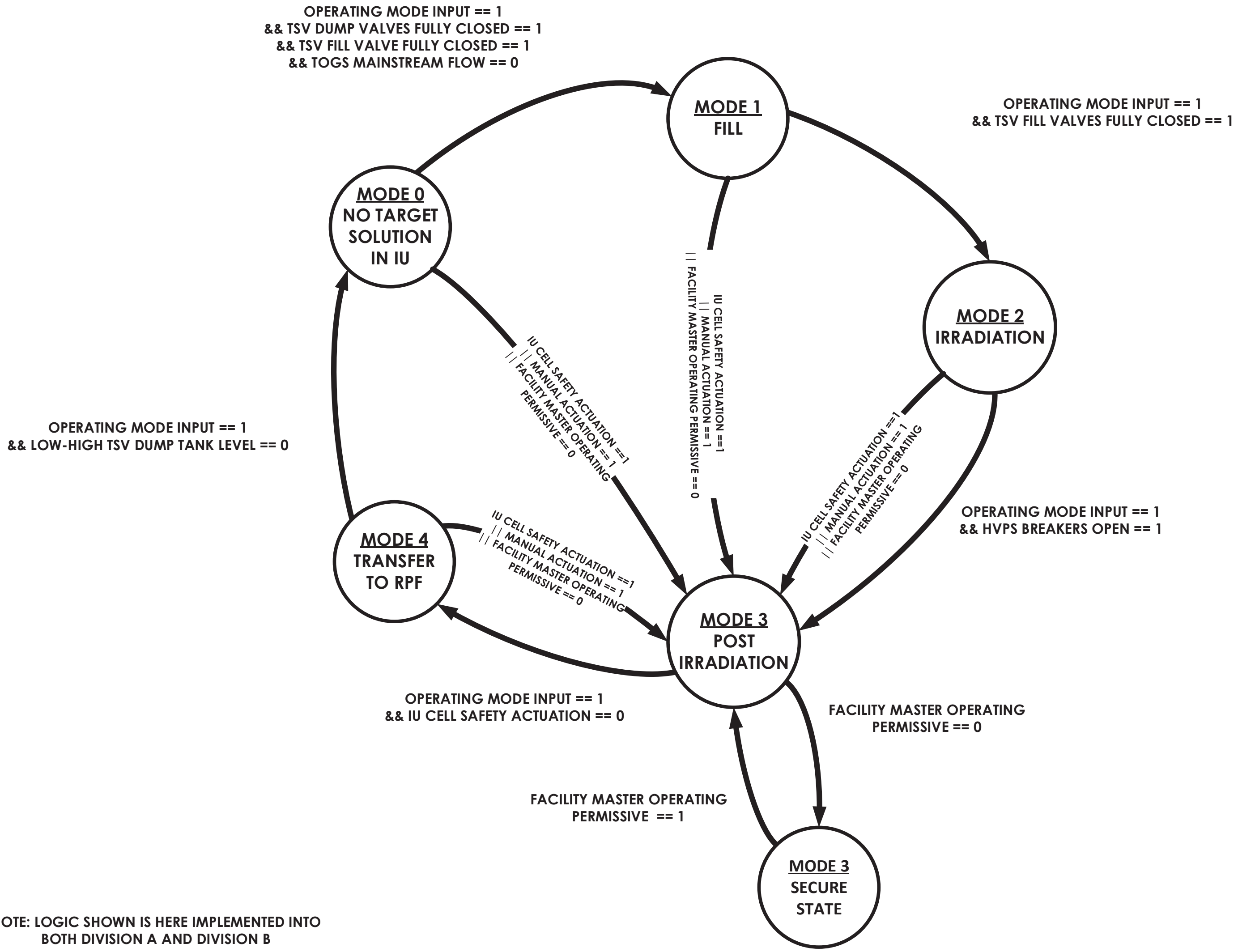
Figure 7.4-1 – TRPS Logic Diagrams (Sheet 6 of 14)


LOW-HIGH TSV DUMP TANK LEVEL SIGNAL
A
C
B
LS
LS
LS
A
A
A
DIV A MODE 3 ACTIVE
DIV A MODE 4 ACTIVE
DIV B MODE 3 ACTIVE
DIV B MODE 4 ACTIVE
2/3
2/3
OR
OR
AND
AND
DIV A IU CELL NITROGEN PURGE
DIV A IU CELL SAFETY ACTUATION
DIV A MODE STATE DIAGRAM
DIV B MODE STATE DIAGRAM
DIV B IU CELL SAFETY ACTUATION
DIV B IU CELL NITROGEN PURGE
HIGH-HIGH TSV DUMP TANK LEVEL SIGNAL
A
C
B
LS
LS
LS
A
A
A
2/3
2/3
DIV A IU CELL NITROGEN PURGE
DIV A IU CELL SAFETY ACTUATION
DIV B IU CELL SAFETY ACTUATION
DIV B IU CELL NITROGEN PURGE
ESFAS LOSS OF EXTERNAL POWER
DIV A MODE 0 ACTIVE
A
B
DIV B MODE 0 ACTIVE
AND
AND
DIV A IU CELL NITROGEN PURGE
DIV B IU CELL NITROGEN PURGE

Trip Determination and Bypasses

Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 7 of 14)

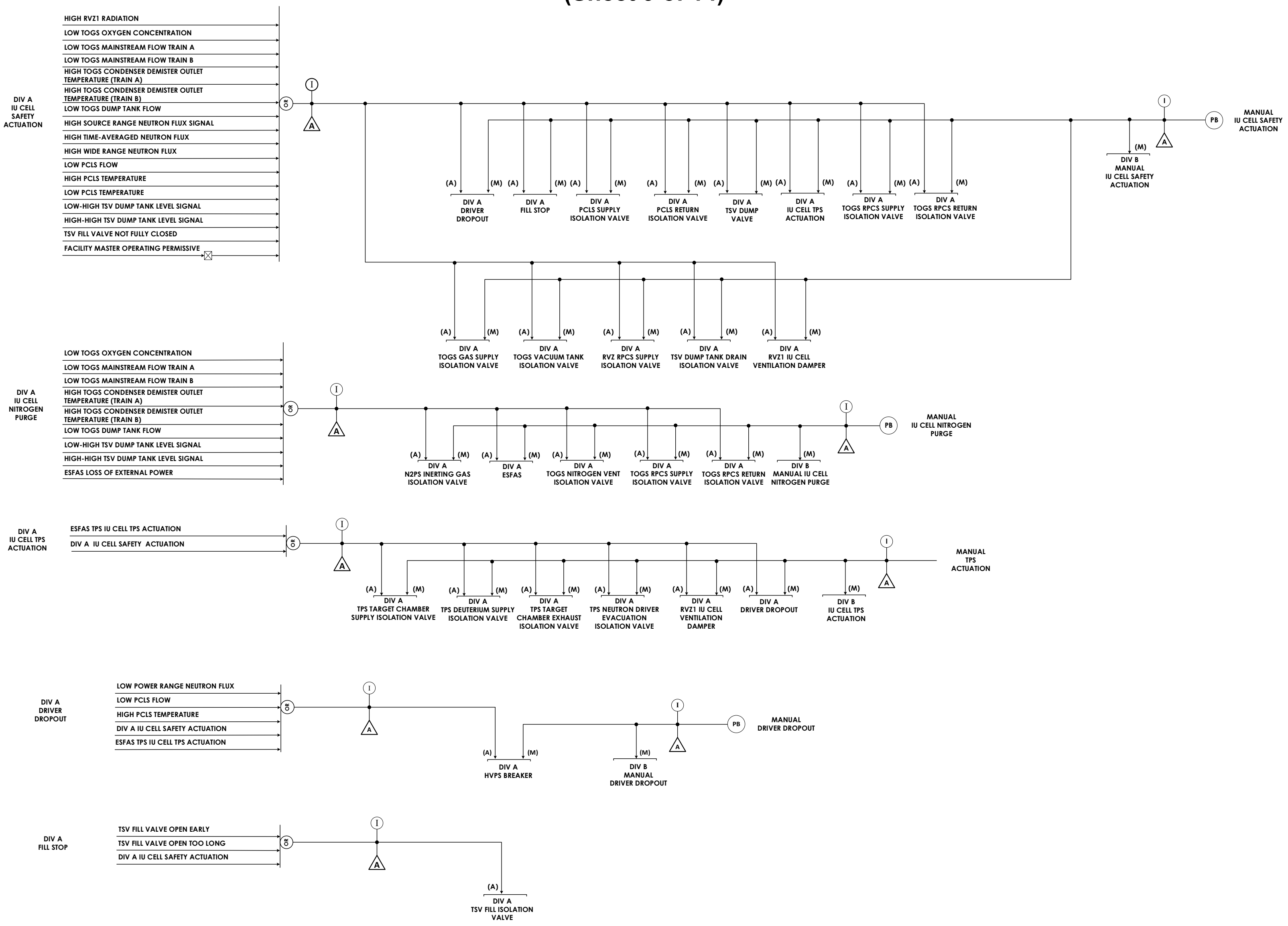
Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 8 of 14)


OPERATING MODE INPUT == 1
&& TSV DUMP VALVES FULLY CLOSED == 1
&& TSV FILL VALVE FULLY CLOSED == 1
&& TOGS MAINSTREAM FLOW == 0
MODE 1
FILL
OPERATING MODE INPUT == 1
&& TSV FILL VALVES FULLY CLOSED == 1
MODE 0
NO TARGET
SOLUTION
IN IU
MODE 2
IRRADIATION
IU CELL SAFETY ACTUATION ==1
|| MANUAL ACTUATION == 1
|| FACILITY MASTER OPERATING PERMISSIVE == 0
IU CELL SAFETY ACTUATION ==1
|| MANUAL ACTUATION == 1
|| FACILITY MASTER OPERATING
PERMISSIVE == 0
OPERATING MODE INPUT == 1
&& LOW-HIGH TSV DUMP TANK LEVEL == 0
IU CELL SAFETY ACTUATION ==1
|| MANUAL ACTUATION == 1
|| FACILITY MASTER OPERATING
PERMISSIVE == 0
OPERATING MODE INPUT == 1
&& HVPS BREAKERS OPEN == 1
MODE 4
TRANSFER
TO RPF
IU CELL SAFETY ACTUATION ==1
|| MANUAL ACTUATION == 1
|| FACILITY MASTER OPERATING
PERMISSIVE == 0
MODE 3
POST
IRRADIATION
OPERATING MODE INPUT == 1
&& IU CELL SAFETY ACTUATION == 0
FACILITY MASTER OPERATING
PERMISSIVE == 0
FACILITY MASTER OPERATING
PERMISSIVE == 1
MODE 3
SECURE
STATE

NOTE: LOGIC SHOWN IS HERE IMPLEMENTED INTO
BOTH DIVISION A AND DIVISION B

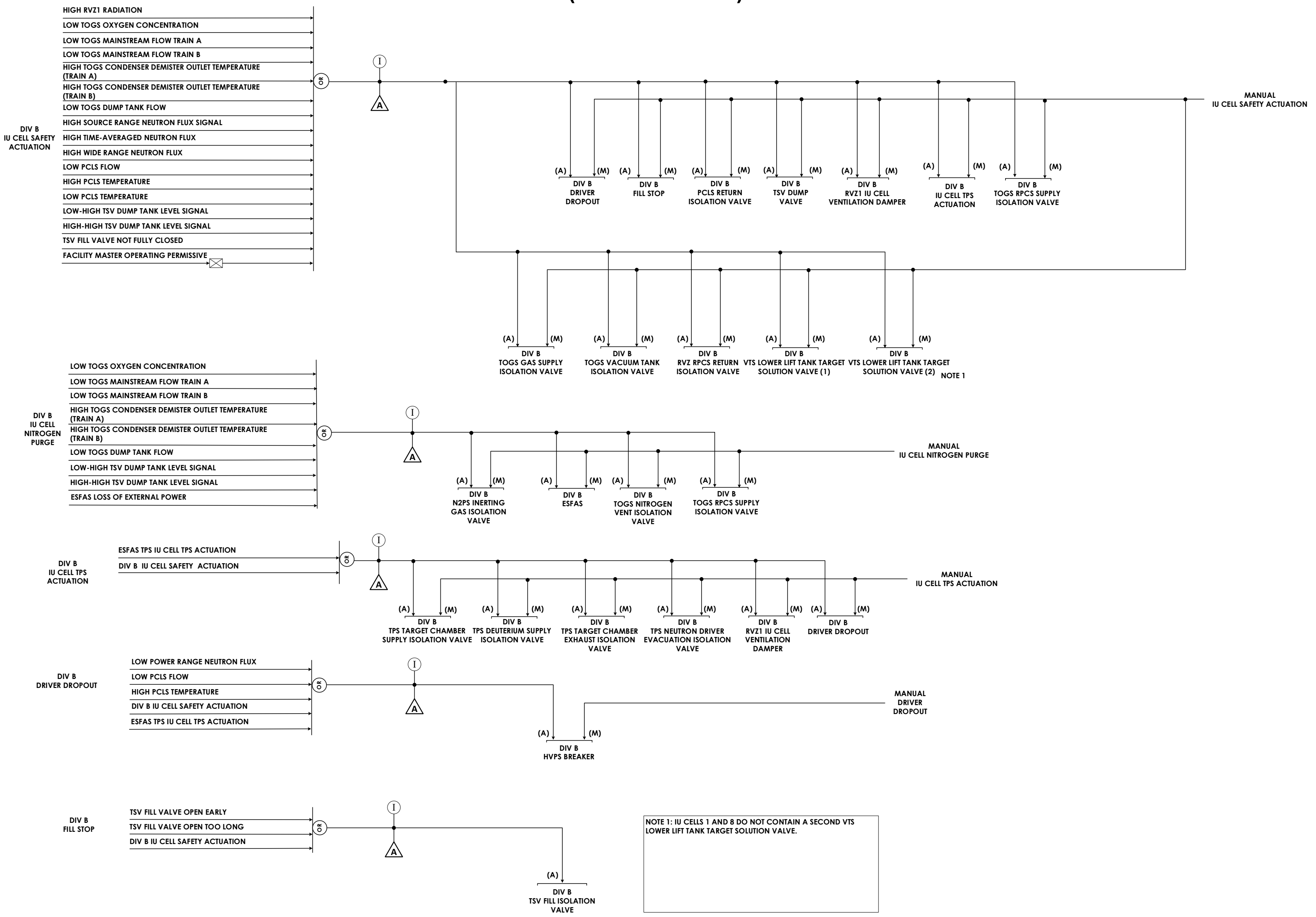
Mode State Machine

Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 9 of 14)


DIV A
IU CELL
SAFETY
ACTUATION
HIGH RVZ1 RADIATION
LOW TOGS OXYGEN CONCENTRATION
LOW TOGS MAINSTREAM FLOW TRAIN A
LOW TOGS MAINSTREAM FLOW TRAIN B
HIGH TOGS CONDENSER DEMISTER OUTLET TEMPERATURE (TRAIN A)
HIGH TOGS CONDENSER DEMISTER OUTLET TEMPERATURE (TRAIN B)
LOW TOGS DUMP TANK FLOW
HIGH SOURCE RANGE NEUTRON FLUX SIGNAL
HIGH TIME-AVERAGED NEUTRON FLUX
HIGH WIDE RANGE NEUTRON FLUX
LOW PCLS FLOW
HIGH PCLS TEMPERATURE
LOW PCLS TEMPERATURE
LOW-HIGH TSV DUMP TANK LEVEL SIGNAL
HIGH-HIGH TSV DUMP TANK LEVEL SIGNAL
TSV FILL VALVE NOT FULLY CLOSED
FACILITY MASTER OPERATING PERMISSIVE
OR
I
A
DIV A DRIVER DROPOUT
DIV A FILL STOP
DIV A PCLS SUPPLY ISOLATION VALVE
DIV A PCLS RETURN ISOLATION VALVE
DIV A TSV DUMP VALVE
DIV A IU CELL TPS ACTUATION
DIV A TOGS RPCS SUPPLY ISOLATION VALVE
DIV A TOGS RPCS RETURN ISOLATION VALVE
DIV B MANUAL IU CELL SAFETY ACTUATION
PB
MANUAL IU CELL SAFETY ACTUATION
DIV A TOGS GAS SUPPLY ISOLATION VALVE
DIV A TOGS VACUUM TANK ISOLATION VALVE
DIV A RVZ RPCS SUPPLY ISOLATION VALVE
DIV A TSV DUMP TANK DRAIN ISOLATION VALVE
DIV A RVZ1 IU CELL VENTILATION DAMPER
(A)
(M)
DIV A
IU CELL
NITROGEN
PURGE
LOW TOGS OXYGEN CONCENTRATION
LOW TOGS MAINSTREAM FLOW TRAIN A
LOW TOGS MAINSTREAM FLOW TRAIN B
HIGH TOGS CONDENSER DEMISTER OUTLET TEMPERATURE (TRAIN A)
HIGH TOGS CONDENSER DEMISTER OUTLET TEMPERATURE (TRAIN B)
LOW TOGS DUMP TANK FLOW
LOW-HIGH TSV DUMP TANK LEVEL SIGNAL
HIGH-HIGH TSV DUMP TANK LEVEL SIGNAL
ESFAS LOSS OF EXTERNAL POWER
DIV A N2PS INERTING GAS ISOLATION VALVE
DIV A ESFAS
DIV A TOGS NITROGEN VENT ISOLATION VALVE
DIV A TOGS RPCS SUPPLY ISOLATION VALVE
DIV A TOGS RPCS RETURN ISOLATION VALVE
DIV B MANUAL IU CELL NITROGEN PURGE
MANUAL IU CELL NITROGEN PURGE
DIV A
IU CELL TPS
ACTUATION
ESFAS TPS IU CELL TPS ACTUATION
DIV A IU CELL SAFETY ACTUATION
DIV A TPS TARGET CHAMBER SUPPLY ISOLATION VALVE
DIV A TPS DEUTERIUM SUPPLY ISOLATION VALVE
DIV A TPS TARGET CHAMBER EXHAUST ISOLATION VALVE
DIV A TPS NEUTRON DRIVER EVACUATION ISOLATION VALVE
DIV A RVZ1 IU CELL VENTILATION DAMPER
DIV A DRIVER DROPOUT
DIV B IU CELL TPS ACTUATION
MANUAL TPS ACTUATION
DIV A
DRIVER
DROPOUT
LOW POWER RANGE NEUTRON FLUX
LOW PCLS FLOW
HIGH PCLS TEMPERATURE
DIV A IU CELL SAFETY ACTUATION
ESFAS TPS IU CELL TPS ACTUATION
DIV A HVPS BREAKER
DIV B MANUAL DRIVER DROPOUT
MANUAL DRIVER DROPOUT
DIV A
FILL STOP
TSV FILL VALVE OPEN EARLY
TSV FILL VALVE OPEN TOO LONG
DIV A IU CELL SAFETY ACTUATION
DIV A TSV FILL ISOLATION VALVE

Safety Function

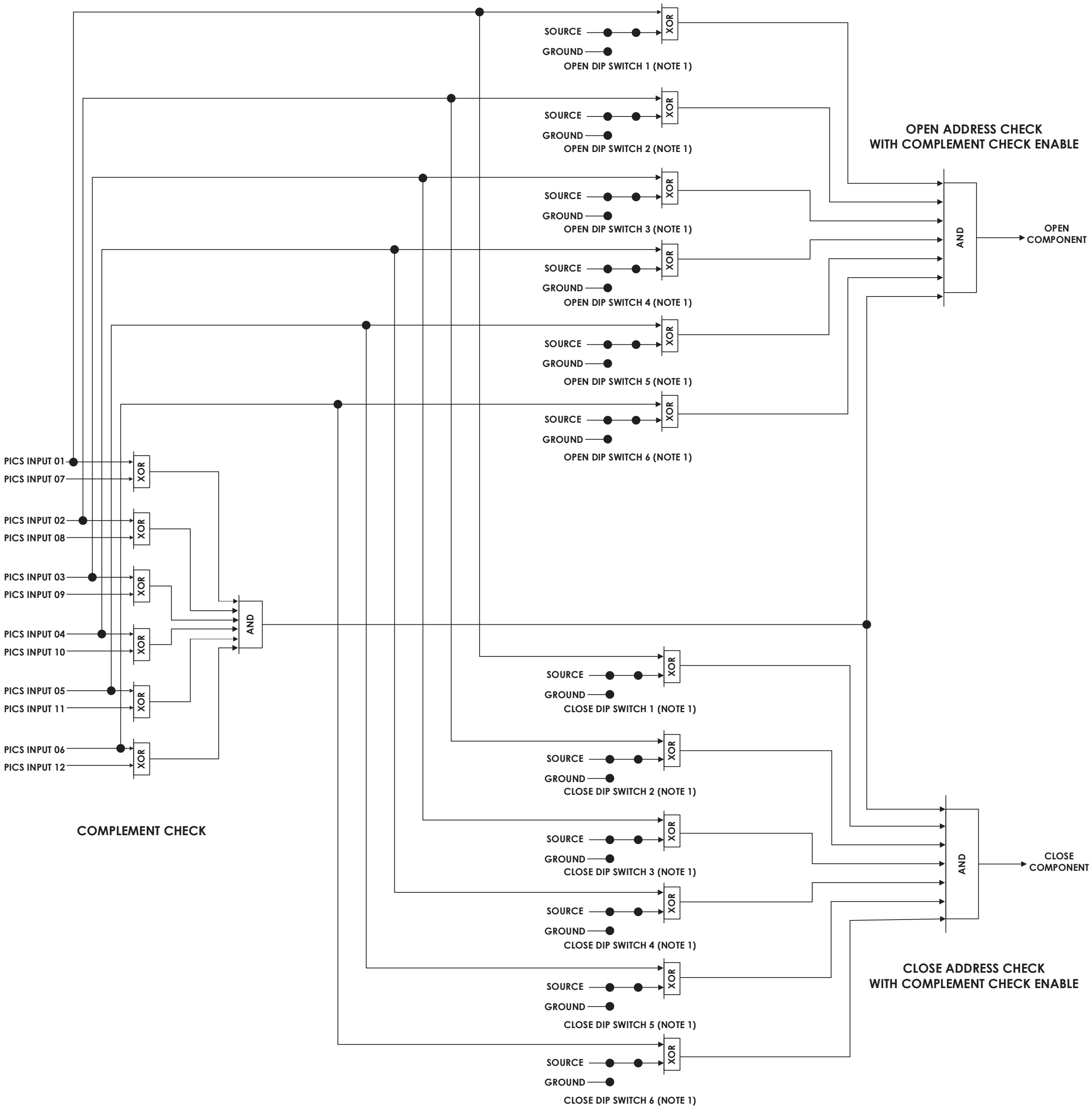
Figure 7.4-1 – TRPS Logic Diagrams (Sheet 10 of 14)



NOTE 1: IU CELLS 1 AND 8 DO NOT CONTAIN A SECOND VTS LOWER LIFT TANK TARGET SOLUTION VALVE.

Safety Function

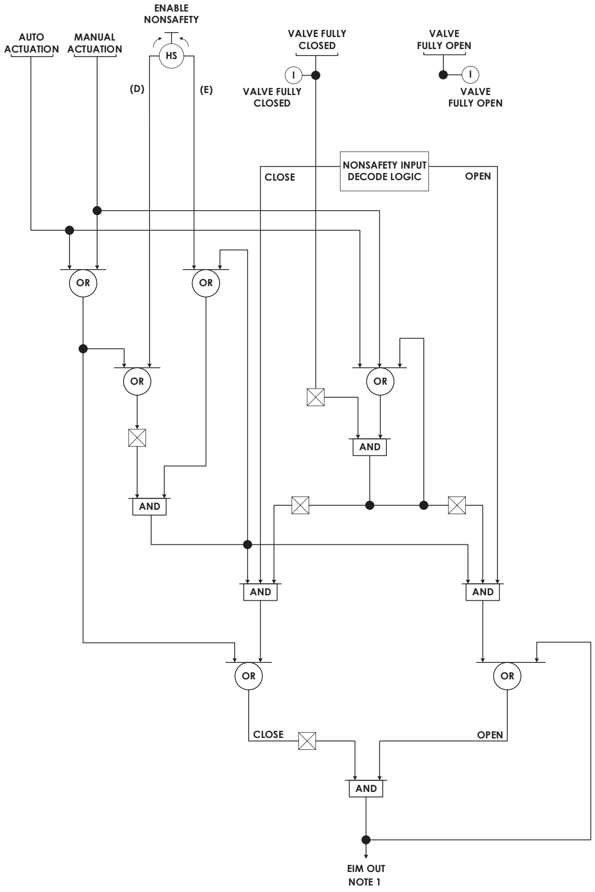
Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 11 of 14)


XOR
SOURCE
GROUND
OPEN DIP SWITCH 1 (NOTE 1)
OPEN DIP SWITCH 2 (NOTE 1)
OPEN DIP SWITCH 3 (NOTE 1)
OPEN DIP SWITCH 4 (NOTE 1)
OPEN DIP SWITCH 5 (NOTE 1)
OPEN DIP SWITCH 6 (NOTE 1)
OPEN ADDRESS CHECK
WITH COMPLEMENT CHECK ENABLE
AND
OPEN COMPONENT
PICS INPUT 01
PICS INPUT 07
PICS INPUT 02
PICS INPUT 08
PICS INPUT 03
PICS INPUT 09
PICS INPUT 04
PICS INPUT 10
PICS INPUT 05
PICS INPUT 11
PICS INPUT 06
PICS INPUT 12
COMPLEMENT CHECK
CLOSE DIP SWITCH 1 (NOTE 1)
CLOSE DIP SWITCH 2 (NOTE 1)
CLOSE DIP SWITCH 3 (NOTE 1)
CLOSE DIP SWITCH 4 (NOTE 1)
CLOSE DIP SWITCH 5 (NOTE 1)
CLOSE DIP SWITCH 6 (NOTE 1)
CLOSE COMPONENT
CLOSE ADDRESS CHECK
WITH COMPLEMENT CHECK ENABLE

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

Nonsafety Interface Decode

Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 12 of 14)

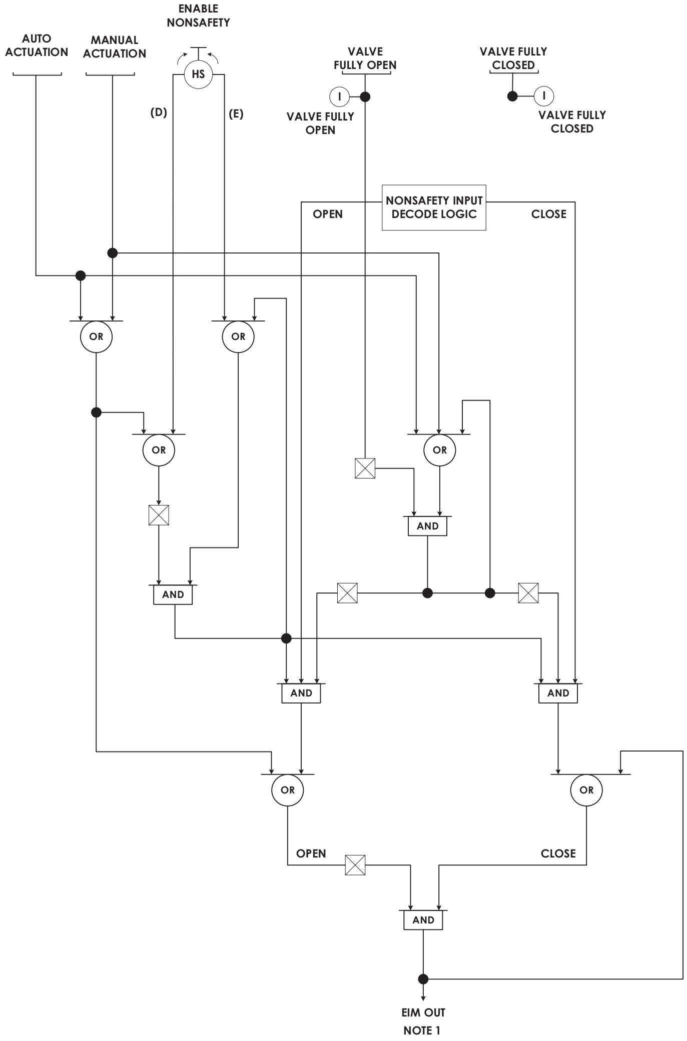


DIV A TSV FILL ISOLATION VALVE	DIV B TSV FILL ISOLATION VALVE
DIV A TSV DUMP TANK DRAIN ISOLATION VALVE	DIV B PCLS RETURN ISOLATION VALVE
DIV A PCLS SUPPLY ISOLATION VALVE	DIV B TPS TARGET CHAMBER SUPPLY ISOLATION VALVE
DIV A PCLS RETURN ISOLATION VALVE	DIV B TPS DEUTERIUM SUPPLY ISOLATION VALVE
DIV A TPS TARGET CHAMBER SUPPLY ISOLATION VALVE	DIV B TPS TARGET CHAMBER EXHAUST ISOLATION VALVE
DIV A TPS DEUTERIUM SUPPLY ISOLATION VALVE	DIV B TPS NEUTRON DRIVER EVACUATION ISOLATION VALVE
DIV A TPS TARGET CHAMBER EXHAUST ISOLATION VALVE	DIV B TOGS GAS SUPPLY LINE ISOLATION VALVE
DIV A TPS NEUTRON DRIVER EVACUATION ISOLATION VALVE	DIV B TOGS VACUUM TANK ISOLATION VALVE
DIV A TOGS GAS SUPPLY LINE ISOLATION VALVE	DIV B TOGS RPCS SUPPLY ISOLATION VALVE
DIV A TOGS VACUUM TANK ISOLATION VALVE	DIV B RVZ RPCS RETURN ISOLATION VALVE
DIV A TOGS RPCS SUPPLY ISOLATION VALVE	DIV B RVZ1 IU CELL VENTILATION DAMPER
DIV A TOGS RPCS RETURN ISOLATION VALVE	DIV B VTS LOWER LIFT TANK TARGET SOLUTION VALVE (1)
DIV A RVZ RPCS SUPPLY ISOLATION VALVE	DIV B VTS LOWER LIFT TANK TARGET SOLUTION VALVE (2)
DIV A RVZ1 IU CELL VENTILATION DAMPER	

NOTE 1: OUTPUT OF EIM IS DEENERGIZE TO ACTUATE TO POSITION DEFINED FOR LOSS OF POWER

Priority Logic

Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 13 of 14)



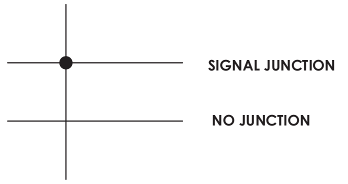
DIV A TSV DUMP VALVE	DIV B TSV DUMP VALVE
DIV A HVPS BREAKER	DIV B HVPS BREAKER
DIV A N2PS INERTING GAS ISOLATION VALVE	DIV B N2PS INERTING GAS ISOLATION VALVE
DIV A TOGS NITROGEN VENT ISOLATION VALVE	DIV B TOGS NITROGEN VENT ISOLATION VALVE

NOTE 1: OUTPUT OF EIM IS DEENERGIZE TO ACTUATE TO POSITION DEFINED FOR LOSS OF POWER

Priority Logic

Figure 7.4-1 – TRPS Logic Diagrams
(Sheet 14 of 14)

A	PROCESS INTEGRATED CONTROL SYSTEM ALARM POINT	NS	NEUTRON FLUX SOURCE RANGE
I	INDICATION PROVIDED TO PROCESS INTEGRATED CONTROL SYSTEM	NW	NEUTRON FLUX WIDE RANGE
OR	LOGICAL "OR" GATE	NP	NEUTRON FLUX POWER RANGE
AND	LOGICAL "AND" GATE	LS	LEVEL SWITCH
☒	LOGICAL "NOT" OR INVERTER GATE	HT	HYDROGEN TRANSMITTER
XOR	LOGICAL "XOR" GATE	OT	OXYGEN TRANSMITTER
2/3	TWO-OUT-OF-THREE VOTING GATE	TT	TRITIUM TRANSMITTER
2/2	TWO-OUT-OF-TWO VOTING GATE	FT	FLOW TRANSMITTER
▁▔	BISTABLE – INCREASING SETPOINT	TE	TEMPERATURE ELEMENT
▔▁	BISTABLE – DECREASING SETPOINT	PT	PRESSURE TRANSMITTER
PB	PUSH BUTTON	ZI	POSITION INDICATION
HS	THREE POSITION HAND SWITCH, RETURN TO CENTER	RM	RADIATION MONITOR
&&	LOGIC "AND" OPERATOR	DI	DISCRETE INPUT
||	LOGIC "OR" OPERATOR	(A)	AUTOMATIC ACTUATION
T = XX seconds	TIMER THAT INITIATES ON A LOGIC "1", RESETS ON LOGIC "0" AND OUTPUTS A LOGIC "1" IF TIMER HAS EXPIRED	(M)	MANUAL ACTUATION
T = XX seconds	TIMER THAT INITIATES ON A LOGIC "1" AND OUTPUTS A LOGIC "1" IF TIMER HAS EXPIRED	(E)	ENABLE NONSAFETY "ENABLED"
XX Second Average	AVERAGE OPERATOR OVER XX AMOUNT OF TIME	(D)	ENABLE NONSAFETY "DISABLED"



ACRONYMS
DIV – DIVISION
HVPS – HIGH VOLTAGE POWER SUPPLY
IU – IRRADIATION UNIT
N2PS – NITROGEN PURGE SYSTEM
PICS – PROCESS INTEGRATED CONTROL SYSTEM
PCLS – PRIMARY CLOSED LOOP COOLING SYSTEM
RPCS – RADIOISOTOPE PROCESS FACILITY COOLING SYSTEM
RPF – RADIOISOTOPE PRODUCTION FACILITY
RVZ – RADIOLOGICAL VENTILATION ZONE
SCAS – SUBCRITICAL ASSEMBLY SYSTEM
TOGS – TSV OFF-GAS SYSTEM
TPS – TRITIUM PURIFICATION SYSTEM
TSV – TARGET SOLUTION VESSEL

Legend

Figure 7.4-2 – TRPS Mode State Diagram

7.5 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

7.5.1 SYSTEM DESCRIPTION

The engineered safety features actuation system (ESFAS) is a three-division safety-related instrumentation and control (I&C) system that performs various control and actuation functions credited by the SHINE safety analysis as required to prevent the occurrence or mitigate the consequences of design basis events within the SHINE facility. The ESFAS provides sense, command, and execute functions necessary to maintain the facility confinement strategy and provides process actuation functions required to shutdown processes and maintain processes in a safe condition. The ESFAS also provides nonsafety-related system status and measured process variable values to the facility process integrated control system (PICS) for viewing, recording, and trending.

