CHAPTER 7

INSTRUMENTATION AND CONTROL SYSTEMS

TABLE OF CONTENTS

CHAPTER 7

INSTRUMENTATION AND CONTROL SYSTEMS

TABLE OF CONTENTS

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
ASAI	application specific action item
BF3	boron trifluoride
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

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
COTS	commercial off-the-shelf
cps	counts per second
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
FCRS	facility chemical reagent system
FDCS	facility data and communications system
FDWS	facility demineralized water system
FHWS	facility heating water system
FNHS	facility nitrogen handling system

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
FPGA	field programmable gate array
FVZ4	facility ventilation zone 4
HIPS	highly integrated protection system
HRS	hardware requirements specification
HSI	human system interfaces
HVAC	heating, ventilation, and air conditioning
HVPS	high voltage power supply
HW-SM	hardwired submodule
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

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
ITS	impurity treatment subsystem
IU	irradiation unit
IXP	iodine and xenon purification
LWPS	light water pol system
μCi	microcurie
M	subcritical multiplication factor
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

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	Definition
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
PLRS	programmable logic requirements specification
PTDA	partial trip determination actuation
PVVS	process vessel vent system
QA	quality assurance
QAPD	quality assurance program description
RAMS	radiation area monitoring system
RCA	radiologically controlled area
RDS	radioactive drain system
RFI	radio-frequency interference
RLWI	radioactive liquid waste immobilization

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
RLWS	radioactive liquid waste storage
RPCS	radioisotope process facility cooling system
RPF	radioisotope production facility
RVZ1	radiological ventilation zone 1
RVZ1e	radiological ventilation zone 1 exhaust subsystem
RVZ1r	radiological ventilation zone 1 recirculating subsystem
RVZ2	radiological ventilation zone 2
RVZ2e	radiological ventilation zone 2 exhaust subsystem
RVZ2r	radiological ventilation zone 2 recirculating subsystem
RVZ2s	radiological ventilation zone 2 supply subsystem
RVZ3	radiological ventilation zone 3
RX	receiver
SASS	subcritical assembly support structure
SBM	scheduling and bypass modules

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
SBVM	scheduling, bypass, and voting 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
TPS	tritium purification system

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Definition**
TRPS	target solution vessel reactivity protection system
TSPS	target solution preparation system
TSSS	target solution storage system
TSV	target solution vessel
TX	transmitter
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) and vendor-provided nonsafety-related control systems
- 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 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 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 provided in the facility control room (FCR) 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 provides control and monitoring of 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.

In addition to the PICS, certain systems contain vendor-provided nonsafety-related control systems which interface with the PICS. These systems consist of the neutron driver assembly system (NDAS) controls, supercell controls, and various auxiliary system controls.

The PICS and other vendor -provided nonsafety-related control systems are 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 uses the HIPS platform as described in Section 2.0 of NuScale Topical Report TR-1015-18653, “Design of Highly Integrated Protection System Platform” (NuScale, 2017). 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. SHINE relies on the prior NRC approval of the HIPS platform described in the HIPS topical report Safety Evaluation Report (SER) (USNRC, 2017) to demonstrate the acceptability of the platform for use in the SHINE facility and to partially demonstrate that the design of the TRPS meets SHINE Design Criteria.

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

- one division of input modules, signal conditioning, and trip determination
- two divisions of input modules, signal conditioning, trip determination, voting and actuation equipment
- two divisions of power distribution panels
- power supplies for sensors and TRPS components
- two nonsafety-related MWSs (shared with the ESFAS)
- 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 main production 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 Section 2.0 of NuScale Topical Report TR-1015-18653, “Design of Highly Integrated Protection System Platform” (NuScale, 2017). 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. SHINE relies on the prior NRC approval of the HIPS platform described in the HIPS topical report Safety Evaluation Report (SER) (USNRC, 2017) to demonstrate the acceptability of the platform for use in the SHINE facility and to partially demonstrate that the design of the ESFAS meets SHINE Design Criteria.

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

- one division of input modules, signal conditioning, and trip determination
- two divisions of input modules, signal conditioning, trip determination, voting and actuation equipment
- two divisions of power distribution panels
- power supplies for sensors and ESFAS components
- two nonsafety-related MWSs (shared with the TRPS)
- 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 platform is a generic digital safety-related I&C platform devoted to the implementation of safety-related applications in nuclear facilities. The platform is a logic-based platform that does not utilize software or microprocessors for operation. It is composed of logic implemented using discrete components and FPGA technology. The platform is described in detail in Section 2.0 of

NuScale Topical Report TR-1015-18653, "Design of the Highly Integrated Protection System Platform" (Nuscale, 2017), and is further described in Subsection 7.4.5.

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. Additional equipment, located between the two operator workstations and usable by either operator, is dedicated to controlling the eight NDAS units located in the IU cells.

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 SHINE 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 actuation and priority logic (APL) output state (i.e., deenergized or energized), and
- the facility operating permissive key, which is used to place the main production 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. SHINE uses human factors engineering principles 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 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 main production facility does not have a normal liquid effluent path from the RCA, and as such no liquid effluent monitoring system is provided.

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 sets of 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. 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.

The NFDS is further described in Section 7.8.

Figure 7.1-1 – Instrumentation and Control System Architecture

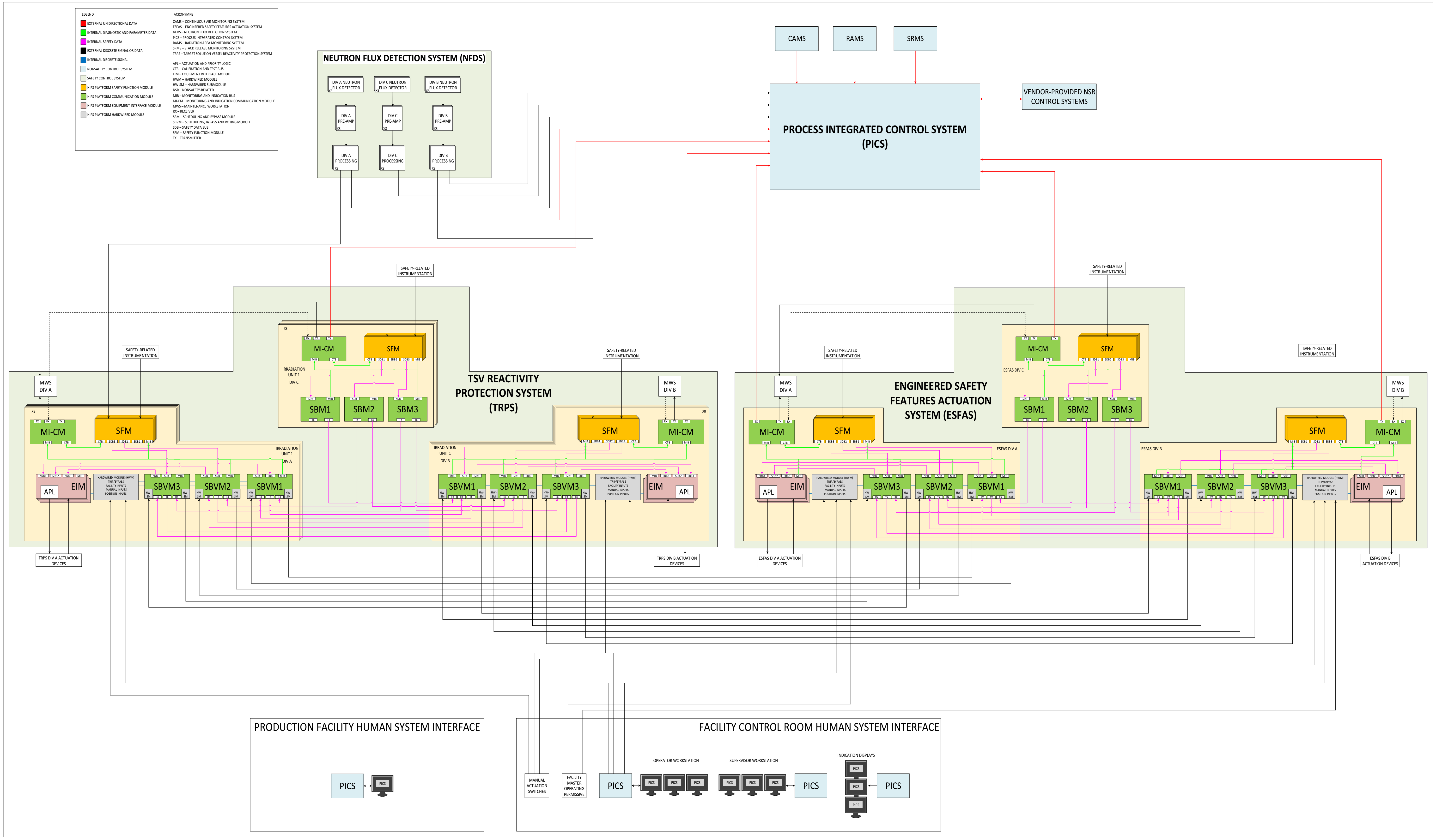

LEGEND
🟥 EXTERNAL UNIDIRECTIONAL DATA
🟩 INTERNAL DIAGNOSTIC AND PARAMETER DATA
🟪 INTERNAL SAFETY DATA
⬛ EXTERNAL DISCRETE SIGNAL OR DATA
🟦 INTERNAL DISCRETE SIGNAL
⬜ NONSAFETY CONTROL SYSTEM
⬜ SAFETY CONTROL SYSTEM
🟨 HIPS PLATFORM SAFETY FUNCTION MODULE
🟩 HIPS PLATFORM COMMUNICATION MODULE
🟫 HIPS PLATFORM EQUIPMENT INTERFACE MODULE
⬜ HIPS PLATFORM HARDWIRED MODULE
ACRONYMNS
CAMS – CONTINUOUS AIR MONITORING SYSTEM
ESFAS – ENGINEERED SAFETY FEATURES ACTUATION SYSTEM
NFDS – NEUTRON FLUX DETECTION SYSTEM
PICS – PROCESS INTEGRATED CONTROL SYSTEM
RAMS – RADIATION AREA MONITORING SYSTEM
SRMS – STACK RELEASE MONITORING SYSTEM
TRPS – TARGET SOLUTION VESSEL REACTIVITY PROTECTION SYSTEM
APL – ACTUATION AND PRIORITY LOGIC
CTB – CALIBRATION AND TEST BUS
EIM – EQUIPMENT INTERFACE MODULE
HWM – HARDWIRED MODULE
HW-SM – HARDWIRED SUBMODULE
NSR – NONSAFETY-RELATED
MIB – MONITORING AND INDICATION BUS
MI-CM – MONITORING AND INDICATION COMMUNICATION MODULE
MWS – MAINTENANCE WORKSTATION
RX – RECEIVER
SBM – SCHEDULING AND BYPASS MODULE
SBVM – SCHEDULING, BYPASS AND VOTING MODULE
SDB – SAFETY DATA BUS
SFM – SAFETY FUNCTION MODULE
TX – TRANSMITTER
NEUTRON FLUX DETECTION SYSTEM (NFDS)
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
X8
CAMS
RAMS
SRMS
PROCESS INTEGRATED CONTROL SYSTEM (PICS)
VENDOR-PROVIDED NSR CONTROL SYSTEMS
SAFETY-RELATED INSTRUMENTATION
TSV REACTIVITY PROTECTION SYSTEM (TRPS)
IRRADIATION UNIT 1 DIV C
IRRADIATION UNIT 1 DIV A
IRRADIATION UNIT 1 DIV B
MWS DIV A
MWS DIV B
MI-CM
SFM
SBM1
SBM2
SBM3
SBVM1
SBVM2
SBVM3
EIM
APL
HARDWIRED MODULE (HWM) TRIP/BYPASS FACILITY INPUTS MANUAL INPUTS POSITION INPUTS
RX
TX
MIB
CTB
SDB1
SDB2
SDB3
HW-SM
TRPS DIV A ACTUATION DEVICES
TRPS DIV B ACTUATION DEVICES
ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (ESFAS)
ESFAS DIV C
ESFAS DIV A
ESFAS DIV B
ESFAS DIV A ACTUATION DEVICES
ESFAS DIV B ACTUATION DEVICES
PRODUCTION FACILITY HUMAN SYSTEM INTERFACE
PICS
FACILITY CONTROL ROOM HUMAN SYSTEM INTERFACE
MANUAL ACTUATION SWITCHES
FACILITY MASTER OPERATING PERMISSIVE
OPERATOR WORKSTATION
SUPERVISOR WORKSTATION
INDICATION DISPLAYS