The ESFAS monitors variables important to the safety functions for confinement of radiation and tritium within the irradiation facility (IF) and the radioisotope production facility (RPF) and for criticality safety to perform the following functions:

- Radiologically Controlled Area (RCA) Isolation
- Supercell Isolation
- Carbon Delay Bed Isolation
- Vacuum Transfer System (VTS) Safety Actuation
- Tritium Purification System (TPS) Train Isolation
- TPS Process Vent Actuation
- Irradiation Unit (IU) Cell Nitrogen Purge
- RPF Nitrogen Purge
- Molybdenum Extraction and Purification System (MEPS) [ ]$^{PROP/ECI}$ Isolation
- Extraction Column Alignment Actuation
- Iodine and Xenon Purification and Packaging (IXP) Alignment Actuation
- Dissolution Tank Isolation

The ESFAS monitors the IF and the RPF continually throughout the operation of processes within the main production facility, via the use of radiation monitoring and other instrumentation. Interlocks and bypass logic necessary for operation are implemented within the ESFAS. If at any point a monitored variable exceeds its predetermined limits, the ESFAS automatically initiates the associated safety function. ESFAS logic diagrams are provided in Figure 7.5-1 and the general architecture of the ESFAS is provided in Figure 7.1-3.

7.5.2 DESIGN CRITERIA

The SHINE design criteria are described in Section 3.1. Table 3.1-1 shows the SHINE design criteria applicable to the ESFAS.

7.5.2.1 Access Control

<u>ESFAS Criterion 1</u> – The ESFAS shall require a key or combination authentication input at the control console to prevent unauthorized use of the ESFAS.

ESFAS Criterion 2 – Developmental phases for ESFAS software shall address the potential cyber security vulnerabilities (physical and electronic) to prevent unauthorized physical and electronic access.

ESFAS Criterion 3 – The ESFAS design shall incorporate design or administrative controls to prevent/limit unauthorized physical and electronic access to critical digital assets (CDAs) during the operational phase, including the transition from development to operations. CDAs are defined as digital systems and devices that are used to perform or support, among other things, physical security and access control, safety-related functions, and reactivity control.

7.5.2.2 Software Requirements Development

ESFAS Criterion 4 – The functional characteristics of the ESFAS software requirements specifications shall be properly and precisely described for each software requirement.

ESFAS Criterion 5 – Development of ESFAS software shall follow a formally defined life cycle process and address potential security vulnerabilities in each phase of the life cycle.

ESFAS Criterion 6 – ESFAS development life cycle phase-specific security requirements shall be commensurate with the risk and magnitude of the harm that would result from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the ESFAS.

ESFAS Criterion 7 – ESFAS software development life cycle process requirements shall be described and documented in appropriate plans which shall address safety analysis, verification and validation (V&V), and configuration control activities.

ESFAS Criterion 8 – Tasks for validating and verifying the ESFAS software development activities shall be carried out in their entirety. Independent V&V tasks shall be performed by individuals or groups with appropriate technical competence in an organization separate from the development and program management organizations. Successful completion of V&V tasks for each software life cycle activity group shall be documented.

ESFAS Criterion 9 – The ESFAS software life cycle configuration control program shall trace software development from software requirement specification to implementation and address any impacts on ESFAS safety, control console, or display instruments.

ESFAS Criterion 10 – The ESFAS configuration control program shall assure that the required ESFAS hardware and software are installed in the appropriate system configuration and ensure that the correct version of the software/firmware is installed in the correct hardware components.

ESFAS Criterion 11 – Qualification testing shall test all portions of ESFAS programmable logic necessary to accomplish its safety functions, and shall exercise those portions whose operation or failure could impair safety functions during testing.

ESFAS Criterion 12 – The ESFAS software development life cycle shall include a software risk management program which addresses vulnerabilities throughout the software life cycle.

ESFAS Criterion 13 – ESFAS equipment not designed under a SHINE approved quality assurance (QA) program shall be qualified under the SHINE commercial-grade dedication program.

7.5.2.3 General Instrumentation and Control Requirements

ESFAS Criterion 14 – The ESFAS safety functions shall perform and remain functional during normal operation and during and following a design basis event.

ESFAS Criterion 15 – Manual controls of ESFAS actuation components shall be implemented downstream of the digital I&C portions of the safety system.

7.5.2.4 Single Failure

ESFAS Criterion 16 – The ESFAS shall be designed to perform its protective functions after experiencing a single random active failure in nonsafety control systems or in the ESFAS, and such failure shall not prevent the ESFAS and credited redundant passive control components from performing the intended functions or prevent safe shutdown of an IU cell.

ESFAS Criterion 17 – The ESFAS shall be designed such that no single failure can cause the failure of more than one redundant component.

ESFAS Criterion 18 – The ESFAS shall be designed so that no single failure within the instrumentation or power sources concurrent with failures as a result of a design basis event should prevent operators from being presented the information necessary to determine the safety status of the facility following the design basis event.

7.5.2.5 Independence

ESFAS Criterion 19 – Interconnections among ESFAS safety divisions shall not adversely affect the functions of the ESFAS.

ESFAS Criterion 20 – A logical or software malfunction of any interfacing nonsafety systems shall not affect the functions of the ESFAS.

ESFAS Criterion 21 – The ESFAS shall be designed with physical, electrical, and communications independence of the ESFAS both between the ESFAS channels and between the ESFAS and nonsafety-related systems to ensure that the safety functions required during and following any design basis event can be accomplished.

ESFAS Criterion 22 – Physical separation and electrical isolation shall be used to maintain the independence of ESFAS circuits and equipment among redundant safety divisions or with nonsafety systems so that the safety functions required during and following any design basis event can be accomplished.

ESFAS Criterion 23 – The ESFAS shall be designed such that no communication – within a single safety channel, between safety channels, and between safety and nonsafety systems – adversely affects the performance of required safety functions.

ESFAS Criterion 24 – ESFAS data communications protocols shall meet the performance requirements of all supported systems.

ESFAS Criterion 25 – The timing of ESFAS data communications shall be deterministic.

ESFAS Criterion 26 – ESFAS communications protocols shall conform to validated protocol specifications by formally generated test procedures and test data vectors and verify that the implementations themselves were constructed using a formal design process that ensures consistency between the product and the validated specification.

ESFAS Criterion 27 – The ESFAS shall be designed such that no unexpected performance deficits exist that could adversely affect the ESFAS architecture.

7.5.2.6 Prioritization of Functions

ESFAS Criterion 28 – ESFAS devices that receive signals from safety and nonsafety sources shall prioritize the signal from the safety system.

7.5.2.7 Fail-Safe

ESFAS Criterion 29 – The ESFAS shall be designed to assume a safe state on loss of electrical power.

7.5.2.8 Setpoints

ESFAS Criterion 30 – Setpoints for an actuation of the ESFAS shall be based on a documented analysis methodology that identifies assumptions and accounts for uncertainties, such as environmental allowances and measurement computational errors associated with each element of the instrument channel. The setpoint analysis parameters and assumptions shall be consistent with the safety analysis, system design basis, technical specifications, and facility design, and expected maintenance practices.

ESFAS Criterion 31 – Adequate margin shall exist between setpoints and safety limits so that the ESFAS initiates protective actions before safety limits are exceeded.

ESFAS Criterion 32 – Where it is necessary to provide multiple setpoints for adequate protection based on particular modes of operation or sets of operating conditions, the ESFAS shall provide positive means of ensuring that the more restrictive setpoint is used when required.

ESFAS Criterion 33 – The sensitivity of each ESFAS sensor channel shall be commensurate with the precision and accuracy to which knowledge of the variable measured is required for the protective function.

7.5.2.9 Operational Bypass, Permissives and Interlocks

ESFAS Criterion 34 – Permissive conditions for each ESFAS operating or maintenance bypass capability shall be documented.

ESFAS Criterion 35 – ESFAS interlocks shall ensure that operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required.

ESFAS Criterion 36 – ESFAS provisions shall exist to prevent activation of an operating bypass unless applicable permissive conditions exist.

ESFAS Criterion 37 – Bypass capability shall not be provided for the mechanisms to manually initiate ESFAS safety functions.

ESFAS Criterion 38 – If provisions for maintenance or operating bypasses are provided, the ESFAS design shall retain the capability to accomplish its safety function while a bypass is in effect.

ESFAS Criterion 39 – Whenever permissive conditions for bypassing a train or channel in the ESFAS are not met, a feature in the ESFAS shall physically prevent or facilitate administrative controls to prevent the unauthorized use of bypasses.

ESFAS Criterion 40 – All ESFAS operating bypasses, either manually or automatically initiated, shall be automatically removed when the facility moves to an operating regime where the protective action would be required if an accident occurred.

ESFAS Criterion 41 – If operating conditions change so that an active operating bypass is no longer permissible, the ESFAS shall automatically accomplish one of the following actions:

- Remove the appropriate active operating bypass(es)
- Restore conditions so that permissive conditions once again exist
- Initiate the appropriate safety function(s)

ESFAS Criterion 42 – Portions of ESFAS that execute features with a degree of redundancy of one shall be designed so that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability to perform the ESFAS action if required.

ESFAS Criterion 43 – Provisions shall exist to allow the operations staff to confirm that a bypassed ESFAS safety function has been properly returned to service.

7.5.2.10 Completion of Protective Actions

ESFAS Criterion 44 – The ESFAS design shall ensure that once initiated the safety actions will continue until the protective function is completed.

ESFAS Criterion 45 – Only deliberate operator action shall be permitted to reset the ESFAS or its components following manual or automatic actuation.

ESFAS Criterion 46 – Mechanisms for deliberate operator intervention in the ESFAS status or its functions shall not be capable of preventing the initiation of ESFAS actions.

7.5.2.11 Equipment Qualification

ESFAS Criterion 47 – The effects of electromagnetic interference/radio-frequency interference (EMI/RFI) and power surges, such as high-energy faults and lightning, on the ESFAS, including field programmable gate array (FPGA)-based digital portions, shall be adequately addressed.

7.5.2.12 Surveillance

ESFAS Criterion 48 – Equipment in the ESFAS (from the input circuitry to output actuation circuitry) shall be designed to allow testing, calibration, and inspection to ensure operability. If testing is required or can be performed as an option during operation, the ESFAS shall retain the capability to accomplish its safety function while under test.

ESFAS Criterion 49 – Testing, calibration, and inspections of the ESFAS shall be sufficient to show that once performed, they confirm that surveillance test and self-test features address failure detection, self-test features, and actions taken upon failure detection.

ESFAS Criterion 50 – The design of the ESFAS and the justification for test intervals shall be consistent with the surveillance testing intervals as part of the facility technical specifications.

7.5.2.13 Classification and Identification

ESFAS Criterion 51 – ESFAS equipment shall be distinctly identified to indicate its safety classification and to associate equipment according to divisional or channel assignments.

7.5.2.14 Human Factors

ESFAS Criterion 52 – Human factors shall be considered at the initial stages and throughout the ESFAS design process to ensure that the functions allocated in whole or in part to the operator(s) can be successfully accomplished to meet ESFAS design goals.

ESFAS Criterion 53 – The ESFAS shall include readily available means for manual initiation of each protective function at the system level.

ESFAS Criterion 54 – The ESFAS shall be designed to provide the information necessary to support annunciation of the channel initiating a protective action to the operator and requiring manual operator reset when all conditions to resume operation are met and satisfied.

7.5.2.15 Quality

ESFAS Criterion 55 – The quality of the components and modules in the ESFAS shall be commensurate with the importance of the safety function to be performed.

ESFAS Criterion 56 – Controls over the design, fabrication, installation, and modification of the ESFAS shall conform to the guidance of ANSI/ANS 15.8-1995, Quality Assurance Program Requirements for Research Reactors (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5, Quality Assurance Program Requirements for Research and Test Reactors (USNRC, 2010).

7.5.3 DESIGN BASIS

7.5.3.1 Safety Functions

7.5.3.1.1 Supercell Area 1 (PVVS Area) Isolation

Supercell Area 1 (Process Vessel Vent System [PVVS] Area) Isolation initiates the following safety functions:

- Deenergize radiological ventilation zone 2 (RVZ2) supercell area 1 (PVVS area) inlet isolation dampers
- Deenergize radiological ventilation zone 1 (RVZ1) supercell area 1 (PVVS area) outlet isolation dampers
- VTS Safety Actuation which returns the VTS to atmospheric pressure

The ESFAS initiates a Supercell Area 1 (PVVS Area) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 1 (PVVS area) radiation
- RCA Isolation

7.5.3.1.2 Supercell Area 2 (Extraction Area A) Isolation

Supercell Area 2 (Extraction Area A) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 2 (extraction area A) inlet isolation dampers
- Deenergize RVZ1 supercell area 2 (extraction area A) outlet isolation dampers
- MEPS A [ ]$^{\text{PROP/ECI}}$ Isolation
- VTS Safety Actuation

The ESFAS initiates a Supercell Area 2 (Extraction Area A) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 2 (extraction area A) radiation
- RCA Isolation

A representation of the Supercell Area 2 Isolation is provided in Figure 7.5-2.

7.5.3.1.3 Supercell Area 3 (Purification Area A) Isolation

Supercell Area 3 (Purification Area A) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 3 (purification area A) inlet isolation dampers
- Deenergize RVZ1 supercell area 3 (purification area A) outlet isolation dampers

The ESFAS initiates a Supercell Area 3 (Purification Area A) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 3 (purification area A) radiation
- RCA Isolation

7.5.3.1.4 Supercell Area 4 (Packaging Area 1) Isolation

Supercell Area 4 (Packaging Area 1) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 4 (packaging area 1) inlet isolation dampers
- Deenergize RVZ1 supercell area 4 (packaging area 1) outlet isolation dampers

The ESFAS initiates a Supercell Area 4 (Packaging Area 1) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 4 (packaging area 1) radiation
- RCA Isolation

7.5.3.1.5 Supercell Area 5 (Purification Area B) Isolation

Supercell Area 5 (Purification Area B) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 5 (purification area B) inlet isolation dampers
- Deenergize RVZ1 supercell area 5 (purification area B) outlet isolation dampers

The ESFAS initiates a Supercell Area 5 (Purification Area B) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 5 (purification area B) radiation
- RCA Isolation

7.5.3.1.6 Supercell Area 6 (Extraction Area B) Isolation

Supercell Area 6 (Extraction Area B) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 6 (extraction area B) inlet isolation dampers
- Deenergize RVZ1 supercell area 6 (extraction area B) outlet isolation dampers
- MEPS B [ ]$^{\text{PROP/ECI}}$ Isolation
- VTS Safety Actuation

The ESFAS initiates a Supercell Area 6 (Extraction Area B) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 6 (extraction area B) radiation
- RCA Isolation
- Supercell Area 10 (IXP area) Isolation

7.5.3.1.7 Supercell Area 7 (Extraction Area C) Isolation

Supercell Area 7 (Extraction Area C) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 7 (purification area C) inlet isolation dampers
- Deenergize RVZ1 supercell area 7 (purification area C) outlet isolation dampers
- MEPS C [ ]$^{\text{PROP/ECI}}$ Isolation
- VTS Safety Actuation

The ESFAS initiates a Supercell Area 7 (Extraction Area C) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 7 (extraction Area C) radiation
- RCA Isolation
- Supercell Area 10 (IXP area) Isolation

7.5.3.1.8 Supercell Area 8 (Purification Area C) Isolation

Supercell Area 8 (Purification Area C) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 8 (purification area C) inlet isolation dampers
- Deenergize RVZ1 supercell area 8 (purification area C) outlet isolation dampers

The ESFAS initiates a Supercell Area 8 (Purification Area C) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 8 (purification area C) radiation
- RCA Isolation

7.5.3.1.9 Supercell Area 9 (Packaging Area 2) Isolation

Supercell Area 9 (Packaging Area 2) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 9 (packaging area 2) inlet isolation dampers
- Deenergize RVZ1 supercell area 9 (packaging area 2) outlet isolation dampers

The ESFAS initiates a Supercell Area 9 (Packaging Area 2) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 9 (packaging area 2) radiation
- RCA Isolation

7.5.3.1.10 Supercell Area 10 (IXP Area) Isolation

Supercell Area 10 (IXP Area) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 10 (IXP area) inlet isolation dampers
- Deenergize RVZ1 supercell area 10 (IXP area) outlet isolation dampers
- Supercell Area 6 (extraction area B) Isolation
- Supercell Area 7 (extraction area C) Isolation

The ESFAS initiates a Supercell Area 10 (IXP Area) Isolation based on the following variable or safety actuation:

- High RVZ1 supercell area 10 (IXP area) radiation
- RCA Isolation

7.5.3.1.11 MEPS A [ ]$^{PROP/ECI}$ Isolation

MEPS A [ ]$^{PROP/ECI}$ Isolation initiates the following safety functions:

- Deenergize MEPS [ ]$^{PROP/ECI}$ A inlet isolation valves
- Deenergize MEPS [ ]$^{PROP/ECI}$ A discharge isolation valves
- Deenergize MEPS A extraction feed pump breakers

The ESFAS initiates a MEPS A [ ]$^{PROP/ECI}$ Isolation based on the following variable or safety actuation:

- High MEPS [ ]$^{PROP/ECI}$ conductivity extraction area A
- Radioactive drain system (RDS) liquid detection switch signal
- Supercell Area 2 Isolation

7.5.3.1.12 MEPS B [ ]$^{PROP/ECI}$ Isolation

MEPS B [ ]$^{PROP/ECI}$ Isolation initiates the following safety functions:

- Deenergize MEPS [ ]$^{PROP/ECI}$ B inlet isolation valves
- Deenergize MEPS [ ]$^{PROP/ECI}$ B discharge isolation valves
- Deenergize MEPS B extraction feed pump breakers

The ESFAS initiates a MEPS B [ ]$^{PROP/ECI}$ Isolation based on the following variable or safety actuation:

- High MEPS [ ]$^{PROP/ECI}$ conductivity extraction area B
- RDS liquid detection switch signal
- Supercell Area 6 Isolation

7.5.3.1.13 MEPS C [ ]$^{PROP/ECI}$ Isolation

MEPS C [ ]$^{PROP/ECI}$ Isolation initiates the following safety functions:

- Deenergize MEPS [ ]$^{PROP/ECI}$ C inlet isolation valves
- Deenergize MEPS [ ]$^{PROP/ECI}$ C discharge isolation valves
- Deenergize MEPS C extraction feed pump breakers

The ESFAS initiates a MEPS C [ ]$^{PROP/ECI}$ Isolation based on the following variable or safety actuation:

- High MEPS [ ]$^{PROP/ECI}$ conductivity extraction area C
- RDS liquid detection switch signal
- Supercell Area 7 Isolation

7.5.3.1.14 Carbon Delay Bed Group 1 Isolation

Carbon Delay Bed Group 1 Isolation initiates the following safety functions:

- Energize PVVS carbon delay bed group 1 three-way valves
- Energize PVVS carbon delay bed group 1 outlet isolation valves

The ESFAS initiates a Carbon Delay Bed Group 1 Isolation based on the following variables:

- High carbon delay bed group 1 exhaust carbon monoxide

7.5.3.1.15 Carbon Delay Bed Group 2 Isolation

Carbon Delay Bed Group 2 Isolation initiates the following safety functions:

- Energize PVVS carbon delay bed group 2 three-way valves
- Energize PVVS carbon delay bed group 2 outlet isolation valves

The ESFAS initiates a Carbon Delay Bed Group 2 Isolation based on the following variables:

- High carbon delay bed group 2 exhaust carbon monoxide

7.5.3.1.16 Carbon Delay Bed Group 3 Isolation

Carbon Delay Bed Group 3 Isolation initiates the following safety functions:

- Energize PVVS carbon delay bed group 3 three-way valves
- Energize PVVS carbon delay bed group 3 outlet isolation valves

The ESFAS initiates a Carbon Delay Bed Group 3 Isolation based on the following variables:

- High carbon delay bed group 3 exhaust carbon monoxide

7.5.3.1.17 VTS Safety Actuation

VTS Safety Actuation Isolation initiates the following safety functions:

- Deenergize VTS vacuum transfer pump 1 breakers
- Deenergize VTS vacuum transfer pump 2 breakers
- Deenergize VTS vacuum transfer pump 3 breakers
- Deenergize VTS vacuum break valves
- MEPS A extraction column wash supply valve
- MEPS A extraction column eluent valve
- MEPS A [ ]$^{PROP/ECI}$ wash supply valve
- MEPS A [ ]$^{PROP/ECI}$ eluent valve
- MEPS B extraction column wash supply valve
- MEPS B extraction column eluent valve
- MEPS B [ ]$^{PROP/ECI}$ wash supply valve
- MEPS B [ ]$^{PROP/ECI}$ eluent valve

- MEPS C extraction column wash supply valve
- MEPS C extraction column eluent valve
- MEPS C [ ]$^{PROP/ECI}$ wash supply valve
- MEPS C [ ]$^{PROP/ECI}$ eluent valve
- IXP recovery column wash supply valve
- IXP recovery column eluent valve
- IXP [ ]$^{PROP/ECI}$ wash supply valve
- IXP [ ]$^{PROP/ECI}$ eluent valve
- IXP FNHS supply valve
- IXP liquid nitrogen supply valve

The ESFAS initiates a VTS Safety Actuation based on the following variables or safety actuations:

- VTS vacuum header liquid detection switch signal
- RDS liquid detection switch signal
- Supercell Area 1 Isolation
- Supercell Area 2 Isolation
- Supercell Area 6 Isolation
- Supercell Area 7 Isolation
- RCA Isolation
- Facility master operating permissive

A representation of the VTS Safety Actuation is provided in Figure 7.5-3.

7.5.3.1.18 TPS Train A Isolation

TPS Train A Isolation initiates the following safety functions:

- TPS train A glovebox pressure control exhaust isolation valve
- Vacuum/impurity treatment subsystem (VAC/ITS) train A process vent ITS isolation valves (TPS train A ITS isolation valves)
- TPS train A helium air operated valve (AOV) supply valve
- TPS train A helium solenoid operated valve (SOV) supply valve
- RVZ2 TPS ventilation supply dampers
- RVZ2 TPS ventilation exhaust dampers
- VAC/ITS train A process vent vacuum isolation valves (TPS train A vacuum isolation valves)
- IU Cell 1 TPS Actuation
- IU Cell 2 TPS Actuation

The ESFAS initiates a TPS Train A Isolation based on the following variables or safety actuation:

- High TPS IU cell 1 target chamber supply pressure
- High TPS IU cell 2 target chamber supply pressure
- High TPS IU cell 1 target chamber exhaust pressure
- High TPS IU cell 2 target chamber exhaust pressure
- High TPS confinement A tritium
- RCA Isolation
- Facility master operating permissive

7.5.3.1.19 TPS Train B Isolation

TPS Train B Isolation initiates the following safety functions:

- TPS train B glovebox pressure control exhaust isolation valve
- VAC/ITS train B process vent ITS isolation valves (TPS train B ITS isolation valves)
- TPS train B helium AOV supply valve
- TPS train B helium SOV supply valve
- RVZ2 TPS ventilation supply dampers
- RVZ2 TPS ventilation exhaust dampers
- VAC/ITS train B process vent vacuum isolation valves (TPS train B vacuum isolation valves)
- IU Cell 3 TPS Actuation
- IU Cell 4 TPS Actuation
- IU Cell 5 TPS Actuation

The ESFAS initiates a TPS Train B Isolation based on the following variables or safety actuation:

- High TPS IU cell 3 target chamber supply pressure
- High TPS IU cell 4 target chamber supply pressure
- High TPS IU cell 5 target chamber supply pressure
- High TPS IU cell 3 target chamber exhaust pressure
- High TPS IU cell 4 target chamber exhaust pressure
- High TPS IU cell 5 target chamber exhaust pressure
- High TPS confinement B tritium
- RCA Isolation
- Facility master operating permissive

7.5.3.1.20 TPS Train C Isolation

TPS Train C Isolation initiates the following safety functions:

- TPS train C glovebox pressure control exhaust isolation valve
- VAC/ITS train C process vent ITS isolation valves (TPS train C ITS isolation valves)
- TPS train C helium AOV supply valve
- TPS train C helium SOV supply valve
- RVZ2 TPS ventilation supply dampers
- RVZ2 TPS ventilation exhaust dampers
- VAC/ITS train C process vent vacuum isolation valves (TPS train C vacuum isolation valves)
- IU Cell 6 TPS Actuation
- IU Cell 7 TPS Actuation
- IU Cell 8 TPS Actuation

The ESFAS initiates a TPS Train C Isolation based on the following variables or safety actuation:

- High TPS IU cell 6 target chamber supply pressure
- High TPS IU cell 7 target chamber supply pressure
- High TPS IU cell 8 target chamber supply pressure

- High TPS IU cell 6 target chamber exhaust pressure
- High TPS IU cell 7 target chamber exhaust pressure
- High TPS IU cell 8 target chamber exhaust pressure
- High TPS confinement C tritium
- RCA Isolation
- Facility master operating permissive

7.5.3.1.21 TPS Process Vent Actuation

TPS Process Vent Actuation initiates the following safety functions:

- TPS train A vacuum isolation valves
- TPS train A ITS isolation valves
- TPS train B vacuum isolation valves
- TPS train B ITS isolation valves
- TPS train C vacuum isolation valves
- TPS train C ITS isolation valves
- IU Cell 1 TPS Actuation
- IU Cell 2 TPS Actuation
- IU Cell 3 TPS Actuation
- IU Cell 4 TPS Actuation
- IU Cell 5 TPS Actuation
- IU Cell 6 TPS Actuation
- IU Cell 7 TPS Actuation
- IU Cell 8 TPS Actuation

The ESFAS initiates a TPS Process Vent Actuation based on the following variables or safety actuation:

- High TPS exhaust to facility stack tritium
- RCA Isolation
- Facility master operating permissive

7.5.3.1.22 IU Cell Nitrogen Purge

IU Cell Nitrogen Purge transitions the nitrogen purge system (N2PS) IU cell header valves to their deenergized state.

The ESFAS also provides the target solution vessel (TSV) reactivity protection system (TRPS) for each IU cell with an actuation signal to initiate an IU Cell Nitrogen purge within the TRPS.

The ESFAS initiates an IU Cell Nitrogen Purge based on the following variables:

- UPSS loss of external power
- TRPS IU cell 1 nitrogen purge signal
- TRPS IU cell 2 nitrogen purge signal
- TRPS IU cell 3 nitrogen purge signal
- TRPS IU cell 4 nitrogen purge signal
- TRPS IU cell 5 nitrogen purge signal
- TRPS IU cell 6 nitrogen purge signal

- TRPS IU cell 7 nitrogen purge signal
- TRPS IU cell 8 nitrogen purge signal

7.5.3.1.23 RPF Nitrogen Purge

RPF Nitrogen Purge initiates the following safety functions:

- Deenergize PVVS blower bypass valves
- Deenergize radioactive liquid waste immobilization (RLWI) PVVS isolation valve
- Deenergize PVVS carbon guard bed bypass valves
- Deenergize N2PS RPF header valves
- Deenergize N2PS RVZ2 north header valves
- Deenergize N2PS RVZ2 south header valves

The ESFAS initiates an RPF Nitrogen Purge based on the following variable:

- Low PVVS flow

7.5.3.1.24 RCA Isolation

RCA Isolation initiates the following safety functions:

- Deenergize RVZ1 exhaust isolation dampers
- Deenergize RVZ2 exhaust isolation dampers
- Deenergize RVZ2 supply train 1 isolation dampers
- Deenergize RVZ2 supply train 2 isolation dampers
- Deenergize RVZ3 supply isolation dampers shipping/receiving IF
- Deenergize RVZ3 supply isolation dampers shipping/receiving RPF
- Deenergize RVZ3 supply isolation dampers main RCA ingress/egress
- Deenergize RVZ3 supply isolation dampers RPF emergency exit
- Deenergize RVZ3 supply isolation dampers IF emergency exit
- Deenergize RVZ3 exhaust isolation dampers IF emergency exit
- Deenergize RVZ1 exhaust train 1 blower breakers
- Deenergize RVZ1 exhaust train 2 blower breakers
- Deenergize RVZ2 exhaust train 1 blower breakers
- Deenergize RVZ2 exhaust train 2 blower breakers
- Deenergize RVZ2 supply train 1 blower breakers
- Deenergize RVZ2 supply train 2 blower breakers
- Supercell Area 1 Isolation
- Supercell Area 2 Isolation
- Supercell Area 3 Isolation
- Supercell Area 4 Isolation
- Supercell Area 5 Isolation
- Supercell Area 6 Isolation
- Supercell Area 7 Isolation
- Supercell Area 8 Isolation
- Supercell Area 9 Isolation
- Supercell Area 10 Isolation
- VTS Safety Actuation

- TPS Train A Isolation
- TPS Train B Isolation
- TPS Train C Isolation

The ESFAS initiates an RCA Isolation based on the following variables:

- High RVZ1 RCA exhaust radiation
- High RVZ2 RCA exhaust radiation

A representation of the RCA Isolation is provided in Figure 7.5-4.

7.5.3.1.25 Extraction Column A Alignment Actuation

Extraction Column A Alignment Actuation initiates the following safety functions:

- Deenergize MEPS area A upper three-way valve
- Deenergize MEPS area A lower three-way valve
- Deenergize MEPS A extraction column eluent valve

The ESFAS initiates the Extraction Column A Alignment Actuation based on both of the following inputs being active:

- MEPS area A upper three-way valve supplying position indication
- MEPS area A lower three-way valve supplying position indication

7.5.3.1.26 Extraction Column B Alignment Actuation

Extraction Column B Alignment Actuation initiates the following safety functions:

- Deenergize MEPS area B upper three-way valve
- Deenergize MEPS area B lower three-way valve
- Deenergize MEPS B extraction column eluent valve

The ESFAS initiates the Extraction Column B Alignment Actuation based on both of the following inputs being active:

- MEPS area B upper three-way valve supplying position indication
- MEPS area B lower three-way valve supplying position indication

7.5.3.1.27 Extraction Column C Alignment Actuation

Extraction Column C Alignment Actuation initiates the following safety functions:

- Deenergize MEPS area C upper three-way valve
- Deenergize MEPS area C lower three-way valve
- Deenergize MEPS C extraction column eluent valve

The ESFAS initiates the Extraction Column C Alignment Actuation based on both of the following inputs being active:

- MEPS area C upper three-way valve supplying position indication
- MEPS area C lower three-way valve supplying position indication

7.5.3.1.28 IXP Alignment Actuation

Iodine and Xenon Purification and Packaging (IXP) Alignment Actuation initiates the following safety functions:

- Deenergize IXP upper three-way valve
- Deenergize IXP lower three-way valve
- Deenergize IXP recovery column eluent valve

The ESFAS initiates the IXP Alignment Actuation based on both of the following inputs being active:

- IXP upper three-way valve supplying position indication
- IXP lower three-way valve supplying position indication

7.5.3.1.29 Dissolution Tank Isolation

Dissolution Tank Isolation initiates the following safety functions:

- Deenergize target solution preparation system (TSPS) radioisotope process facility cooling system (RPCS) supply cooling valves
- Deenergize TSPS RPCS return cooling valve
- Deenergize RVZ2 TSPS supply damper
- Deenergize RVZ1 TSPS exhaust damper

The ESFAS initiates the Dissolution Tank Isolation based on the following input being active:

- High TSPS dissolution tank 1 level switch signal
- High TSPS dissolution tank 2 level switch signal

7.5.3.2 ESFAS Monitored Variables

Table 7.5-1 identifies the specific variables that provide input to the ESFAS and includes the instrument range for covering normal and accident conditions, the accuracy for each variable, the analytical limit, and the response time of the sensor element.