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

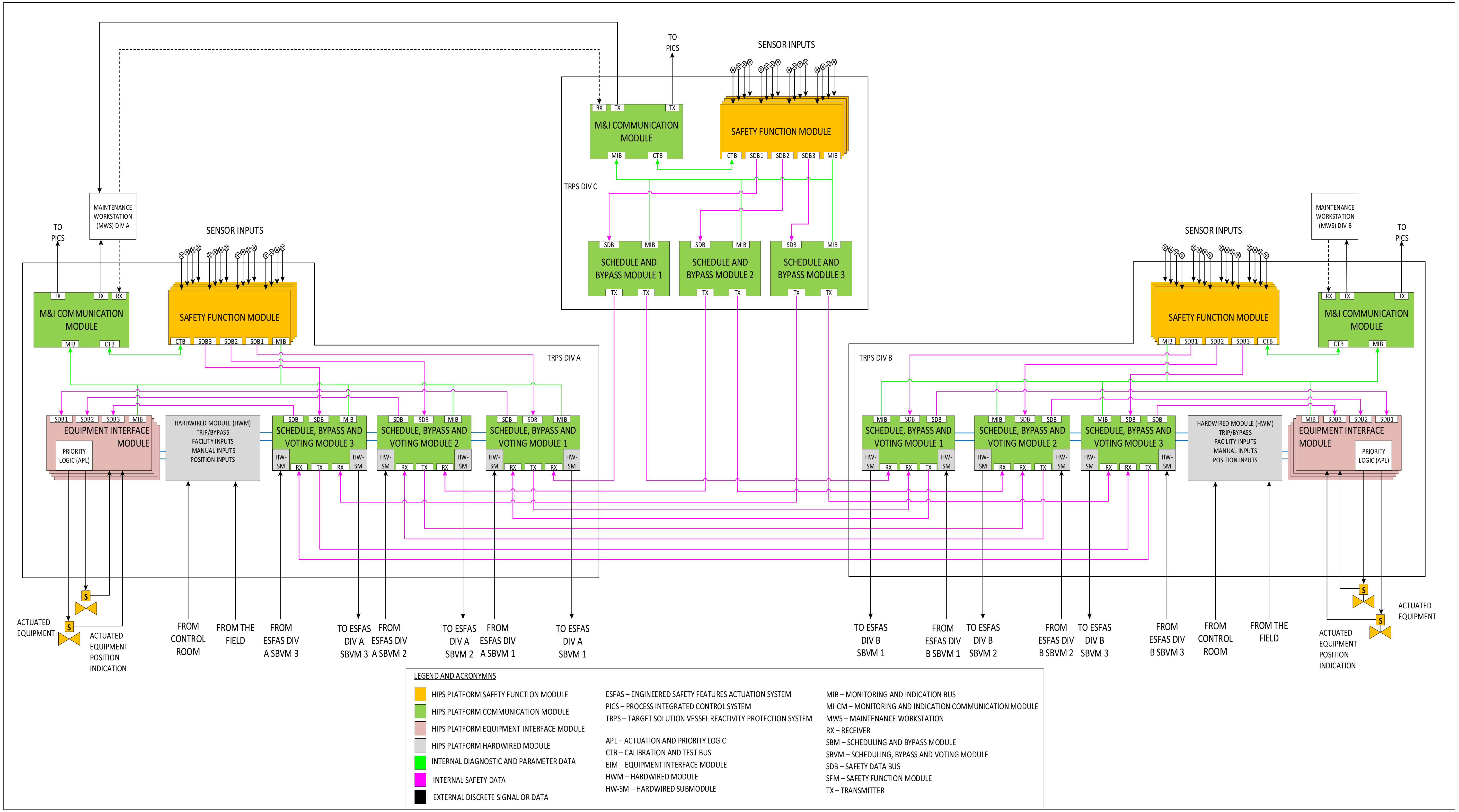
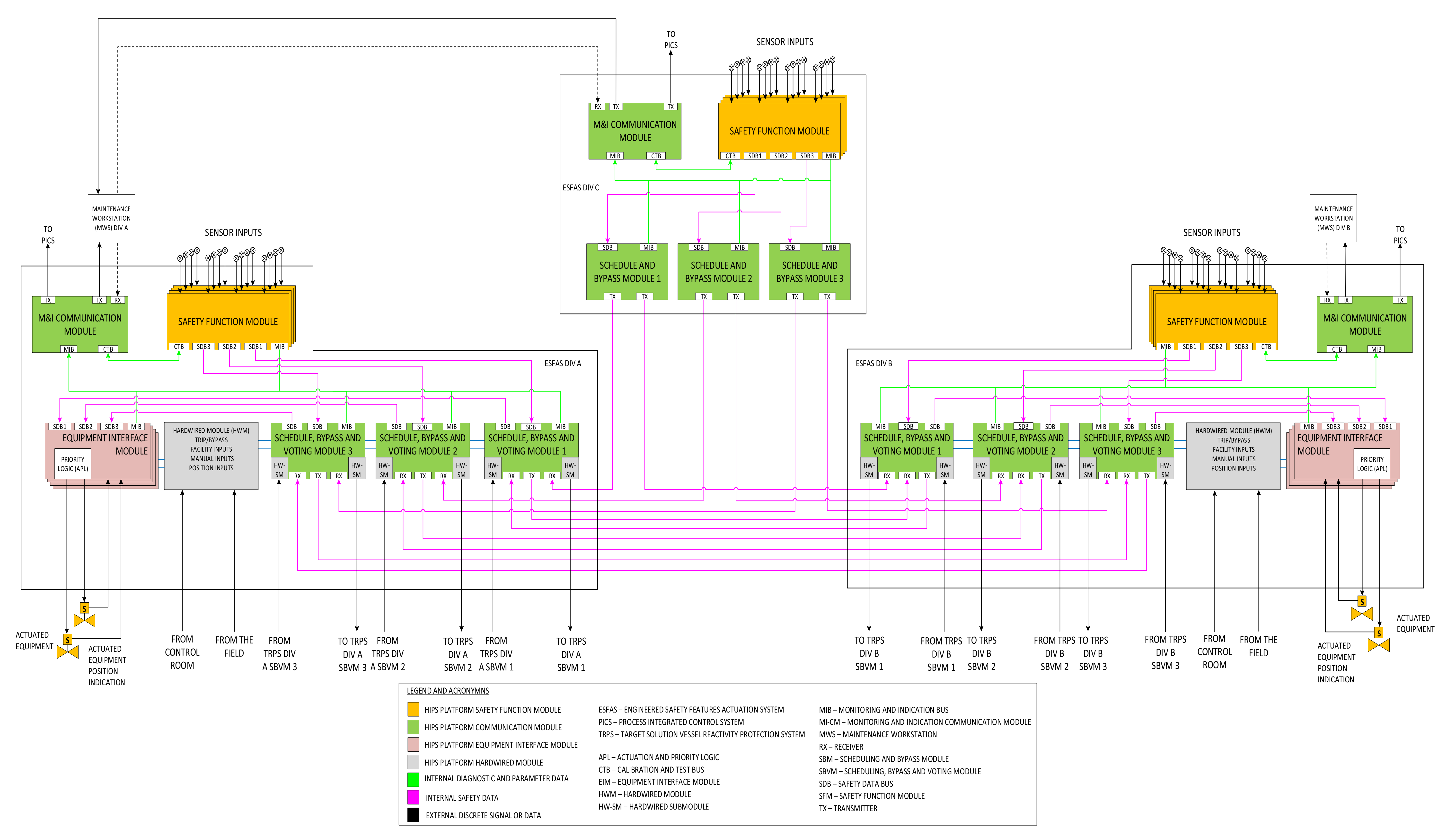

TO PICS
SENSOR INPUTS
RX TX TX
M&I COMMUNICATION MODULE
MIB CTB
SAFETY FUNCTION MODULE
CTB SDB1 SDB2 SDB3 MIB
TRPS DIV C
SDB MIB
SCHEDULE AND BYPASS MODULE 1
SCHEDULE AND BYPASS MODULE 2
SCHEDULE AND BYPASS MODULE 3
TX TX
MAINTENANCE WORKSTATION (MWS) DIV A
MAINTENANCE WORKSTATION (MWS) DIV B
TRPS DIV A
TRPS DIV B
EQUIPMENT INTERFACE MODULE
PRIORITY LOGIC (APL)
HARDWIRED MODULE (HWM) TRIP/BYPASS FACILITY INPUTS MANUAL INPUTS POSITION INPUTS
SCHEDULE, BYPASS AND VOTING MODULE 1
SCHEDULE, BYPASS AND VOTING MODULE 2
SCHEDULE, BYPASS AND VOTING MODULE 3
HW-SM RX TX RX HW-SM
S
ACTUATED EQUIPMENT
ACTUATED EQUIPMENT POSITION INDICATION
FROM CONTROL ROOM
FROM THE FIELD
FROM ESFAS DIV A SBVM 3
TO ESFAS DIV A SBVM 3
FROM ESFAS DIV A SBVM 2
TO ESFAS DIV A SBVM 2
FROM ESFAS DIV A SBVM 1
TO ESFAS DIV A SBVM 1
TO ESFAS DIV B SBVM 1
FROM ESFAS DIV B SBVM 1
TO ESFAS DIV B SBVM 2
FROM ESFAS DIV B SBVM 2
TO ESFAS DIV B SBVM 3
FROM ESFAS DIV B SBVM 3
LEGEND AND ACRONYMNS
🟨 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
ESFAS – ENGINEERED SAFETY FEATURES ACTUATION SYSTEM
PICS – PROCESS INTEGRATED CONTROL SYSTEM
TRPS – TARGET SOLUTION VESSEL REACTIVITY PROTECTION SYSTEM
APL – ACTUATION AND PRIORITY LOGIC
CTB – CALIBRATION AND TEST BUS
EIM – EQUIPMENT INTERFACE MODULE
HWM – HARDWIRED MODULE
HW-SM – HARDWIRED SUBMODULE
MIB – MONITORING AND INDICATION BUS
MI-CM – MONITORING AND INDICATION COMMUNICATION MODULE
MWS – MAINTENANCE WORKSTATION
RX – RECEIVER
SBM – SCHEDULING AND BYPASS MODULE
SBVM – SCHEDULING, BYPASS AND VOTING MODULE
SDB – SAFETY DATA BUS
SFM – SAFETY FUNCTION MODULE
TX – TRANSMITTER

Figure 7.1-3 – Engineered Safety Feature Actuation System Architecture


TO PICS
SENSOR INPUTS
M&I COMMUNICATION MODULE
SAFETY FUNCTION MODULE
ESFAS DIV C
SCHEDULE AND BYPASS MODULE 1
SCHEDULE AND BYPASS MODULE 2
SCHEDULE AND BYPASS MODULE 3
MAINTENANCE WORKSTATION (MWS) DIV A
MAINTENANCE WORKSTATION (MWS) DIV B
ESFAS DIV A
ESFAS DIV B
EQUIPMENT INTERFACE MODULE
PRIORITY LOGIC (APL)
HARDWIRED MODULE (HWM) TRIP/BYPASS FACILITY INPUTS MANUAL INPUTS POSITION INPUTS
SCHEDULE, BYPASS AND VOTING MODULE 1
SCHEDULE, BYPASS AND VOTING MODULE 2
SCHEDULE, BYPASS AND VOTING MODULE 3
HW-SM
RX
TX
SDB
SDB1
SDB2
SDB3
MIB
CTB
ACTUATED EQUIPMENT
ACTUATED EQUIPMENT POSITION INDICATION
FROM CONTROL ROOM
FROM THE FIELD
FROM TRPS DIV A SBVM 3
TO TRPS DIV A SBVM 3
FROM TRPS DIV A SBVM 2
TO TRPS DIV A SBVM 2
FROM TRPS DIV A SBVM 1
TO TRPS DIV A SBVM 1
TO TRPS DIV B SBVM 1
FROM TRPS DIV B SBVM 1
TO TRPS DIV B SBVM 2
FROM TRPS DIV B SBVM 2
TO TRPS DIV B SBVM 3
FROM TRPS DIV B SBVM 3
LEGEND AND ACRONYMNS
🟧 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
ESFAS – ENGINEERED SAFETY FEATURES ACTUATION SYSTEM
PICS – PROCESS INTEGRATED CONTROL SYSTEM
TRPS – TARGET SOLUTION VESSEL REACTIVITY PROTECTION SYSTEM
APL – ACTUATION AND PRIORITY LOGIC
CTB – CALIBRATION AND TEST BUS
EIM – EQUIPMENT INTERFACE MODULE
HWM – HARDWIRED MODULE
HW-SM – HARDWIRED SUBMODULE
MIB – MONITORING AND INDICATION BUS
MI-CM – MONITORING AND INDICATION COMMUNICATION MODULE
MWS – MAINTENANCE WORKSTATION
RX – RECEIVER
SBM – SCHEDULING AND BYPASS MODULE
SBVM – SCHEDULING, BYPASS AND VOTING MODULE
SDB – SAFETY DATA BUS
SFM – SAFETY FUNCTION MODULE
TX – TRANSMITTER

7.2 DESIGN OF INSTRUMENTATION AND CONTROL SYSTEMS

7.2.1 SYSTEM DESCRIPTION

The SHINE facility instrumentation and control systems are described in Section 7.1 and are more fully described in Chapter 7.

The SHINE safety-related instrumentation and control systems are:

- the target solution vessel (TSV) reactivity protection system (TRPS) (Section 7.4)
- the engineered safety feature actuation system (ESFAS) (Section 7.5)
- the neutron flux detection system (NFDS) (Section 7.8)
- safety-related process radiation monitors associated with the TRPS, ESFAS and tritium purification system (TPS) (Section 7.7)

The SHINE nonsafety-related instrumentation and control systems are:

- the process integrated control system (PICS) and vendor-provided controls (Section 7.3)
- facility control room (FCR) control consoles and displays (Section 7.6)
- nonsafety-related radiation monitors (Section 7.7)

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. Instrument drift between calibrations is accounted for in the setpoint methodology. 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.

7.2.2 DESIGN CRITERIA

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 guidance provided in Chapter 7 of NUREG-1537, Part 1 and the Final Interim Staff Guidance (ISG) Augmenting NUREG-1537, Part 1. The criteria were applied in a graded approach to each I&C system.

The SHINE facility design criteria are described in Section 3.1. Table 3.1-1 and Table 3.1-2 show how the facility design criteria are applied to each I&C system. System-specific design criteria are provided in Sections 7.3 through 7.8. Sections 7.3 through 7.8 additionally describe how the facility design criteria and system-specific design criteria are met or implemented for each I&C system.

Codes and standards used in the design of each I&C system are also identified in Sections 7.3 through 7.8.

7.2.3 DESIGN BASES

The design bases requirements identified for each I&C system in Sections 7.3 through 7.8 are established for safe facility operation and to prevent or mitigate the process hazards and potential accident sequences identified in the accident analysis described in FSAR Chapter 13. The I&C design meets established design criteria to ensure safety functions are performed consistently and completely to fulfill the safety intent.

Safety functions, applicable modes of operation, 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 applicable to 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.

7.2.4 OPERATION AND PERFORMANCE

Operation and performance are addressed for each instrumentation and control system in Sections 7.3 through 7.8. The operation and performance analysis describes how the system design criteria and design bases are met for performance of the system design functions. The discussions include, but are not limited to, descriptions of instrumentation and control system actions, setpoints, and how a single failure affects the ability of the system to perform the safety functions.

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)

7.3 PROCESS INTEGRATED CONTROL SYSTEM

The SHINE facility is provided with nonsafety-related control systems necessary to perform normal operational activities within the facility. The process integrated control system (PICS) is a nonsafety-related digital control system that performs various functions throughout the SHINE facility. The PICS is the primary interface for operators to perform tasks in both the irradiation facility (IF) and the radioisotope production facility (RPF). PICS functions include signal conditioning, system controls, interlocks, and monitoring of the process variables and system status.

Vendor-provided nonsafety-related control systems, which interface and communicate with the PICS, are also present within the SHINE facility and are used to monitor and control specific facility systems.

The main control board and operator workstations in the facility control room are also part of the PICS and are described in Section 7.6.

7.3.1 SYSTEM DESCRIPTION

The PICS is a collection of instrumentation and control equipment located throughout the facility to support monitoring, indication, and control of various systems. 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. An architecture of the PICS is provided in Figure 7.3-1.

The following vendor-provided nonsafety-related control systems are also provided for the SHINE facility:

- The building automation system is a digital control system capable of integrating multiple building functions, including equipment supervision and control, alarm management, energy management, and trend data collection. It provides control for the facility heating water system (FHWS), the facility chilled water system (FCHS), the process chilled water system (PCHS), the radioisotope process facility cooling system (RPCS), facility ventilation zone 4 (FVZ4) air handling, and radiological ventilation zone 1, 2, and 3 (RVZ1/2/3) air handling. The building automation system receives commands from the PICS to start and stop select control sequences and provides information to the PICS for monitoring.
- The supercell contains a local control system and human system interface equipment for controlling hot cell functions including interior lighting, interior temperature and pressure, and operation of the doors, ports, and waste export system. The supercell control system provides information to PICS for monitoring only.
- The radioactive liquid waste immobilization (RLWI) system contains a local control system and human system interface equipment for controlling RLWI equipment functions including lighting inside the RLWI enclosure, interior temperature and pressure, operation of the doors and other access ports, and operation of equipment used to handle solidified waste. The RLWI control system provides information to PICS for monitoring only.
- The neutron driver assembly system (NDAS) control system is used to monitor and make adjustments to any of the eight neutron drivers in the eight irradiation unit (IU) cells. Two NDAS control stations are provided in the facility control room as described in Subsection 7.6.1.2, and a portable local station is provided as described in

Subsection 7.6.1.6. The NDAS control system is further described in Subsection 4a2.3.4. The NDAS control system receives permissive signals from the PICS to allow or disable use of the system and provides information to PICS for monitoring.

- The standby generator system (SGS) generator, facility demineralized water system (FDWS) reverse osmosis (RO) unit, facility nitrogen handling system (FNHS) unit, FHWS boilers, and FCHS and PCHS chillers are each provided with integral controllers that interface with the PICS (for the SGS generator, FDWS RO unit, and FNHS unit) or the building automation system (for boilers and chillers).

A description of the PICS process monitoring functions, control functions, interlocks, alarms, and displays is provided for each facility system where the PICS provides these functions. If applicable, the vendor-provided nonsafety-related controls are also described for each facility system. In addition to the variables described below, PICS monitors valve or damper position feedback as needed to perform control functions or implement interlocks and permissives.

7.3.1.1 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 target solution vessel (TSV)

Mode 2 – Irradiation: Operating mode (neutron driver active)

Mode 3 – Post-Irradiation: TSV dump valves open

Mode 4 – Transfer to the RPF: Dump tank drain valve opens to permit solution transfer

The systems associated with SCAS modes of operation include the SCAS itself, the 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 IU 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 tritium purification system (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 the TSV reactivity protection system (TRPS), the PICS is used to open the TSV fill valves and operate the vacuum transfer system (VTS) to add target solution to the TSV from the associated target solution hold tank.

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 provides 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 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.

7.3.1.1.1 Subcritical Assembly System

The SCAS maintains fissile material in a subcritical, but highly multiplying configuration during the irradiation process to produce molybdenum-99 (Mo-99) and other fission products. The SCAS is described in Section 4a2.2.

Monitoring and Alarms

The PICS is used to monitor and provide alarms for TSV level, TSV temperature, and TSV headspace pressure for each IU. TSV dump tank level is monitored using two level switches (low-high and high-high), which are provided to PICS via TRPS (Subsections 7.4.4.1.8 and 7.4.4.1.9).