7.5.3.3 Operating Conditions

The ESFAS control and logic functions operate inside of the facility control room where the environment is mild and not exposed to the irradiation process. However, the cables for the ESFAS are routed through the radiologically controlled area to the process areas. The routed cables have the potential to be exposed to more harsh conditions than the mild environment of the facility control room. The sensors are located inside the process confinement boundary;

therefore, the terminations of the cables routed to the sensors are exposed to the high radiation environment.

During normal operation, the ESFAS equipment will operate in the applicable normal radiation environments identified in Table 7.2-1 for up to 20 years, replaced at a frequency sufficient such that the radiation qualification of the affected components is not exceeded.

The environmental conditions for ESFAS components are outlined in Table 7.2-1 through Table 7.2-3. The facility heating, ventilation and air conditioning (HVAC) systems are relied upon to maintain the temperature and humidity parameters in these areas. The facility HVAC systems are described in Section 9a2.1.

7.5.4 DESIGN ATTRIBUTES

7.5.4.1 Access Control

A detailed description of access control is provided in Subsection 7.2.5.

7.5.4.2 Software Requirements Development

A detailed description of the development of software requirements is provided in Subsection 7.2.6.

7.5.4.3 General Instrumentation and Control Requirements

The ESFAS is powered from the uninterruptible electrical power supply system (UPSS), which provides a reliable source of power to maintain the ESFAS functional during normal operation and during and following a design basis event. The UPSS is designed to provide power to the ESFAS controls for six hours after a loss of off-site power. The UPSS is described in Section 8a2.2.

The actuation and priority logic (APL) portions within an equipment interface module (EIM) support the implementation of different actuation methods. The APL is implemented using discrete components and is not vulnerable to a software common cause failure (CCF). Having the capability for hardwired signals into each EIM supports the capability for additional and diverse actuation means from automated actuation. As an example, a division of APL circuits may receive inputs automatically from the programmable logic portion of the ESFAS, inputs from manual controls in the facility control room, and input signals from a nonsafety control system. Both the manual controls and nonsafety control system inputs come individually into the APL and are downstream of the programmable logic portion of the ESFAS architecture as shown in Figure 7.1-3.

7.5.4.4 Single Failure

The ESFAS consists of three divisions of input processing and trip determination and two divisions of actuation logic (see Figure 7.1-2) arranged so that no single failure within the ESFAS results in the loss of the protective function.

The only nonsafety inputs into the ESFAS are those from the PICS for controls. The nonsafety control signals from the PICS are implemented through a hardwired parallel interface that requires the PICS to send a binary address associated to the output state of the EIM along with a mirrored complement address. The mirrored complement address prevents any single incorrectly presented bit from addressing the wrong EIM output state. To prevent the PICS from inadvertently presenting a valid address, the ESFAS contains a safety-related enable nonsafety switch that controls when the hardwired parallel interface within the APL is active, thus controlling when the PICS inputs are allowed to pass through the input circuitry and for use in the priority logic within the APL. When the enable nonsafety switch is not active, the nonsafety-related control signal is ignored. If the enable nonsafety is active, and no automatic or manual actuation command is present, the nonsafety-related control signal can control the ESFAS output. The hardwired module provides isolation for the nonsafety-related signal path.

7.5.4.5 Independence

A description of the application of independence to the ESFAS is provided in Subsection 7.2.2.

7.5.4.6 Prioritization of Functions

Each division of the ESFAS includes the analog logic circuitry necessary to prioritize the ESFAS inputs. Automatic Safety Actuation or Manual Actuation are highest priority and PICS nonsafety control inputs are lower in priority.

7.5.4.7 Fail-Safe

The fail-safe positions of components upon loss of power to ESFAS are provided in Table 7.5-2.

7.5.4.8 Setpoints

Setpoints in the ESFAS are based on a documented methodology that identifies each of the assumptions and accounts for the uncertainties in each instrument channel. The setpoint methodology is described in Subsection 7.2.3.

7.5.4.9 Operational Bypass, Permissives and Interlocks

Maintenance bypasses are described in Subsection 7.1.4.

The ESFAS starts a 180 second timer on loss of external power to the UPSS. If the indication of loss of external power to the UPSS clears prior to the 180 second timer expiring, the timer resets. If the timer expires, the ESFAS initiates an IU Cell Nitrogen Purge on loss of external power to the UPSS.

Nonsafety inputs into the ESFAS are transferred from PICS through the hardwired module. The PICS inputs are bypassed with the enable nonsafety switch permitting the inputs to control ESFAS outputs when administrative procedures permit the operator to use the switch to enable the PICS functionality with the ESFAS.

The manual actuation inputs from the operators in the facility control room are connected directly to the discrete APL. The manual actuation input into the priority logic does not have the ability to be bypassed and will always have equal priority to the automated actuation signals over any other signals that are present.

7.5.4.10 Completion of Protective Actions

The ESFAS is designed so that once initiated, protective actions will continue to completion. Only deliberate operator action can be taken to reset the ESFAS following a protective action. Figure 7.5-1 shows how the ESFAS latches in a protective action and maintains the state of a protective action until operator input is initiated to reset the output of the ESFAS to normal operating conditions.

The output of the ESFAS is designed so that actuation through automatic or manual means of a safety function can only change when a new position is requested. If there is no signal present from the automatic safety actuation or manual actuation, then the output of the EIM remains in its current state. A safety-related enable nonsafety switch allows an operator, after the switch has been brought to enable, to control the output state of the ESFAS with a hardwired binary control signal from the nonsafety-related controls. The enable nonsafety switch is classified as part of the safety system and is used to prevent spurious nonsafety-related control signals from adversely affecting safety-related components. If the enable nonsafety switch is active, and no automatic safety actuation or manual actuation signals are present, the operator is capable of energizing or deenergizing any EIM outputs using the nonsafety-related hardwired control signals. If the enable nonsafety switch is not active, the nonsafety-related hardwired control signals are ignored.

7.5.4.11 Equipment Qualification

ESFAS rack mounted equipment is installed in a mild operating environment and is designed to meet the environmental conditions described in Subsection 7.4.3.4. Rack mounted ESFAS equipment is tested to appropriate standards to show that the effects of EMI/RFI and power surges are adequately addressed. Appropriate grounding of the ESFAS is performed in accordance with Section 5.2.1 of Institute of Electrical and Electronics Engineers (IEEE) Standard 1050-2004, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations (IEEE, 2004b).

7.5.4.12 Surveillance

The TRPS supports calibration and testing to ensure operability as described in Subsection 7.2.4.

7.5.4.13 Classification and Identification

Each division of the ESFAS is uniquely labeled and identified in accordance with SHINE identification and classification procedures.

7.5.4.14 Human Factors

The ESFAS provides manual actuation capabilities for each of the safety functions identified in Subsection 7.5.3. To support the use of manual actuations, the ESFAS includes isolated outputs for each safety-related instrument channel to provide monitoring and indication information to the PICS. To facilitate operator indication of ESFAS actuation function status, manual initiation and reset of protective actions, the ESFAS, at the division level, includes isolated input/output for the following:

- Indication of ESFAS variable values
- Indication of ESFAS parameter values
- Indication of ESFAS logic status
- Indication of ESFAS equipment status
- Indication of ESFAS actuation device status

7.5.4.15 Codes and Standards

The following codes and standards are applied to the ESFAS design.

1) Section 8 of IEEE Standard 344-2013, IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations (IEEE, 2013); invoked as guidance to meet SHINE Design Criterion 2, Natural phenomena hazards.
2) IEEE Standard 379-2000, IEEE Standard Application of Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (IEEE, 2000); invoked to meet SHINE Design Criterion 15, Protection system reliability and testability.
3) IEEE Standard 384-2008, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (IEEE, 2008); invoked for separation of safety-related and nonsafety-related cables and raceways, as described in Subsection 8a2.1.3 and Subsection 8a2.1.5.
4) IEEE Standard 1023-2004, IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities (IEEE, 2004c); invoked as a guidance to support implementation of human factors into the design of I&C systems.
5) Section 5.2.1 of IEEE Standard 1050-2004, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations (IEEE, 2004b); invoked as guidance to support electromagnetic compatibility qualification for digital I&C equipment.
6) Regulatory Guide 1.152, Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (USNRC, 2011); invoked to demonstrate secure development and operating environment.
7) The guidance of ANSI/ANS 15.8-1995, Quality Assurance Program Requirements for Research Reactors (R2013) (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5, Quality Assurance Program Requirements for Research and Test Reactors (USNRC, 2010), is applied as part of the SHINE Quality Assurance Program for complying with the programmatic requirements of 10 CFR 50.34(b)(6)(ii).

7.5.5 OPERATION AND PERFORMANCE

7.5.5.1 High RVZ RCA Exhaust Radiation

The high RVZ RCA exhaust radiation signal protects against confinement leakage or accidents that could potentially result in excess radiation doses to the public. The RZV RCA exhaust radiation is measured by an analog interface on three different channels, one for each division of ESFAS. When two-out-of-three or more high RVZ RCA exhaust radiation channels are active, then an RCA Isolation is initiated.

7.5.5.2 High RVZ1 Supercell Radiation (PVVS Cell)

The high RVZ1 supercell radiation signal protects against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public. The

RVZ1 supercell radiation is measured by an analog interface on three different channels, one for each division of ESFAS. When two-out-of-three or more high RVZ1 supercell radiation channels are active, then a Supercell Isolation for that area and VTS Safety Actuation are initiated.

7.5.5.3 High RVZ1 Supercell Radiation (MEPS Extraction Cells)

The high RVZ1 supercell radiation signal protects against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public. The RVZ1 supercell radiation is measured by an analog interface on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more high RVZ1 supercell radiation channels are active, then a Supercell Isolation for that area, MEPS [ ]$^{PROP/ECI}$ Isolation and VTS Safety Actuation are initiated.

7.5.5.4 High RVZ1 Supercell Radiation (IXP Extraction Cell)

The high RVZ1 supercell radiation signal protects against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public. The RVZ1 supercell radiation is measured by an analog interface on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more high RVZ1 supercell radiation channels are active, then a Supercell Isolation for that area and VTS Safety Actuation are initiated.

7.5.5.5 High RVZ1 Supercell Radiation (Purification and Packaging Cells)

The high RVZ1 supercell radiation signal protects against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public. The RVZ1 supercell radiation is measured by an analog interface on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more high RVZ1 supercell radiation channels are active, then a Supercell Isolation for that area is initiated.

7.5.5.6 High MEPS [ ]$^{PROP/ECI}$ Conductivity

The high MEPS [ ]$^{PROP/ECI}$ conductivity signal protects against leakage of high radiation solutions into the [ ]$^{PROP/ECI}$, which is partially located outside the supercell shielding and could potentially result in an excess dose to the workers. The MEPS [ ]$^{PROP/ECI}$ conductivity is measured by an analog interface on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more high MEPS [ ]$^{PROP/ECI}$ conductivity channels are active, then a MEPS [ ]$^{PROP/ECI}$ Isolation is initiated.

7.5.5.7 High PVVS Carbon Delay Bed Exhaust Carbon Monoxide

The high PVVS carbon delay bed exhaust carbon monoxide signal protects against a fire in the PVVS delay bed. The PVVS carbon delay bed exhaust carbon monoxide is measured with an analog interface on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more high PVVS carbon delay bed exhaust carbon monoxide channels are active, then a Carbon Delay Bed Isolation for the affected group is initiated.

7.5.5.8 VTS Lift Tank Liquid Detection Switch

The VTS lift tank liquid detection switch signals protect against an overflow of the vacuum lift tanks. The VTS lift tank liquid detection switch signals are measured with a discrete input interface with redundant detection signals common to all lift tanks at the VTS vacuum header. If one-out-of-two or more (Division A and Division B) VTS lift tank liquid detection switch signals are active, then a VTS Safety Actuation is initiated.

7.5.5.9 RDS Liquid Detection Switch

The RDS liquid detection switch signal detects leakage or overflow from other tanks and piping. The RDS liquid detection switch signal is measured with a discrete signal input on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more RDS liquid detection switch signal channels are active, then a VTS Safety Actuation is initiated.

7.5.5.10 High TPS IU Cell 1/2/3/4/5/6/7/8 Target Chamber Exhaust Pressure

The high TPS IU Cell 1/2/3/4/5/6/7/8 target chamber exhaust pressure signal protects against a break in the tritium exhaust lines in the IU cell. The TPS IU Cell 1/2/3/4/5/6/7/8 target chamber exhaust pressure is measured with an analog interface on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more TPS IU Cell 1/2/3/4/5/6/7/8 target chamber exhaust pressure inputs exceed the allowable limit, the appropriate TPS Train A/B/C Isolation is initiated.

7.5.5.11 High TPS IU Cell 1/2/3/4/5/6/7/8 Target Chamber Supply Pressure

The high TPS IU Cell 1/2/3/4/5/6/7/8 target chamber supply pressure signal protects against a break in the tritium supply lines in the IU cell. The TPS IU Cell 1/2/3/4/5/6/7/8 target chamber supply pressure is measured with an analog interface on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more TPS IU Cell 1/2/3/4/5/6/7/8 target chamber supply pressure inputs exceed the allowable limit, the appropriate TPS Train A/B/C Isolation is initiated.

7.5.5.12 High TPS Exhaust to Facility Stack Tritium

The high TPS exhaust to facility stack tritium signal protects against a release of tritium from the TPS glovebox pressure control exhaust and VAC/ITS process vent exhaust into the facility ventilation systems. The TPS exhaust to facility stack tritium is measured with an analog interface on three different channels, one for each division of ESFAS. When two-out-of-three or more high TPS exhaust to facility stack tritium channels are active, then a TPS Process Vent Actuation is initiated.

7.5.5.13 High TPS Confinement Tritium

The high TPS confinement tritium signal protects against a release of tritium from TPS equipment into the TPS glovebox. There is an independent and separate tritium measurement for each of the three TPS trains. The TPS confinement tritium concentration is measured with an analog interface on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more high TPS confinement tritium channels are active, then a TPS

Train A Isolation, TPS Train B Isolation, or TPS Train C Isolation is initiated for the respective TPS train.

7.5.5.14 TRPS IU Cell Nitrogen Purge

The TRPS IU cell nitrogen purge signal protects against a loss of hydrogen mitigation capabilities in the irradiation units. The TRPS IU cell nitrogen purge signal is transmitted with a discrete input from the TRPS on two different channels, one for each Division A and Division B of ESFAS. When a TRPS IU cell nitrogen purge signal is active, then an ESFAS IU Cell Nitrogen Purge is initiated.

7.5.5.15 Low PVVS Flow

The PVVS flow signal protects against loss of hydrogen mitigation capabilities in the RPF. The PVVS flow is measured with an analog interface on three different channels, one for each division of ESFAS. When two-out-of-three or more high or low PVVS flow channels are active, then an RPF Nitrogen Purge is initiated.

7.5.5.16 MEPS Upper and Lower Three-Way Valves Misaligned

The MEPS upper and lower three-way valves misalignment signal protects against a misalignment of the upper and lower three-way valves, degrading one of the barriers preventing misdirection of chemical reagents or target solution. The MEPS upper and lower three-way valve position indication is measured with a discrete input signal through the respective division the three-way valve is designed to. When two-out-of-two MEPS upper and lower three-way valve position indications indicate they are energized, then a MEPS Alignment Actuation for that area is initiated.

7.5.5.17 IXP Upper and Lower Three-Way Valves Misaligned

The IXP upper and lower three-way valves misalignment signal protects against a misalignment of the upper and lower three-way valves, degrading one of the barriers preventing misdirection of chemical reagents or target solution. The IXP upper and lower three-way valve position indication is measured with a discrete input signal through the respective division the three-way valve is designed to. When two-out-of-two IXP upper and lower three-way valve position indications indicate they are energized, then an IXP Alignment Actuation is initiated.

7.5.5.18 TSPS Dissolution Tank Level Switch

The TSPS dissolution tank level switch signal protects against a criticality event due to excess fissile material in a non-favorable geometry system. The TSPS dissolution tank level switch signal is measured with a discrete input signal on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more TSPS dissolution tank level switch signals are active for either dissolution tank, a Dissolution Tank Isolation is initiated.

7.5.5.19 UPSS Loss of External Power

The UPSS loss of external power signal protects against an anticipatory loss of hydrogen mitigation in the IU cell (i.e., loss of TSV off-gas system (TOGS) blowers and recombiners after the UPSS runtime of that equipment has been exceeded). The UPSS loss of external power signal is measured with a discrete input signal on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more UPSS loss of external power signals are active, a timer is started that must run to completion before initiating an IU Cell Nitrogen Purge. If, while the timer is running, less than one-out-of-two UPSS loss of external power signals are active, the timer is reset and the ESFAS continues operating under normal conditions. The timer is set at three minutes to provide margin to the loss of TOGS equipment after five minutes of runtime on the UPSS.

Table 7.5-1 – ESFAS Monitored Variables
(Sheet 1 of 6)

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
RVZ1 RCA exhaust radiation	5x background radiation	2/3↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
RVZ2 RCA exhaust radiation	5x background radiation	2/3↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 1 (PVVS area) radiation	5x background radiation	2/3↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 2 (extraction area A) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 3 (purification area A) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 4 (packaging area 1) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 5 (purification area B) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 6 (extraction area B) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 7 (extraction area C) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 8 (purification area C) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 9 (packaging area 2) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 10 (IXP area) radiation	5x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds

Table 7.5-1 – ESFAS Monitored Variables (Sheet 2 of 6)

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
MEPS [ ]$^{PROP/ECI}$ conductivity extraction area A	8.8 micromho/cm	1/2↑	0.1 to 50 micromho/cm	3 percent	5 seconds
MEPS [ ]$^{PROP/ECI}$ conductivity extraction area B	8.8 micromho/cm	1/2↑	0.1 to 50 micromho/cm	3 percent	5 seconds
MEPS [ ]$^{PROP/ECI}$ conductivity extraction area C	8.8 micromho/cm	1/2↑	0.1 to 50 micromho/cm	3 percent	5 seconds
Carbon delay bed group 1 exhaust carbon monoxide	20 ppm	1/2↑	0 to 30 ppm	10 percent	15 seconds
Carbon delay bed group 2 exhaust carbon monoxide	20 ppm	1/2↑	0 to 30 ppm	10 percent	15 seconds
Carbon delay bed group 3 exhaust carbon monoxide	20 ppm	1/2↑	0 to 30 ppm	10 percent	15 seconds
VTS vacuum header liquid detection switch signal	Active	1/2↑	Active/Inactive	Discrete input signal	5.5 seconds
RDS liquid detection switch signal	Active	1/2↑	Active/Inactive	Discrete input signal	5.5 seconds
TPS exhaust to facility stack tritium	1Ci/m^3	2/3↑	1 to 2,000,000 µCi/m^3	10 percent	5 seconds
TPS IU cell 1 target chamber exhaust pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 2 target chamber exhaust pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 3 target chamber exhaust pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds

Table 7.5-1 – ESFAS Monitored Variables
(Sheet 3 of 6)

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
TPS IU cell 4 target chamber exhaust pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 5 target chamber exhaust pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 6 target chamber exhaust pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 7 target chamber exhaust pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 8 target chamber exhaust pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 1 target chamber supply pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 2 target chamber supply pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 3 target chamber supply pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 4 target chamber supply pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 5 target chamber supply pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 6 target chamber supply pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds

Table 7.5-1 – ESFAS Monitored Variables
(Sheet 4 of 6)

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
TPS IU cell 7 target chamber supply pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS IU cell 8 target chamber supply pressure	8 psia	1/2↑	0 to 19.5 psia	1 percent	10 seconds
TPS confinement A tritium	1000 Ci/m^3	1/2↑	0.001 to 50,000 Ci/m^3	10 percent	5 seconds
TPS confinement B tritium	1000 Ci/m^3	1/2↑	0.001 to 50,000 Ci/m^3	10 percent	5 seconds
TPS confinement C tritium	1000 Ci/m^3	1/2↑	0.001 to 50,000 Ci/m^3	10 percent	5 seconds
PVVS flow	5.0 scfm	2/3↓	1-20 scfm	3 percent	0.5 seconds
TSPS dissolution tank 1 level switch signal	Active	1/2↑	Active/Inactive	Discrete input signal	1 second
TSPS dissolution tank 2 level switch signal	Active	1/2↑	Active/Inactive	Discrete input signal	1 second
TRPS IU cell 1 nitrogen purge signal	Active	1/1↑	Active/Inactive	Discrete input signal	500 ms
TRPS IU cell 2 nitrogen purge signal	Active	1/1↑	Active/Inactive	Discrete input signal	500 ms
TRPS IU cell 3 nitrogen purge signal	Active	1/1↑	Active/Inactive	Discrete input signal	500 ms
TRPS IU cell 4 nitrogen purge signal	Active	1/1↑	Active/Inactive	Discrete input signal	500 ms
TRPS IU cell 5 nitrogen purge signal	Active	1/1↑	Active/Inactive	Discrete input signal	500 ms
TRPS IU cell 6 nitrogen purge signal	Active	1/1↑	Active/Inactive	Discrete input signal	500 ms

Table 7.5-1 – ESFAS Monitored Variables (Sheet 5 of 6)

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
TRPS IU cell 7 nitrogen purge signal	Active	1/1↑	Active/Inactive	Discrete input signal	500 ms
TRPS IU cell 8 nitrogen purge signal	Active	1/1↑	Active/Inactive	Discrete input signal	500 ms
MEPS area A lower three-way valve supplying position indication[(a)]	Active	1/2↑ & 1/2↑	Active/Inactive	Discrete input signal	1 second
MEPS area A upper three-way valve supplying position indication[(a)]	Active	1/2↑ & 1/2↑	Active/Inactive	Discrete input signal	1 second
MEPS area B lower three-way valve supplying position indication[(a)]	Active	1/2↑ & 1/2↑	Active/Inactive	Discrete input signal	1 second
MEPS area B upper three-way valve supplying position indication[(a)]	Active	1/2↑ & 1/2↑	Active/Inactive	Discrete input signal	1 second
MEPS area C lower three-way valve supplying position indication[(a)]	Active	1/2↑ & 1/2↑	Active/Inactive	Discrete input signal	1 second
MEPS area C upper three-way valve supplying position indication[(a)]	Active	1/2↑ & 1/2↑	Active/Inactive	Discrete input signal	1 second

Table 7.5-1 – ESFAS Monitored Variables (Sheet 6 of 6)

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
IXP lower three-way valve supplying position indication[a]	Active	1/2↑ & 1/2↑	Active/Inactive	Discrete input signal	1 second
IXP upper three-way valve supplying position indication[a]	Active	1/2↑ & 1/2↑	Active/Inactive	Discrete input signal	1 second
UPSS loss of external power	Active	1/2↓	Active/Inactive	Discrete input signal	1 second

(a) A safety actuation is initiated when both the lower and upper three-way valve supplying position indications show one-out-of-two of the redundant indications are active.

Table 7.5-2 – Fail Safe Component Positions on ESFAS Loss of Power (Sheet 1 of 2)

FAIL-SAFE POSITION: CLOSED

RVZ1 exhaust isolation dampers

RVZ2 exhaust isolation dampers

RVZ2 supply train 1 isolation dampers

RVZ2 supply train 2 isolation dampers

RVZ3 supply isolation dampers shipping/receiving IF

RVZ3 supply isolation dampers shipping/receiving RPF

RVZ3 supply isolation dampers main RCA ingress/egress

RVZ3 supply isolation dampers RPF emergency exit

RVZ3 supply isolation dampers IF emergency exit

RVZ3 exhaust isolation dampers IF emergency exit

RVZ2 TSPS supply damper

RVZ1 TSPS exhaust damper

RVZ2 supercell area 1 (PVVS area) inlet isolation dampers

RVZ1 supercell area 1 (PVVS area) outlet isolation dampers

RVZ2 supercell area 2 (extraction area A) inlet isolation dampers

RVZ1 supercell area 2 (extraction area A) outlet isolation dampers

RVZ2 supercell area 3 (purification area A) inlet isolation dampers

RVZ1 supercell area 3 (purification area A) outlet isolation dampers

RVZ2 supercell area 4 (packaging area 1) inlet isolation dampers

RVZ1 supercell area 4 (packaging area 1) outlet isolation dampers

RVZ2 supercell area 5 (purification area B) inlet isolation dampers

RVZ1 supercell area 5 (purification area B) outlet isolation dampers

RVZ2 supercell area 6 (extraction area B) inlet isolation dampers

RVZ1 supercell area 6 (extraction area B) outlet isolation dampers

RVZ2 supercell area 7 (extraction area C) inlet isolation dampers

RVZ1 supercell area 7 (extraction area C) outlet isolation dampers

RVZ2 supercell area 8 (purification area C) inlet isolation dampers

RVZ1 supercell area 8 (purification area C) outlet isolation dampers

RVZ2 supercell area 9 (packaging area 2) inlet isolation dampers

RVZ1 supercell area 9 (packaging area 2) outlet isolation dampers

RVZ2 supercell area 10 (IXP area) inlet isolation dampers

RVZ1 supercell area 10 (IXP area) outlet isolation dampers

RVZ TPS ventilation dampers

RLWI PVVS isolation valve

MEPS [ ]$^{PROP/ECI}$ A inlet isolation valve

MEPS [ ]$^{PROP/ECI}$ B inlet isolation valve

MEPS [ ]$^{PROP/ECI}$ C inlet isolation valve

MEPS [ ]$^{PROP/ECI}$ A discharge isolation valve

MEPS [ ]$^{PROP/ECI}$ B discharge isolation valve

MEPS [ ]$^{PROP/ECI}$ C discharge isolation valve

MEPS A extraction column wash supply valve

MEPS A extraction column eluent valve

MEPS A [ ]$^{PROP/ECI}$ wash supply valve

MEPS A [ ]$^{PROP/ECI}$ eluent valve

MEPS B extraction column wash supply valve

MEPS B extraction column eluent valve

MEPS B [ ]$^{PROP/ECI}$ wash supply valve

MEPS B [ ]$^{PROP/ECI}$ eluent valve

MEPS C extraction column wash supply valve

MEPS C extraction column eluent valve

MEPS C [ ]$^{PROP/ECI}$ wash supply valve

MEPS C [ ]$^{PROP/ECI}$ eluent valve

IXP recovery column wash supply valve

IXP recovery column eluent valve

IXP [ ]$^{PROP/ECI}$ wash supply valve

IXP [ ]$^{PROP/ECI}$ eluent valve

Table 7.5-2 – Fail Safe Component Positions on ESFAS Loss of Power (Sheet 2 of 2)

IXP FNHS supply valve
IXP liquid nitrogen supply valve
TPS train A glovebox pressure control exhaust isolation valve
TPS train A ITS isolation valves
TPS train A helium AOV supply valve
TPS train A helium SOV supply valve
TPS train A vacuum isolation valves
TPS train B glovebox pressure control exhaust isolation valve
TPS train B ITS isolation valves
TPS train B helium AOV supply valve
TPS train B helium SOV supply valve
TPS train B vacuum isolation valves
TPS train C glovebox pressure control exhaust isolation valve
TPS train C ITS isolation valves
TPS train C helium AOV supply valve
TPS train C helium SOV supply valve
TPS train C vacuum isolation valves
N2PS RVZ2 north header valves
N2PS RVZ2 south header valves
TSPS RPCS supply cooling valves
TSPS RPCS return cooling valve

FAIL-SAFE POSITION: OPEN

RVZ1 exhaust train 1 blower breakers
RVZ1 exhaust train 2 blower breakers
RVZ2 exhaust train 1 blower breakers
RVZ2 exhaust train 2 blower breakers
RVZ2 supply train 1 blower breakers
RVZ2 supply train 2 blower breakers
VTS vacuum transfer pump 1 breakers
VTS vacuum transfer pump 2 breakers
VTS vacuum transfer pump 3 breakers
VTS vacuum break valves
PVVS blower bypass valves
PVVS carbon guard bed bypass valves
PVVS carbon delay bed group 1 outlet isolation valves
PVVS carbon delay bed group 2 outlet isolation valves
PVVS carbon delay bed group 3 outlet isolation valves
MEPS A extraction feed pump breakers
MEPS B extraction feed pump breakers
MEPS C extraction feed pump breakers
N2PS IU cell header valves
N2PS RPF header valves

FAIL-SAFE POSITION: SUPPLYING

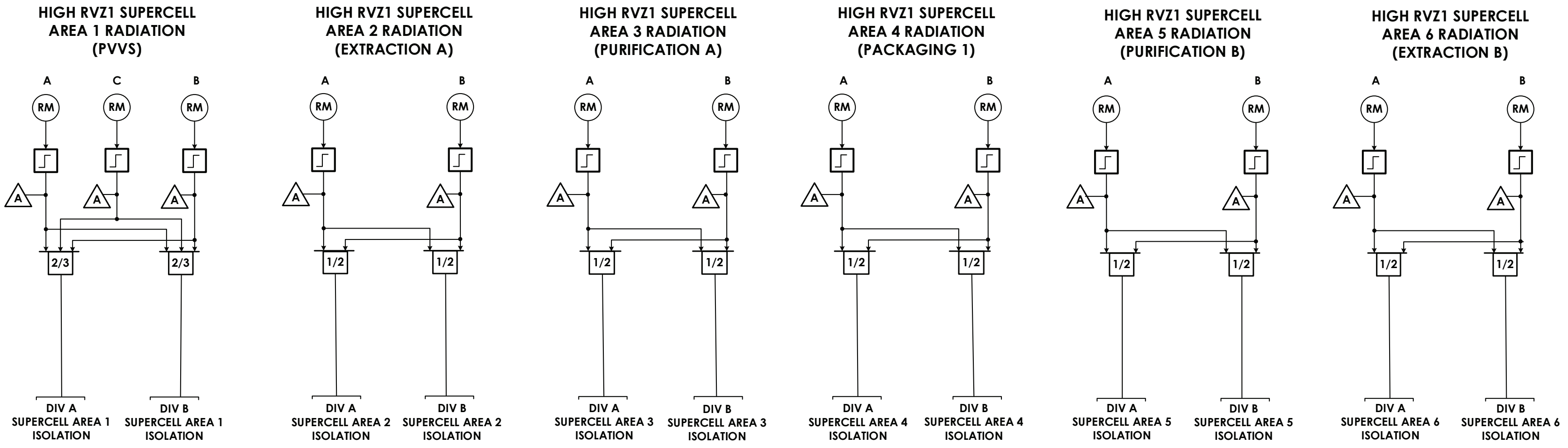
PVVS carbon delay bed group 1 three-way valves
PVVS carbon delay bed group 2 three-way valves
PVVS carbon delay bed group 3 three-way valves

FAIL-SAFE POSITION: DISCHARGING

MEPS area A lower three-way valve
MEPS area A upper three-way valve
MEPS area B lower three-way valve
MEPS area B upper three-way valve
MEPS area C lower three-way isolation valve
MEPS area C upper three-way isolation valve
IXP upper three-way valve
IXP lower three-way valve