PICS also provides alarms for automatic or manual actuation of the TRPS safety functions described in Subsection 7.4.3.1 and the TRPS Fill Stop described in Subsection 7.4.4.1.18.

Control Functions

The operator is able to use the PICS to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by TRPS are controlled by PICS as described in Subsection 7.3.1.3.11.

The PICS provides a signal to the TRPS, when manually initiated by the operator, to sequentially transition the TRPS from one mode to the next.

When a TSV fill sequence is manually initiated, the PICS opens and closes the TSV lift tank vacuum valve and the TSV fill valves according to a programmed sequence to add a manually entered prescribed volume to the TSV. The PICS uses feedback from the TSV fill lift tank level switches and valve position indication to accomplish this sequence. At or above 40 percent of the maximum 95 percent fill neutron flux, the time the TSV fill valve is open is limited to less than [ ]$^{PROP/ECI}$ to prevent reliance on the TRPS Fill Stop function (Subsection 7.4.4.1.18).

The TSV fill lift sequence can be manually aborted by the operator.

When a TSV drain sequence is manually initiated and the operator manually enters a solution hold time, the PICS provides a signal to the TRPS to transition to Mode 3, opens the TSV dump valves, verifies the TSV lift tank vacuum valve is closed, and opens the TSV fill valves to drain any target solution remaining in the fill lines to the TSV dump tank via the TSV. When TSV level indicates the TSV is drained, the PICS closes the TSV fill valves and starts a timer for the previously entered solution hold time.

The solution hold time portion of the TSV drain sequence can be manually aborted by the operator.

Interlocks and Permissives

The PICS provides an interlock at or above 40 percent of the maximum 95 percent fill neutron flux to limit the fill rate of the TSV.

The PICS additionally provides permissives and interlocks to:

- Prevent the NDAS high voltage power supply (HVPS) from being energized if any of the TSV fill valves, TSV dump valves, TSV dump tank drain valve, or nitrogen purge system (N2PS) inerting gas isolation valves are open.
- Prevent the TSV fill valves from opening in Mode 1 if the median value of the three values of TOGS mainstream flow inputs for both TOGS trains is below the allowable value.
- Prevent the TSV fill valves from opening in Mode 1 if either TSV dump valve is open.
- Prevent the TSV dump tank drain valve from opening until the solution hold time has elapsed.

- Allow transition from Mode 0 to Mode 1 only when both TSV dump valves are closed, both TSV fill valves are closed, and TSV level is below an allowable level, indicating solution is not present.
- Allow transition from Mode 1 to Mode 2 only when both TSV dump valves are closed, both TSV fill valves are closed, and TSV level is above an allowable level, indicating the TSV contains sufficient solution for irradiation.
- Allow transition from Mode 3 to Mode 4 only when TSV level is below an allowable level indicating solution has been drained, and the TSV dump tank low-high level signal is present indicating solution is in the TSV dump tank.
- Allow transition from Mode 4 to Mode 0 only when TSV level is below an allowable level indicating solution has been drained, the TSV dump tank low-high level signal is clear indicating solution has been removed from the TSV dump tank, and the TSV fill valves are closed.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.1.2 Target Solution Vessel Off-Gas System

The TOGS is used to manage radiolysis and fission product gases generated in the TSV during irradiation operation and present in the TSV dump tank during target solution cooldown to maintain concentrations within safe limits. The TOGS is described in Section 4a2.8.

Monitoring and Alarms

The PICS receives input from the TRPS and provides alarms for TOGS oxygen concentration (Subsection 7.4.4.1.10), mainstream flow for both train A and B (Subsection 7.4.4.1.11), condenser demister outlet temperatures for both train A and B (Subsection 7.4.4.1.13), and dump tank flow for train A (Subsection 7.4.4.1.12).

The PICS directly monitors and provides alarms for TOGS hydrogen concentration, gas injection flowrate, TOGS blower outlet and sidestream pressures, instrument demister condensate high level switch and condenser demister outlet, sweep gas supply, recombiner inlet, recombiner outlet, zeolite bed inlet, and zeolite bed outlet temperatures.

Control Functions

The operator is able to use the PICS to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by TRPS are controlled by PICS as described in Subsection 7.3.1.3.11.

The following functions are performed while TOGS is running (Mode 1, 2, 3, or 4):

PICS automatically controls mainstream flow for each TOGS train based on the median value of the three mainstream flow inputs received from TRPS by adjusting the variable speed motor of the associated train TOGS blower.

PICS automatically controls the temperature of the recombiners (trains A and B) and the zeolite bed (train A) by energizing or deenergizing the associated heater based on the inlet and outlet temperature of each component.

PICS automatically opens the TOGS oxygen inlet valve when oxygen concentration is low, based on the median value of the three TOGS oxygen concentration inputs received from TRPS.

If TSV headspace pressure (Subsection 7.3.1.1.1) increases above the allowable setpoint, PICS opens the TOGS vacuum tank inlet valve. If TSV headspace pressure is too high while TOGS oxygen concentration is low, PICS closes the TOGS oxygen inlet valve prior to opening the TOGS vacuum tank inlet valve. If TSV headspace pressure is too low, PICS opens the TOGS nitrogen inlet valve.

PICS automatically controls the position of the TOGS gas inlet flow control valve to maintain a constant gas injection flowrate when either the TOGS oxygen or nitrogen inlet valve is open.

The following functions are performed while TOGS is not running (Mode 0):

When manually initiated by the operator, the PICS executes a programmed sequence to evacuate the TOGS vacuum tank by opening and closing the TOGS vacuum tank inlet valve, opening and closing the TOGS vacuum tank outlet valve, and opening and closing the vacuum supply valves in a specific order.

When manually initiated by the operator, the PICS executes a programmed sequence to start the TOGS by ensuring TOGS valves are in their required states, enabling the TOGS control loops, and starting the TOGS blowers. This sequence places the TOGS in a Running state.

Interlocks and Permissives

PICS provides interlocks and permissives to:

- Prevent the TOGS vacuum tank inlet valve and TOGS vacuum tank outlet valve from being open simultaneously.
- Prevent the TOGS oxygen inlet valve and TOGS nitrogen inlet valve from being open simultaneously.
- Prevent the TOGS vacuum tank inlet valve from being open when either the TOGS oxygen inlet valve or the TOGS nitrogen inlet valve is open.
- Allow the transition from Mode 0 to Mode 1 only when TOGS is in a Running state.
- Allow the transition from Mode 1 to Mode 2 only when TOGS is in a Running state.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.1.3 Primary Closed Loop Cooling System

The PCLS provides forced convection water cooling to the TSV and neutron multiplier during irradiation of the target solution and immediately prior to transferring target solution from the TSV to the TSV dump tank. The PCLS is described in Section 5a2.2.

Monitoring and Alarms

The PICS receives input from the TRPS and provides alarms for PCLS cooling water flow (Subsection 7.4.4.1.7) and PCLS cooling water supply temperature (Subsections 7.4.2.1.5 and 7.4.2.1.6).

The PICS receives direct input and provides alarms for PCLS pressure, PCLS conductivity, PCLS expansion tank level, PCLS cleanup side stream flow, PCLS cooling water temperature (measured separately from safety-related PCLS cooling water supply temperature), and various other system parameters.

PCLS instrumentation is further described in Subsections 5a2.2.3 and 5a2.5.2.

Control Functions

The operator is able to use the PICS to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by TRPS are controlled by PICS as described in Subsection 7.3.1.3.11.

PICS automatically controls the position of the RPCS outlet control valve from the PCLS heat exchanger to maintain the nonsafety-related PCLS cooling water supply temperature indication within an acceptable band.

When manually initiated by the operator, the PICS executes a programmed sequence to start or stop the PCLS by ensuring PCLS valves are in their required states, enabling or disabling the PCLS temperature control loop, and allowing the operator to start or stop the PCLS pump motors. Starting at least one PCLS pump places PCLS in a Running state.

Interlocks and Permissives

PICS provides interlocks and permissives to:

- Prevent the PCLS pumps from starting if the PCLS supply isolation valve or either PCLS return isolation valve is closed.
- Prevent the PCLS pumps from starting if PCLS expansion tank level is low.
- Prevent the PCLS pumps from starting if PCLS suction pressure is low.
- Allow the transition from Mode 0 to Mode 1 only when PCLS is in a Running state.
- Allow the transition from Mode 1 to Mode 2 only when PCLS is in a Running state.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.1.4 Light Water Pool System

The light water pool system (LWPS) provides neutron moderation and reflection to reduce neutron leakage, radiation shielding, and decay heat removal from target solution following irradiation. The LWPS is described in Subsection 4a2.4.2.

Monitoring and Alarms

The PICS receives input and provides alarms for LWPS pool level, LWPS pool temperature, and LWPS pool leak chase level for each IU.

Control Functions

None

Interlocks

None

7.3.1.1.5 Neutron Driver Assembly System

The NDAS is the source of neutrons used to generate the neutron fluxes required to create medical isotopes in the TSV. The NDAS produces neutrons by colliding a deuterium (D) ion beam with tritium (T) gas. The NDAS is directly controlled by a vendor-provided nonsafety-related control system. The NDAS is described in Section 4a2.3.

Monitoring and Alarms

The NDAS is directly monitored by a vendor-provided nonsafety-related control system. The NDAS control system monitors deuterium-tritium (DT) neutron yield, beam current, target pressure, leakage indications, various system voltages, currents and temperatures, and feedback from vacuum pumps and other system components.

The NDAS control system provides a subset of these monitored parameters and the status of the system (System Off, Vacuum, Prepared, Standby, or Beam On) to the PICS for display on the PICS workstations and generation of alarms.

Control Functions

The NDAS control system allows the operator to manually adjust (e.g., focus or direct) the deuterium beam by changing voltages and currents applied to various solenoid magnets. The NDAS control system also allows the operator to control the ion source by adjusting microwave power, current, and voltage to manually start and stop various system auxiliaries (e.g., vacuum pumps, blowers, cooling pumps), and to open and close NDAS system valves.

The local NDAS control station is only used for maintenance and commissioning activities for an NDAS unit installed in an IU, or for an NDAS unit located in the NDAS service cell.

The operator uses PICS to provide signals to manually open or close the neutron driver HVPS breakers to meet TRPS mode transition criteria and allow the beam to be energized. The operator is able to use the PICS to manually open and close individual valves that are capable of being actuated by TRPS as described in Subsection 7.3.1.3.11.

Interlocks and Permissives

The PICS provides permissive signals to the NDAS control system to:

- Allow the use of the control room NDAS control station, specific to each NDAS unit.
- Allow the control room NDAS control station to transition a specific NDAS unit to Beam On status.
- Allow the use of the local NDAS control station.

Removal of the PICS permissive signal for Beam On operation causes the beam to deenergize.

The PICS additionally provides interlocks and permissives to:

- Prevent the transition of an NDAS unit to Beam On when the NFDS source range count rate is below an allowable value.
- Allow the transition from Mode 1 to Mode 2 only when the NDAS is in Standby.
- Allow the transition from Mode 2 to Mode 3 only when the NDAS is not in Beam On.
- Allow the transition from Mode 3 to Mode 4 only when the NDAS is not in Beam On.
- Allow the transition from Mode 4 to Mode 0 only when the NDAS is not in Beam On.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.1.6 Neutron Flux Detection System

The NFDS monitors the neutron flux in the IU during TSV fill and irradiation. The NFDS is described in Section 7.8.

Monitoring and Alarms

The PICS receives input from the TRPS for monitoring and provides alarms for source range neutron flux (Subsection 7.4.4.1.1), wide range neutron flux (Subsection 7.4.4.1.4), and power range neutron flux (Subsections 7.4.2.1.2 and 7.4.4.1.3), as described in Subsection 7.8.3.9.

The PICS directly receives discrete signals from the NFDS for “source range missing” and “power range missing” faults for the generation of alarms (Subsection 7.8.3.10).

Control Functions

None

Interlocks and Permissives

None

7.3.1.2 Supercell Systems

The PICS provides automated and manual control of systems associated with the supercell, which are used to transfer target solution between locations within the facility and extract and purify isotopes of interest. The supercell includes a vendor-provided nonsafety-related control system that is used by the operator to manually control hot cell (non-process) functions.

7.3.1.2.1 Molybdenum Extraction and Purification System

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. The MEPS is located in six hot cells of the supercell (extraction areas A, B, and C and purification areas A, B, and C) and is used to extract molybdenum from target solution and purify it, as described in Section 4b.3.

Three local operator PICS stations are provided at the supercell, one located near each extraction hot cell.

Monitoring and Alarms

The PICS receives input from the engineered safety features actuation system (ESFAS) and provides alarms for the position of the MEPS extraction column three-way valves (Subsection 7.5.4.1.16) and the MEPS [ ]$^{PROP/ECI}$ conductivity (Subsection 7.5.4.1.6).

The PICS directly monitors and provides alarms for molybdenum eluate hold tank level, discharge pressure and status feedback from system pumps, MEPS evaporator temperature, and various other system temperatures and pressures. The PICS also monitors the weight of samples obtained from various processes, but no alarms are provided.

For the MEPS [ ]$^{PROP/ECI}$, the PICS monitors and provides alarms for temperature, flow, and pressure at various locations.

The PICS also provides alarms for automatic or manual Extraction Column A/B/C Alignment Actuations and MEPS A/B/C [ ]$^{PROP/ECI}$ Isolations described in Subsection 7.5.3.1.

Control Functions

When a target solution extraction sequence is manually initiated by the operator, the PICS executes a programmed sequence to transfer solution from one manually selected TSV dump tank to a manually selected supercell extraction hot cell using the VTS. The PICS opens and closes the associated TSV dump tank drain isolation valve and appropriate system isolation valves based on feedback from associated VTS lift tank level switches and the selected TSV dump tank low-high level switch to accomplish the solution transfer. The PICS also starts and stops the associated extraction feed pump as part of the sequence.

During a target solution extraction sequence, the PICS automatically controls the [

]$^{PROP/ECI}$.

When initiated by the operator during a purification operation, the PICS automatically controls the temperature of the MEPS evaporator by energizing and deenergizing the evaporator heater.

Other than performance of a target solution extraction sequence and the automatic PICS control functions described above, the tasks performed by the operator for the MEPS are manual. The operator is able to use the PICS local supercell control stations to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by ESFAS are controlled by PICS as described in Subsection 7.3.1.3.11.

The supercell control system is used by the operator to manually control hot cell (non-process) functions.

Interlocks and Permissives

The PICS provides permissives and interlocks to:

- Prevent initiation of a target solution extraction sequence if the associated IU from where solution is being transferred is not in Mode 4.
- Prevent opening of any of the supercell reagent feed isolation valves while a target solution extraction sequence is in progress.
- Prevent alignment of MEPS three-way valves in a way that could misdirect fluid and challenge the operation of system check valves.
- Prevent operation of the extraction feed pump if more than one target solution discharge valve is open (i.e., valves used to direct post-extraction target solution to the IXP hot cell, or a target solution staging system [TSSS] or radioactive liquid waste storage [RLWS] tank).
- Stop or prevent from starting system pumps when discharge pressure is above an allowable limit or when the pump discharge flow path is isolated.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.2.2 Molybdenum Isotope Product Packaging System

The MIPS is located in two hot cells of the supercell (packaging areas 1 and 2) and is used to package isotopes received from the MEPS and IXP, as described in Subsection 9b.7.1.

Monitoring and Alarms

PICS monitors the weight of the Mo-99 product from the MEPS and the weight of the Xe-133 and I-131 products from the IXP system. No alarms are provided.

Control Functions

The supercell control system is used by the operator to manually control hot cell (non-process) functions.

Interlocks and Permissives

None

7.3.1.2.3 Iodine and Xenon Purification and Packaging System

The IXP is located in a hot cell of the supercell (IXP area) and is used to extract and purify isotopes of iodine and xenon. The IXP is described in Subsection 4b.3.1.

Monitoring and Alarms

The PICS receives input from the ESFAS and provides alarms for the position of the IXP three-way valves (Subsection 7.5.4.1.17).