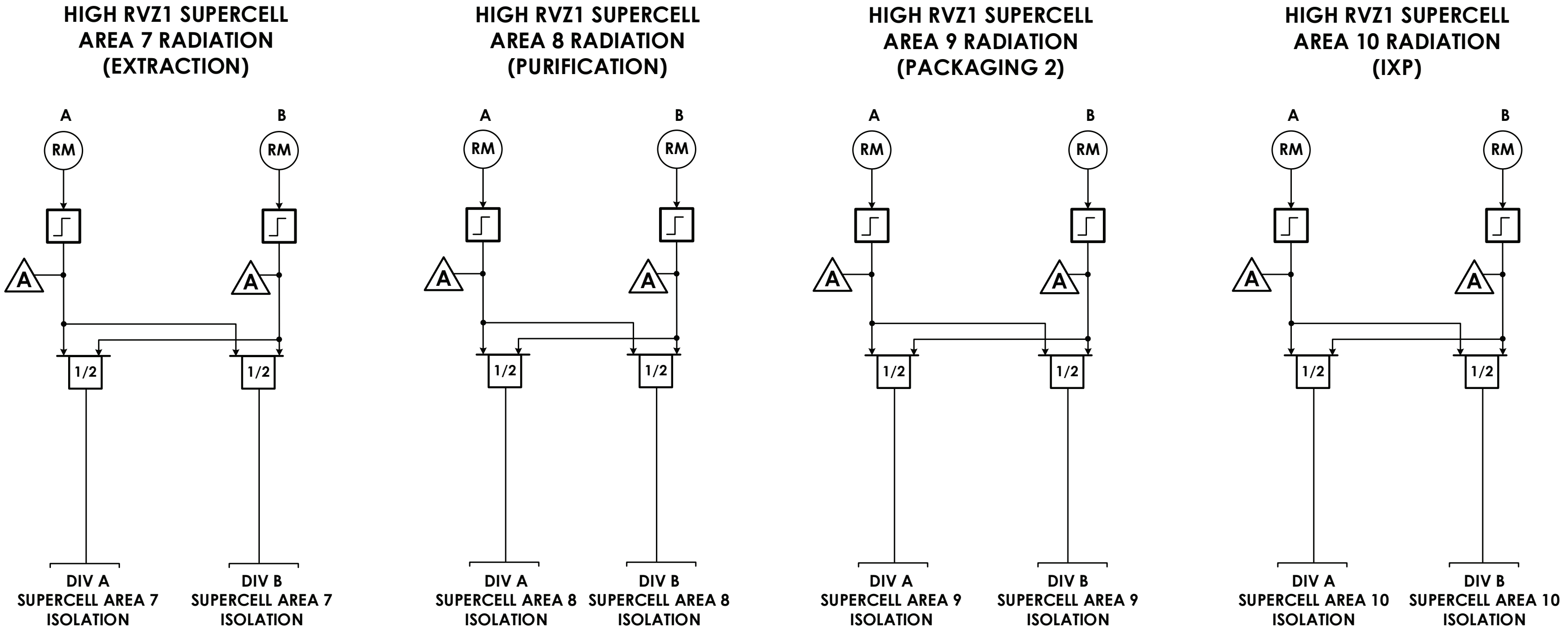
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 1 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 2 of 27)


HIGH RVZ1 SUPERCELL AREA 1 RADIATION (PVVS)
A
C
B
RM
RM
RM
A
A
A
2/3
2/3
DIV A SUPERCELL AREA 1 ISOLATION
DIV B SUPERCELL AREA 1 ISOLATION
HIGH RVZ1 SUPERCELL AREA 2 RADIATION (EXTRACTION A)
A
B
RM
RM
A
A
1/2
1/2
DIV A SUPERCELL AREA 2 ISOLATION
DIV B SUPERCELL AREA 2 ISOLATION
HIGH RVZ1 SUPERCELL AREA 3 RADIATION (PURIFICATION A)
A
B
RM
RM
A
A
1/2
1/2
DIV A SUPERCELL AREA 3 ISOLATION
DIV B SUPERCELL AREA 3 ISOLATION
HIGH RVZ1 SUPERCELL AREA 4 RADIATION (PACKAGING 1)
A
B
RM
RM
A
A
1/2
1/2
DIV A SUPERCELL AREA 4 ISOLATION
DIV B SUPERCELL AREA 4 ISOLATION
HIGH RVZ1 SUPERCELL AREA 5 RADIATION (PURIFICATION B)
A
B
RM
RM
A
A
1/2
1/2
DIV A SUPERCELL AREA 5 ISOLATION
DIV B SUPERCELL AREA 5 ISOLATION
HIGH RVZ1 SUPERCELL AREA 6 RADIATION (EXTRACTION B)
A
B
RM
RM
A
A
1/2
1/2
DIV A SUPERCELL AREA 6 ISOLATION
DIV B SUPERCELL AREA 6 ISOLATION

Trip Determination

**Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 3 of 27)**



HIGH RVZ1 SUPERCELL AREA 7 RADIATION (EXTRACTION)

HIGH RVZ1 SUPERCELL AREA 8 RADIATION (PURIFICATION)

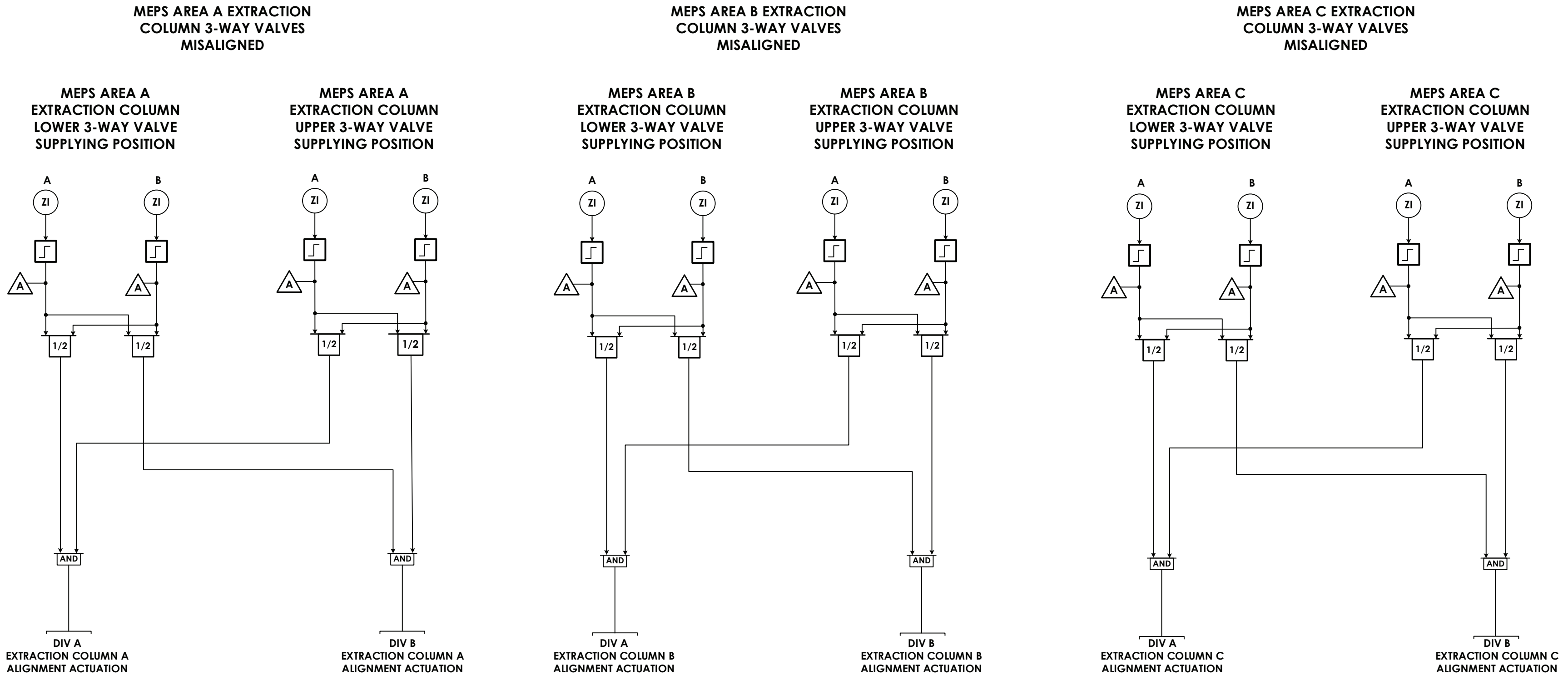
HIGH RVZ1 SUPERCELL AREA 9 RADIATION (PACKAGING 2)

HIGH RVZ1 SUPERCELL AREA 10 RADIATION (IXP)

A
B
RM
RM
A
A
1/2
1/2
DIV A SUPERCELL AREA 7 ISOLATION
DIV B SUPERCELL AREA 7 ISOLATION
DIV A SUPERCELL AREA 8 ISOLATION
DIV B SUPERCELL AREA 8 ISOLATION
DIV A SUPERCELL AREA 9 ISOLATION
DIV B SUPERCELL AREA 9 ISOLATION
DIV A SUPERCELL AREA 10 ISOLATION
DIV B SUPERCELL AREA 10 ISOLATION

Trip Determination

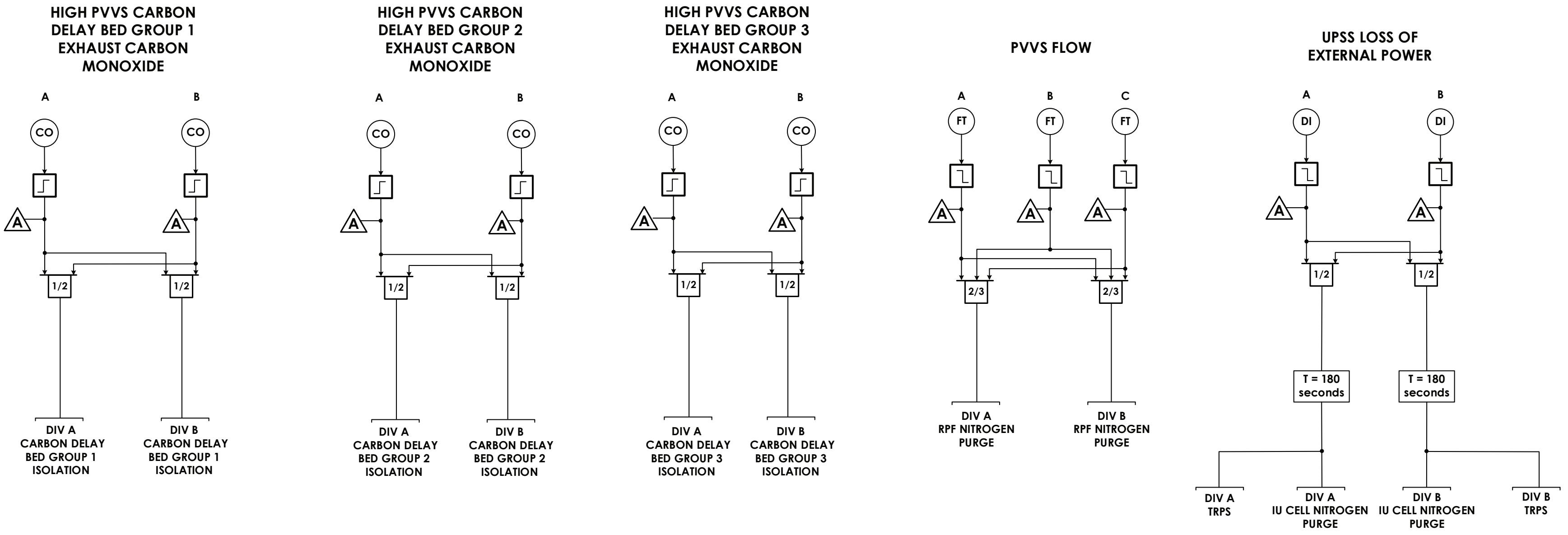
Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 4 of 27)


MEPS AREA A EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
MEPS AREA B EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
MEPS AREA C EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
MEPS AREA A EXTRACTION COLUMN LOWER 3-WAY VALVE SUPPLYING POSITION
MEPS AREA A EXTRACTION COLUMN UPPER 3-WAY VALVE SUPPLYING POSITION
MEPS AREA B EXTRACTION COLUMN LOWER 3-WAY VALVE SUPPLYING POSITION
MEPS AREA B EXTRACTION COLUMN UPPER 3-WAY VALVE SUPPLYING POSITION
MEPS AREA C EXTRACTION COLUMN LOWER 3-WAY VALVE SUPPLYING POSITION
MEPS AREA C EXTRACTION COLUMN UPPER 3-WAY VALVE SUPPLYING POSITION
A
B
ZI
A
1/2
AND
DIV A EXTRACTION COLUMN A ALIGNMENT ACTUATION
DIV B EXTRACTION COLUMN A ALIGNMENT ACTUATION
DIV A EXTRACTION COLUMN B ALIGNMENT ACTUATION
DIV B EXTRACTION COLUMN B ALIGNMENT ACTUATION
DIV A EXTRACTION COLUMN C ALIGNMENT ACTUATION
DIV B EXTRACTION COLUMN C ALIGNMENT ACTUATION

Trip Determination

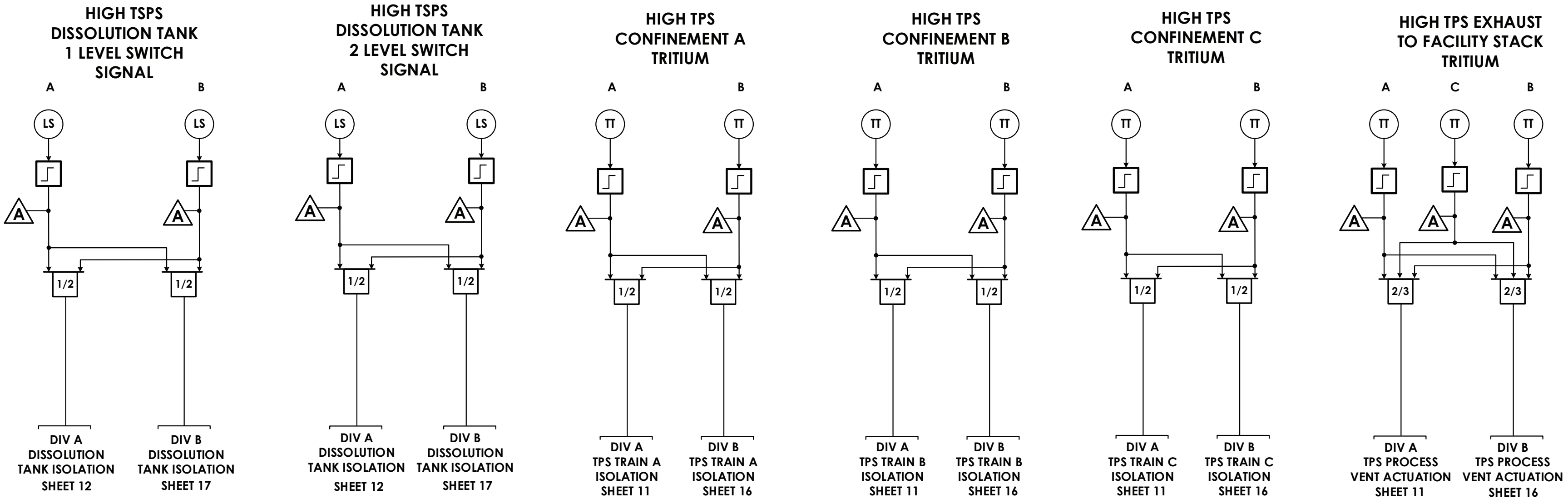
Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 5 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 6 of 27)


HIGH PVVS CARBON DELAY BED GROUP 1 EXHAUST CARBON MONOXIDE
A
B
CO
CO
A
A
1/2
1/2
DIV A CARBON DELAY BED GROUP 1 ISOLATION
DIV B CARBON DELAY BED GROUP 1 ISOLATION
HIGH PVVS CARBON DELAY BED GROUP 2 EXHAUST CARBON MONOXIDE
A
B
CO
CO
A
A
1/2
1/2
DIV A CARBON DELAY BED GROUP 2 ISOLATION
DIV B CARBON DELAY BED GROUP 2 ISOLATION
HIGH PVVS CARBON DELAY BED GROUP 3 EXHAUST CARBON MONOXIDE
A
B
CO
CO
A
A
1/2
1/2
DIV A CARBON DELAY BED GROUP 3 ISOLATION
DIV B CARBON DELAY BED GROUP 3 ISOLATION
PVVS FLOW
A
B
C
FT
FT
FT
A
A
A
2/3
2/3
DIV A RPF NITROGEN PURGE
DIV B RPF NITROGEN PURGE
UPSS LOSS OF EXTERNAL POWER
A
B
DI
DI
A
A
1/2
1/2
T = 180 seconds
T = 180 seconds
DIV A TRPS
DIV A IU CELL NITROGEN PURGE
DIV B IU CELL NITROGEN PURGE
DIV B TRPS

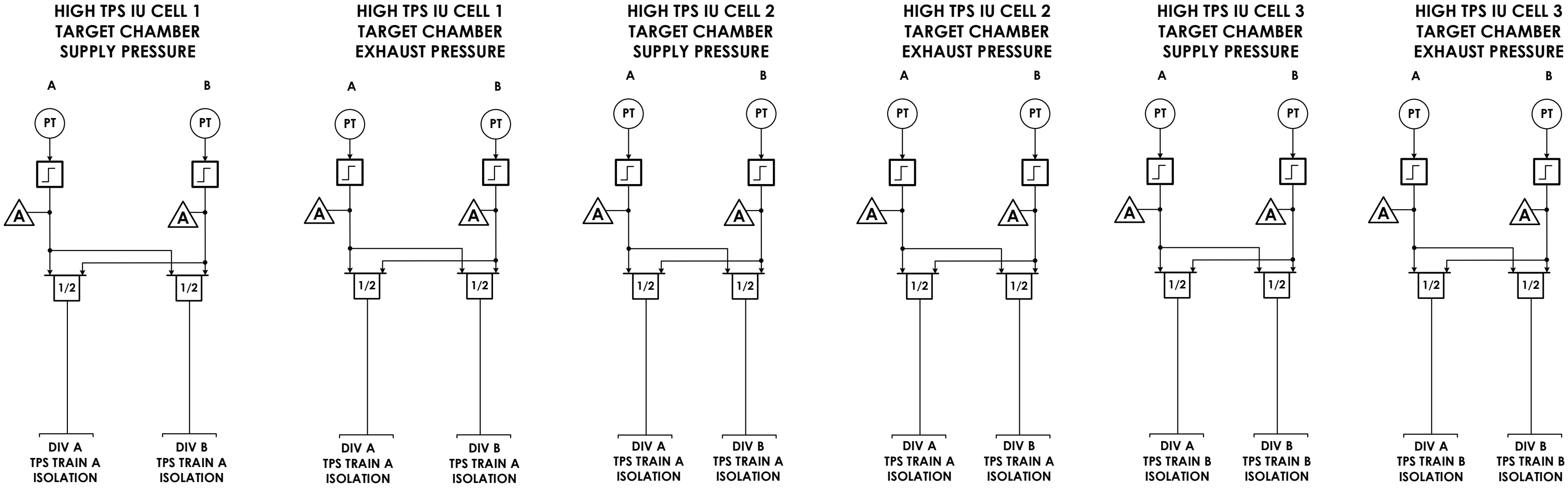
Trip Determination

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 7 of 27)


HIGH TSPS DISSOLUTION TANK 1 LEVEL SWITCH SIGNAL
A
B
LS
LS
A
A
1/2
1/2
DIV A DISSOLUTION TANK ISOLATION SHEET 12
DIV B DISSOLUTION TANK ISOLATION SHEET 17
HIGH TSPS DISSOLUTION TANK 2 LEVEL SWITCH SIGNAL
A
B
LS
LS
A
A
1/2
1/2
DIV A DISSOLUTION TANK ISOLATION SHEET 12
DIV B DISSOLUTION TANK ISOLATION SHEET 17
HIGH TPS CONFINEMENT A TRITIUM
A
B
TT
TT
A
A
1/2
1/2
DIV A TPS TRAIN A ISOLATION SHEET 11
DIV B TPS TRAIN A ISOLATION SHEET 16
HIGH TPS CONFINEMENT B TRITIUM
A
B
TT
TT
A
A
1/2
1/2
DIV A TPS TRAIN B ISOLATION SHEET 11
DIV B TPS TRAIN B ISOLATION SHEET 16
HIGH TPS CONFINEMENT C TRITIUM
A
B
TT
TT
A
A
1/2
1/2
DIV A TPS TRAIN C ISOLATION SHEET 11
DIV B TPS TRAIN C ISOLATION SHEET 16
HIGH TPS EXHAUST TO FACILITY STACK TRITIUM
A
C
B
TT
TT
TT
A
A
A
2/3
2/3
DIV A TPS PROCESS VENT ACTUATION SHEET 11
DIV B TPS PROCESS VENT ACTUATION SHEET 16

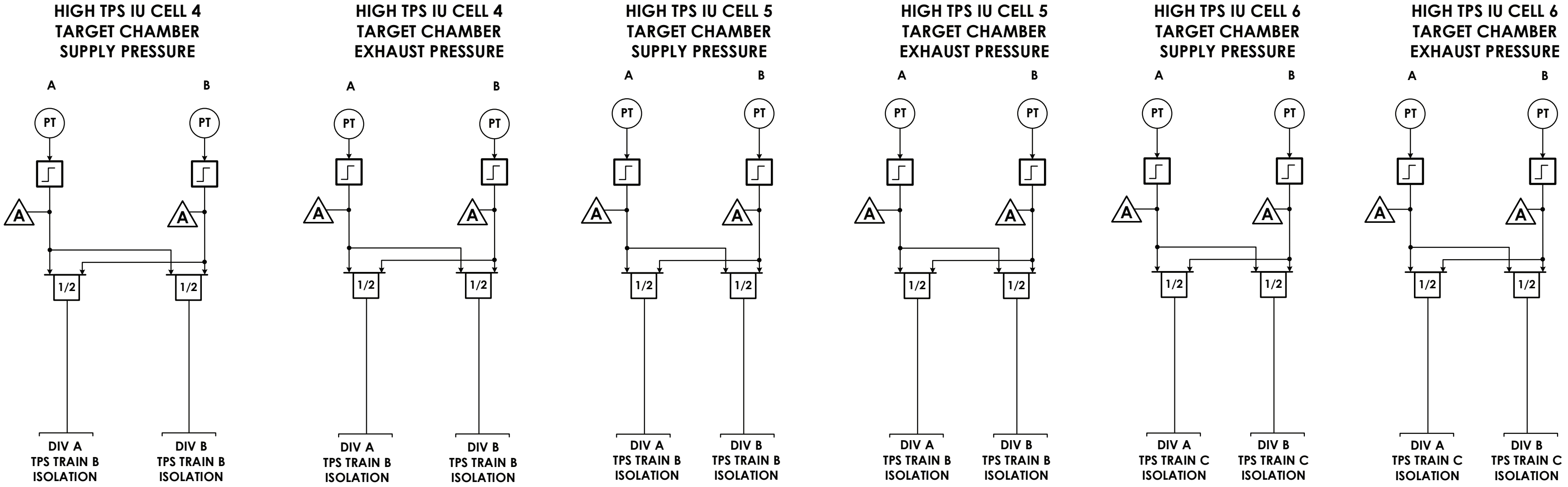
Trip Determination

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 8 of 27)


HIGH TPS IU CELL 1 TARGET CHAMBER SUPPLY PRESSURE
A
B
PT
PT
A
A
1/2
1/2
DIV A TPS TRAIN A ISOLATION
DIV B TPS TRAIN A ISOLATION
HIGH TPS IU CELL 1 TARGET CHAMBER EXHAUST PRESSURE
A
B
PT
PT
A
A
1/2
1/2
DIV A TPS TRAIN A ISOLATION
DIV B TPS TRAIN A ISOLATION
HIGH TPS IU CELL 2 TARGET CHAMBER SUPPLY PRESSURE
A
B
PT
PT
A
A
1/2
1/2
DIV A TPS TRAIN A ISOLATION
DIV B TPS TRAIN A ISOLATION
HIGH TPS IU CELL 2 TARGET CHAMBER EXHAUST PRESSURE
A
B
PT
PT
A
A
1/2
1/2
DIV A TPS TRAIN A ISOLATION
DIV B TPS TRAIN A ISOLATION
HIGH TPS IU CELL 3 TARGET CHAMBER SUPPLY PRESSURE
A
B
PT
PT
A
A
1/2
1/2
DIV A TPS TRAIN B ISOLATION
DIV B TPS TRAIN B ISOLATION
HIGH TPS IU CELL 3 TARGET CHAMBER EXHAUST PRESSURE
A
B
PT
PT
A
A
1/2
1/2
DIV A TPS TRAIN B ISOLATION
DIV B TPS TRAIN B ISOLATION

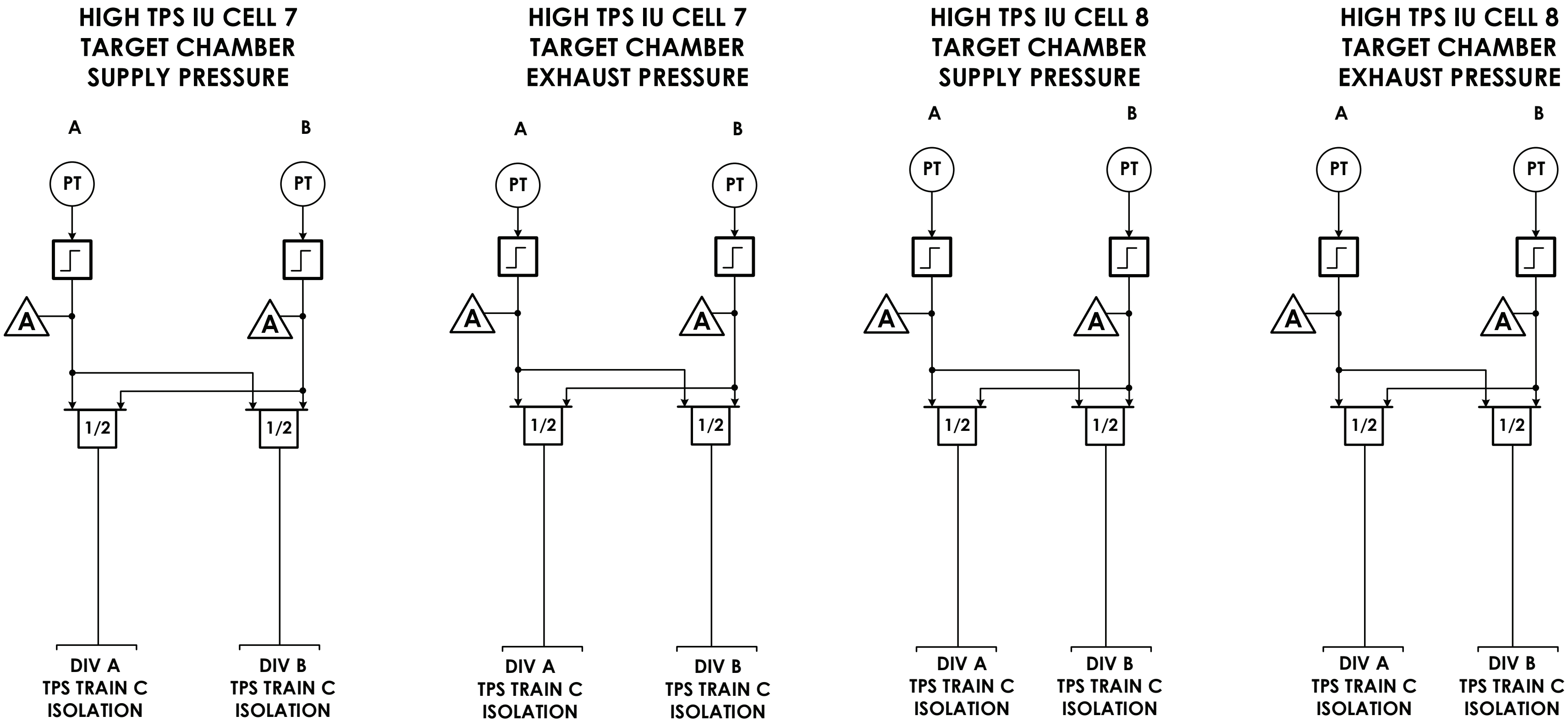
Trip Determination

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 9 of 27)


HIGH TPS IU CELL 4 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 4 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS IU CELL 5 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 5 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS IU CELL 6 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 6 TARGET CHAMBER EXHAUST PRESSURE
A
B
PT
A
1/2
DIV A TPS TRAIN B ISOLATION
DIV B TPS TRAIN B ISOLATION
DIV A TPS TRAIN C ISOLATION
DIV B TPS TRAIN C ISOLATION

Trip Determination

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 10 of 27)



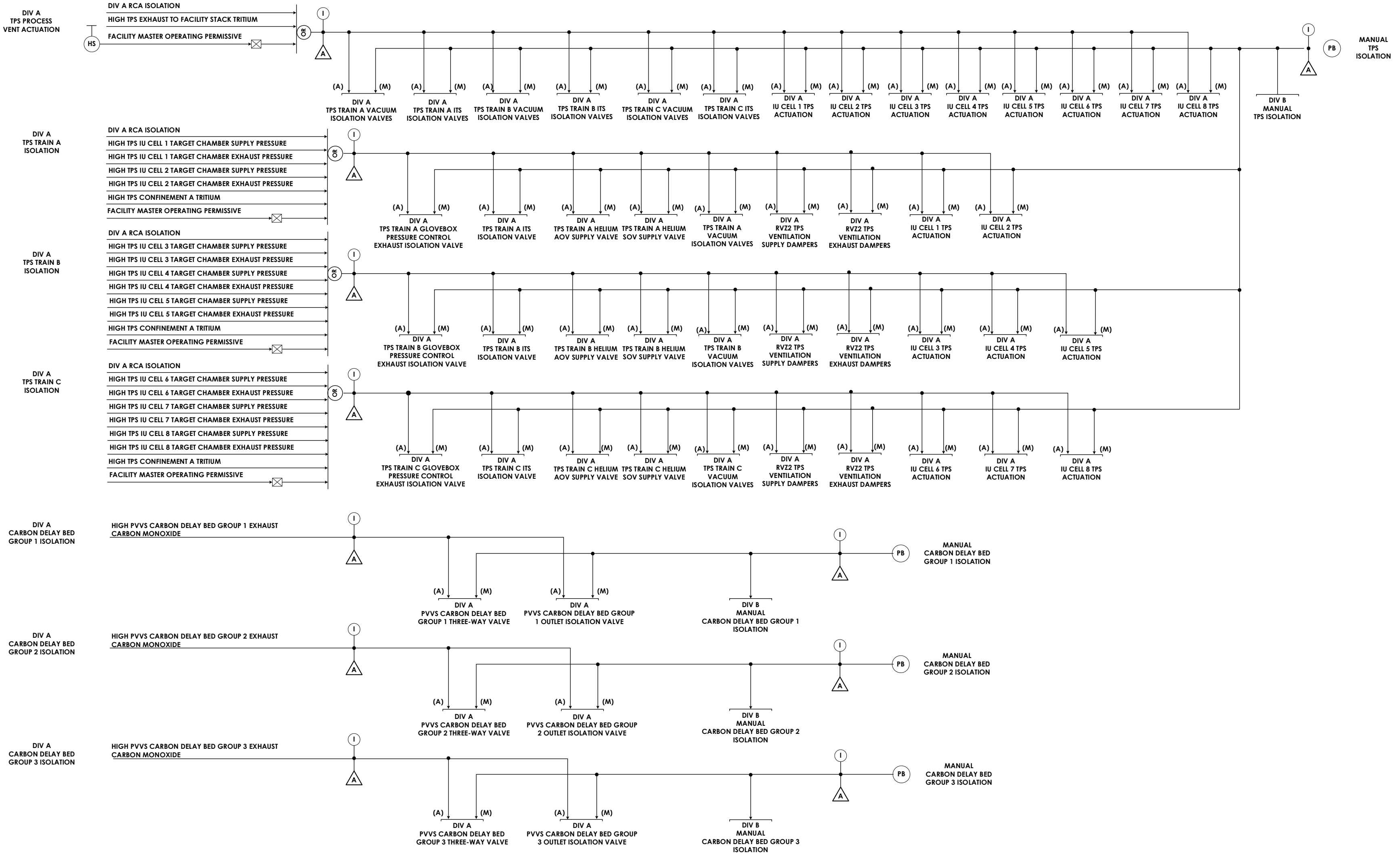
Trip Determination

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 11 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 12 of 27)