The PICS directly monitors and provides alarms for IXP eluate hold tank level, [ ]PROP/ECI, xenon cryotrap temperature, and various other system temperatures and pressures. The PICS also monitors the weight of samples obtained from various processes, but no alarms are provided.

The PICS also provides alarms for automatic or manual IXP Alignment Actuations described in Subsection 7.5.3.1.

Control Functions

The tasks performed by the operator for the IXP are manual. The operator is able to use the PICS local supercell control stations to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by ESFAS are controlled by PICS as described in Subsection 7.3.1.3.11.

The supercell control system is used by the operator to manually control hot cell (non-process) functions.

Interlocks and Permissives

The PICS provides permissives and interlocks to:

- Prevent opening of any of the supercell reagent feed isolation valves while an IXP target solution supply valve is open.
- Prevent alignment of IXP three-way valves in a way that could misdirect fluid and challenge the operation of system check valves.
- Prevent operation of the B and C extraction feed pumps if more than one target solution discharge valve is open (i.e., valves used to direct post-IXP recovery target solution to a TSSS or RLWS tank).
- [ ]PROP/ECI

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.2.4 Process Vessel Vent System

The process vessel vent system (PVVS) provides ventilation of tanks and vessels located in the RPF that may contain radioactive solutions in order to mitigate the potential buildup of hydrogen that is generated via radiolysis. A portion of the PVVS equipment is located in a hot cell of the supercell (PVVS area), with other equipment located in the main production facility mezzanine or in below grade vaults. The PVVS is described in Subsection 9b.6.1.

Monitoring and Alarms

The PICS receives input from the ESFAS and provides alarms for PVVS flow (Subsection 7.5.4.1.15) and PVVS carbon delay bed exhaust carbon monoxide (Subsection 7.5.4.1.7).

The PICS directly monitors and provides alarms for nonsafety-related PVVS supply flow to individual tanks and vessels serviced by PVVS, PVVS reheater temperatures, PVVS condensate tank level, PVVS condenser cooling water temperature, PVVS carbon guard bed train exhaust temperature and differential pressure, PVVS carbon delay bed temperatures, and other system temperatures, pressures, and flows.

The PICS also provides alarms for automatic or manual Carbon Delay Bed Group 1/2/3 Isolations described in Subsection 7.5.3.1.

Control Functions

The operator is able to use the PICS to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by ESFAS are controlled by PICS as described in Subsection 7.3.1.3.11.

The PICS provides automatic control of PVVS condensate transfer by stopping the condensate discharge pump on low PVVS condensate tank level after the operator has manually selected the destination tank and initiated the transfer.

The PICS provides automatic control of the PVVS makeup air supply valve by monitoring nonsafety-related PVVS return flow (from tanks and vessels serviced by PVVS), to maintain total flow to the PVVS blowers constant.

The PICS automatically controls temperature by energizing and deenergizing the PVVS reheaters based on the PVVS reheater downstream temperature.

The supercell control system is used by the operator to manually control hot cell (non-process) functions.

Interlocks and Permissives

The PICS provides interlocks and permissives to:

- Close the PVVS inlet valve to a carbon guard bed train if differential pressure for the associated carbon guard bed train is above an allowable limit, and open the PVVS inlet and outlet valves and start the PVVS reheater for the redundant carbon guard bed train.
- Close the PVVS inlet and outlet valves for a carbon guard bed train if exhaust temperature for the associated carbon guard bed train is above an allowable limit, and open the PVVS inlet and outlet valves and start the PVVS reheater for the redundant carbon guard bed train.
- Open the carbon guard bed bypass valves if both carbon guard bed train PVVS inlet valves are closed.
- Isolate flow from the PVVS condensate tank on high level in the first uranium liquid waste tank.
- Isolate flow from the PVVS condensate tank on high level in the liquid waste blending tanks.
- Prevent from starting or stop the PVVS condensate pump when all PVVS condensate pump discharge valves are closed.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.2.5 Vacuum Transfer System

Target solution transfer activities occur throughout the main production 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 TSSS. The VTS consists of vacuum pumps and a vacuum buffer tank located in a hot cell of the supercell (co-located with the PVVS in the PVVS area) and lift tanks, as described in Subsection 9b.2.5.

Monitoring and Alarms

The PICS receives input from the ESFAS and provides alarms for the VTS vacuum header liquid detection switches (Subsection 7.5.4.1.8).

The PICS directly monitors and provides alarms for vacuum system pressure, individual VTS lift tank level switches, VTS vacuum buffer tank level switches, target solution sample line level switches, and status feedback information from the VTS vacuum pumps.

The PICS also provides alarms for automatic or manual VTS Safety Actuation described in Subsection 7.5.3.1.

Control Functions

The operator is able to use the PICS to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by TRPS or ESFAS are controlled by PICS as described in Subsection 7.3.1.3.11.

When initiated by the operator, the PICS starts or stops the VTS by enabling or disabling the vacuum system pressure control loop.

The PICS automatically starts and stops the second of two VTS vacuum pumps to maintain vacuum system pressure within an allowable range.

The supercell control system is used by the operator to manually control hot cell (non-process) functions.

Interlocks and Permissives

The PICS provides interlocks and permissives to:

- Close or prevent opening of individual VTS lift tank or target solution sample line vacuum valves when the corresponding VTS lift tank or target solution sample line high level switch signal is active.
- Close or prevent opening VTS vacuum buffer tank vacuum valves, stop or prevent from starting the VTS vacuum pumps, and open the VTS vacuum buffer tank drain valve on high level in the VTS vacuum buffer tank.
- Prevent the vacuum transfer sequence from starting if level in the destination tank selected is above an allowable limit.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.2.6 Target Solution Staging System

The TSSS is used in conjunction with the VTS (Subsection 7.3.1.2.5), and consists of hold tanks and storage tanks located in subgrade vaults. The TSSS is described in more detail in Subsection 4b.4.1.1.

Monitoring and Alarms

The PICS monitors and provides alarms for two diverse methods of level indication for the individual TSSS tanks, and temperature indication for the individual TSSS tanks. The PICS additionally provides alarms when tank level or transfer time is outside of expected parameters during a solution transfer sequence.

Control Functions

When manually initiated by the operator, the PICS executes a programmed sequence to transfer solution from one manually selected TSSS tank to another manually selected tank using the VTS. The PICS opens and closes the appropriate system isolation valves based on feedback from VTS lift tank level switches and the selected hold or storage tank level indication to accomplish the solution transfer.

An in-progress solution transfer sequence can be manually aborted by the operator.

When manually initiated by the operator, the PICS executes a programmed sequence to obtain a sample from a manually selected TSSS tank. The PICS opens and closes the appropriate vacuum valves and sampling isolation valves to accomplish the sampling activity.

The operator is able to use the PICS to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences.

Interlocks and Permissives

The PICS provides interlocks to:

- Prevent a vacuum transfer sequence from starting in a hold or storage tank when the temperature in the associated tank is above an allowable limit.
- Stop a vacuum transfer sequence on high level in the destination tank.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.3 Ancillary Process Systems

The PICS provides automated and manual control of systems used to prepare target solution, manage radioactive waste, control tritium provided to the neutron drivers, and perform other facility process monitoring and control functions.

7.3.1.3.1 Uranium Receipt and Storage System

The uranium receipt and storage system (URSS) is used to receive uranium prior to conversion to target solution. The URSS is described in detail in Subsection 4b.4.2.1.

Monitoring and Alarms

The PICS monitors and provides alarms for URSS glovebox pressures, URSS glovebox air flow, and URSS glovebox temperatures.

A single local control station is associated with the URSS and target solution preparation system (TSPS) which is capable of displaying URSS and TSPS indications and alarms to the local operator.

Control Functions

None

Interlocks and Permissives

None

7.3.1.3.2 Target Solution Preparation System

The TSPS is used to prepare uranyl sulfate target solution. 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. The TSPS is described in detail in Subsection 4b.4.2.2.

Monitoring and Alarms

The PICS receives input from the ESFAS and provides alarms for the TSPS dissolution tank level switches (Subsection 7.5.4.1.18).

The PICS directly monitors and provides alarms for TSPS dissolution tank temperature and level indications, TSPS preparation tank temperature and level indications, and various additional system temperatures and pressures.

A single local control station is associated with the URSS and TSPS which is capable of displaying these indications and alarms to the local operator.

The PICS also provides alarms for automatic or manual Dissolution Tank Isolation described in Subsection 7.5.3.1.

Control Functions

The PICS automatically controls the operation of the individual TSPS dissolution tank heaters based on the associated TSPS dissolution tank temperature.

The operator is able to use the PICS, either locally or remotely, to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by ESFAS are controlled by PICS as described in Subsection 7.3.1.3.11.

Interlocks and Permissives

The PICS provides interlocks to:

- Prevent the operation of the TSPS filter pump when TSPS dissolution tank temperature is above an allowable limit.
- Stop or prevent from starting system pumps when discharge pressure is above an allowable limit or when the pump discharge flow path is isolated.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.3.3 Radioactive Drain System

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 and the presence of liquid in the RDS sump tanks to alert the operator of abnormal situations.

Monitoring and Alarms

The PICS receives input from the ESFAS and provides alarms for the RDS liquid detection switches (Subsection 7.5.4.1.9).

The PICS directly monitors and provides alarms for RDS sump tank temperature and level.

Control Functions

When manually initiated by the operator, the PICS executes a programmed sequence to transfer solution from the RDS sump tanks to another manually selected tank using the VTS. The PICS opens and closes the appropriate system isolation valves based on feedback from VTS lift tank level switches and the RDS sump tank level indication to accomplish the solution transfer.

An in-progress solution transfer sequence can be manually aborted by the operator.

The operator is able to use the PICS to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences.

Interlocks and Permissives

The PICS provides interlocks to prevent a vacuum transfer sequence from starting in the RDS sump tanks when the temperature in the associated tank is above an allowable limit.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.3.4 Radioactive Liquid Waste Storage System

Radioactive liquid waste is stored in the RLWS, described in Subsection 9b.7.4. 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.

Monitoring and Alarms

The PICS monitors and provides alarms for two diverse methods of level indication for the individual RLWS tanks, temperature indication for the individual RLWS tanks, and status feedback from the mixers provided in the blending and collection tanks.

Control Functions

When manually initiated by the operator, the PICS executes a programmed sequence to transfer solution from a selected RLWS tank to another manually selected tank using the VTS. The PICS opens and closes the appropriate system isolation valves based on feedback from VTS lift tank level switches and RLWS tank and destination tank level indication to accomplish the solution transfer.

An in-progress solution transfer sequence can be manually aborted by the operator.

When manually initiated by the operator, the PICS executes a programmed sequence to obtain a sample from a manually selected RLWS tank. The PICS opens and closes the appropriate vacuum valves and sampling isolation valves to accomplish the sampling activity.

The operator is able to use the PICS to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences.

Interlocks and Permissives

The PICS provides interlocks and permissives to:

- Prevent a vacuum transfer sequence from starting in a RLWS tank when the temperature in the associated tank is above an allowable limit.
- Prevent a vacuum transfer sequence from starting if the selected destination tank indicates level above an allowable limit.
- Allow tank solution transfers to the second uranium liquid waste tank or to the liquid waste blending tanks only when uranium sampling results have been entered and verified to be within allowable limits and when an operations supervisor has verified the results.

Indication to the operator is provided on the PICS operator workstation displays when an interlock or permissive is bypassed.

7.3.1.3.5 Radioactive Liquid Waste Immobilization System

Radioactive liquid waste is immobilized in the RLWI system, described in detail in Subsection 9b.7.3. PICS interfaces with the RLWI vendor-provided nonsafety-related control system for monitoring purposes only.

Monitoring and Alarms

The PICS directly monitors and provides alarms for RLWI immobilization feed tank level and temperature and RLWI feed pump discharge pressure and flow rate.

The RLWI control system directly monitors the status of immobilization drum filling and mixing equipment, and various other system parameters. The RLWI control system provides a subset of these monitored parameters and the status of the system to the PICS for display on the local and control room PICS workstations for generation of alarms.

Control Functions

The RLWI control system is used by the local operator to manually start and stop operations to transfer drums into and out of the enclosure, and to fill and mix drums of liquid waste to be solidified.

The RWLI control system is also used by the operator to manually control RLWI enclosure (non-process) functions.

When manually initiated by the operator, the PICS executes a programmed sequence to transfer solution from a selected RLWS tank to the immobilization feed tank as described in Subsection 7.3.1.3.4.

Interlocks and Permissives

The PICS provides an interlock to prevent the transfer of liquid waste into the RLWI enclosure unless the RLWI control system provides indication that it is in a “ready” status.

Indication to the operator is provided on the PICS local and control room operator workstation displays when an interlock or permissive is bypassed.

7.3.1.3.6 Tritium Purification System

The TPS, which supplies tritium to the neutron drivers located in the IUs, is described in Subsection 9a2.7.1. The TPS consists of three separate, identical trains. Train A serves IU cells 1 and 2; Train B serves IU cells 3, 4, and 5; and Train C serves IU cells 6, 7, and 8.

Monitoring and Alarms

The PICS receives input from the ESFAS and provides alarms for the IU cell (NDAS) target chamber supply and exhaust pressures (Subsections 7.5.4.1.10 and 7.5.4.1.11), TPS exhaust to facility stack tritium (Subsection 7.5.4.1.12), and TPS confinement tritium (Subsection 7.5.4.1.13).

The PICS directly monitors and provides alarms for:

- Glovebox pressure, helium flow, and dew point;
- Target gas exhaust humidity;
- Nonsafety-related tritium concentration at various points in the system;
- Status feedback from TPS heaters; and
- Various other system pressures, temperatures, dew points, and flows.

The PICS also provides alarms for automatic or manual TPS Train A/B/C Isolations and TPS Process Vent Actuations described in Subsection 7.5.3.1.

Control Functions

When initiated by the operator, the PICS executes programmed sequences to start or stop a TPS train. The PICS opens and closes TPS valves to control the flow of gas through the TPS train and between the separation columns. The PICS starts or stops pumps to transport process gas through the TPS and to circulate the TPS glovebox atmosphere. Temperature and pressure control loops, listed below, are also enabled and disabled as applicable as part of the programmed sequence.

The PICS provides automatic temperature control of permeators, depleted uranium storage beds, oxide and hydride beds, and other TPS components by energizing and deenergizing the heater associated with each component.

The PICS provides automatic temperature control of cryopumps and separation columns by controlling the position of liquid nitrogen supply valves and energizing or deenergizing the heater associated with each component.

The PICS provides control of glovebox pressures by opening and closing valves to add helium to the glovebox or remove glovebox atmosphere to the zone 1 ventilation system.

When initiated by the operator, the PICS executes programmed sequences to start or stop gas supply to an individual NDAS unit. As part of the sequence, automatic control of valve positions is enabled and disabled to maintain gas supply flow to each NDAS unit individually as selected by the operator, and controls gas return flow pressure within an allowable pressure band.

When initiated by the operator, the PICS executes programmed sequences to perform other periodic or maintenance tasks, including the addition of tritium from a depleted uranium storage bed to the process by energizing or deenergizing heaters, and the evacuation of process lines.

The operator is able to use the PICS, either locally or remotely, to manually open and close individual valves and manually start or stop individual components unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by TRPS or ESFAS are controlled by PICS as described in Subsection 7.3.1.3.11.

Interlocks and Permissives

The PICS provides an interlock to prevent the introduction of tritium to an NDAS target chamber when the associated IU is not in Mode 2.

The PICS also provides interlocks to prevent the initiation of certain TPS programmed sequences while conflicting sequences are in progress.

7.3.1.3.7 Stack Release Monitoring System

The stack release monitoring system (SRMS) consists of a stack release monitor (SRM) and a carbon delay bed effluent monitor (CDBEM) to monitor gaseous effluents from the main production facility. The SRMS is described in Subsection 7.7.5.

Monitoring and Alarms

The PICS provides monitoring and alarms for SRM noble gas activity, pressure, flow, and mass flow rate, and CDBEM noble gas activity and mass flow rate.

Control Functions

None

Interlocks and Permissives

None

7.3.1.3.8 Radiation Area Monitoring System

The radiation area monitoring system (RAMS) provides radiation monitoring within the main production facility where personnel may be present and radiation levels could become significant, as described in Subsection 7.7.3.

Monitoring and Alarms

The PICS provides monitoring and alarms for the radiation level associated with each RAMS unit. The PICS additionally provides alarms for communication errors and loss of power for each RAMS unit.

Control Functions

None

Interlocks and Permissives

None

7.3.1.3.9 Continuous Air Monitoring System

The continuous air monitoring system (CAMS) provides airborne radiation monitoring within the main production facility, either alpha and beta activities for airborne particulates or beta activities for airborne tritium, as described in Subsection 7.7.4.

Monitoring and Alarms

The PICS provides monitoring and alarms for the contamination level associated with each CAMS unit. The PICS additionally provides alarms for communication errors and loss of power for each CAMS unit.

Control Functions

None

Interlocks and Permissives

None

7.3.1.3.10 Quality Control and Analytical Testing Laboratory

The main production facility contains two laboratories to provide analytical testing support as described in Subsection 9b.5.4.

Monitoring and Alarms

The PICS monitors and provides alarms for fume hood air flow rates.

Control Functions

None

Interlocks and Permissives

None

7.3.1.3.11 Target Solution Vessel Reactivity Protection System and Engineered Safety Features Actuation System

The TRPS and ESFAS are the safety-related control systems for the main production facility, as described in Sections 7.4 and 7.5, respectively.

Safety-related radiation monitors are also within the scope of the TRPS and ESFAS, as described in Subsection 7.7.1. These components are used to monitor radiation in the radiological ventilation (RV) system and are discussed in Subsection 7.3.1.4.5

Monitoring and Alarms

The PICS receives input from the TRPS and ESAFS and provides alarms related to the status and functionality of the safety-related control systems (e.g., communication errors, faulted modules, failed power supplies).

Control Functions

The PICS provides signals to the TRPS and ESFAS to provide normal control of components that are capable of being actuated by TRPS or ESFAS. Control signals from the PICS are only accepted by the TRPS and ESFAS when the associated enable nonsafety switch located on the main control board is in the “enable” position. Details of the control signals provided by PICS are described in Subsections 7.4.3.4 and 7.5.3.3.

Interlocks and Permissives

None

7.3.1.4 Other Facility Systems

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

7.3.1.4.1 Normal Electrical Power Supply System

The normal electrical power supply system (NPSS) is the normal electrical power supply for the SHINE facility, as described in Subsection 8a2.1.3. The NPSS provides normal power to the PICS, and the PICS provides monitoring, control, and alarms for the NPSS as described in this section.

The PICS remains operational through the use of local PICS power supplies upon a loss of off‘-site power for a minimum of 10 minutes (Subsection 7.3.3.6).

Monitoring and Alarms

The PICS provides monitoring and alarms for voltage, current, frequency, and power for each main electrical service branch for the SHINE facility. The PICS additionally provides status indication (closed, open, or trip) and alarms for main service breakers, switchgear breakers, and tie breakers, as well as safety-related equipment breakers (i.e., NDAS HVPS breakers, VTS vacuum pump breakers, MEPS extraction pump breakers, and RVZ1 exhaust subsystem [RVZ1e] exhaust, RVZ2 exhaust subsystem [RVZ2e] exhaust, and RVZ2 supply subsystem [RVZ2s] supply fan breakers), and alarms for main service breaker undervoltage, overvoltage, phase reversal, loss of phase, out of frequency, or loss of utility power.

Control Functions

The PICS provides the operator the ability to manually open or close the main service breakers, tie breakers, switchgear breakers, and the NDAS HVPS breakers.

The PICS automatically disconnects the on-site electric power systems from the utility by opening the affected main service breaker on undervoltage, overvoltage, phase reversal, or loss of phase.

Interlocks and Permissives

The PICS provides interlocks to prevent a main service breaker and the tie breaker for that same service from being closed simultaneously, to prevent paralleling two AC power sources.

7.3.1.4.2 Uninterruptible Electrical Power Supply System

The uninterruptible electrical power supply system (UPSS) provides safety-related power for the main production facility, as described in Subsection 8a2.2.3.

Monitoring and Alarms

The PICS receives input from the ESFAS and provides alarms for UPSS loss of external power (Subsection 7.5.4.1.19).

The PICS directly monitors and provides alarms for battery room and UPS equipment room temperatures, battery room hydrogen concentration, battery charge level, battery charger current, inverter bypass status, inverter current, and various other system parameters for both divisions of the UPSS. The PICS also provides alarms for fault conditions of UPSS components (e.g., battery fault, battery charger fault, UPS fault, DC bus ground) and unexpected system alignments (e.g., battery charger breakers open, bypass transformer breakers open, inverter bypass breaker closed, load breakers open).

Control Functions

None

Interlocks and Permissives

None

7.3.1.4.3 Standby Generator System

The SGS provides nonsafety-related backup power for the SHINE facility, as described in Subsection 8a2.2.6. The SGS generator includes a vendor-provided nonsafety-related controller.

Monitoring and Alarms

The PICS provides monitoring and alarms for SGS voltage, current, and power. The internal vendor-provided SGS generator controller additionally monitors for generator status and faults, including oil pressure, water temperature, engine temperature, fuel pressure, coolant level, overcrank or overspeed conditions, and other generator parameters. The SGS controller provides a subset of these monitored parameters to the PICS for display and alarming.

Control Functions

The PICS provides the operator the ability to manually start or stop the generator by providing a signal to the SGS automatic transfer switch(es), and to manually transfer loads between the generator and the off-site utility by opening and closing breakers.

The SGS generator controller automatically starts the generator in response to a loss of off-site power event. PICS automatically sequences the loads onto the generator.

Interlocks and Permissives

The generator automatic transfer switch design prevents paralleling the generator with either service entrance.

7.3.1.4.4 Nitrogen Purge System

The N2PS provides a backup supply of sweep gas to each IU and to all tanks normally ventilated by the PVVS during a loss of normal power or loss of normal sweep gas flow. The off-gas resulting from the nitrogen purge is treated by passive PVVS equipment prior to being discharged to the stack. The N2PS is described in Subsections 6b.2.3 and 9b.6.2.

Monitoring and Alarms

The PICS monitors and provides alarms for N2PS storage tube pressures, N2PS flows, and oxygen concentration in the N2PS structure general area.

The PICS also provides alarms for automatic or manual IU Cell Nitrogen Purge and RPF Nitrogen Purge described in Subsection 7.5.3.1.

Control Functions

The operator is able to use the PICS to manually open and close individual valves that are capable of being actuated by TRPS or ESFAS, as described in Subsection 7.3.1.3.11.

Interlocks and Permissives

None

7.3.1.4.5 Radiological Ventilation Systems

The RV systems are constant volume systems that include supply air, recirculating, and exhaust subsystems required to condition the air and provide the confinement and isolation needed to mitigate design basis accidents, as described in Section 9a2.1. The main production facility uses three ventilation zones and five subsystems in the radiologically controlled area (RCA) to maintain the temperature and humidity of the RCA and to maintain a pressure gradient from areas of least potential for contamination to areas with the most potential for contamination:

- RVZ1
- RVZ1 recirculating subsystem (RVZ1r)
- RVZ1e
- RVZ2
- RVZ2e
- RVZ2s
- RVZ2 recirculating subsystem (RVZ2r)
- RVZ3

The RV systems interface with the vendor-provided building automation system.

<u>Monitoring and Alarms</u>

The PICS receives input from the ESFAS and provides alarms for RVZ1 and RVZ2 RCA exhaust radiation (Subsection 7.5.4.1.1), RVZ1 supercell radiation in all 10 supercell areas (Subsection 7.5.4.1.2 through Subsection 7.5.4.1.5), and RVZ1e IU cell radiation for each IU (Subsection 7.4.4.1.5).

The building automation system continuously monitors hot water supply and return temperatures, chilled water supply and return temperatures, unit mixed air temperature, and discharge air temperature for the RVZ2s air handling units. The building automation system also monitors system flow rates and various other system parameters. The building automation system provides a subset of the monitored variables to PICS for display and alarming.

The PICS directly monitors and provides alarms for:

- RVZ1r IU cell and TOGS cell flows, temperatures, differential pressures, and status feedback from blowers,
- RVZ1e filter bank differential pressures and status feedback from blowers,
- RVZ2e filter bank differential pressures and status feedback from blowers,
- RVZ2r area temperatures, and status feedback from blowers and fans, and
- RVZ3 differential pressures.

The PICS also provides alarms for automatic or manual Supercell Isolation and RCA Isolation described in Subsection 7.5.3.1.

<u>Control Functions</u>

When manually initiated by the operator, the building automation system provides automatic control of RVZ2s air handling units, RVZ1e and RVZ2e exhaust fans, make-up air supply, and the position of dampers to maintain the air pressure cascade from areas with the least potential for contamination (RVZ3) to the areas with the most potential for contamination (RVZ1). The building automation system controls supply air temperature and humidity by modulating the position of hot water heating and chilled water-cooling control valves.

When manually initiated by the operator, the PICS executes a programmed sequence to start or stop the RVZ1r subsystem for a selected IU by verifying dampers are in the correct position and enabling or disabling RVZ1r automatic temperature control. The PICS maintains temperature within an allowable band by controlling the position of RPCS cooling water valves for the RVZ1r air handling units.

When manually initiated by the operator, the PICS executes a programmed sequence to start or stop the RVZ1e subsystem by verifying dampers are in the correct position and enabling or disabling RVZ1e automatic pressure control. The PICS maintains pressure within an allowable band by controlling the operation of the variable speed RVZ1e blowers.

When manually initiated by the operator, the PICS executes a programmed sequence to start or stop the RVZ2r subsystem by verifying dampers are in the correct position and enabling or disabling RVZ2r automatic temperature control. The PICS maintains temperatures within an allowable band by controlling the position of RPCS cooling water valves for the RVZ2r air handling units starting and stopping the RVZ2r RPCS pumps.

The operator is able to use the PICS to provide limited start and stop commands to building automation system control sequences. The operator may also use the PICS to manually open and close individual valves and dampers and manually start or stop individual components directly controlled by the PICS unless operation is prevented by interlocks, permissives, or active sequences. Components that are capable of being actuated by TRPS or ESFAS are controlled by PICS as described in Subsection 7.3.1.3.11.

Interlocks and Permissives

The PICS provides interlocks and permissives to prevent operation of fans or blowers where the associated discharge damper is closed.

7.3.1.4.6 Facility Ventilation System

The facility ventilation system (FVZ4) is a variable air volume system that provides heating, ventilation, and cooling to the non-RCAs of the main production facility, as described in Section 9a2.1. FVZ4 interfaces with the vendor-provided building automation system.

Monitoring and Alarms

The building automation system continuously monitors hot water supply and return temperatures, chilled water supply and return temperatures, unit mixed air temperature, and discharge air temperature for the RVZ2s air handling units. The building automation system also monitors system flow rates and various other system parameters. The building automation system provides a subset of the monitored variables to PICS for display and alarming.

Control Functions

When manually initiated by the operator, the building automation system provides automatic control of FVZ4 air handling units, exhaust fans, make-up air supply, and the position of dampers. The building automation system controls supply air temperature and humidity by modulating the position of hot water heating and chilled water-cooling control valves, or when outdoor conditions allow for free cooling, by adjusting the percentage of outside air supplied as make-up.

The operator is able to use the PICS to provide limited start and stop commands to building automation system control sequences.

Interlocks and Permissives

None

7.3.1.4.7 Facility Chilled Water System

The FCHS includes air cooled chillers and distribution pumps and provides chilled water to the main production facility RVZ2s and FVZ4 supply air handling units. The FCHS is described in Subsection 9a2.1.3. FCHS interfaces with the vendor-provided building automation system.

Monitoring and Alarms

The building automation system continuously monitors and provides alarms leaving chilled water temperatures of chillers, return chilled water temperature, chiller flow rates, system pressure, and control valve positions. The building automation system provides a subset of the monitored variables to PICS for display and alarming in the facility control room.

Control Functions

When manually initiated by the operator, the building automation system provides automatic control of the FCHS temperature. Each FCHS chiller is provided with an integral controller that controls onboard operations (e.g., capacity control and safeties) and requires a signal from building automation system to engage or disable the chiller. If temperature requirements are not met, the building automation system enables or disables redundant chillers as necessary to maintain FCHS temperature.

The building automation system provides automatic control to enable and disable primary pumps as required to maintain loop flow rates between minimum and maximum chiller flow rates while maintaining real-time response to air handling unit load changes.

Interlocks and Permissives

None

7.3.1.4.8 Facility Heating Water System

The FHWS includes boilers and distribution pumps and provides heating water to the main production facility RVZ2s and FVZ4 supply air handling units and to various terminal hot water units. The FHWS is described in Subsection 9a2.1.4. FHWS interfaces with the vendor-provided building automation system.

Monitoring and Alarms

The building automation system continuously monitors and provides alarms for leaving hot water temperatures of boilers, return hot water temperature, hot water flow rates, and control valve positions. The building automation system provides a subset of the monitored variables to PICS for display and alarming in the facility control room.

Control Functions

When manually initiated by the operator, the building automation system provides automatic control of the FHWS temperature. Each FHWS boiler is provided with an integral controller that controls onboard operations (e.g., capacity control and safeties) and requires a signal from building automation system to engage or disable the boiler. If temperature requirements are not met, the building automation system enables or disables redundant boilers as necessary to maintain FHWS temperature.

The building automation system provides automatic control to enable and disable primary pumps as required to maintain loop flow rates between minimum and maximum boiler flow rates while maintaining real-time response to connected load changes.

Interlocks and Permissives

None

7.3.1.4.9 Radioisotope Process Facility Cooling Water System

The RPCS includes a heat exchanger cooled by the PCHS and primary RPCS distribution pumps, and provides cooling to various main production facility loads as described in Section 5a2.3. RPCS interfaces with the vendor-provided building automation system.

Monitoring and Alarms

The building automation system continuously monitors and provides alarms for leaving chilled water temperature from the RPCS heat exchanger, return chilled water temperature, system flow rates, system pressure, and control valve positions. The building automation system provides a subset of the monitored variables to PICS for display and alarming in the facility control room.

Control Functions

When manually initiated by the operator, the building automation system maintains RPCS heat exchanger flow within an allowable band by enabling and disabling the primary RPCS distribution pumps and controlling the position of RPCS valves.

The operator is able to use the PICS to provide limited start and stop commands to building automation system control sequences.

Interlocks and Permissives

None

7.3.1.4.10 Process Chilled Water System

The PCHS includes air cooled chillers and distribution pumps and provides chilled water to the RPCS heat exchanger. The PCHS is described in Section 5a2.4. PCHS interfaces with the vendor-provided building automation system.

Monitoring and Alarms

The building automation system continuously monitors and provides alarms for leaving chilled water temperatures of chillers, return chilled water temperature, chiller flow rates, system pressure, and control valve positions. The building automation system provides a subset of the monitored variables to PICS for display and alarming in the facility control room.

Control Functions

When manually initiated by the operator, the building automation system provides automatic control of the PCHS temperature. Each PCHS chiller is provided with an integral controller that controls all onboard operations (e.g., capacity control and safeties) and requires a signal from building automation system to engage or disable the chiller. If temperature requirements are not met, the building automation system enables or disables redundant chillers as necessary to maintain PCHS temperature.

The building automation system provides automatic control to enable and disable primary pumps as required to maintain loop flow rates between minimum and maximum chiller flow rates while maintaining real-time response to changes in RPCS heat exchanger load.

Interlocks and Permissives

None

7.3.1.4.11 Facility Nitrogen Handling System

The FNHS provides gaseous and liquid nitrogen to various systems in the main production facility, as described in Subsection 9b.7.8. The FNHS unit contains an integral vendor-provided controller.

Monitoring and Alarms

The PICS provides monitoring and alarms for main production facility general area oxygen concentration and nitrogen pressure in nitrogen receivers for end users.