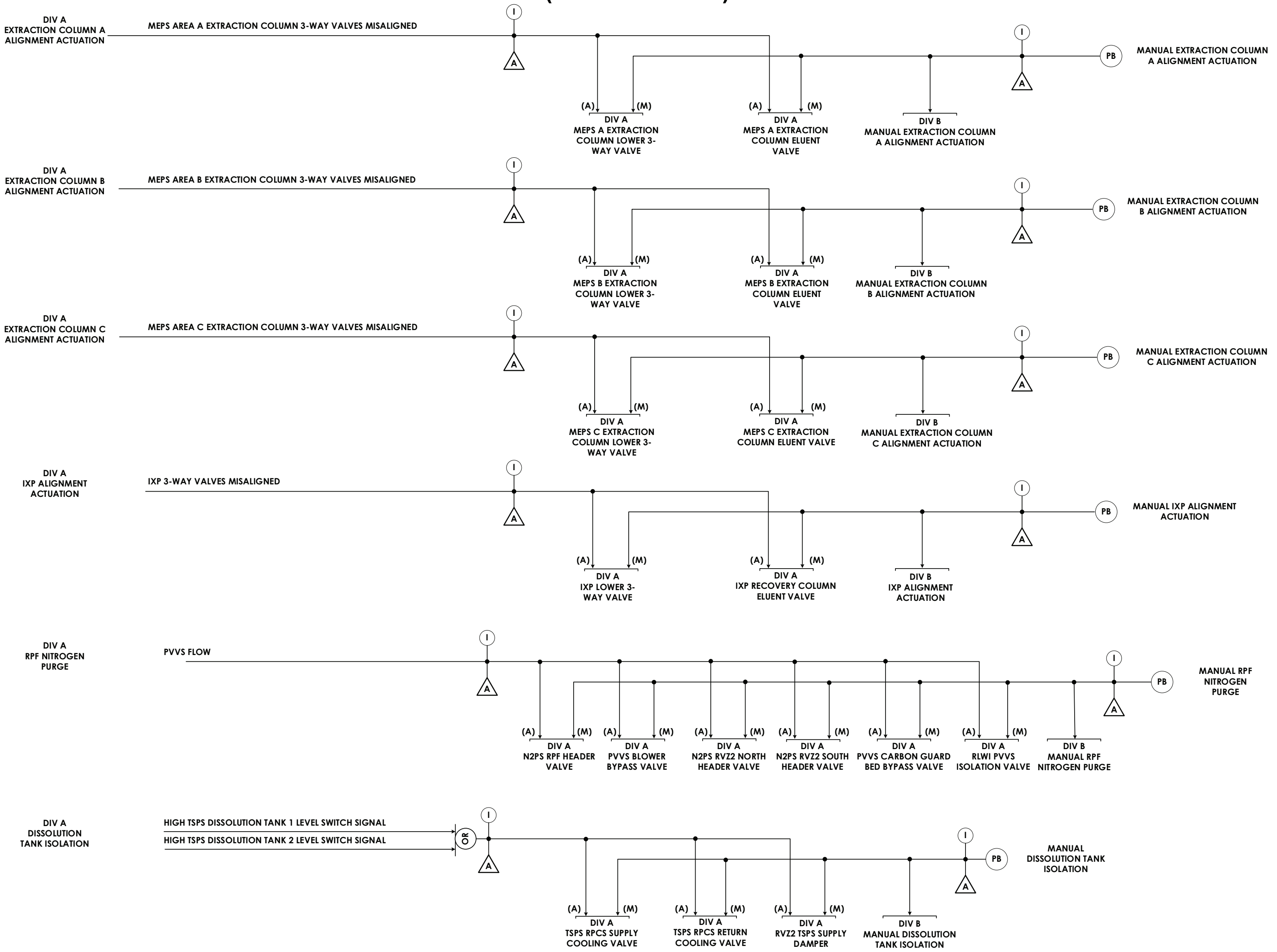
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 13 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 14 of 27)



Safety Actuation

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 15 of 27)


DIV A
EXTRACTION COLUMN A ALIGNMENT ACTUATION
MEPS AREA A EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
I
A
(A)
(M)
DIV A
MEPS A EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A
MEPS A EXTRACTION COLUMN ELUENT VALVE
DIV B
MANUAL EXTRACTION COLUMN A ALIGNMENT ACTUATION
PB
MANUAL EXTRACTION COLUMN A ALIGNMENT ACTUATION
DIV A
EXTRACTION COLUMN B ALIGNMENT ACTUATION
MEPS AREA B EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
DIV A
MEPS B EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A
MEPS B EXTRACTION COLUMN ELUENT VALVE
DIV B
MANUAL EXTRACTION COLUMN B ALIGNMENT ACTUATION
MANUAL EXTRACTION COLUMN B ALIGNMENT ACTUATION
DIV A
EXTRACTION COLUMN C ALIGNMENT ACTUATION
MEPS AREA C EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
DIV A
MEPS C EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A
MEPS C EXTRACTION COLUMN ELUENT VALVE
DIV B
MANUAL EXTRACTION COLUMN C ALIGNMENT ACTUATION
MANUAL EXTRACTION COLUMN C ALIGNMENT ACTUATION
DIV A
IXP ALIGNMENT ACTUATION
IXP 3-WAY VALVES MISALIGNED
DIV A
IXP LOWER 3-WAY VALVE
DIV A
IXP RECOVERY COLUMN ELUENT VALVE
DIV B
IXP ALIGNMENT ACTUATION
MANUAL IXP ALIGNMENT ACTUATION
DIV A
RPF NITROGEN PURGE
PVVS FLOW
DIV A
N2PS RPF HEADER VALVE
DIV A
PVVS BLOWER BYPASS VALVE
DIV A
N2PS RVZ2 NORTH HEADER VALVE
DIV A
N2PS RVZ2 SOUTH HEADER VALVE
DIV A
PVVS CARBON GUARD BED BYPASS VALVE
DIV A
RLWI PVVS ISOLATION VALVE
DIV B
MANUAL RPF NITROGEN PURGE
MANUAL RPF NITROGEN PURGE
DIV A
DISSOLUTION TANK ISOLATION
HIGH TSPS DISSOLUTION TANK 1 LEVEL SWITCH SIGNAL
HIGH TSPS DISSOLUTION TANK 2 LEVEL SWITCH SIGNAL
OR
DIV A
TSPS RPCS SUPPLY COOLING VALVE
DIV A
TSPS RPCS RETURN COOLING VALVE
DIV A
RVZ2 TSPS SUPPLY DAMPER
DIV B
MANUAL DISSOLUTION TANK ISOLATION
MANUAL DISSOLUTION TANK ISOLATION

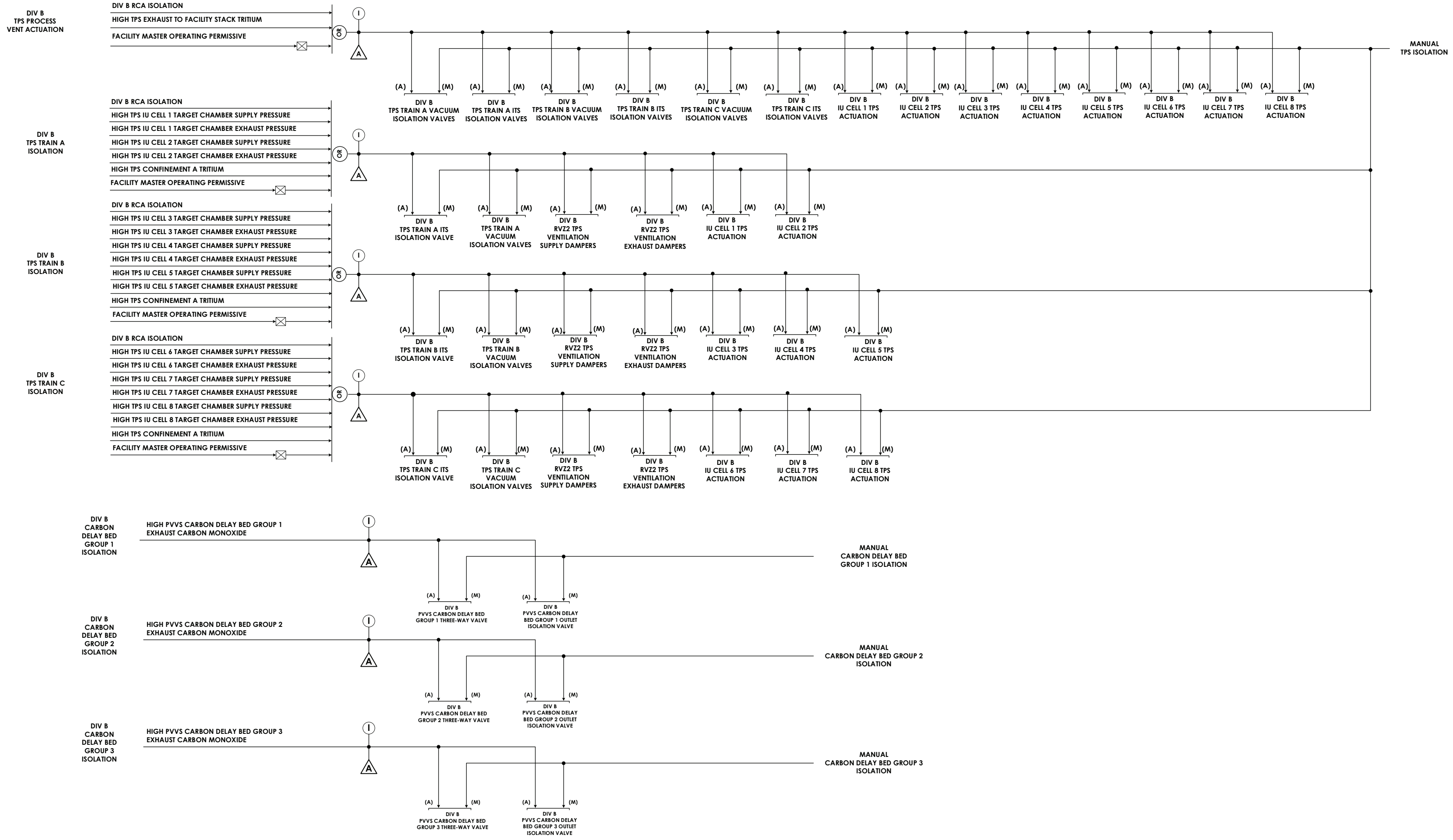
Safety Actuation

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 16 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 17 of 27)

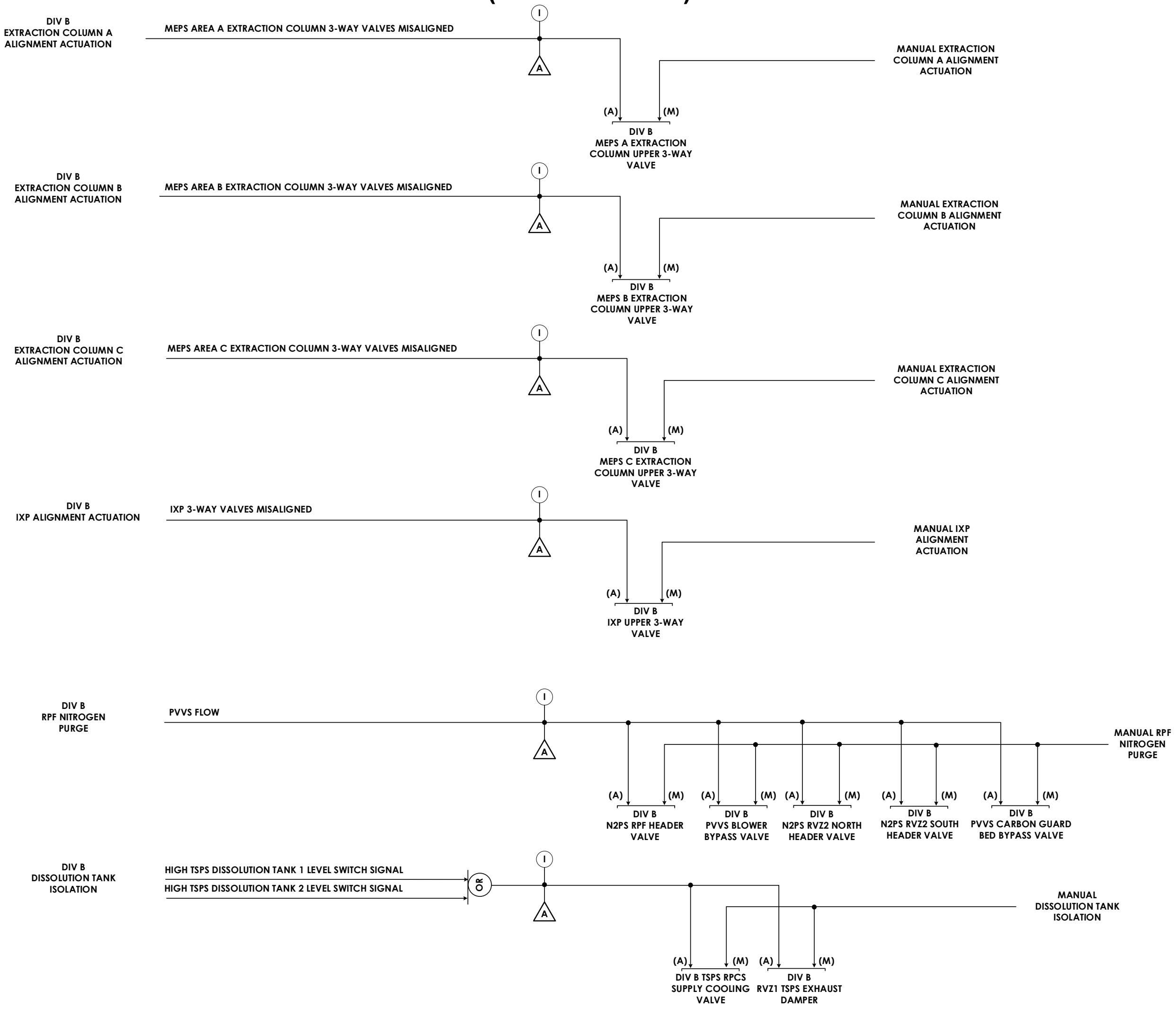
Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 18 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 19 of 27)


DIV B TPS PROCESS VENT ACTUATION
DIV B RCA ISOLATION
HIGH TPS EXHAUST TO FACILITY STACK TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
OR
I
A
MANUAL TPS ISOLATION
(A)
(M)
DIV B TPS TRAIN A VACUUM ISOLATION VALVES
DIV B TPS TRAIN A ITS ISOLATION VALVES
DIV B TPS TRAIN B VACUUM ISOLATION VALVES
DIV B TPS TRAIN B ITS ISOLATION VALVES
DIV B TPS TRAIN C VACUUM ISOLATION VALVES
DIV B TPS TRAIN C ITS ISOLATION VALVES
DIV B IU CELL 1 TPS ACTUATION
DIV B IU CELL 2 TPS ACTUATION
DIV B IU CELL 3 TPS ACTUATION
DIV B IU CELL 4 TPS ACTUATION
DIV B IU CELL 5 TPS ACTUATION
DIV B IU CELL 6 TPS ACTUATION
DIV B IU CELL 7 TPS ACTUATION
DIV B IU CELL 8 TPS ACTUATION
DIV B TPS TRAIN A ISOLATION
DIV B RCA ISOLATION
HIGH TPS IU CELL 1 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 1 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS IU CELL 2 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 2 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS CONFINEMENT A TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
DIV B TPS TRAIN A ITS ISOLATION VALVE
DIV B TPS TRAIN A VACUUM ISOLATION VALVES
DIV B RVZ2 TPS VENTILATION SUPPLY DAMPERS
DIV B RVZ2 TPS VENTILATION EXHAUST DAMPERS
DIV B IU CELL 1 TPS ACTUATION
DIV B IU CELL 2 TPS ACTUATION
DIV B TPS TRAIN B ISOLATION
DIV B RCA ISOLATION
HIGH TPS IU CELL 3 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 3 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS IU CELL 4 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 4 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS IU CELL 5 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 5 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS CONFINEMENT A TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
DIV B TPS TRAIN B ITS ISOLATION VALVE
DIV B TPS TRAIN B VACUUM ISOLATION VALVES
DIV B RVZ2 TPS VENTILATION SUPPLY DAMPERS
DIV B RVZ2 TPS VENTILATION EXHAUST DAMPERS
DIV B IU CELL 3 TPS ACTUATION
DIV B IU CELL 4 TPS ACTUATION
DIV B IU CELL 5 TPS ACTUATION
DIV B TPS TRAIN C ISOLATION
DIV B RCA ISOLATION
HIGH TPS IU CELL 6 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 6 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS IU CELL 7 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 7 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS IU CELL 8 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 8 TARGET CHAMBER EXHAUST PRESSURE
HIGH TPS CONFINEMENT A TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
DIV B TPS TRAIN C ITS ISOLATION VALVE
DIV B TPS TRAIN C VACUUM ISOLATION VALVES
DIV B RVZ2 TPS VENTILATION SUPPLY DAMPERS
DIV B RVZ2 TPS VENTILATION EXHAUST DAMPERS
DIV B IU CELL 6 TPS ACTUATION
DIV B IU CELL 7 TPS ACTUATION
DIV B IU CELL 8 TPS ACTUATION
DIV B CARBON DELAY BED GROUP 1 ISOLATION
HIGH PVVS CARBON DELAY BED GROUP 1 EXHAUST CARBON MONOXIDE
MANUAL CARBON DELAY BED GROUP 1 ISOLATION
DIV B PVVS CARBON DELAY BED GROUP 1 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 1 OUTLET ISOLATION VALVE
DIV B CARBON DELAY BED GROUP 2 ISOLATION
HIGH PVVS CARBON DELAY BED GROUP 2 EXHAUST CARBON MONOXIDE
MANUAL CARBON DELAY BED GROUP 2 ISOLATION
DIV B PVVS CARBON DELAY BED GROUP 2 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 2 OUTLET ISOLATION VALVE
DIV B CARBON DELAY BED GROUP 3 ISOLATION
HIGH PVVS CARBON DELAY BED GROUP 3 EXHAUST CARBON MONOXIDE
MANUAL CARBON DELAY BED GROUP 3 ISOLATION
DIV B PVVS CARBON DELAY BED GROUP 3 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 3 OUTLET ISOLATION VALVE

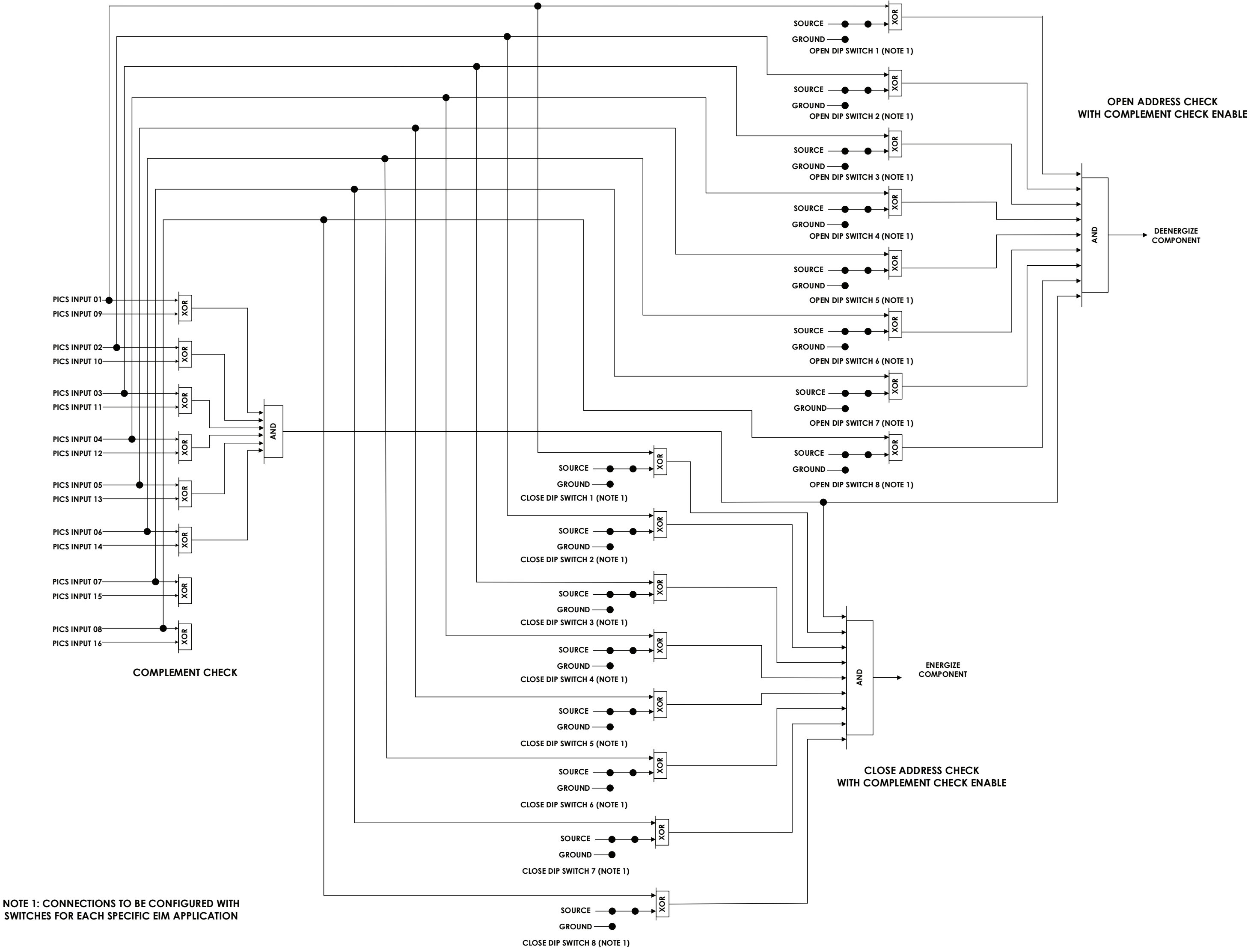
Safety Actuation

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 20 of 27)


DIV B EXTRACTION COLUMN A ALIGNMENT ACTUATION
MEPS AREA A EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
I
A
MANUAL EXTRACTION COLUMN A ALIGNMENT ACTUATION
(A)
(M)
DIV B MEPS A EXTRACTION COLUMN UPPER 3-WAY VALVE
DIV B EXTRACTION COLUMN B ALIGNMENT ACTUATION
MEPS AREA B EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
I
A
MANUAL EXTRACTION COLUMN B ALIGNMENT ACTUATION
(A)
(M)
DIV B MEPS B EXTRACTION COLUMN UPPER 3-WAY VALVE
DIV B EXTRACTION COLUMN C ALIGNMENT ACTUATION
MEPS AREA C EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
I
A
MANUAL EXTRACTION COLUMN C ALIGNMENT ACTUATION
(A)
(M)
DIV B MEPS C EXTRACTION COLUMN UPPER 3-WAY VALVE
DIV B IXP ALIGNMENT ACTUATION
IXP 3-WAY VALVES MISALIGNED
I
A
MANUAL IXP ALIGNMENT ACTUATION
(A)
(M)
DIV B IXP UPPER 3-WAY VALVE
DIV B RPF NITROGEN PURGE
PVVS FLOW
I
A
MANUAL RPF NITROGEN PURGE
(A)
(M)
DIV B N2PS RPF HEADER VALVE
(A)
(M)
DIV B PVVS BLOWER BYPASS VALVE
(A)
(M)
DIV B N2PS RVZ2 NORTH HEADER VALVE
(A)
(M)
DIV B N2PS RVZ2 SOUTH HEADER VALVE
(A)
(M)
DIV B PVVS CARBON GUARD BED BYPASS VALVE
DIV B DISSOLUTION TANK ISOLATION
HIGH TSPS DISSOLUTION TANK 1 LEVEL SWITCH SIGNAL
HIGH TSPS DISSOLUTION TANK 2 LEVEL SWITCH SIGNAL
OR
I
A
MANUAL DISSOLUTION TANK ISOLATION
(A)
(M)
DIV B TSPS RPCS SUPPLY COOLING VALVE
(A)
(M)
DIV B RVZ1 TSPS EXHAUST DAMPER

Safety Actuation

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 21 of 27)

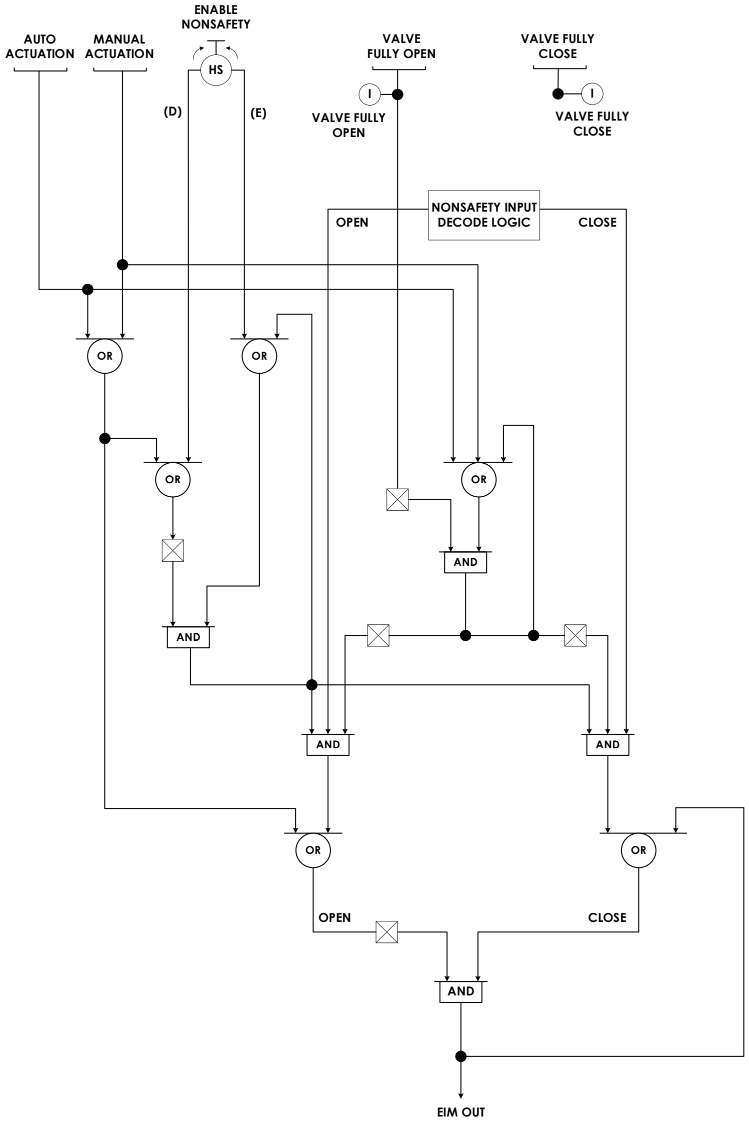

PICS INPUT 01
PICS INPUT 09
PICS INPUT 02
PICS INPUT 10
PICS INPUT 03
PICS INPUT 11
PICS INPUT 04
PICS INPUT 12
PICS INPUT 05
PICS INPUT 13
PICS INPUT 06
PICS INPUT 14
PICS INPUT 07
PICS INPUT 15
PICS INPUT 08
PICS INPUT 16
XOR
AND
COMPLEMENT CHECK
SOURCE
GROUND
OPEN DIP SWITCH 1 (NOTE 1)
OPEN DIP SWITCH 2 (NOTE 1)
OPEN DIP SWITCH 3 (NOTE 1)
OPEN DIP SWITCH 4 (NOTE 1)
OPEN DIP SWITCH 5 (NOTE 1)
OPEN DIP SWITCH 6 (NOTE 1)
OPEN DIP SWITCH 7 (NOTE 1)
OPEN DIP SWITCH 8 (NOTE 1)
OPEN ADDRESS CHECK
WITH COMPLEMENT CHECK ENABLE
DEENERGIZE
COMPONENT
CLOSE DIP SWITCH 1 (NOTE 1)
CLOSE DIP SWITCH 2 (NOTE 1)
CLOSE DIP SWITCH 3 (NOTE 1)
CLOSE DIP SWITCH 4 (NOTE 1)
CLOSE DIP SWITCH 5 (NOTE 1)
CLOSE DIP SWITCH 6 (NOTE 1)
CLOSE DIP SWITCH 7 (NOTE 1)
CLOSE DIP SWITCH 8 (NOTE 1)
ENERGIZE
COMPONENT
CLOSE ADDRESS CHECK
WITH COMPLEMENT CHECK ENABLE

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

Nonsafety Interface Decode

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 22 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 23 of 27)

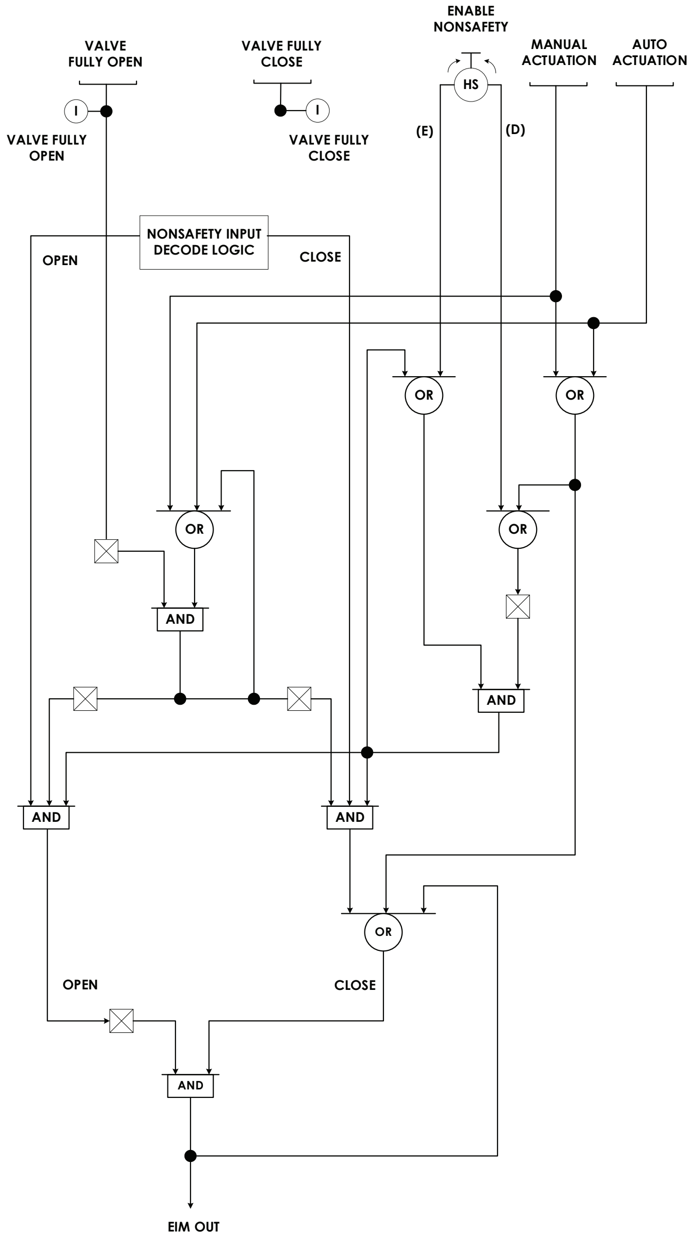


DIV A RZV1 EXHAUST TRAIN 1 BLOWER BREAKER	DIV B RZV1 EXHAUST TRAIN 1 BLOWER BREAKER
DIV A RZV1 EXHAUST TRAIN 2 BLOWER BREAKER	DIV B RZV1 EXHAUST TRAIN 2 BLOWER BREAKER
DIV A RZV2 EXHAUST TRAIN 1 BLOWER BREAKER	DIV B RZV2 EXHAUST TRAIN 1 BLOWER BREAKER
DIV A RZV2 EXHAUST TRAIN 2 BLOWER BREAKER	DIV B RZV2 EXHAUST TRAIN 2 BLOWER BREAKER
DIV A RZV2 SUPPLY TRAIN 1 BLOWER BREAKER	DIV B RZV2 SUPPLY TRAIN 1 BLOWER BREAKER
DIV A RZV2 SUPPLY TRAIN 2 BLOWER BREAKER	DIV B RZV2 SUPPLY TRAIN 2 BLOWER BREAKER
DIV A VTS VACUUM TRANSFER PUMP BREAKER 1	DIV B VTS VACUUM TRANSFER PUMP BREAKER 1
DIV A VTS VACUUM TRANSFER PUMP BREAKER 2	DIV B VTS VACUUM TRANSFER PUMP BREAKER 2
DIV A VTS VACUUM TRANSFER PUMP BREAKER 3	DIV B VTS VACUUM TRANSFER PUMP BREAKER 3
DIV A VTS VACUUM BREAK VALVE	DIV B VTS VACUUM BREAK VALVE
DIV A N2PS IU CELL HEADER VALVE	DIV B N2PS IU CELL HEADER VALVE
DIV A N2PS RPF HEADER VALVE	DIV B N2PS RPF HEADER VALVE
DIV A PVVS BLOWER BYPASS VALVE	DIV B PVVS BLOWER BYPASS VALVE
DIV A MEPS A EXTRACTION FEED PUMP BREAKER	DIV B MEPS A EXTRACTION FEED PUMP BREAKER
DIV A MEPS B EXTRACTION FEED PUMP BREAKER	DIV B MEPS B EXTRACTION FEED PUMP BREAKER
DIV A MEPS C EXTRACTION FEED PUMP BREAKER	DIV B MEPS C EXTRACTION FEED PUMP BREAKER

NOTE: OUTPUT OF EIM IS DEENERGIZE TO ACTUATE TO POSITION DEFINED FOR LOSS OF POWER

Priority Logic

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 24 of 27)

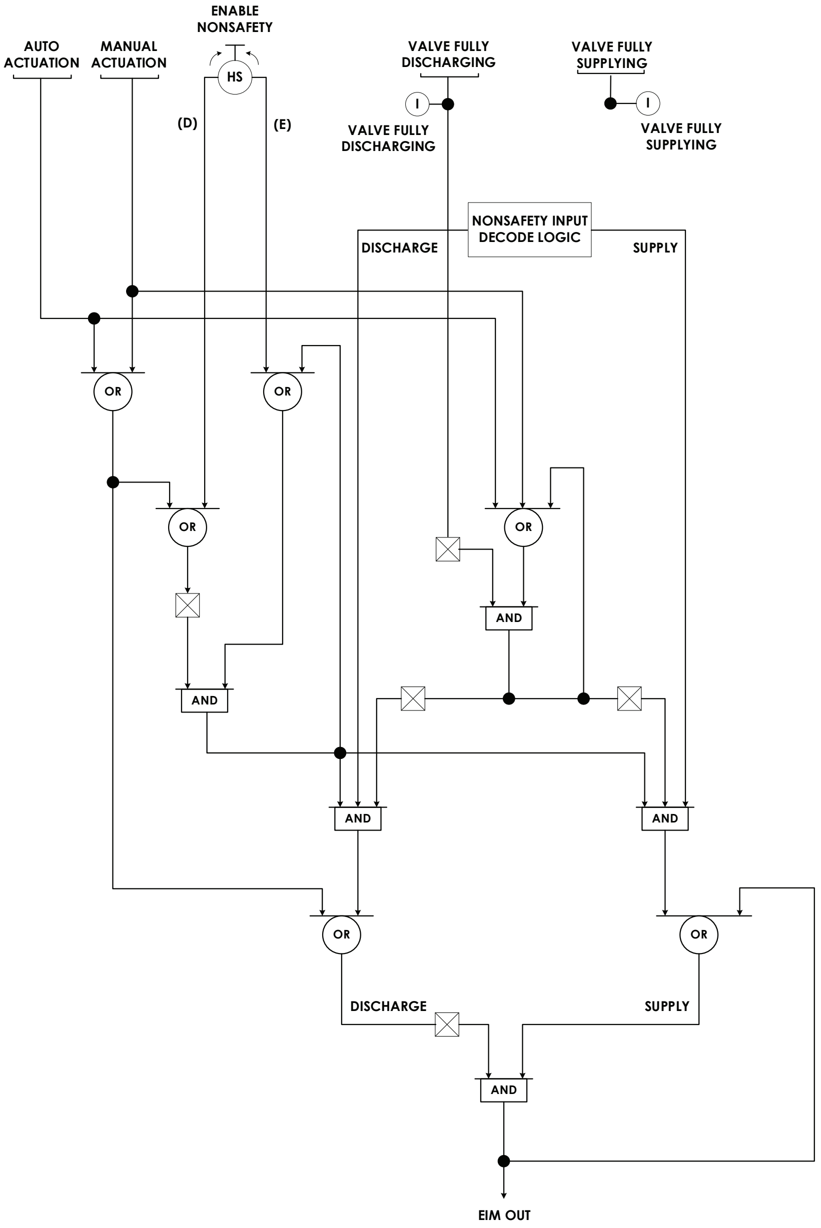


DIV A PVVS CARBON DELAY BED GROUP 1 OUTLET ISOLATION VALVE
DIV A PVVS CARBON DELAY BED GROUP 2 OUTLET ISOLATION VALVE
DIV A PVVS CARBON DELAY BED GROUP 3 OUTLET ISOLATION VALVE
DIV B PVVS CARBON DELAY BED GROUP 1 OUTLET ISOLATION VALVE
DIV B PVVS CARBON DELAY BED GROUP 2 OUTLET ISOLATION VALVE
DIV B PVVS CARBON DELAY BED GROUP 3 OUTLET ISOLATION VALVE

NOTE: OUTPUT OF EIM IS DEENERGIZE TO ACTUATE TO POSITION DEFINED FOR LOSS OF POWER

Priority Logic

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 25 of 27)

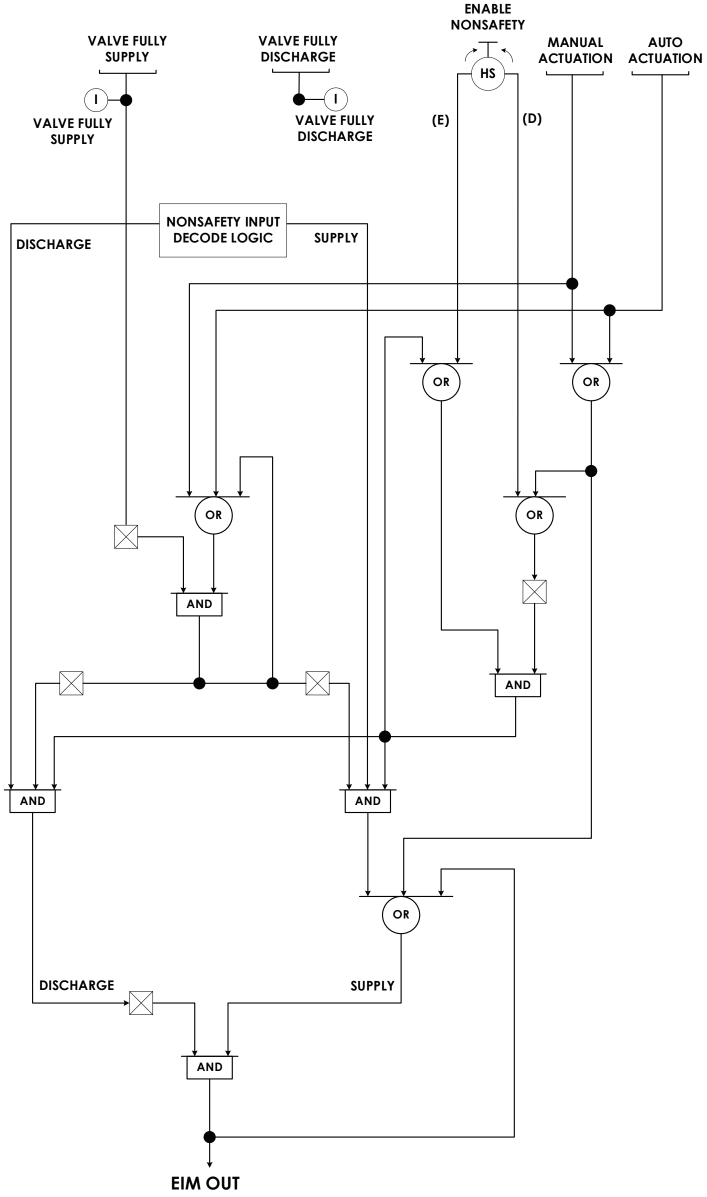


DIV A MEPS A EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A MEPS B EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A MEPS C EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A IXP LOWER 3-WAY VALVE
DIV B MEPS A EXTRACTION COLUMN UPPER 3-WAY VALVE
DIV B MEPS B EXTRACTION COLUMN UPPER 3-WAY VALVE
DIV B MEPS C EXTRACTION COLUMN UPPER 3-WAY VALVE
DIV B IXP UPPER 3-WAY VALVE

NOTE: OUTPUT OF EIM IS DEENERGIZE TO ACTUATE TO POSITION DEFINED FOR LOSS OF POWER

Priority Logic

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 26 of 27)



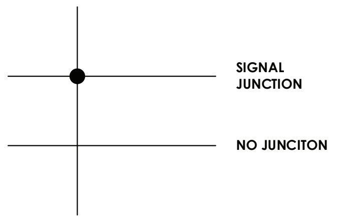
DIV A PVVS CARBON DELAY BED GROUP 1 THREE-WAY VALVE
DIV A PVVS CARBON DELAY BED GROUP 2 THREE-WAY VALVE
DIV A PVVS CARBON DELAY BED GROUP 3 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 1 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 2 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 3 THREE-WAY VALVE

NOTE: OUTPUT OF EIM IS DEENERGIZE TO ACTUATE TO POSITION DEFINED FOR LOSS OF POWER

Priority Logic

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 27 of 27)

A	ALARM PROVIDED TO PROCESS INTEGRATED CONTROL SYSTEM	RM	RADIATION MONITOR
I	INDICATION PROVIDED TO PROCESS INTEGRATED CONTROL SYSTEM	LS	LEVEL SWITCH
OR	LOGICAL "OR" GATE	ZI	POSITION INDICATION
AND	LOGICAL "AND" GATE	CT	CONDUCTIVITY TRANSMITTER
☒	LOGICAL "NOT" OR INVERTER GATE	PT	PRESSURE TRANSMITTER
XOR	LOGICAL "XOR" GATE	TT	TRITIUM TRANSMITTER
2/3	TWO-OUT-OF-THREE VOTING GATE	TE	TEMPERATURE ELEMENT
1/2	ONE-OUT-OF-TWO VOTING GATE	CO	CARBON MONOXIDE TRANSMITTER
_|‾	BISTABLE – INCREASING SETPOINT	FT	FLOW TRANSMITTER
‾|_	BISTABLE – DECREASING SETPOINT	DI	DISCRETE INPUT
PB	PUSH BUTTON	(A)	AUTOMATIC ACTUATION
HS	THREE POSITION HAND SWITCH, RETURN TO CENTER	(M)	MANUAL ACTUATION
HS	TWO POSITION HAND SWITCH	(E)	ENABLE NONSAFETY "ENABLED"
T = XX Seconds	TIMER THAT INITIATES ON A LOGIC "1", RESETS ON LOGIC "0" AND OUTPUTS A LOGIC "1" IF TIMER HAS EXPIRED	(D)	ENABLE NONSAFETY "DISABLED"



ACRONYMS
DIV – DIVISION
EIM – EQUIPMENT INTERFACE MODULE
FNHS – FACILITY NITROGEN HANDLING SYSTEM
GBSS – GLOVEBOX STRIPPER SYSTEM
IU – IRRADIATION UNIT
IXP – IODINE AND XENON PURIFICATION SYSTEM
MEPS – MOLYBDENUM EXTRACTION AND PURIFICATION SYSTEM
N2PS – NITROGEN PURGE SYSTEM
PICS – PROCESS INTEGRATED CONTROL SYSTEM
PVVS – PROCESS VESSEL VENTILATION SYSTEM
RCA – RADIOLOGICAL CONTROLLED AREA
RLWI – RADIOLOGICAL LIQUID WASTE IMMOBILIZATION
RVZ1 – RADIOLOGICAL VENTILATION ZONE 1
RVZ2 – RADIOLOGICAL VENTILATION ZONE 2
RVZ3 – RADIOLOGICAL VENTILATION ZONE 3
SSS – STORAGE AND SEPARATION SYSTEM
TPS – TRITIUM PURIFICATION SYSTEM
TSPS – TARGET SOLUTION PREPARATION SYSTEM
VTS – VACUUM TRANSFER SYSTEM

Legend

Figure 7.5-2 – Extraction Hot Cell
(Sheet 1 of 2)

Figure 7.5-2 – Extraction Hot Cell
(Sheet 2 of 2)

Figure 7.5-3 – Vacuum Transfer System (Sheet 1 of 2)

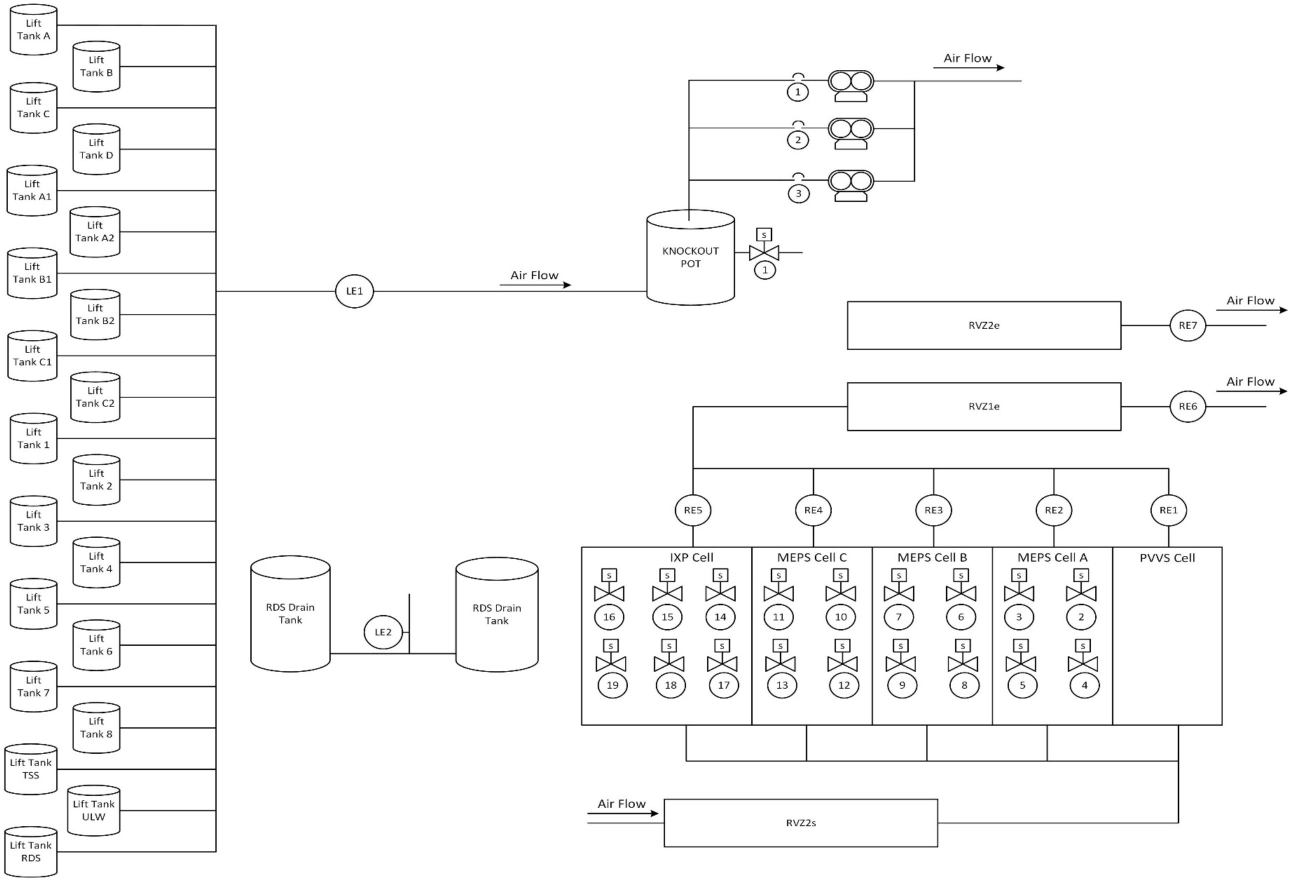


Figure 7.5-3 – Vacuum Transfer System
(Sheet 2 of 2)

Figure 7.5-4 – Radiologically Controlled Area Isolation (Sheet 1 of 2)

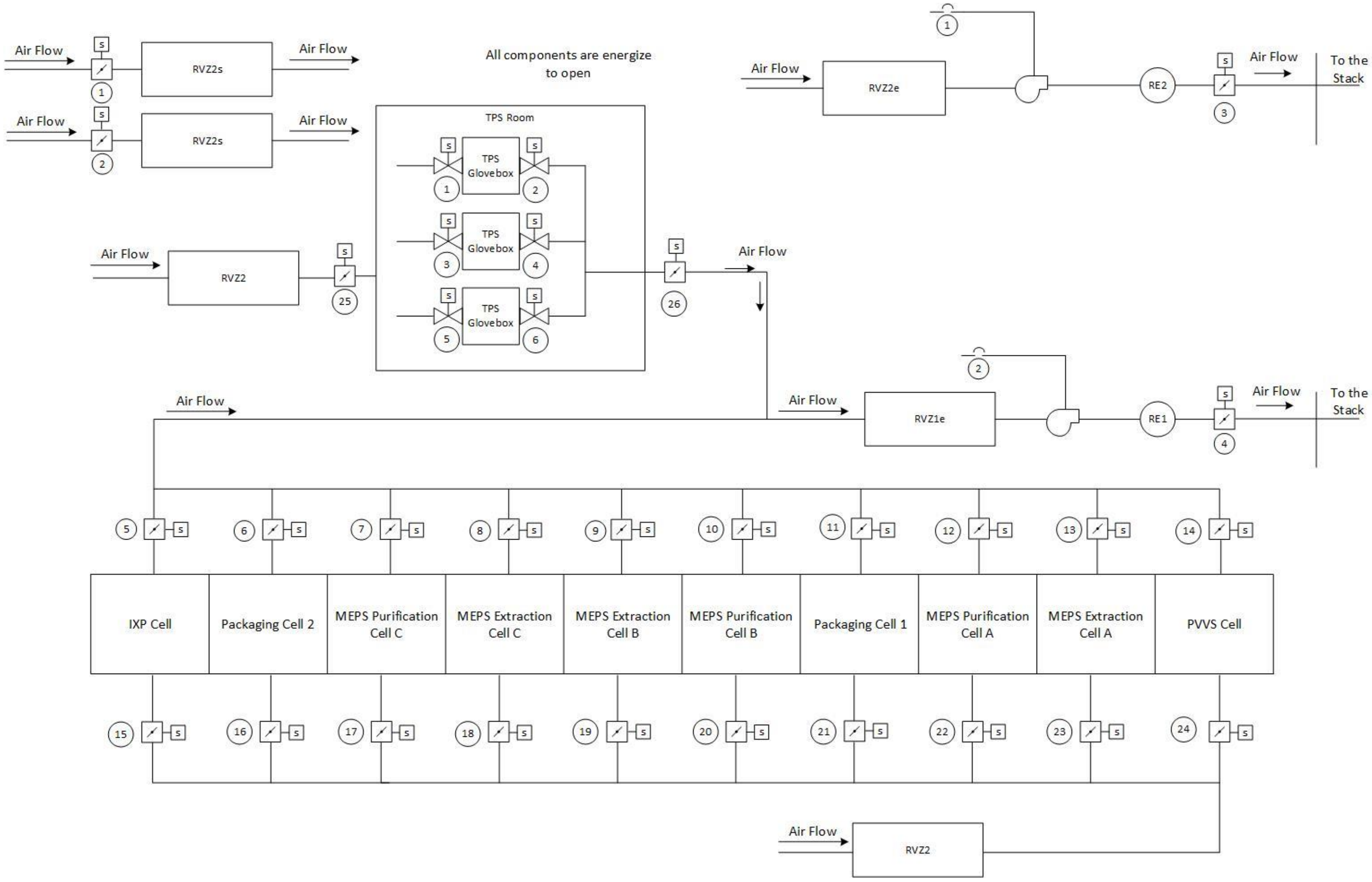


Figure 7.5-4 – Radiologically Controlled Area Isolation (Sheet 2 of 2)

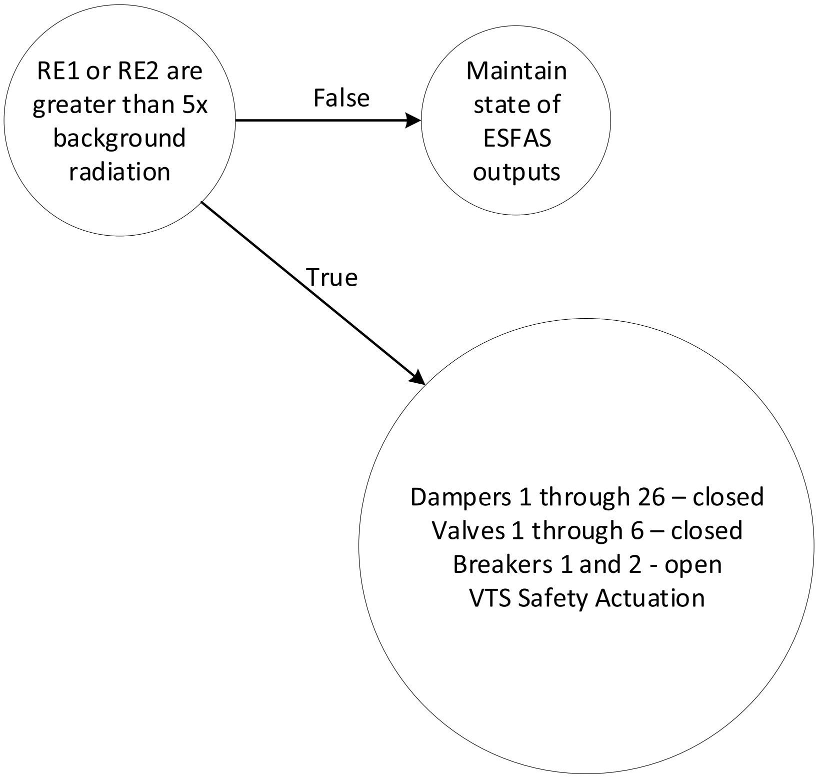
Damper 1 – RVZ2 train 1 RCA supply damper
Damper 2 – RVZ2 train 2 RCA supply damper
Damper 3 – RVZ2 RCA exhaust damper
Damper 4 – RVZ1 RCA exhaust damper
Damper 5 – 14 – supercell outlet isolation dampers
Damper 15 – 24 – supercell inlet isolation dampers
Damper 25 – TPS room inlet isolation damper
Damper 26 – TPS room outlet isolation damper

Breaker 1 – RVZ1 blower breaker
Breaker 2 – RVZ2 blower breaker

Valve 1 – TPS train A RVZ1e valve
Valve 2 – TPS train A confinement valves
Valve 3 – TPS train B RVZ1e valve
Valve 4 – TPS train B confinement valves
Valve 5 – TPS train C RVZ1e valve
Valve 6 – TPS train C confinement valves

RE1 – RVZ1 RCA exhaust radiation detector
RE2 – RVZ2 RCA exhaust radiation detector

RCA Isolation


RE1 or RE2 are greater than 5x background radiation
False
Maintain state of ESFAS outputs
True
Dampers 1 through 26 – closed
Valves 1 through 6 – closed
Breakers 1 and 2 - open
VTS Safety Actuation

7.6 CONTROL CONSOLE AND DISPLAY INSTRUMENTS

The SHINE facility control room contains the necessary workstations, displays, and control cabinets needed for the operation of the SHINE facility. Within the facility control room there is a main control board, two operator workstations, and a supervisor workstation. The operator workstations consist of equipment control display screens and human interface equipment, and the main control board consists of status indication panels, static display screens, and manual actuation interfaces. The supervisor workstation is similar to the other operator workstations, with the exception that the display screens, called equipment display screens, are for monitoring purposes only. The main control board, operator and supervisor workstations, and associated control cabinets are considered part of the process integrated control system (PICS). As part of the PICS, the main control board, operator workstations, and supervisor workstation are not credited with performing safety functions and only assist operators in performance of normal operations or diverse actuations to the safety systems.

7.6.1 DESCRIPTION

7.6.1.1 Main Control Board

The main control board is located on the east wall of the facility control room between the two entrances to the room, as shown in Figure 7.6-1. The main control board sits 25 feet wide along the east wall and contains eight status indication panels, each dedicated to a single irradiation unit (IU), and a ninth status indication panel section dedicated to other processes within the facility. The ninth panel for the facility is located between the fourth and fifth IU panel sections.

The static display screens, which show the variables important to the safety functions of the IU and other facility processes, are located on the upper half of the main control board. The configuration of the status indication panels, including the location of the static display screens, is shown in Figure 7.6-2. The static display screens are used by the operator to verify the status of the SHINE facility. The current mode of operation for each IU is displayed on a static display screen on the associated status indication panel.

Manual actuation interfaces (i.e., physical push buttons and switches), which provide diverse means to actuate automated safety functions, are located in the space directly below the static display screens at each status indication panel, as shown in Figure 7.6-2. In the same area as the manual actuation interfaces, there is an enable nonsafety switch (labeled “E/D” for “Enable/Disable”), which allows operators to enable the PICS ability to manipulate equipment after control had been overwritten by the target solution vessel (TSV) reactivity protection system (TRPS) or the engineered safety features actuation system (ESFAS). Manual actuations are not required to ensure adequate safety of the facility, as described in Chapter 13.

The facility status indication panel also includes the facility master operating permissive (labeled “O/S” for “Operating/Secure”) in the same area as the manual actuation interfaces.

Facility and IU alarms are visually alerted on the main control board above the associated static display screens.

7.6.1.2 Operator Workstation

Two operator workstations are centrally located in the facility control room facing the main control board. Each workstation contains multiple equipment control display screens. One of the display screens is used to display the alarms present in the facility. Configuration of the operator workstations is shown in Figure 7.6-1.

Either workstation can display any of the available PICS display screens for monitoring purposes. Control of the IUs is split between the two workstations, with one workstation normally responsible for control of IUs one through four, and the other workstation normally responsible for control of IUs five through eight. Control of the process systems is split between the two workstations to prevent the two operators from inputting conflicting commands. While control of each UI or process is normally assigned to a particular workstation, control can also be transferred between workstations for operational flexibility. Only one workstation is allowed to input control commands to a particular IU at any time. One of the screens at the operator workstation is designated as monitoring only, so that when an alarm is present, the screen automatically changes the content displayed to the current alarms that are present without interrupting a control process. The remaining screens can be used for control or monitoring as the operator tasks demand.

Modes of operation are advanced by the operator at the operator workstation through the use of the equipment control screens. Even though the operator has the ability to advance the mode of operation at the workstation, maintaining of the current mode of operation is done in the safety-related control systems. If permissive conditions are not met to achieve the next mode of operation, the operator will not be able to move on to the following mode of operation until permissive conditions have been achieved.

7.6.1.3 Supervisor Workstation

The supervisor workstation is located on the west side of the facility control room facing the operator workstations and the main control board. The supervisor workstation is raised from the facility control room floor and contains display screens used for monitoring facility status only. The supervisor workstation allows the supervisor to select and monitor the appropriate screen to the current tasks being supported by the supervisor.

7.6.1.4 Maintenance Workstation

The maintenance workstation receives diagnostic and indication information for the TRPS and the ESFAS. Any module failure or warning is shown at the maintenance workstation and a log of each is maintained there for use. The maintenance workstation is also used to update setpoints within the safety function module in the chassis. This is done through a temporary connection to the monitoring and indication communication module of the associated division, as described in Section 7.2.

The Division A maintenance workstation is located in the Division A TRPS cabinet that houses the TRPS for IUs 7 and 8. Division A of the TRPS is located on the south side of the facility control room. The Division A maintenance workstation can also be used for performing maintenance on Division C cabinets.

The Division B maintenance workstation is located in the Division B TRPS cabinet that houses the TRPS for IUs 7 and 8. Division B of the TRPS is located on the north side of the facility control room. The typical arrangement of the maintenance workstation in a TRPS cabinet is shown in Figure 7.6-3.

7.6.2 DESIGN CRITERIA

The SHINE design criteria applicable to the control console and display instruments are provided in Subsection 7.2.1. The SHINE design criteria are described in Section 3.1.

Additional criteria applicable to these components are as follows:

7.6.2.1 Access Control

PICS Criterion 10 – The operator workstation and main control board design shall incorporate design or administrative controls to prevent or limit unauthorized physical and electronic access to critical digital assets (CDAs) during the operational phase, including the transition from development to operations. CDAs are defined as digital systems and devices that are used to perform or support, among other things, physical security and access control, safety-related functions, and reactivity control.

7.6.2.2 Software Requirements Development

PICS Criterion 11 – A structured process, which is commensurate with the risk associated with its failure or malfunction and the potential for the failures challenging safety systems, shall be used in developing software for the operator workstations and the main control board.

PICS Criterion 12 – The operator workstation and main control board development life cycle phase-specific security requirements shall be commensurate with the risk and magnitude of the harm that would result from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the operator workstation and main control board and display instruments.

PICS Criterion 13 – The operator workstation and main control board software development life cycle process requirements shall be described and documented in appropriate plans which shall address verification and validation (V&V) and configuration control activities.

PICS Criterion 14 – The operator workstation and main control board configuration control program shall assure that the required hardware and software are installed in the appropriate system configuration and ensure that the correct version of the software/firmware is installed in the correct hardware components.

7.6.2.3 General I&C Requirements

PICS Criterion 15 – The main control board shall be functional, accessible within the time constraints of operator responses, and available during operating conditions to confirm safety system status.

PICS Criterion 16 – Loss of power, power surges, power interruption, and any other credible event to the operator workstations shall not result in spurious actuation or stoppage of any system displaying variables important to the safe operation of the safety systems.

PICS Criterion 17 – Displays of variables important to the safe operation of the SHINE facility that the operator shall monitor to keep variables within a limiting value, and those that can affect reactivity of the target solution vessel, shall be readily accessible and understandable to the operator.

7.6.2.4 Independence

PICS Criterion 18 – Operator workstations and the main control board, where associated with both safety and nonsafety functions, shall not impede execution of the safety function.

PICS Criterion 19 – The operator workstations and main control board data that is transmitted to remote displays shall be protected by one-way communication through the use of hardware devices to a processor that is protected by a firewall.

7.6.2.5 Fail Safe

PICS Criterion 20 – The operator workstations and main control board shall be designed to assume a safe state on loss of electrical power or exposure to adverse environments.

PICS Criterion 21 – When required by the safety analysis, the main control board shall have a reliable source of emergency power sufficient to sustain operation of the indications on loss of normal electrical power.

7.6.2.6 Surveillance

PICS Criterion 22 – The operator workstations and main control board shall be readily testable.

7.6.2.7 Human Factors

PICS Criterion 23 – Human factors shall be considered at the initial stages and throughout the operator workstation and main control board design process to ensure that the outputs and display devices showing irradiation unit and process facility status are readily observable by the operator while the operator is positioned at the controls and manual actuation switches.

7.6.2.8 Annunciators

PICS Criterion 24 – Alarms and annunciators shall clearly show the status of the operating systems, interlocks, engineered safety feature initiations, confinement and containment status, radiation fields and concentration, and confinement and containment status.

PICS Criterion 25 – Hardware and software failures shall be assessed in reliability analyses of the annunciators used to support normal and emergency operations.

7.6.2.9 Quality

PICS Criterion 26 – Controls over the design, fabrication, installation, and modification of the operator workstations and main control board shall conform to the guidance of ANSI/ANS 15.8-1995 (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5 (USNRC, 2010).

7.6.3 DESIGN BASIS

7.6.3.1 Display and Control Functions

Each IU-specific status indication panel indicates variables important for verifying proper operation of safety systems following automatic actuation of the TRPS. The facility specific status indication panel indicates variables important for verifying proper operation of safety systems used in other facility systems following automatic actuation of the ESFAS. Each set of static display screens on the status indication panels is used to support an operator in performing manual actuation of a safety function. Manual actuations are performed from the main control board, where the static display screens are visible from the manual actuation push buttons.

The operator workstations have multiple equipment control display screens available to support normal control functions and provide indication of alarms. The equipment control display screens have the capability of providing at least 30 minutes of data trending from instrumentation variables obtained from the ESFAS, TRPS, and those variables associated with identifying a breach of the primary system boundary or determining and assessing the magnitude of radioactive material release to assist operators’ actions. Operator interaction with the equipment control display screens is through a keyboard and mouse interface.

The supervisor workstation provides monitoring only displays so that the supervisor can select and monitor the appropriate screen to the current tasks being supported by the operator.

7.6.3.2 Operating Conditions

The operator workstations and the main control board are designed to operate in the normal environmental conditions of the facility control room, presented in Table 7.2-2. The main control board status indication panels are designed to operate in the transient environmental conditions listed in Table 7.2-2 for a minimum of two hours after initiation of a protective action resulting from a design basis event.

In the event of a loss of ventilation to the facility control room, the environment within the facility control room is calculated to remain below 120ºF after two hours. This result is based on the following assumptions:

- Initial facility control room temperature: 75ºF
- Outdoor air temperature: 102.6ºF
- Facility control room occupancy: 10
- Facility control room equipment load: 29 kW

This is within the temperature indicated in Table 7.2-2 for the required two-hour runtime. Therefore, no safety-related ventilation or cooling systems are required to ensure the safety-related I&C systems located in the control room can continue to perform their safety function as required.