The FNHS unit contains an integral controller that monitors system status (e.g., vaporizer status and tank level) and provides a subset of monitored parameters to the PICS for display and alarming.

Control Functions

The operator is able to use the PICS to provide limited start and stop commands to the FNHS integral controller and to manually open and close individual valves.

Interlocks and Permissives

None

7.3.1.4.12 Facility Chemical Reagent System

The portion of the facility chemical reagent system (FCRS) that interfaces with the PICS provides gaseous oxygen to the TOGS, as described in Subsection 9b.7.10

Monitoring and Alarms

The PICS provides monitoring and alarms for pressure in oxygen receivers for end users.

Control Functions

None

Interlocks and Permissives

None

7.3.1.4.13 Facility Demineralized Water System

The FDWS provides demineralized water to various systems in the main production facility as described in Section 5a2.6. The FDWS RO unit contains an integral vendor-provided controller.

Monitoring and Alarms

The FDWS RO unit contains an integral controller that monitors system status (e.g., storage tank level) and provides a subset of monitored parameters to the PICS for display and alarming.

Control Functions

The operator is able to use the PICS to provide limited start and stop commands to the RO unit integral controller and to manually open and close individual valves.

Interlocks and Permissives

None

7.3.1.4.14 Seismic Monitoring System

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.

Monitoring and Alarms

The PICS provides monitoring and alarms for the acceleration status of the seismic monitors located in the main production facility.

Control Functions

None

Interlocks and Permissives

None

7.3.2 DESIGN CRITERIA

The SHINE facility design criteria applicable to the PICS are stated in Table 3.1-2. The facility design criteria applicable to the PICS, and the PICS system design criteria, are addressed in this section. Discussion of other vendor-provided nonsafety-related control systems is also provided, where applicable.

7.3.2.1 SHINE Facility Design Criteria

SHINE facility design criterion 13 applies to the PICS.

> SHINE Design Criterion 13 – Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated transients, and for postulated accidents as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the primary system boundary, the primary confinement and its associated systems, and the process confinement boundary and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating ranges.

The PICS interfaces with the safety-related TRPS, ESFAS, NFDS, and safety-related radiation monitors to provide nonsafety-related system status and measured process variable values for viewing, recording, and trending. The TRPS, ESFAS, NFDS, and safety-related radiation monitors and applicable operating ranges are described in Sections 7.4, 7.5, 7.7, and 7.8. The PICS is designed to operate in a normal environment and during normal radiological conditions (Subsection 7.3.3.3).

7.3.2.2 PICS System Design Criteria

7.3.2.2.1 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.

The PICS and other vendor-provided nonsafety-related control systems do not allow remote access and include the capability to disable unneeded networks, communication ports, and removable media drives or provide engineered barriers (Subsection 7.3.3.5). Physical access to the SHINE facility is controlled in accordance with the physical security plan. Physical access to the control room and access to the equipment within is controlled as described in Subsection 7.6.3.4.

7.3.2.2.2 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.

The PICS is developed under a structured process commensurate with the risk associated with its failure or malfunction, as described in Subsection 7.3.3.4. The development of other vendor provided nonsafety-related control systems is also described in Subsection 7.3.3.4.

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

The PICS is developed in accordance with the PICS validation master plan, which addresses V&V and configuration control activities, as described in Subsection 7.3.3.4. The development of other vendor-provided nonsafety-related control systems is also described in Subsection 7.3.3.4.

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.

The PICS validation master plan assures that the required PICS hardware and software are installed in the appropriate system configuration and ensures that the correct version of the hardware/firmware is installed in the correct hardware components as described in Subsection 7.3.3.4. Configuration control of other vendor-provided nonsafety-related control systems is also described in Subsection 7.3.3.4.

7.3.2.2.3 Fail Safe

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

Components controlled by the PICS assume a defined safe state on loss of electrical power (Subsection 7.3.3.6).

7.3.2.2.4 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 TRPS or ESFAS from performing its designated functions.

Nonsafety-related PICS inputs into the TRPS and ESFAS are designed and controlled so they do not prevent the TRPS or ESFAS from performing its safety functions as described in Subsections 7.4.3.4 and 7.5.3.3. Other vendor-provided nonsafety-related control systems do not provide input to the TRPS or ESFAS.

7.3.2.2.5 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.

Bypassing of interlocks is performed from the PICS workstations under the direct control of the control room operator. Bypassing an interlock generates a notification that is visible on the PICS workstation displays (Subsection 7.3.4.2). Interlocks applicable to each system served by the PICS are described in Subsection 7.3.1.

7.3.2.2.6 Surveillance

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

Testing, calibration and inspection of PICS equipment are allowable to ensure functionality as described in Subsection 7.3.4.2.

> 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.

Testing, calibration, and inspection of PICS equipment are described in Subsection 7.3.4.2.

7.3.3 DESIGN BASIS

7.3.3.1 Design Basis Functions

The PICS is designed to allow the operator to perform irradiation cycles, transfer target solution to and from the IU as well as through the main production facility, and interface with the TPS, supercell, waste handling, and auxiliary systems, as described in Subsection 7.3.1.

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.

7.3.3.2 Modes of Operation

The modes of operation for the functions of the PICS that interface with individual IUs correspond to the mode of that IU (see Subsection 7.3.1). Portions of the PICS that monitor or control common or facility-wide systems are not mode-dependent.

7.3.3.3 Operating Conditions

The PICS control cabinets are located in the non-RCAs 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.

7.3.3.4 Software Development

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

The PICS software development lifecycle process requirements, including V&V and configuration control requirements to ensure that 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, are described in the PICS validation master plan. The PICS validation master plan additionally includes provisions for operational qualification testing to verify the operation and functionality of various aspects of the PICS, including operator graphics accuracy and functionality, security, interface communications, interlock functionality, and control logic operation and failure monitoring and handling.

Vendor-provided nonsafety-related control systems are developed under structured processes commensurate with the risk associated with their failure or malfunction and the potential for challenging safety systems.

The process for development of the NDAS control system includes the definition of functional requirements, a documented development and implementation process, and a plan of verification of software outputs. The NDAS control system software development lifecycle process requirements, including V&V and configuration control requirements to ensure that 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, are described in the NDAS vendor software quality assurance plan.

Both the PICS and NDAS control systems are subject to acceptance by SHINE as part of factory acceptance testing, site acceptance testing, and system turnover processes.

Other vendor-provided nonsafety-related control systems, which include the building automation system, the supercell control system, and the RLWI control system, are independently developed by the vendor, and accepted by SHINE as part of factory acceptance testing, site acceptance testing, and system turnover.

7.3.3.5 Access Control and Cyber Security

The PICS and other vendor-provided nonsafety-related control systems do not use the secure development and operating environment implemented for the safety-related control systems described in Subsection 7.4.5, but rather incorporate 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 and other vendor-provided nonsafety-related control systems do 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 and other vendor-provided nonsafety-related control systems include the capability to disable, through software or physical disconnection, unneeded networks, communication ports, and removable media drives, or provide engineered barriers.

The PICS and other vendor-provided nonsafety-related control systems do 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.

Vendor-provided nonsafety-related control systems communicate with the PICS via ethernet or other industry standard digital communication protocols.

Security requirements imposed on the PICS during the development phase are commensurate with the risk and magnitude of the harm that would result from unauthorized and inappropriate access, use, disclosure, disruption, or destruction. Security requirements for the PICS development include limiting access to the software to those individuals involved in the PICS development project.

Security requirements imposed on the vendor-provided nonsafety-related control systems during the development phase are commensurate with the risk and magnitude of the harm that would result from unauthorized and inappropriate access, use, disclosure, disruption, or destruction. Security requirements for the NDAS control system include limiting access to the software to those individuals employed by the NDAS vendor and other individuals involved in the NDAS control system development project.

No special security requirements are imposed on the vendors for other nonsafety-related control systems, which include the building automation system, the supercell control system, and the RLWI control system, as these systems are not considered part of the control console and display instruments.

7.3.3.6 Loss of Power

The PICS design 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 (Section 8a2.2).

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

7.3.4 OPERATION AND PERFORMANCE

7.3.4.1 System Operation

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

7.3.4.2 Testing and Maintenance

PICS initial hardware testing is performed in accordance with the PICS validation master plan. Hardware testing is to be performed on the control cabinets, the localized I/O cabinets and the HMI panels, the operator workstations, and the main control board.

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 is designed to allow testing, calibration, and inspection to ensure functionality, and includes features for failure detection and self-test capabilities.

PICS controllers and I/O panels are located in general areas of the SHINE facility and are accessible for inspection.

The PICS has in-service self-testing capabilities such that the system will alarm if individual points or an entire rack or cabinet lose communications or faults.

Each PICS analog I/O module has status indicators that display module status. The PICS analog I/O modules allow for calibration on a channel-by-channel or module-wide basis.

Nonsafety-related interlocks are provided in the PICS as described in Subsection 7.3.1. Bypassing of interlocks is performed from the PICS workstations under the direct control of the control room operator. Bypassing an interlock generates an alarm that is visible on the PICS workstation displays.

7.3.4.3 Technical Specifications and Surveillance

The PICS contains no safety-related controls and has no safety-related functions; however, the PICS monitors parameters and provides control room alarms.

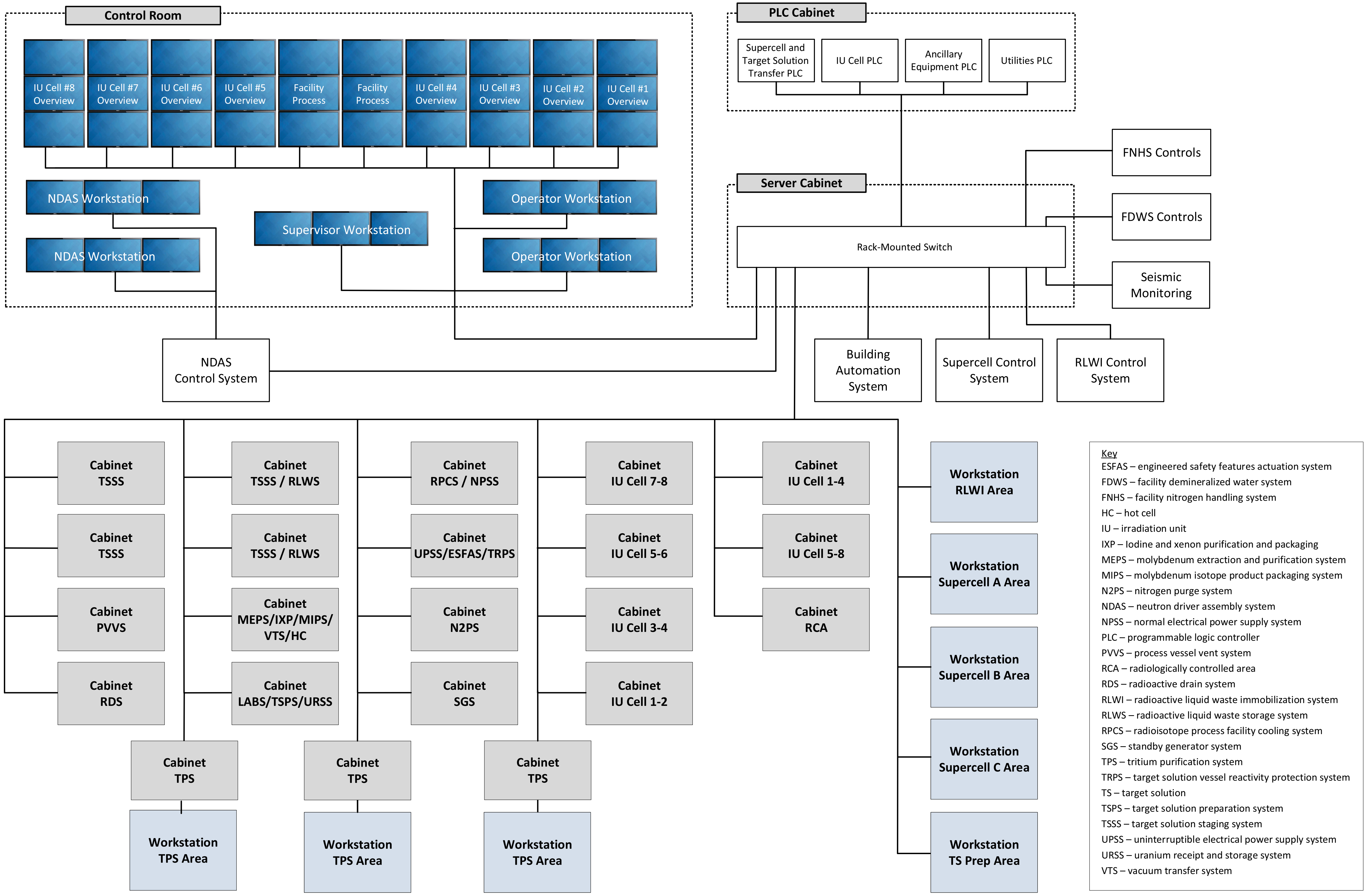
Certain material in this section provides information that is used in the technical specifications. This includes limiting conditions for operation, setpoints, design features, and means for accomplishing surveillances. In addition, significant material is also applicable to, and may be referenced by,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

7.3.5 CONCLUSION

The PICS is designed to allow the operator to perform facility activities in a safe and efficient manner. The PICS contains no safety-related controls and has no safety-related functions; however, the PICS interfaces with the safety-related TRPS, ESFAS, NFDS, and safety-related radiation monitors to provide nonsafety-related system status and measured process variable values for viewing, recording, and trending. Other vendor-provided nonsafety-related control systems interface with the PICS as needed to allow the operator to monitor and control facility equipment.

The PICS and other vendor-provided nonsafety-related control systems do not use the highly integrated protection system (HIPS) design, but instead are developed under structured processes commensurate with the risk associated with each system’s failure or malfunction.

Figure 7.3-1 – Process Integrated Control System Architecture



Key
ESFAS – engineered safety features actuation system
FDWS – facility demineralized water system
FNHS – facility nitrogen handling system
HC – hot cell
IU – irradiation unit
IXP – Iodine and xenon purification and packaging
MEPS – molybdenum extraction and purification system
MIPS – molybdenum isotope product packaging system
N2PS – nitrogen purge system
NDAS – neutron driver assembly system
NPSS – normal electrical power supply system
PLC – programmable logic controller
PVVS – process vessel vent system
RCA – radiologically controlled area
RDS – radioactive drain system
RLWI – radioactive liquid waste immobilization system
RLWS – radioactive liquid waste storage system
RPCS – radioisotope process facility cooling system
SGS – standby generator system
TPS – tritium purification system
TRPS – target solution vessel reactivity protection system
TS – target solution
TSPS – target solution preparation system
TSSS – target solution staging system
UPSS – uninterruptible electrical power supply system
URSS – uranium receipt and storage system
VTS – vacuum transfer system

7.4 TARGET SOLUTION VESSEL REACTIVITY PROTECTION SYSTEM

7.4.1 SYSTEM DESCRIPTION

The target solution vessel (TSV) reactivity protection system (TRPS) is a safety-related instrumentation and control (I&C) system consisting of eight independent instances, or subsystems, each dedicated to one of the eight irradiation units (IU) in the SHINE irradiation facility.

The TRPS performs various design basis safety functions as required by the SHINE safety analysis described in Chapter 13 for accelerator-based irradiation processes taking place within each IU cell. 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 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 Tritium Purification System (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.

The TRPS is designed using the highly integrated protection system (HIPS) platform, which is described in Subsection 7.4.5. TRPS equipment is separated into three divisions (A, B, and C). The TRPS redundantly receives safety-related inputs from field instrumentation (input devices) to either two divisions (A and B) or all three divisions, dependent on the input variable. The input signals are provided to the TRPS safety function modules (SFMs) or, in the case of the TSV fill valve position indication, to a hardwired module (HWM). More than one input device provides a signal to each SFM. The inputs are allocated to the different SFMs (or HWM) within a division as described in the technical specifications. Each SFM can be placed in maintenance bypass or in a trip state by use of the out-of-service (OOS) switch located on the front of the SFM and an associated trip/bypass switch located below the SFM, as described in Subsection 7.4.4.3. Placing an SFM in trip or bypass causes all channels associated with that SFM to be placed in trip or bypass, respectively.