7.6.3.3 Human Factors

The design of the facility control room, display screens, and operator interfaces incorporate human factors principles. The layout of screens presenting the same information on equipment control display screens and static display screens are identical for each operator workstation, supervisor workstation and status indication panel. The displays and controls are grouped by system to aid the operator in the recognition and operation of the controls. Displays that an operator may use to perform a task are placed such that they are visible from the operator workstation, with the displays most frequently used being placed closest to the operator.

The supervisor workstation is placed and arranged so that the supervisor has a visual of both operator workstations, the displays that the operators are working from, and the main control board. Operator workstations are oriented such that the status indication panels associated with the IUs the operator is responsible for are directly ahead of the operator from the operator workstation. The point where the main control board transitions from displays that are associated from one operator to the next is occupied by the facility status indication panel, as both operators are typically responsible for information on the static display screens located there.

The manual actuation push buttons are located directly below the static display screens so that the operator can be directly monitoring the variables important to the safe operation of the facility when the manual actuation is performed. The use of selector switch and push buttons in the same product line ensure consistency in look and function. These push buttons also include a positive position indication and a protective guard to prevent inadvertent actuation.

7.6.4 OPERATIONAL PERFORMANCE OVERVIEW

7.6.4.1 Displays

Displays of information related to the operation of the SHINE facility are available to the operator on the workstations and the main control board. The displays at each of the operator workstations, supervisor workstation, and main control board are digital displays. Displays are programed such that the range of the displayed information includes the expected range of variation of the monitored variable.

Each of the variables listed in Table 7.4-1 and Table 7.5-1 is continuously displayed on the static displays of the main control board. The position indication of actuation components identified in Sections 7.4 and 7.5 are also available on the static display screens.

Variables available to the PICS, including the variables from Table 7.4-1 and Table 7.5-1, are available for display on the various PICS displays on the equipment control displays at the operator workstations and supervisor workstation.

Display of interlock and bypass status is available on each of the PICS displays of the equipment control display screens for the equipment or instrument channel that has been bypassed. Bypassed channels for the safety systems are also visible on the maintenance workstation.

Included in displayed variables at the equipment control displays, the following variables associated with a breach of the primary system boundary are uniquely identified:

- TSV level
- TSV dump tank level

Also included in displayed variables at the equipment control displays, the following variables used in determining and assessing the magnitude of radioactive material release are provided for display on equipment control display screens:

- Stack release monitor
- Carbon delay bed effluent monitor
- Radiological ventilation zone 1 (RVZ1) radiologically control area (RCA) exhaust radiation detectors
- Radiological ventilation zone 2 (RVZ2) RCA exhaust radiation detectors

Radiation monitoring information is conveyed from the radiation monitoring instruments described in Section 7.7 to the PICS and displayed in the facility control room. Radiation monitoring information is available on demand at the operator workstations.

The operator workstation provides detailed visual alarms to the operator to represent unfavorable status of the facility systems. Indications at the operator workstation are provided as visual feedback as well as visual features to indicate that systems are operating properly. An “alarm present” indication is provided for each IU and for the facility process systems on each status indication panel.

Display values on each PICS display screen are automatically updated as more current data becomes available. Each PICS display screen presented on the operator workstation has a title or header and unique identification to distinguish each display page.

The maintenance workstation provides diagnostic information received from the ESFAS and TRPS on system status to be used as a test interface.

Limited function local displays, including radiation monitoring information, are also provided in the irradiation facility (IF) and radioisotope production facility (RPF) at select locations.

7.6.4.2 Controls

Manual controls are provided on both of the operator workstations, via input to the PICS, and on the main control board.

Manual controls for the safety-related protective functions are located at each status indication panel. Nonsafety manual push buttons that provide a diverse actuation to the automatically generated safety actuations are located directly below the static display screens for the respective status indication panel that the manual push button is associated. Where the configuration of the actuation components does not allow for regular control of the PICS during normal operation, or in the event that an automated actuation has occurred, a safety-related enable nonsafety switch is located next to the manual push buttons to provide the operator the ability to control actuation components or to reset the safety-related control systems using the PICS following the actuation of a protective function. The enable nonsafety switch is a three-position return-to-center switch with states for Enable, Disable and the return-to-center operating as-is state. To provide the operators the ability to place the facility into the Facility Secure state, an additional manual key switch is located at the facility status indication panel below the static display screens. The switch has two positions of operation, Secured and Operating.

Controls for normal operation are provided at the operator workstations. Multiple equipment control displays are set up at each operator workstation for operators to select the PICS display screen that coincides with the task that the operator is currently performing. Interface with the equipment control displays is through a keyboard and mouse provided for each operator workstation. Distribution of controls between the two operator workstations will be provided, such that each operator workstation is normally assigned a specific set of IUs for which the PICS displays provide control functions. For the remaining set of IUs, the PICS displays provide monitoring capabilities only. Control screens that are not specific to an IU are similarly assigned to only one operator workstation at a time. The supervisor workstation is provided each of the same PICS displays; however, no control functions are provided at the supervisor workstation. Only providing control capabilities for each IU or facility system or process to a single workstation prevents the operators from entering conflicting commands to a single component or process. On a failure of one operator workstation, control functions assigned to that station can be transferred to the remaining operator workstation.

Manual actuation inputs are connected downstream of the safety-related control system programmable logic functions as described in Subsection 7.2.2.3.

7.6.4.3 Information Retrieval

The variables monitored by each of the safety systems, radiation monitoring systems, and the PICS is recorded into a data historian. The PICS obtains the information that is to be recorded and provides that information to the facility data and communication system (FDCS) where the data historian is located. Through the use of the information provided to the FDCS, off-site monitoring is provided. Information from the FDCS historian is able to be retrieved by operations personnel in the facility control room on demand.

The data historian provides the ability to retrieve at least 12 hours of post-event data logging as prescribed in the interim staff guidance (ISG) document for Chapter 7 of NUREG-1537.

7.6.4.4 Reliability

Local batteries are provided for PICS servers, the operator workstations, and the main control board such that the PICS continues to operate for at least 10 minutes after a loss of external power. The standby generator system (SGS) provides back-up power to the PICS if normal power is interrupted.

Display screens in the facility control room are industrial flat panel displays to ensure compliance with electromagnetic compatibility requirements in an industrial setting.

Transmission of information between systems is through unidirectional data transfers. Each of the safety system communications to the nonsafety PICS system is through one-way data communications from the safety systems to the nonsafety system. There are no unidirectional communications that allow the nonsafety system to communicate back to the safety systems preventing the ability to propagate a failure from the nonsafety control system displays to the safety control systems. The PICS communication to the FDCS is through a one-way data diode such that no communication from outside of the PICS (other than the inputs from the safety-related control systems) can have an impact on the operation of the PICS. Communications of the indication and diagnostic information of the TRPS and ESFAS to the maintenance workstation are through a unidirectional point-to-point communication bus so that the maintenance workstation does not have an effect on the TRPS or ESFAS.

A failure in the display systems results in distinct display changes, which directly indicate that depicted plant conditions are invalid.

The PICS is designed in a manner that allows operators to remove static display screens and equipment control displays from service without impacting the operation of the remaining portions of the PICS displays.

7.6.5 TECHNICAL SPECIFICATIONS

Certain material in this section provide information that is used in the technical specifications. This includes limiting conditions for operation, setpoints, design features, and means for accomplishing surveillances. In addition, significant material is also applicable to, and may be referenced in the bases that are described in the technical specifications.

Figure 7.6-1 – Facility Control Room Layout

Figure 7.6-2 – Status Indication Panels

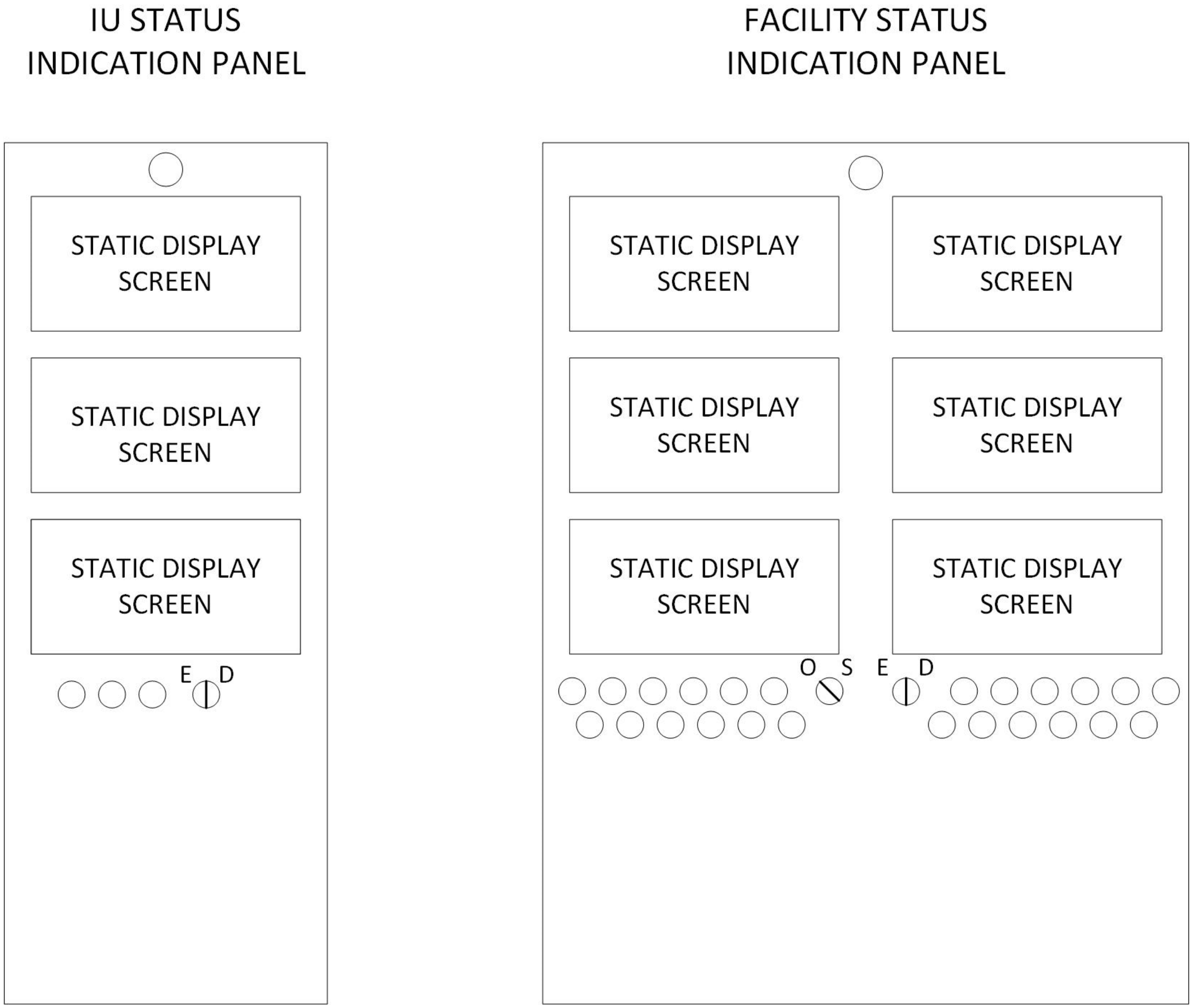
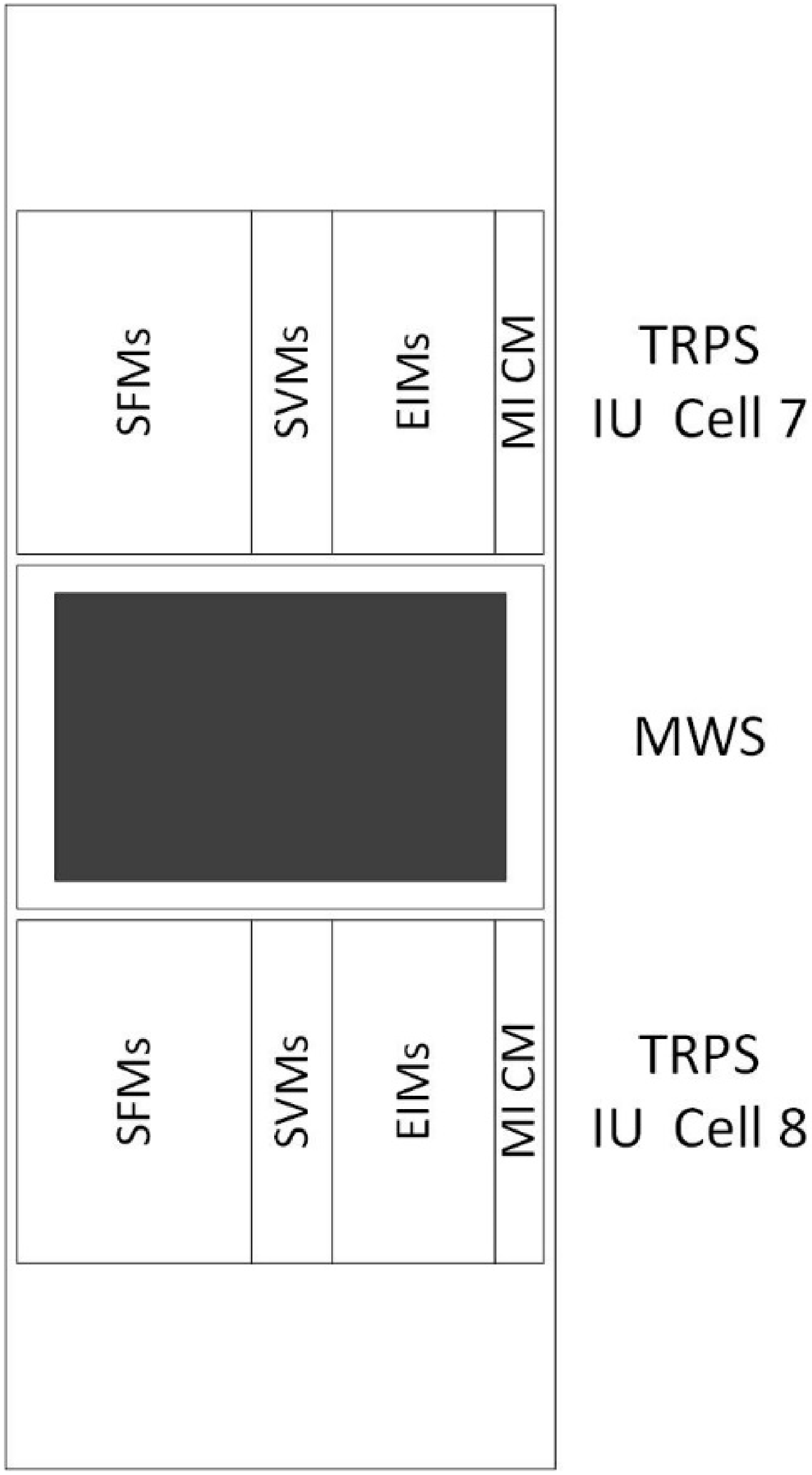


Figure 7.6-3 – Maintenance Workstation



7.7 RADIATION MONITORING SYSTEMS

This section describes systems and components that perform radiation monitoring functions within the SHINE facility. Radiation monitoring systems and components include:

- safety-related process radiation monitors included as part of the engineered safety features actuation system (ESFAS), target solution vessel (TSV) reactivity protection system (TRPS), and tritium purification system (TPS);
- nonsafety-related process radiation monitors included as part of other facility processes;
- area radiation monitoring consisting of the radiation area monitoring system (RAMS);
- continuous air monitoring consisting of the continuous air monitoring system (CAMS);
- effluent monitoring consisting of the stack release monitoring system (SRMS); and
- criticality accident monitoring consisting of the criticality accident alarm system (CAAS).

The objective of the radiation monitoring systems is to:

- provide SHINE facility control room personnel with a continuous record and indication of radiation levels at selected locations within processes and within the facility;
- provide local radiation and criticality safety information and alarms for personnel within the facility;
- provide input to safety-related control systems to actuate safety systems; and
- provide the ability to monitor radioactive releases to the environment.

A diagram showing how the facility radiation monitoring systems relate to the overall facility instrumentation and control (I&C) architecture is provided as Figure 7.1-1.

7.7.1 SAFETY-RELATED PROCESS RADIATION MONITORING

7.7.1.1 System Description

Safety-related process radiation monitors provide input to the safety-related ESFAS or TRPS control systems. These components monitor for either fission products (via beta detection) or tritium. Beta detection radiation monitors are part of the ESFAS or TRPS. The type of safety-related process radiation monitor (fission product or tritium) is selected based on the location and identity of the radioactive material present. The ESFAS and TRPS process radiation monitors (beta detection) are intended to detect abnormal situations within the facility ventilation systems and provide actuation signals to the ESFAS controls. Safety-related tritium monitors are part of the TPS. The TPS monitors are installed within various portions of the TPS to detect potential tritium releases, provide actuation signals to the ESFAS controls, and provide interlock inputs to the TRPS controls. Information from safety-related process radiation monitors is displayed in the facility control room on the operator workstations (via the process integrated control system [PICS]).

A list of safety-related process radiation monitors is provided in Table 7.7-1.

Logic diagrams depicting how the safety-related process radiation monitors provide inputs to ESFAS and TRPS are provided in Figures 7.4-1 and 7.5-1.

7.7.1.2 Design Criteria

The SHINE design criteria are described in Section 3.1. The SHINE design criteria applicable to the safety-related process radiation monitoring are provided in Table 3.1-1

7.7.1.3 Design Bases

The safety functions of the process radiation monitors are: (1) to detect radioactivity in excess of normal levels and provide an actuation signal to the ESFAS or TRPS controls, or (2) to provide input to TRPS for interlocking the operation of the neutron driver. Additional discussion of TRPS and ESFAS functions, interlocks, and bypasses are provided in Sections 7.4 and 7.5.

Each location that requires process radiation monitoring as determined by the safety analysis is equipped with safety-related process radiation monitors. The specified minimum number of process radiation monitors (divisions) are only required to be operable when the location being monitored contains radioactive material, as specified in Table 7.7-1.

Process radiation monitors are selected for compatibility with the normal and postulated accident environmental and radiological conditions.

During normal operation, the process radiation monitors are designed to operate in the normal environmental conditions identified in Table 7.2-2 through 7.2-5 for an expected 20-year lifetime of the equipment. During normal operation, the process radiation monitors will operate in the applicable normal radiation environments identified in Table 7.2-1 for up to 20 years, replaced at a frequency sufficient such that the radiation qualification of the affected components are not exceeded. The monitors are designed to operate in the transient conditions identified in Tables 7.2-1 through 7.2-5 until the associated protective function has continued to completion.

A list of safety-related process radiation monitors, specifying the monitored location, number of sensing divisions provided, and operability requirements, is provided in Table 7.7-1.

The variables to be monitored and their ranges, accuracies, setpoints and response times of safety-related process radiation monitors are provided in Table 7.5-1. Instrument accuracies are appropriate for the associated setpoints. Signal processing time for the ESFAS and TRPS is provided in Subsection 7.2.2.3.

Safety-related radiation monitoring channels produce a full-scale reading when subject to radiation fields higher than the full-scale reading, however, they are expected to remain on-scale during accident conditions. The safety-related process radiation monitors that provide actuation signals are designed to function in the range necessary to detect accident conditions and provide safety-related inputs to the ESFAS and TRPS control systems. For defense-in-depth, the radiologically controlled area (RCA) exhaust, general area direct radiation levels, and general area airborne particulates are monitored by stack release, radiation area, and continuous area monitors, respectively.

7.7.1.4 Design Attributes

Single Failure

At least two process radiation monitors are provided for each protection function input parameter, each providing input to the associated division of the safety-related control system. Redundancy in monitors ensure that a failure of one monitor will not prevent the control system from performing its safety function.

The Division A process radiation monitors receive power from Division A of the uninterruptible power supply system (UPSS), and Division B monitors receive power from UPSS Division B. Division C monitors, when provided, receive auctioneered power from both UPSS Division A and B.

Therefore, no single failure of a detector, control division, or power division will prevent the safety-related control system from performing its safety function.

Independence

Safety-related process radiation monitors provide analog communication to the ESFAS and TRPS controls. Divisional communication independence is maintained by implementing separate hardwired connections to the separate ESFAS or TRPS controls divisions.

Radiation monitoring data provided to nonsafety control systems is through one-way isolated outputs.

Safety-related process radiation monitors from separate divisions are physically separated from each other and independently powered from the associated UPSS division.

Redundancy

Each location that requires engineered safety features to actuate in response to radiation levels, as determined by the safety analysis, is provided with at least two independent safety-related process radiation monitors, designated as Divisions A and B. For locations where spurious actuation of a process radiation monitor could significantly impact overall facility operation, a third sensing division (Division C) is provided.

Human Factors, Display and Recording

Selection and display of process radiation monitor variables are designed with consideration of human factors principles.

See Section 7.6 for additional discussion of information presented to facility operators and recorded for future use.

Quality

Safety-related process radiation monitors are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

The following codes and standards are applied to the design of the safety-related process radiation monitors:

- Institute of Electrical and Electronics Engineers (IEEE) 344-2013, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations (IEEE, 2013), Section 8, for seismic qualification of radiation monitors

7.7.1.5 Operation and Performance

The safety-related process radiation monitors are designed to operate under normal conditions, during anticipated transients, and during design basis accidents such that they will perform their safety function.

Functionality

TRPS process radiation monitors monitor the ventilation line from the primary closed loop cooling system (PCLS) expansion tanks, which are located in each irradiation unit (IU) cell. These monitors provide an actuation signal when radiation levels exceed pre-determined limits, indicative of a release of target solution or fission products within the PCLS or the primary confinement atmosphere (with which the tank communicates). The actuation results in an IU Cell Safety Actuation for that unit.

ESFAS process monitors associated with the supercell monitor the ventilation exhaust from each hot cell and provide an actuation signal when radiation levels exceed pre-determined limits, indicative of a release of target solution or fission products within that hot cell. The actuation results in isolation of the affected hot cell.

ESFAS process monitors associated with the radiological ventilation zone 1 (RVZ1) and radiological ventilation zone 2 (RVZ2) exhaust are designed to provide an actuation signal when radiation levels in the RCA ventilation exhaust systems exceed pre-determined limits, indicative of a failure of a confinement boundary within the facility. The actuation results in isolation of RVZ1, RVZ2, and radiological ventilation zone 3 (RVZ3) ventilation.

The TPS process monitors associated with tritium confinement are designed to provide an actuation signal when tritium concentrations within the TPS gloveboxes exceed predetermined limits, indicative of a failure of TPS process equipment and release of tritium into the TPS glovebox. The actuation results in isolation of the tritium confinement and ventilation associated with the TPS room.

The TPS tritium monitors associated with the TPS exhaust to facility stack are designed to provide an actuation signal when tritium concentrations in the TPS exhaust to facility stack exceed predetermined limits, indicative of a release of tritium out of the TPS. The actuation results in isolation of the TPS process vent exhaust lines and ventilation associated with the TPS room.

Additional discussion of safety-related process radiation monitor functionality is provided in Sections 7.4 and 7.5.

Reliability, Adequacy, and Timeliness

Two safety-related process radiation monitors are provided for each location requiring monitoring. For locations where spurious actuation of the process radiation monitor could significantly impact overall facility operation, a third sensing division (Division C) is provided for two-out-of-three voting capability.

Instrument ranges and response times are provided in Table 7.5-1.

Setpoints, Calibration and Surveillance

Setpoints for safety-related process radiation monitors are selected based on analytical limits and calculated to account for known uncertainties in accordance with the setpoint determination methodology described in Subsection 7.2.3.

Monitors are periodically functionally tested and maintained in accordance with the facility technical specifications to verify operability.

Instrument background count rate is observed to ensure proper functioning of the monitors. Safety-related process radiation monitors located in a low background area are equipped with a check source to be able to verify proper operation.

Safety-related process radiation monitors are calibrated using commercial radionuclide standards that have been standardized using a measurement system traceable to the National Institute of Standards and Technology (NIST).

7.7.1.6 Technical Specifications

Certain material in this section provides information that is used in the technical specifications. This includes limiting conditions for operation, setpoints, design features, and means for accomplishing surveillances. In addition, significant material is also applicable to, and may be referenced by the bases that are described in the technical specifications.

7.7.2 NONSAFETY-RELATED PROCESS RADIATION MONITORING

Nonsafety-related process radiation monitoring is provided as part of various systems to provide information to the operator on the status and effectiveness of processes. They may be used to diagnose process upsets but are not relied upon to prevent or mitigate accidents. Nonsafety-related process radiation monitoring is not used to control personnel or environmental radiological exposures.

7.7.3 AREA RADIATION MONITORING

7.7.3.1 System Description

Area radiation monitoring within the facility is provided by the RAMS. Area radiation monitors are located in areas where personnel may be present and where radiation levels could become significant. The monitors provide local and remote indication of radiation levels and provide local alarms to notify personnel of potentially hazardous conditions. The RAMS provides a nonsafety-related defense-in-depth as low as reasonably achievable (ALARA) function of alerting personnel of the need to evacuate an area if required. Personnel entering radiation areas are provided with personal electronic dosimetry, which serve as the primary means of alerting individuals of the need to evacuate those area if conditions warrant. Additional discussion of radiation protection practices is provided in Chapter 11.

Each RAMS unit consists of a dose rate meter/controller, Geiger Mueller or silicon detector, local radiation level display, audible horn, and an alarm beacon. RAMS unit locations are provided in Table 7.7-2.

The RAMS also provides remote indication of the radiological status of the facility to control room personnel. RAMS information is provided on both the operator workstations (via the PICS) and on a central control terminal located in the control room.

RAMS units are powered from the normal power supply system and provided backup power from the standby generator system (SGS). Electrical power systems are discussed further in Chapter 8.

7.7.3.2 Design Criteria

The SHINE design criteria are described in Section 3.1. The SHINE design criteria applicable to the RAMS are provided in Table 3.1-2.

7.7.3.3 Design Bases

The RAMS functions continuously to alert facility personnel entering or working in low radiation areas of increasing or abnormally high radiation levels which, if unnoticed, could possibly result in inadvertent overexposures. The RAMS also serves to inform the control room operator of the occurrence and approximate location of an abnormal radiation increase in low-radiation areas.

RAMS units are designed to operate in the normal environmental conditions presented in Table 7.2-2.

7.7.3.4 Operation and Performance

The RAMS area radiation monitors are designed to operate under normal facility conditions and to detect radiation that may be indicative of anticipated transients or design basis accidents.

The RAMS includes the area radiation monitoring units located in the main production facility RCA. Each RAMS unit is designed to detect direct radiation from 0.1 mrem/hr up to 10 rem/hr.

Alarm setpoints are set conservatively as required to notify workers to potential hazards or significant changes to radiological conditions in the area.

RAMS units have an accuracy of at least 25 percent of the measured value. Monitors are periodically calibrated using calibration sources that are traceable to factory tests that verified initial calibration and accuracy. The units are calibrated at least annually and as recommended by the instrument manufacturer. Monitors are periodically functionally tested using installed check sources, which simulate a radiation level in the area.

7.7.3.5 Technical Specifications

There are no technical specifications applicable to the RAMS.

7.7.4 CONTINUOUS AIR MONITORING

7.7.4.1 System Description

Continuous airborne contamination monitoring within the facility is provided by the CAMS. Each CAMS unit samples air and provides real time alpha and beta activities or tritium activity to alert personnel when airborne contamination is above preset limits. CAMS units are located in areas where personnel may be present and where contamination levels could become significant. Each CAMS unit provides local and remote indication of airborne radiation levels and alarm capabilities. The CAMS provides a nonsafety-related defense-in-depth ALARA function of alerting personnel of the need to evacuate an area if required. Additional discussion of radiation protection practices is provided in Chapter 11.

Particulate continuous air monitors are alpha-beta air monitors, which are self-contained units equipped with a vacuum pump, particulate filter and a silicon-based detector. Real time tritium air monitors are self-contained units equipped with a vacuum pump and dual ionization chambers. CAMS unit locations are provided in Table 7.7-3.

CAMS units are powered from the normal power supply system and provided backup power from the SGS. Electrical power systems are discussed further in Chapter 8.

7.7.4.2 Design Criteria

The SHINE design criteria are described in Section 3.1. The SHINE design criteria applicable to the CAMS are provided in Table 3.1-2.

7.7.4.3 Design Bases

The CAMS functions continuously to immediately alert facility personnel entering or working in low radiation areas of increasing or abnormally high airborne contamination levels which, if unnoticed, could possibly result in inadvertent overexposures. The CAMS also serves to inform the control room operator of the occurrence and approximate location of an abnormal radiation increase in low-radiation areas.

CAMS units are designed to operate in the normal environmental conditions presented in Table 7.2-2.

7.7.4.4 Operation and Performance

The CAMS airborne contamination monitors are designed to operate under normal facility conditions and to detect radiation that may be indicative of anticipated transients or design basis accidents.

The CAMS includes the continuous airborne contamination monitoring units located in the main production facility RCA. Each particulate CAMS unit has a minimum sensitivity of 1E-12 µCi/cc alpha and 1E-10 µCi/cc beta, with a span of at least six decades of monitoring capability. Each tritium CAMS unit has a minimum sensitivity of 1 μCi/m^3, with a span of at least four decades of monitoring capability.

Alarm setpoints are set conservatively as required to notify workers to potential hazards or significant changes to radiological conditions in the area. Monitors are periodically calibrated using calibration sources that are traceable to factory tests that verified initial calibration and accuracy. The calibration of instrumentation is at least annually and as recommended by the instrument manufacturer. Operation and response tests of instruments are performed consistent with the manufacturer's recommendations and are conducted at a frequency consistent with industry practices.

7.7.4.5 Technical Specifications

There are no technical specifications applicable to the CAMS.

7.7.5 EFFLUENT MONITORING

7.7.5.1 System Description

Effluent monitoring for the facility is provided by the SRMS. The SRMS is composed of two monitoring units: the main facility stack release monitor (SRM), and the carbon delay bed effluent monitor (CDBEM).

The SRM is used to demonstrate that gaseous effluents from the SHINE facility are within regulatory limits and does not have an accident mitigation or personnel protection function. The SRM performs its function by drawing a representative air sample from the stack and providing a means to measure the air sample for noble gases (continuous measurement) and capturing particulates, iodine, and tritium for collective measurement.

The CDBEM monitors for noble gases at the exhaust of the process vessel vent system (PVVS) carbon delay beds to provide information about the health of the PVVS carbon delay beds and to provide the ability to monitor the safety-related exhaust point effluent release pathway when it is in use. The CDBEM is used on an as needed basis to demonstrate that gaseous effluents from the SHINE facility are within regulatory limits (e.g., during a loss of off-site power when the normal heating, ventilation, and air conditioning (HVAC) systems and the PVVS are not operating) and does not have an accident mitigation or personnel protection function. Two particulate and iodine filters (redundant configuration) are provided for in-line capturing and collective measurement when the safety-related exhaust point is in use.

The locations of the SRM and CDBEM within the facility ventilation systems are shown in Figure 7.7-1.

7.7.5.2 Design Criteria

The SHINE design criteria are described in Section 3.1. The SHINE design criteria applicable to the SRMS are provided in Table 3.1-2.

7.7.5.3 Design Bases

The SRMS functions to continuously monitor noble gases that are present in facility effluent streams and to allow for the collection and analysis of particulate, iodine, and tritium.

SRMS units are designed to operate in the normal environmental conditions presented in Table 7.2-3 and the radioisotope production facility (RPF) general area radiological environment presented in Table 7.2-1.

7.7.5.4 Design Attributes

The following standard is applied to the design of the facility effluent monitors:

- ANSI N13.1-1999, Sampling and Monitoring Release of Airborne Radioactive Substances from the Stacks and Ducts of Nuclear Facilities (ANSI, 1999)

7.7.5.5 Operation and Performance

The SRMS units are designed to operate under normal facility conditions and to detect radiation that may be indicative of anticipated transients or design basis accidents.

The SRM is used to monitor the main facility stack, which is the normal release path for gaseous effluents from the PVVS and RCA ventilation systems. A shrouded probe is used in the SRM to withdraw air from the main facility stack flow stream. The probe is designed for high efficiency extraction of aerosols from ventilation stacks, meeting requirements for ANSI N13.1-1999 (ANSI, 1999). The SRM includes a mass flow controller to regulate sample flow rate in the isokinetic region relative to stack flow. A vacuum pump is used to draw sampled air through particulate and iodine filter cartridges, which are removed and analyzed periodically. The sampled air is then drawn into a sample chamber, which houses a beta detector used to measure the noble gas radionuclides. The ratemeter for the beta radiation monitor indicates and displays the radiation level inside the sampler from the sampled air. From the sampler, the air is drawn through the flow controller assembly, pump, and exhausted into the return line. Downstream of the particulate and iodine filter a connection for the tritium detection system is provided. The tritium monitor has its own pump and flow control. The tritium detector is a passive sampler collecting system (i.e., bubble system) to continuously collect and concentrate elemental tritium and tritiated water in small vials. The contents of the vials are assayed using a scintillation counter at regular intervals.