The TRPS bypass logic is implemented in all three divisions using scheduling, bypass, and voting modules (SBVMs), for divisions A and B, or scheduling and bypass modules (SBMs), for division C. The TRPS voting and actuation logic is implemented in only divisions A and B. For divisions A and B, the three SBVMs, in each division, generate actuation signals when the SFMs in any two of the three divisions determine that an actuation is required. Both TRPS divisions A and B evaluate the input signals from the SFMs in each of three redundant SBVMs. Each SBVM compares the inputs received from the SFMs and generates an appropriate actuation signal if required by two or more of the three divisions.

The output of the three redundant SBVMs in divisions A and B is communicated via three independent safety data buses to the associated equipment interface modules (EIMs). There are two independent EIMs for each actuation component, associated with each division A and B of TRPS. The EIMs compare inputs from the three SBVMs and initiate an actuation if two out of three signals agree on the need to actuate. Both EIMs associated with a component are required to be deenergized for the actuation component(s) to fail to their actuated (deenergized) states.

7.4.2 DESIGN CRITERIA

The SHINE facility design criteria applicable to the TRPS are stated in Table 3.1-1. The facility design criteria applicable to the TRPS, and the TRPS system design criteria, are addressed in this section.

7.4.2.1 SHINE Facility Design Criteria

SHINE facility design criteria 13 through 19, 38, and 39 apply to the TRPS.

7.4.2.1.1 Instrumentation and Controls

> <u>SHINE Design Criterion 13</u> – Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated transients, and for postulated accidents as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the primary system boundary, the primary confinement and its associated systems, and the process confinement boundary and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating range.

The TRPS monitored variables for performance of design basis functions are presented in Table 7.4-1 and include the instrument range for covering normal and accident conditions, the accuracy for each variable, and the analytical limit. Operation of the TRPS in response to the analyzed events is presented in Subsection 7.4.4.1.

7.4.2.1.2 Protection System Functions

> SHINE Design Criterion 14 – The protection systems are designed to: (1) initiate, automatically, the operation of appropriate systems to ensure that specified acceptable target solution design limits are not exceeded as a result of anticipated transients; and (2) sense accident conditions and to initiate the operation of safety-related systems and components.

Operation of the TRPS in response to the analyzed events is presented in Subsection 7.4.4.1. This section describes the automatic system response to actuation setpoints in monitored variables.

7.4.2.1.3 Protection System Reliability and Testability

> SHINE Design Criterion 15 – The protection systems are designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection systems are sufficient to ensure that: (1) no single failure results in loss of the protection function, and (2) 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 protection systems are designed to permit periodic testing, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

High functional reliability is addressed in SHINE Design Criterion 19. The HIPS design incorporates predictability and repeatability principles to ensure an extremely high probability of accomplishing safety functions (Subsection 7.4.5.2.3).

The TRPS contains capabilities for inservice testing for those functions that cannot be tested while the IU is out of service (Subsection 7.4.4.4).

The TRPS design utilizes functional independence. 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 (Subsection 7.4.5.2.1).

The TRPS consists of three divisions of input processing and trip determination and two divisions of actuation logic arranged such that no single failure can prevent a safety actuation when required, and no single failure in a single measurement channel can generate an unnecessary safety actuation (Subsection 7.4.3.4). A single failure analysis of the TRPS was performed in accordance with Institute of Electrical and Electronics Engineers (IEEE) Standard 379-2000 (IEEE, 2000).

The maintenance bypass function allows an individual safety function module to be removed from service for required testing without loss of redundancy (Subsection 7.4.4.3). Self-test features are provided for components that do not have setpoints or tunable parameters. The discrete logic of the actuation and priority logic (APL) of the EIM does not have self-test capability but is instead functionally tested (SSubsection 7.4.4.4). Calibration, testing, and diagnostics are addressed in Section 8.0 of Topical Report TR-1015-18653, “Design of the Highly Integrated Protection System Platform” (NuScale, 2017).

7.4.2.1.4 Protection System Independence

SHINE Design Criterion 16 – The protection systems are designed to ensure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels, do not result in loss of the protection function or are demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, are used to the extent practical to prevent loss of the protection function.

The TRPS is designed as Seismic Class 1 and is protected from the effects of earthquakes, tornadoes, and floods (Subsection 7.4.3.6). The TRPS 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, extending from the sensor to the devices actuating the protective function (Subsection 7.4.5.2.1). The architecture provides two diverse methods for an actuation of the safety functions at the division level, automatic (Subsections 7.4.3.1 and 7.4.4.1) and manual (Subsection 7.4.3.7), and field programmable gate arrays (FPGAs) in each division are of a different physical architecture to prevent common cause failure (CCF) (Subsection 7.4.5.2.4).

7.4.2.1.5 Protection System Failure Modes

SHINE Design Criterion 17 – The protection systems are designed to fail into a safe state if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments are experienced.

Controlled components associated with safety actuations are designed to go to their safe state when deenergized (Subsection 7.4.3.8.) The TRPS equipment is qualified for radiological and environmental hazards present during normal operation and postulated accidents (Subsection 7.4.3.5).

7.4.2.1.6 Separation of Protection and Control Systems

SHINE Design Criterion 18 – The protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.

Nonsafety-related inputs into the TRPS are designed and controlled so they do not prevent the TRPS from performing its safety functions (Subsection 7.4.3.4).

7.4.2.1.7 Protection Against Anticipated Transients

SHINE Design Criterion 19 – The protection systems are designed to ensure an extremely high probability of accomplishing their safety functions in the event of anticipated transients.

The TRPS design utilizes functional independence; 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 (Subsection 7.4.5.2.1). The TRPS includes redundancy such that no single failure can prevent a safety actuation when required (Subsection 7.4.3.4). The architecture provides two diverse methods for an actuation of the safety functions at the division level, automatic (Subsections 7.4.3.1 and 7.4.4.1) and manual (Subsection 7.4.3.7), and FPGAs in each division are of a different physical architecture to prevent CCF (Subsection 7.4.5.2.4).

7.4.2.1.8 Monitoring Radioactivity Releases

SHINE Design Criterion 38 – Means are provided for monitoring the primary confinement boundary, hot cell, and glovebox atmospheres to detect potential leakage of gaseous or other airborne radioactive material. Potential effluent discharge paths and the plant environs are monitored for radioactivity that may be released from normal operations, including anticipated transients, and from postulated accidents.

The TRPS monitors for potential radioactivity releases from the primary confinement boundary. Specific monitored variables are addressed in Subsection 7.4.4.1. Additional radioactivity release monitoring is provided by the engineered safety features actuation system (ESFAS) (Section 7.5) and by nonsafety-related radiation monitoring systems (Section 7.7).

7.4.2.1.9 Hydrogen Mitigation

SHINE Design Criterion 39 – Systems to control the buildup of hydrogen that is released into the primary system boundary and tanks or other volumes that contain fission products and produce significant quantities of hydrogen are provided to ensure that the integrity of the system and confinement boundaries is maintained.

The TRPS monitors variables and provides actuations to prevent and mitigate hydrogen deflagration in the primary system boundary or TSV dump tank (Subsection 7.4.4.1).

7.4.2.2 TRPS System Design Criteria

7.4.2.2.1 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.

The TRPS utilizes a HIPS design which is described in Subsection 7.4.5. Unauthorized use of the TRPS is prevented by required use of a physical key as described in Subsection 7.4.5.3.3.

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.

The TRPS development design uses a defensive system architecture described in Subsection 7.4.5.3.2 that prevents 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.

Access control features prevent unauthorized physical and electronic access to CDAs during the operational phase and during transition from development to operations. Access control, cyber security, and the secure development operating environment are described in Subsection 7.4.5.3. Subsection 7.4.5.3 describes prevention of unauthorized access during the development and operational phases. Post-development installation and testing is performed and controlled by the safety-related control system vendor as described in Subsections 7.4.5.4 and 7.4.5.4.2.6.

7.4.2.2.2 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.

The system design requirements are specified in the system requirements specification (SyRS) which is generated in accordance with the vendor SyRS development procedure (Subsection 7.4.5.4.2.1). A system design description is generated to define the system design details. Software requirements development is addressed in Subsection 7.4.5.4.

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

The programmable logic lifecycle process is described in Subsection 7.4.5.4.2. The lifecycle process includes a Project Security Plan as stated in Subsection 7.4.5.4.2.1. The development process addresses security vulnerabilities (physical and electronic) in the developmental phases of the software and addresses controls to prevent unauthorized physical and electronic access. Programmable logic lifecycle activities are performed within a secure development environment (SDE) using an isolated development network (IDN) (Subsections 7.4.5.3.1 and 7.4.5.4.2.2).

TRPS Criterion 6 – TRPS development lifecycle 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.

Programmable logic lifecycle activities necessitate use of a SDE using an IDN from the Requirements Phase forward (Subsection 7.4.5.4.2.2). Software requirements development, including lifecycle phase-specific security requirements, is addressed in TRPS Criterion 5.

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

Design basis requirements are specified in the SyRS and system design description (Subsection 7.4.5.4.2.1). The lifecycle process includes development of a V&V Plan and Configuration Management Plan to control V&V and configuration management activities (Subsection 7.4.5.4.2.1).

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 lifecycle activity group shall be documented.

SHINE has delegated V&V activities related to the safety-related control system development, including V&V documentation, to the vendor. The vendor Project V&V Plan for the system development was tailored and adapted for FPGA technology from the guidance in IEEE Standard 1012-2004 (IEEE, 2004a). The V&V activities are performed using an internal V&V team from within the design organization (Subsection 7.4.5.4.5).

TRPS Criterion 9 – The TRPS software lifecycle 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.

The programmable logic lifecycle process addresses design interfaces, which includes addressing any impacts on the safety system, control console, or display instruments during the lifecycle process, as stated in Subsection 7.4.5.4.2.

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.

Subsection 7.4.5.4.6.3 addresses compliance with TRPS Criterion 10 and ensures the correct version of software/firmware is installed in the correct hardware components. The development phase configuration management process is described in Subsection 7.4.5.4.6.1 and states that components of the system (hardware) and programmable logic and its development process data (software) are controlled by the Project Configuration Management Plan. Post-installation phase configuration management is addressed in Subsection 7.4.5.4.6.2.

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.

Implementation phase V&V activities, described in Subsection 7.4.5.4.5.5, verify the design accuracy to accomplish safety functions and include functional verification and timing verification activities. Test phase V&V (Subsection 7.4.5.4.5.6) includes system functional, interface, and performance testing.

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

The vendor utilizes a Project Risk Management Plan for development of the TRPS, as described in Subsection 7.4.5.4.8. Risk identification activities occur throughout the project lifecycle. Identified risks are documented in a project risk register and actions are developed to address identified risks or vulnerabilities.

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

The developmental process for creating the safety-related TRPS has been delegated to SHINE's safety-related control system vendor (Subsection 7.4.5.3.1), including any modifications to the system logic after initial development (Subsection 7.4.5.4). 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 (Subsection 7.4.5.4.1).

7.4.2.2.3 General Instrumentation and Control Requirements

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

The TRPS equipment is installed in the seismically qualified portion of the main production facility where it is protected from earthquakes, tornadoes, and floods. The TRPS equipment is Seismic Category I, designed in accordance with Section 8 of IEEE Standard 344-2013 (IEEE, 2013) (Subsection 7.4.3.6). The TRPS control and logic equipment is located in a mild operating environment inside the facility control room, protected from radiological and environmental hazards during normal operation, maintenance, testing, and postulated accidents, and cables and sensors outside the facility control room are designed for their respective environments (Subsection 7.4.3.5).

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

The TRPS logic diagrams (Figure 7.4-1) display where the manual actuation is brought into the logic. Manual controls and nonsafety control system inputs come individually into the APL and are downstream of the programmable logic portion of the TRPS architecture shown in Figure 7.1-2 (Subsection 7.4.5.2.4).

7.4.2.2.4 Single Failure

<u>TRPS Criterion 16</u> – 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.

The TRPS consists of three divisions of input processing and trip determination and two divisions of actuation logic 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. Redundancy is addressed in Subsection 7.4.5.2.2. Nonsafety-related inputs into the TRPS are designed and controlled so they do not prevent the TRPS from performing its safety functions. Single failure is additionally addressed in Subsection 7.4.3.4.

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

The TRPS is comprised of three divisions of signal condition and trip determination, and two divisions of voting and actuation. This configuration allows for the architecture to handle a single failure of a field input, signal conditioning circuit, or trip determination and still maintain the ability to provide needed number of valid inputs to the voting circuitry. A single failure of the voting logic or the actuation logic is also acceptable within the configuration as the redundant division of voting logic and actuation logic is capable of performing the safety function. Functional independence is addressed in Subsection 7.4.5.2.1 and redundancy is addressed in Subsection 7.4.5.2.2.

7.4.2.2.5 Independence

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

Safety-related inputs to the TRPS which originate within a specific division of the TRPS are input to, and processed in, only the same division prior to being provided to any other division of the system for voting purposes (Subsection 7.4.5.2.1).

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

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 Actuation, and 2) PICS nonsafety control signals (Subsection 7.4.3.12). When the enable nonsafety control is not active, the nonsafety-related control signals are ignored. If the enable nonsafety control is active, and no automatic safety actuation or manual actuation command is present, the nonsafety control signal can control the component (Subsection 7.4.3.3).

> 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.

The TRPS 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 (Subsection 7.4.5.2.1) and nonsafety-related TRPS inputs and outputs are routed in non-divisional cable raceways and are segregated from safety-related inputs and outputs (Subsection 7.4.3.9). Wiring for redundant divisions uses physical separation and isolation to provide independence for circuits (Subsection 7.4.5.2.1) in accordance with IEEE Standard 384-2008 (IEEE, 2008). HIPS communication paths are designed such that a single failure does not cause all safety functions of a division to be inoperable (Subsection 7.4.5.2).

> 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.

The TRPS 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 (Subsection 7.4.5.2.1) and nonsafety-related TRPS inputs and outputs are routed in non-divisional cable raceways and are segregated from safety-related inputs and outputs (Subsection 7.4.3.9). Wiring for redundant divisions uses physical separation and isolation to provide independence for circuits (Subsection 7.4.5.2.1) in accordance with IEEE Standard 384-2008 (IEEE, 2008).

> <u>TRPS Criterion 22</u> – 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.

HIPS communication paths are designed with simplicity such that a single failure does not cause all safety functions of a division to be inoperable. The design uses triple redundant communication paths. A single failure does not cause all safety functions of that division to be inoperable (Subsection 7.4.5.2). Communication ports that are for communication outside of a HIPS chassis implement the one-way communication with hardware (Subsection 7.4.5.3.2).

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

TRPS data communications protocol is detailed in Section 7.5.1 of Topical Report TR-1015-18653 (NuScale, 2017). The protocol is used on the safety buses as a simple master-slave communication protocol and employs a cyclic redundancy checksum feature to ensure the integrity of the communicated information between modules. Data communications is discussed in Subsection 7.4.5.2.5.

> <u>TRPS Criterion 24</u> – The timing of TRPS data communications shall be deterministic.

The maximum response time of the TRPS components from when an input signal exceeds a predetermined setpoint to the time that the TRPS deenergizes the EIM output switching for actuated components is conservatively set to a maximum of 500 milliseconds (Subsection 7.4.5.2.3).

> <u>TRPS Criterion 25</u> – 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 communication protocols are verified as conforming to the validated protocol specifications by the Project V&V Plan (Subsection 7.4.5.4.5.

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

For communications independence, the TRPS platform is designed such that each safety division functions independently of other safety divisions. With the exception of interdivisional voting, communication within a division does not rely on communication outside the respective division to perform the safety function. Safety-related inputs to the TRPS which originate within a specific division of the TRPS are input to, and processed in, only the same division prior to being provided to any other division of the system for voting purposes (Subsection 7.4.5.2.1).