The CDBEM monitors noble gases at the exhaust of the PVVS carbon delay beds using a sampling system. Redundant particulate and iodine filters are installed in-line with the effluent stream, upstream of the safety-related exhaust point, which operates at a much lower flow rate (approximately 16 standard cubic feet per minute) than the main facility stack. The safety-related exhaust point is only used while nitrogen purge is in operation. The PVVS system does not receive gases from process locations expected to contain tritium; therefore, the CDBEM does not include a tritium monitor. See Section 9b.6 for additional discussion on the PVVS and nitrogen purge operations.

The SRM noble gas radiation monitor has a range of 1.0E-06 μCi/cc to 1.0E-01 μCi/cc, with a minimum sensitivity of 3.1E-07 μCi/cc (xenon-133 equivalent). The SRM tritium monitor has a minimum sensitivity of 1.0E-10 μCi/cc.

The CDBEM noble gas radiation monitor has a range of 1.0E-06 µCi/cc to 1.0E+01 µCi/cc.

The initial channel calibration for the SRM and CDBEM noble gas detectors are performed using standards traceable to NIST.

For both the SRM and CDBEM, filter medium collection efficiency is 99 percent for 0.3 micron or larger particles. Halogen isotopes are collected on a filter having a collection efficiency of 95 percent or better for iodine.

7.7.5.6 Technical Specifications

Certain material in this section provide information that is used in the technical specifications. This includes limiting conditions for operation, setpoints, design features, and means for accomplishing surveillances. In addition, significant material is also applicable to, and may be referenced by the bases that are described in the technical specifications.

7.7.6 CRITICALITY MONITORING

7.7.6.1 System Description

Criticality monitoring of the RPF, a sub-division of the main production facility, is provided by the CAAS. CAAS coverage is not provided in the irradiation facility (IF) containing the IUs, since other safety control systems (e.g., TRPS) are actively monitoring and detecting conditions outside normal operational limits.

7.7.6.2 Design Criteria

The SHINE design criteria are described in Section 3.1. The SHINE design criteria applicable to the CAAS are provided in Table 3.1-2.

7.7.6.3 Design Basis, Operation and Performance

The CAAS meets the requirements of 10 CFR 70.24(a) and follows the guidance of ANSI/ANS 8.3-1997 (R2017) (ANSI/ANS, 1997). A detailed description of the CAAS is provided in Subsection 6b.3.3.

7.7.6.4 Technical Specifications

Certain material in this section provide information that is used in the technical specifications. This includes limiting conditions for operation, setpoints, design features, and means for accomplishing surveillances. In addition, significant material is also applicable to, and may be referenced by the bases that are described in the technical specifications.

Table 7.7-1 – Safety-Related Process Radiation Monitors (Sheet 1 of 4)

Unit	Monitored Material	Monitored Location	Unit Location	Function	Total Available Divisions	Minimum Required Divisions	Operability Requirements
1	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from process vessel ventilation cell (input to ESFAS)	3	2	Whenever PVVS, VTS, or N2PS is operating and hot cell isolation dampers are not closed
2	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from extraction cell A (input to ESFAS)	2	2	Whenever target solution or radioisotope products are present in the hot cell and hot cell isolation dampers are not closed
3	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from purification cell A (input to ESFAS)	2	2	Whenever radioisotope products are present in the hot cell and hot cell isolation dampers are not closed
4	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from packaging cell 1 (input to ESFAS)	2	2	
5	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from purification cell B (input to ESFAS)	2	2	
6	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from extraction cell B (input to ESFAS)	2	2	Whenever target solution or radioisotope products are present in the hot cell and hot cell isolation dampers are not closed
7	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from extraction cell C (input to ESFAS)	2	2	Whenever target solution or radioisotope products are present in the hot cell and hot cell isolation dampers are not closed

Table 7.7-1 – Safety-Related Process Radiation Monitors (Sheet 2 of 4)

Unit	Monitored Material	Monitored Location	Unit Location	Function	Total Available Divisions	Minimum Required Divisions	Operability Requirements
8	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from purification cell C (input to ESFAS)	2	2	Whenever radioisotope products are present in the hot cell and hot cell isolation dampers are not closed
9	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from packaging cell 2 (input to ESFAS)	2	2	
10	Fission products	Supercell exhaust ventilation	Supercell exterior	Detect elevated radiation levels from iodine and xenon purification cell (input to ESFAS)	2	2	
11	Fission products	RVZ1 exhaust	Mezzanine (RPF general area)	Detect elevated radiation levels from RVZ1 RCA exhaust (input to ESFAS)	3	2	Whenever facility operations are not secured or RVZ isolation dampers are not closed
12	Fission products	RVZ2 exhaust	Mezzanine (RPF general area)	Detect elevated radiation levels from RVZ2 RCA exhaust (input to ESFAS)	3	2	
13	Tritium	TPS confinement A atmosphere	TPS room	Detect elevated tritium concentration in tritium purification system confinement (input to ESFAS)	2	2	Whenever tritium is present in the TPS confinement in gaseous form
14	Tritium	TPS confinement B atmosphere	TPS room	Detect elevated tritium concentration in tritium purification system confinement (input to ESFAS)	2	2	Whenever tritium is present in the TPS confinement in gaseous form

Table 7.7-1 – Safety-Related Process Radiation Monitors (Sheet 3 of 4)

Unit	Monitored Material	Monitored Location	Unit Location	Function	Total Available Divisions	Minimum Required Divisions	Operability Requirements
15	Tritium	TPS confinement C atmosphere	TPS room	Detect elevated tritium concentration in tritium purification system confinement (input to ESFAS)	2	2	Whenever tritium is present in the TPS confinement in gaseous form
16	Tritium	TPS exhaust	TPS room	Detect elevated tritium concentration in tritium purification system exhaust to RVZ1e (input to ESFAS)	3	2	Whenever tritium is present in the TPS exhaust to RVZ1e in gaseous form and TPS confinement isolation devices are not closed
17	Fission products	IU 1 primary closed loop cooling system (PCLS) expansion tank exhaust	Cooling room	Detect elevated radiation levels from IU 1 PCLS expansion tank exhaust (input to TRPS)	3	2	Modes 1 through 4
18	Fission products	IU 2 PCLS expansion tank exhaust	Cooling room	Detect elevated radiation levels from IU 2 PCLS expansion tank exhaust (input to TRPS)	3	2	Modes 1 through 4
19	Fission products	IU 3 PCLS expansion tank exhaust	Cooling room	Detect elevated radiation levels from IU 3 PCLS expansion tank exhaust (input to TRPS)	3	2	Modes 1 through 4
20	Fission products	IU 4 PCLS expansion tank exhaust	Cooling room	Detect elevated radiation levels from IU 4 PCLS expansion tank exhaust (input to TRPS)	3	2	Modes 1 through 4
21	Fission products	IU 5 PCLS expansion tank exhaust	Cooling room	Detect elevated radiation levels from IU 5 PCLS expansion tank exhaust (input to TRPS)	3	2	Modes 1 through 4

Table 7.7-1 – Safety-Related Process Radiation Monitors (Sheet 4 of 4)

Unit	Monitored Material	Monitored Location	Unit Location	Function	Total Available Divisions	Minimum Required Divisions	Operability Requirements
22	Fission products	IU 6 PCLS expansion tank exhaust	Cooling room	Detect elevated radiation levels from IU 6 PCLS expansion tank exhaust (input to TRPS)	3	2	Modes 1 through 4
23	Fission products	IU 7 PCLS expansion tank exhaust	Cooling room	Detect elevated radiation levels from IU 7 PCLS expansion tank exhaust (input to TRPS)	3	2	Modes 1 through 4
24	Fission products	IU 8 PCLS expansion tank exhaust	Cooling room	Detect elevated radiation levels from IU 8 PCLS expansion tank exhaust (input to TRPS)	3	2	Modes 1 through 4

Table 7.7-2 – Radiation Area Monitor Locations

Unit	Function	Location
Area Monitor 1	Alert supercell operators of high radiation levels	Near supercell, ground floor
Area Monitor 2	Alert personnel of high radiation levels from tank vaults near the north-west RPF emergency exit	North end of RPF tank vaults, ground floor
Area Monitor 3	Alert personnel of high radiation levels from tank vaults near the main RPF exit	South end of RPF tank vaults, ground floor
Area Monitor 4	Alert waste cell operators of high radiation levels	Near waste enclosure, ground floor
Area Monitor 5	Alert personnel of high radiation levels from north off-gas or cooling rooms near the north-east IF emergency exit	North end of main IF corridor, ground floor
Area Monitor 6	Alert personnel of high radiation levels from south off-gas, cooling rooms, and NDAS service cell near the IF overhead doors	South end of main IF corridor, ground floor
Area Monitor 7	Alert personnel of high radiation levels from north IU cells	North end of IU vaults, top of vault elevation
Area Monitor 8	Alert personnel of high radiation levels from south IU cells	South end of IU vaults, top of vault elevation
Area Monitor 9	Alert personnel of high radiation levels from the NDAS service cell	TPS room roof elevation
Area Monitor 10	Alert personnel of high radiation levels from filter banks	Safety-related area, facility mezzanine

Table 7.7-3 – Continuous Airborne Monitor Locations
(Sheet 1 of 2)

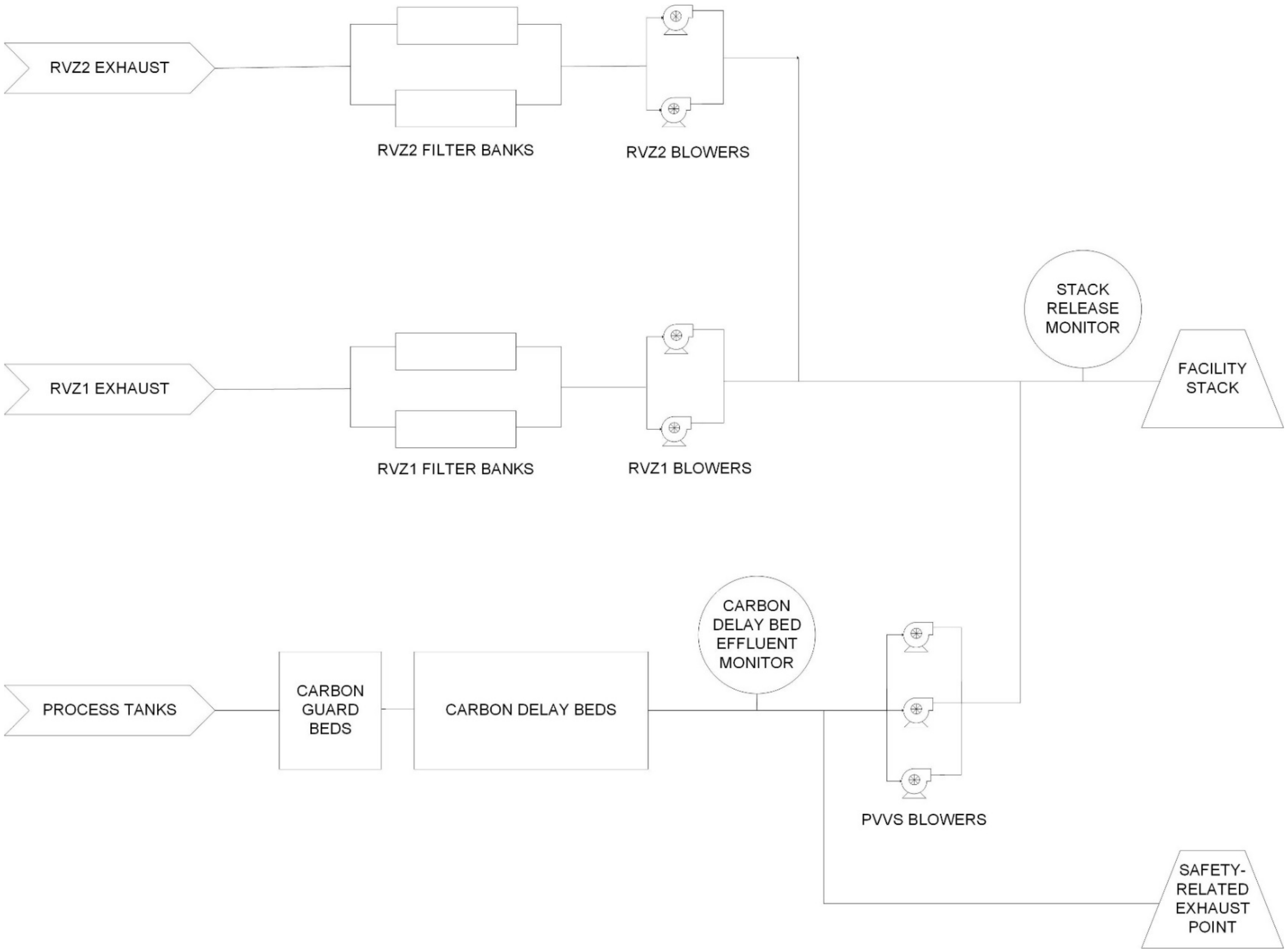
Unit	Function	Location
Airborne Monitor 1	Alert supercell operators of high contamination levels	Near supercell, ground floor
Airborne Monitor 2	Alert personnel of high contamination levels from tank vaults near the north-west RPF emergency exit	North end of RPF tank vaults, ground floor
Airborne Monitor 3	Alert personnel of high contamination levels from tank vaults near the main RPF exit	South end of RPF tank vaults, ground floor
Airborne Monitor 4	Alert waste cell operators of high contamination levels	Near waste enclosure, ground floor
Airborne Monitor 5	Alert personnel of high contamination levels from north off-gas or cooling rooms near the north-east IF emergency exit	North end of main IF corridor, ground floor
Airborne Monitor 6	Alert personnel of high contamination levels from south off-gas or cooling rooms near the IF overhead doors	South end of main IF corridor, ground floor
Tritium Monitor 7	Alert personnel of high tritium levels from north ATIS gloveboxes	North end of IU vaults, top of vault
Tritium Monitor 8	Alert personnel of high radiation levels from south ATIS gloveboxes	South end of IU vaults, top of vault
Airborne Monitor 10	Alert personnel of high contamination levels from filter banks	Safety-related area mezzanine, facility mezzanine
Airborne Monitor 11	Alert laboratory personnel of high contamination levels	North laboratory, ground floor
Airborne Monitor 12	Alert laboratory personnel of high contamination levels	South laboratory, ground floor
Airborne Monitor 13	Alert personnel of high contamination levels from target solution preparation activities	Target solution preparation room, ground floor
Airborne Monitor 14	Alert personnel of high contamination levels from target solution preparation activities	Uranium storage room, ground floor
Tritium Monitor 15	Alert personnel of high tritium levels from the TPS glovebox	TPS room, ground floor

Table 7.7-3 – Continuous Airborne Monitor Locations
(Sheet 2 of 2)

Unit	Function	Location
Tritium Monitor 16	Alert personnel of high tritium levels in the main IF corridor	Main IF corridor, ground floor

NOTE: CAMS unit numbers are not necessarily sequential but correspond to radiation area monitor system (RAMS) unit locations where the two monitors are co-located. See Table 7.7-2 for RAMS locations.

Figure 7.7-1 – Effluent Monitor Locations



7.8 NEUTRON FLUX DETECTION SYSTEM

7.8.1 SYSTEM DESCRIPTION

The neutron flux detection system (NFDS) performs the task of monitoring and indicating the neutron flux to determine the multiplication factor and power level during filling of the target solution vessel (TSV) and irradiating the target solution. The signal from the detectors is transmitted to the pre-amplifiers where the signal is amplified and filtering for noise reduction is performed. The output of the pre-amplifier is transmitted to cabinets in the facility control room (FCR) where the signal processing units are located. The signal processing units perform measurement of the neutron flux signal from the pre-amplifier, signal processing, trip determination, indication and interfacing with other systems. The NFDS interfaces with the TSV reactivity protection system (TRPS) for safety-related interfaces and monitoring and indication, and interfaces with the process integrated control system (PICS) for nonsafety-related functions.

The NFDS monitors variables important to the safety functions of the irradiation process during each operating mode of the irradiation unit (IU) to provide input to the TRPS to perform its safety functions.

The NFDS provides continuous indication of the neutron flux during operation, from filling through maximum power during irradiation. To cover the entire range of neutron flux levels, there are three different ranges provided from the NFDS: source range, wide range, and power range. Source range covers the low levels expected while the TSV is being filled while power range covers the higher flux levels anticipated while the neutron driver is on and irradiating. To cover the gap between the source and power ranges, the wide range monitors the flux levels between the source and power range with a minimum two decade overlap with the high end of the source range and the low end of the power range. In addition to providing flux levels, both the source range and wide range provide rate of change.

The NFDS is a three-division system with three detectors positioned around the subcritical assembly support structure (SASS) at 120-degree intervals to the TSV. Each division of the NFDS consists of a watertight detector located in the light water pool, a pre-amplifier mounted in the radioisotope production facility (RPF), and a signal processing unit inside the FCR. The three watertight detectors located in a light water pool are supported using brackets attached to the outer shell of the SASS. These brackets serve to locate the flux detectors in a fixed location relative to the TSV, ensuring flux profiles are measured consistently such that the sensitivity in the source range reliably indicates the neutron flux levels through the entire range of the filling the target solution.

7.8.2 DESIGN CRITERIA

7.8.2.1 General Instrumentation and Control

NFDS Criterion 1 – The range of operation of detector channels for the NFDS shall be sufficient to cover the expected range of variation of monitored neutron flux during normal and transient operation.

NFDS Criterion 2 – The NFDS shall give continuous indication of the neutron flux from subcritical source multiplication level through licensed maximum power range. The continuous indication shall ensure at least two decades of overlap in indication is maintained while observation is transferred from one channel to another.

NFDS Criterion 3 – The NFDS power range channels shall provide reliable TSV power level while the source range channel provides count rate information from detectors that directly monitor the neutron flux.

NFDS Criterion 4 – The NFDS log power range channel (i.e., wide range channel) and a linear flux monitoring channel (i.e., power range channel) shall accurately sense neutrons during irradiation, even in the presence of intense high gamma radiation.

NFDS Criterion 5 – The NFDS shall provide redundant TSV power level indication through the licensed maximum power range.

NFDS Criterion 6 – The location and sensitivity of at least one NFDS detector in the source range channel, along with the location and emission rate of the subcritical multiplication source, shall be designed to ensure that changes in reactivity will be reliably indicated even with the TSV shut down.

NFDS Criterion 7 – The NFDS shall have at least one detector in the power range channel to provide reliable readings to a predetermined power level above the licensed maximum power level.

NFDS Criterion 8 – The NFDS shall be separated from the PICS to the extent that any removal of a component or channel common to both the NFDS and the PICS preserves the reliability, redundancy, and independence of the NFDS.

NFDS Criterion 9 – The NFDS detectors shall be qualified for continuous submerged operation within the light water pool. The NFDS detector housings shall be watertight and supported by a sleeve structure, mounted to the SASS, at specific locations surrounding the SASS.

NFDS Criterion 10 – The timing of NFDS communications shall be deterministic.

7.8.2.2 Single Failure

NFDS Criterion 11 – The NFDS shall be designed to perform its protective functions after experiencing a single random active failure in nonsafety control systems or in the NFDS, and such failure shall not prevent the NFDS from performing its intended functions or prevent safe shutdown of an IU cell.

NFDS Criterion 12 – The NFDS shall be designed such that no single failure can cause the failure of more than one redundant component.

7.8.2.3 Independence

NFDS Criterion 13 – Physical separation and electrical isolation shall be used to maintain the independence of NFDS circuits and equipment among redundant safety divisions or with nonsafety systems so that the safety functions required during and following any maximum hypothetical accident or postulated accident can be accomplished.

NFDS Criterion 14 – The NFDS shall be designed such that no communication – within a single safety channel, between safety channels, and between safety and nonsafety systems – adversely affects the performance of required safety functions.

7.8.2.4 Fail Safe

NFDS Criterion 15 – The NFDS and associated components shall be designed to assume a safe state on loss of electrical power.

NFDS Criterion 16 – The NFDS shall not be designed to fail or operate in a mode that could prevent the TRPS from performing its intended safety function. The design of the NFDS shall consider:

1) The effect of NFDS on accidents
2) The effects of NFDS failures
3) The effects of NFDS failures caused by accidents.

The failure analyses shall cover hardware and software failures associated with the NFDS.

7.8.2.5 Setpoints

NFDS Criterion 17 – Neutron flux setpoints for an actuation of the NFDS shall be based on a documented analysis methodology that identifies assumptions and accounts for uncertainties, such as environmental allowances and measurement computational errors associated with each element of the instrument channel. The setpoint analysis parameters and assumptions shall be consistent with the safety analysis, system design basis, technical specifications, facility design, and expected maintenance practices.

NFDS Criterion 18 – Adequate margin shall exist between setpoints and safety limits so that the TRPS initiates protective actions before safety limits are exceeded.

NFDS Criterion 19 – The sensitivity of each NFDS sensor channel shall be commensurate with the precision and accuracy to which knowledge of the variable measured is required for the protective function.

7.8.2.6 Equipment Qualification

NFDS Criterion 20 – The effects of electromagnetic interference/radio-frequency interference (EMI/RFI) and power surges on the NFDS shall be adequately addressed.

7.8.2.7 Surveillance

NFDS Criterion 21 – The NFDS shall provide the capability for calibration, inspection, and testing to validate the desired functionality of the NFDS.

NFDS Criterion 22 – Equipment in the NFDS (from the input circuitry to output actuation circuitry) shall be designed to allow testing, calibration, and inspection to ensure operability. If testing is required or can be performed as an option during operation, the NFDS shall retain the capability to accomplish its safety function while under test.

NFDS Criterion 23 – Testing, calibration, and inspections of the NFDS shall be sufficient to confirm that surveillance test and self-test features address failure detection, self-test capabilities, and actions taken upon failure detection.

NFDS Criterion 24 – The design of the NFDS and the justification for test intervals shall be consistent with the surveillance testing intervals as part of the facility technical specifications.

7.8.2.8 Classification and Identification

NFDS Criterion 25 – NFDS equipment shall be distinctively identified to indicate its safety classification and to associate equipment according to divisional or channel assignments.

7.8.2.9 Human Factors

NFDS Criterion 26 – The NFDS shall be designed to provide the information necessary to support annunciation of the channel initiating a protective action to the operator.

7.8.2.10 Quality

NFDS Criterion 27 – Controls over the design, fabrication, installation, and modification of the NFDS shall conform to the guidance of ANSI/ANS 15.8-1995, Quality Assurance Program Requirements for Research Reactors (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5, Quality Assurance Program Requirements for Research and Test Reactors (USNRC, 2010).

NFDS Criterion 28 – The quality of the components and modules in the NFDS shall be commensurate with the importance of the safety function to be performed.

7.8.3 DESIGN BASIS

The NFDS monitors neutron flux levels inside the target solution vessel and provides signals to the TRPS that predetermined limits have been reached or exceeded as well as continuous indication of flux level to assist in the TRPS initiating its safety functions.

7.8.3.1 Monitored Variables

The NFDS measures the flux over three separate ranges, source range, wide range, and power range. The source range measures low flux levels common to what would be expected during the filling cycle prior to irradiation of the target solution. The power range measures high flux levels in the ranges that are expected when the neutron driver is operating and irradiating the target solution. The wide range connects the gap between the source range and the power range with overlap and is usable during both source and power range levels.

In the source range, individual pulses are created as a result of neutron interaction with the detector and are recorded by the NFDS. The range of the source range measurement counts pulses up to 1.0E+05 counts per second (cps). The inverse of the count rate can also be used to estimate the critical fill level using the 1/M methodology.

In the power range, the neutron flux is measured in terms of the design power levels of the TSV. The range of measurement of the power range is indicated as 0 percent to 125 percent.

The wide range measurement monitors the power level in a logarithmic scale over 10 decades from 1E-08 percent up to 250 percent covering the irradiation cycle both during deuterium-deuterium reactions and deuterium-tritium reactions.

The source range neutron flux signal has an accuracy of less than or equal to 2 percent of the full linear scale, with a response time of 30 seconds or less in the range of 1 to 100 cps, and a response time of less than or equal to 200 milliseconds in the range of 100 to 1.0E+05 cps.

The power range neutron flux signal has an accuracy of less than or equal to 1 percent of the full linear scale with a response time of less than or equal to 50 milliseconds.

The wide range neutron flux signal has an accuracy of less than or equal to 1 percent of the full logarithmic scale, with a response time of 30 seconds or less in the range of 1.0E-08 percent to 1.0E-05 percent, and a response time of less than or equal to 200 milliseconds in the range of 1.0E-05 percent to 2.5E+02 percent.

7.8.3.2 Logic Processing Functions

The NFDS performs a trip determination for the source range to support filling of the IU cell. The trip determination is provided to the TRPS of the respective IU as a discrete level signal.

The analytical limit for the high source range trip determination is:

- Increasing at 1.5 times the nominal flux at 95 percent volume of the critical fill height

The NFDS has a maximum response time of 250 milliseconds from the time an input signal exceeds predetermined limits to the time that the NFDS transmits a trip determination.

The NFDS provides the following analog signals to the TRPS in addition to the trip determination outputs:

- NFDS source range
- NFDS source range rate
- NFDS wide range
- NFDS wide range rate
- NFDS power range

The NFDS also provides a “source range missing” and “power range missing” signal to the PICS for use as an alarm to the operator in alerting that the NFDS is not operating properly.

7.8.3.3 Operating Conditions

The NFDS control and logic functions are located inside the FCR where the environment is mild and not exposed to the irradiation process. The preamplifiers are located in the RPF where operating conditions are a mild operating environment. The detectors are located within the IU cell where they are exposed to high radiation levels (approximately 3.44E+05 rad/hour) and are qualified to survive that environment.

The environmental conditions present in areas where NFDS is located are provided in Table 7.2-2 through Table 7.2-4. The facility heating, ventilation, and air conditioning (HVAC) systems are relied upon to maintain the temperature and humidity parameters in these areas. The facility HVAC systems are described in Section 9a2.1.

During normal operation, the NFDS equipment will operate in the applicable normal radiation environments identified in Table 7.2-1 for up to 20 years, and will be replaced at a frequency sufficient such that the radiation qualification of the affected components is not exceeded.

7.8.4 DESIGN ATTRIBUTES

7.8.4.1 General Instrumentation and Control

The NFDS is a fully analog system. Communications from the NFDS to the TRPS and PICS are continuous through isolated outputs. The output isolation devices only allow for the data to be transmitted out of the system so that no failure from an interfacing system can affect the functions of the NFDS.

The NFDS is supplied power from the uninterruptible power supply system (UPSS). The UPSS battery backup supplies power to the NFDS for a minimum of 10 minutes following a loss of off-site power.

7.8.4.2 Single Failure

The NFDS is comprised of three redundant divisions of detectors, preamplifiers, and processing circuits. A single failure of any one of the divisions will not affect the functionality of the other two redundant divisions. Interfacing systems with the NFDS are downstream of the NFDS such that a failure of an interfacing nonsafety system will not impact the NFDS.

7.8.4.3 Independence

The three divisions of the NFDS are physically and electrically independent of each other. Detectors are placed at 120-degree intervals around the SASS and are routed back to the control room where the cabinets are located through physically and electrically separated routes. Each division of the NFDS is capable of monitoring the neutron flux levels in the detector, reading and amplifying the levels in the preamplifier, and processing the measurement readings within each division independently without aid of another NFDS division or external safety or nonsafety system.

7.8.4.4 Fail Safe

The NFDS is designed so that a failure due to loss of power to the NFDS or a removal of an NFDS channel interacts the same with the TRPS as if there was a positive trip determination output to the TRPS. The interaction between NFDS and TRPS is shown in Figure 7.4-1 (Sheet 3).

7.8.4.5 Setpoints

Setpoints in the NFDS are based on a documented methodology that identifies each of the assumptions and accounts for the uncertainties in each instrument channel. The setpoint methodology is further described in Subsection 7.2.3.

7.8.4.6 Equipment Qualification

NFDS rack mounted equipment is installed in a mild operating environment and is designed to meet the environmental conditions described in Subsection 7.8.3.3. Rack mounted TRPS equipment is tested to appropriate standards to show that the effects of EMI/RFI and power surges are adequately addressed. Appropriate grounding of the NFDS is performed in accordance with Section 5.2.1 of Institute of Electrical and Electronics Engineers (IEEE) Standard 1050-2004, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations (IEEE, 2004b).

7.8.4.7 Surveillance

The NFDS supports testing and calibration to ensure operability as required by the technical specifications. The NFDS is designed to allow operators to remove portions of the NFDS from service when not required for operation without impacting NFDS components specific to other IU cells. As an all analog system, the only form of fault detection normally available is the “source range missing” and “power range missing” discrete signals provided to the PICS.

7.8.4.8 Classification and Identification

Each division of the NFDS is uniquely labeled and identified in accordance with SHINE identification and classification procedures.

7.8.4.9 Human Factors

The NFDS provides the following signals to the TRPS to transmit to the PICS for display to the operator:

- Source range neutron flux
- Source range rate
- Wide range neutron flux
- Wide range rate
- Power range neutron flux
- Source range missing signal
- Power range missing signal

Operator display criteria and design are addressed in Section 7.6.

7.8.4.10 Codes and Standards

The following codes and standards are applied to the NFDS design:

1) Section 8 of IEEE Standard 344-2013, IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations (IEEE, 2013); invoked as guidance to meet SHINE Design Criterion 2, Natural phenomena hazards.
2) IEEE Standard 379-2000, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (IEEE, 2000); invoked to meet SHINE Design Criterion 15, Protection system reliability and testability.
3) IEEE Standard 384-2008, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (IEEE, 2008); invoked for separation of safety-related and

nonsafety-related cables and raceways, as described in Subsection 8a2.1.3 and Subsection 8a2.1.5.

4) Section 5.2.1 of IEEE Standard 1050-2004, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations (IEEE, 2004b); invoked as guidance to support electromagnetic compatibility qualification for digital I&C equipment.
5) The guidance of ANSI/ANS 15.8-1995, Quality Assurance Program Requirements for Research Reactors (R2013) (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5, Quality Assurance Program Requirements for Research and Test Reactors (USNRC, 2010), is applied as part of the SHINE Quality Assurance Program for complying with the programmatic requirements of 10 CFR 50.34(b)(6)(ii).

7.9 REFERENCES

ANSI, 1999. Sampling and Monitoring Releases of Airborne Radioactive Substances from the Stacks and Ducts of Nuclear Facilities, ANSI N13.1-1999, American National Standards Institute, 1999.

ANSI/ANS, 1995. Quality Assurance Program Requirements for Research Reactors, ANSI/ANS 15.8-1995 (R2013), American National Standards Institute/American Nuclear Society, 1995.

ANSI/ANS, 1997. Criticality Accident Alarm System, ANSI/ANS 8.3-1997 (R2017), American National Standards Institute/American Nuclear Society, 1997.

IEEE, 2000. IEEE Standard Application of Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE 379-2000, Institute of Electrical and Electronics Engineers, 2000.

IEEE, 2004a. IEEE Standard for Software Verification and Validation, IEEE 1012-2004, Institute of Electrical and Electronics Engineers, 2004.

IEEE, 2004b. IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations, IEEE 1050-2004, Institute of Electrical and Electronics Engineers, 2004.

IEEE, 2004c. IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE 1023-2004, Institute of Electrical and Electronics Engineers, 2004.

IEEE, 2008. IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits, IEEE 384-2008, Institute of Electrical and Electronics Engineers, 2008.

IEEE, 2013. IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations, IEEE 344-2013, Institute of Electrical and Electronics Engineers, 2013.

NuScale, 2017. NuScale Power, LLC Submittal of the Approved Version of NuScale Topical Report TR-1015-18653, “Design of the Highly Integrated Protection System Platform,” Revision 2 (CAC No. RQ6005), NuScale Power, LLC, September 13, 2017 (ML17256A892).

USNRC, 2010. Quality Assurance Program Requirements for Research and Test Reactors, Regulatory Guide 2.5, Revision 1, U.S. Nuclear Regulatory Commission, June 2010.

USNRC, 2011. Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.152, Revision 3, U.S. Nuclear Regulatory Commission, July 2011.