7.4.2.2.6 Prioritization of Functions

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

Priority is provided to automatic and manual safety-related actuation signals over nonsafety-related signals as described in Subsection 7.4.3.12.

7.4.2.2.7 Fail Safe

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

Controlled components associated with safety actuations are designed to go to their safe state when deenergized (Subsection 7.4.3.8).

7.4.2.2.8 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.

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 Subsections 7.2.1 and 7.4.3.11.

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

Setpoints in the TRPS are based on a documented methodology that ensures adequate margin exists between setpoints and analytical limits or safety limits. The setpoint methodology is further described in Subsections 7.2.1 and 7.4.3.11.

> 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.

Multiple setpoints are used for safety actuations based on neutron flux dependent on the IU operating conditions. Operational bypasses are used as described in Subsection 7.4.4.2 to ensure 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.

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 Subsections 7.2.1 and 7.4.3.11. Setpoint analysis parameters typically consider instrument precision, sensitivity, accuracy, loop uncertainties, and computational errors.

7.4.2.2.9 Operational Bypass, Permissives, and Interlocks

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

TRPS operating permissives are used to control the modes of operation of the IU cells. The mode transition functions are described in Subsection 7.4.3.2. Operational use of the permissives and conditions to be satisfied and operational bypasses is addressed in Subsection 7.4.4.2. A maintenance bypass function is available and is described in Subsection 7.4.4.3.

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.

Operator action is required to transition the TRPS between normal operating modes as described in Subsection 7.4.3.2. Operational bypasses are initiated or removed dependent on the TRPS mode of operation as described in Subsection 7.4.4.2. Interlocks are provided by TRPS to prevent the operator from transitioning to the next operating mode unless certain conditions are met, as described in Subsection 7.4.3.2, to 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 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 (Subsection 7.4.4.2).

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

Manual safety actuations are shown in the logic diagrams (Figure 7.4-1). There are no conditions that allow manually initiated TRPS safety functions to be bypassed.

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.

By design, certain variables as input to the safety actuations are bypassed in each operating mode, as described in Subsection 7.4.4.2. The TRPS logic associated with each mode of operation prevents an operator from activating a bypass through changing the IU cell mode out of sequential order (Subsection 7.4.4.2). Use of the maintenance bypass either preserves the single failure criterion where three channels are provided or is performed in accordance with technical specification requirements (Subsection 7.4.4.3).

> 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.

Operator action is required to transition the TRPS between normal operating modes as described in Subsection 7.4.3.2. Operational bypasses are initiated or removed dependent on the TRPS mode of operation as described in Subsection 7.4.4.2. Interlocks are provided by TRPS to prevent the operator from transitioning to the next operating mode unless certain conditions are met, as described in Subsection 7.4.3.2.

> 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.

Operational bypasses are automatically initiated or removed dependent on the TRPS mode of operation, as described in Subsection 7.4.4.2, when the associated IU is moved from one mode of operation to another, to ensure the automatic protective functions are available when required.

> 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).

Operator action is required to transition the TRPS between normal operating modes as described in Subsection 7.4.3.2. Operational bypasses are initiated or removed dependent on the TRPS mode of operation as described in Subsection 7.4.4.2. Interlocks are provided by TRPS to prevent the operator from transitioning to the next operating mode unless certain conditions are met, as described in Subsection 7.4.3.2.

> 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.

Where three channels are provided, taking an SFM out of service preserves the single failure criterion for variables associated with that SFM. In cases where only two channels are provided, taking a channel out of service will actuate the associated safety function. For testing purposes, placing a channel in maintenance bypass will be allowed by technical specifications for up to two hours to perform required testing. Two hours is considered acceptable due to the continued operability of the redundant channel(s) and the low likelihood that an accident would occur in those two hours (Subsection 7.4.4.3).

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.

When a mode of operation changes, the bypasses from the previous mode are automatically removed as they are no longer appropriate. The status of each bypass is provided to the operator through the monitoring and indication bus to the PICS, including any channel placed in maintenance bypass (Subsection 7.4.4.3), which allows the operator to confirm that a function has been bypassed or returned to service (Subsection 7.4.4.2). The PICS is described in Section 7.3 and operator displays and human factors considerations are addressed in Section 7.6.

7.4.2.2.10 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.

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. Completion of protective actions is described in Subsection 7.4.3.3.

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

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. Completion of protective actions is described in Subsection 7.4.3.3.

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.

A safety-related enable nonsafety switch (when enabled) allows a facility operator to control the output state of the TRPS with a hardwired binary control signal from the nonsafety-related controls. 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 (Subsection 7.4.3.3). Additionally, safety-related signals are prioritized over nonsafety-related signals (Subsection 7.4.3.12).

7.4.2.2.11 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 FPGA-based digital portions, shall be adequately addressed.

TRPS rack mounted equipment is installed in a mild operating environment and is designed to meet the environmental conditions described in Subsection 7.4.3.5. 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 IEEE Standard 1050-2004 (IEEE, 2004b).

7.4.2.2.12 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.

The TRPS design supports testing, maintenance, and calibration, as described in Subsection 7.4.4.3 and 7.4.4.4. Testing performed during operation is controlled in accordance with the technical specifications to ensure that at least one division of the TRPS is capable of performing its safety functions when required.

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.

The TRPS design supports testing, maintenance, and calibration, as described in Subsection 7.4.4.3 and 7.4.4.4. End-to-end testing of the entire TRPS platform can be performed through overlap testing. All TRPS components have self-testing capabilities, except the discrete APL of EIM which is functionally tested.

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.

The TRPS design supports testing, maintenance, and calibration, as described in Subsections 7.4.4.3 and 7.4.4.4. Testing intervals are established in the technical specifications (Subsection 7.4.4.5).

7.4.2.2.13 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.

Each TRPS cable and component is uniquely identified in accordance with the SHINE component numbering guidelines. The unique identification number indicates the applicable system and division (Subsection 7.4.3.10).

7.4.2.2.14 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.

Human factors is a design consideration for development of the TRPS. Changes to the design throughout the lifecycle process include human factors considerations (Subsection 7.4.5.4.2). Human factors design is described in Subsection 7.4.3.7.

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

The TRPS provides manual safety actuation capability as shown in the logic diagrams. Figure 7.4-1 displays where the manual actuation is bought into the logic. Human factors design in support of manual initiation is described in Subsection 7.4.3.7.

> 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.

To support the use of manual safety actuations, the TRPS associated with each IU includes isolated outputs for each safety-related instrument channel to provide monitoring and indication information to the PICS (Subsection 7.4.3.7). See also TRPS Criterion 44 regarding manual operator reset in Subsection 7.4.2.2.10.

7.4.2.2.15 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.

The safety-related TRPS is designed, fabricated, erected, and tested by SHINE's safety-related control system vendor in accordance with the vendor's Project Quality Assurance Plan (Subsection 7.4.5.4). SHINE is responsible for oversight of the vendor and maintaining the vendor as an approved supplier on the SHINE approved supplier list (Subsection 7.4.5.4.1).

> 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).

The TRPS design conforms to the guidance of ANSI/ANS 15.8-1995 (ANSI/ANS, 1995) as endorsed by Regulatory Guide 2.5 (USNRC, 2010) (Subsection 7.4.3.13).

7.4.3 DESIGN BASIS

The TRPS monitors variables important to the safety functions of the irradiation process during each operating mode of the IU and performs one or more of the following safety actuations upon reaching specified analytical values:

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

The TRPS also contains pre-established interlocks and permissives to control transition between IU operating modes to ensure safe operation of the main production facility.

Subsection 7.4.4 addresses the specific variables that provide input into the TRPS, the instrument range for covering normal and accident conditions, the accuracy for each variable, the analytical limit, and response time.

The technical specifications and bases describe the limiting safety system settings associated with the TRPS monitored variables and margins to the analytical limits.

7.4.3.1 Safety Functions

The TRPS consists of eight subsystems, one for each of the eight IUs. The safety functions described in this subsection are applicable to each TRPS subsystem independently.

7.4.3.1.1 IU Cell Safety Actuation

An IU Cell Safety Actuation is initiated in response to process variables indicating 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for insertion of excess reactivity events (Subsection 13a2.1.2, Scenarios 1, 2, 3, 4, 5, 6, 10, and 11), reduction in cooling events (Subsection 13a2.1.3, Scenarios 1 and 2), mishandling or malfunction of target solution events (Subsection 13a2.1.4, Scenario 4), external events (Subsection 13a2.1.6, Scenarios 2 and 5), large undamped power oscillations (Subsection 13a2.1.8), detonation and deflagration in the primary system boundary (Subsection 13a2.1.9, Scenarios 1 and 2), system interaction events (Subsection 13a2.1.11, Scenarios 1 and 2), and facility specific – neutron driver assembly system (NDAS) events (Subsection 13a2.1.12, Scenario 3).

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.

<u>Mode 3 Transition Components</u>
- TSV dump valves
- NDAS high voltage power supply (HVPS) breakers

<u>Primary System Boundary Components</u>
- TSV fill isolation valves
- TSV dump tank drain isolation valve
- TSV off-gas system (TOGS) gas supply isolation valves
- TOGS vacuum tank isolation valves
- Vacuum transfer system (VTS) lower lift tank target solution valves*

<u>Primary Confinement Boundary Components</u>
- Primary closed loop cooling system (PCLS) supply isolation valve
- PCLS return isolation valves
- Radiological ventilation zone 1 exhaust (RVZ1e) subsystem IU cell isolation valves
- Radiological ventilation zone 1 recirculation (RVZ1r) subsystem radioisotope process facility cooling system (RPCS) supply isolation valve
- RVZ1r RPCS return isolation valve
- TPS target chamber supply isolation valves
- TPS deuterium supply isolation valves
- TPS target chamber exhaust isolation valves
- TPS neutron driver evacuation isolation valves

- NDAS target/ion source cooling supply isolation valve
- NDAS target/ion source cooling return isolation valve
- NDAS vacuum pump cooling supply isolation valve
- NDAS vacuum pump cooling return isolation valve

* IU Cells 1 and 8 only have a single valve to the extraction lower lift tanks. The VTS lower lift tank target solution valves are redundant to the TSV dump tank drain isolation valve for an IU Cell Safety Actuation.

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

- High source range neutron flux
- High time-averaged neutron flux*
- High wide range 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
- IU Cell Nitrogen Purge
- Facility master operating permissive

* High time averaged neutron flux is calculated from power range neutron flux over a 45 second rolling average.

Subsection 7.4.4 provides additional details for each condition that results in an IU Cell Safety Actuation.

7.4.3.1.2 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 for the affected IU with nitrogen.

An IU Cell Nitrogen Purge is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for insertion of excess reactivity events (Subsection 13a2.1.2, Scenario 5), and detonation and deflagration in the primary system boundary (Subsection 13a2.1.9, Scenario 1).

An IU Cell Nitrogen Purge consists of an automatically or manually initiated transition of each of the following components associated with the affected IU to their deenergized state and provides a signal to the ESFAS to initiate an ESFAS IU Cell Nitrogen Purge to deenergize the common nitrogen purge system (N2PS) IU cell header valves (see Subsection 7.5.3.1.22).

- 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 condenser demister outlet temperature (Train A)
- High TOGS condenser demister outlet temperature (Train B)
- ESFAS loss of external power

7.4.3.1.3 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 Subsection 7.4.3.1.4):

- 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 isolation valves

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

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

7.4.3.1.4 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 subcritical assembly system (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.

A Driver Dropout is relied upon as a safety-related control for insertion of excess reactivity events (Subsection 13a2.1.2, Scenario 4), and reduction in cooling events (Subsection 13a2.1.3, Scenarios 1 and 2). 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 7.4.3.1.1.

7.4.3.2 Mode Transition

The design of the TRPS includes use of permissives and interlocks to control transition between IU operating modes to ensure safe operation of the main production facility. IU operating modes are described in Subsection 7.3.1.1.

Each mode transition in the TRPS is initiated manually through the PICS; however, transition to Mode 3 can occur automatically by an IU Cell Safety Actuation or by use of the control key to deactivate the facility master operating permissive. Before an operator is able to manually transition to a different mode, the transition criteria conditions must be met. Figure 7.4-1 shows a state diagram of the mode transitions.

<u>Mode 0 to Mode 1 Transition Criteria</u>

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 NDAS 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.

7.4.3.3 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 to normal operating conditions.

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.

7.4.3.4 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.

Nonsafety-related inputs into the TRPS are designed and controlled so they do not prevent the TRPS from performing its safety functions. 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 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.

Situations exist in the design where TRPS only actuates a Division A component and there is no corresponding Division B component, or, there is a passive check valve credited as a redundant component. These situations are considered acceptable since the safety function includes a separate, redundant, and passive component (i.e., check valve) which does not need to be monitored or manipulated by the TRPS.

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 or the variable is used only for actuated component position indication), 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.

The TRPS provides separate communication paths to the PICS display systems from each of the three TRPS divisions. TRPS divisions A and B are powered from a separate division of the uninterruptible electrical power supply system (UPSS); TRPS division C receives auctioneered power from both UPSS divisions A and B.

7.4.3.5 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, and is not subjected to operational cycling. 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.

7.4.3.6 Seismic, Tornado, Flood

The TRPS equipment is installed in the seismically qualified portion of the main production facility where it is protected from earthquakes, tornadoes, and floods. The TRPS equipment is Seismic Category I, designed in accordance with Section 8 of IEEE Standard 344-2013 (IEEE, 2013).

7.4.3.7 Human Factors

The TRPS provides the following manual actuation capabilities via individual manual push buttons for each TRPS subsystem:

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

Both TRPS Divisions A and B respond to the activation of a push button. A manual IU Cell TPS Actuation on all eight TRPS subsystems is initiated via the manual TPS Isolation push button located on the ESFAS main control board panel (see Subsection 7.5.3.6).

To support the use of manual safety actuations, the TRPS subsystem 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

Operator display criteria and design are addressed in Section 7.6.

7.4.3.8 Loss of External Power

The TRPS is powered from the 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.

Controlled components associated with safety actuations are designed to 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:

Mode 3 Transition Components
- TSV dump valves – Open
- NDAS HVPS breakers – Open

Primary System Boundary Components
- 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

Primary Confinement Components
- PCLS supply isolation valve – Closed
- PCLS return isolation valves – Closed
- RVZ1e IU cell isolation valves – Closed
- RVZ1r RPCS supply isolation valve – Closed
- RVZ1r RPCS return isolation valve – 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
- TOGS RPCS supply isolation valves – Closed
- TOGS RPCS return isolation valve – Closed
- NDAS target/ion source cooling supply isolation valve – Closed
- NDAS target/ion source cooling return isolation valve – Closed
- NDAS vacuum pump cooling supply isolation valve – Closed
- NDAS vacuum pump cooling return isolation valve – Closed

Nitrogen Purge Components
- N2PS inerting gas isolation valves – Open
- TOGS nitrogen vent isolation valves – Open

7.4.3.9 Fire Protection

The TRPS design utilizes physical separation to minimize the effects from fire or explosion. Safety-related equipment for different divisions is located in separate fire areas when practical. Exceptions include components for all three divisions located in the facility control room, in an individual irradiation unit (IU) or in TOGS cells, and in other locations where end devices are installed.

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 cables are routed along the south side of the RPF to go to the facility control room and Division B cables are routed on the north side of the RPF. Where possible, conduit is routed subgrade to provide additional separation. Instrument transmitters are located in separate areas: A and C instrumentation is located primarily on the east side of the main production facility G-line wall, while Division B is along the west side of the wall.

Division A and C TRPS cabinets are separated by a minimum of four feet and are located on the opposite side of the facility control room from where the Division B cabinets are located. Class A and Class C fire extinguishers for fire suppression are utilized in the facility control room to extinguish fires originating within a cabinet, console, or connecting cables. Wet sprinklers are not used in the facility control room to avoid potentially impairing the ability of the TRPS to perform its safety functions.

Noncombustible and heat resistant materials are used whenever practical in the TRPS design, particularly in locations such as confinement boundaries and the facility control room. Use of materials that release toxic or corrosive gases under combustion is minimized.

Nonsafety-related TRPS inputs and outputs are routed in non-divisional cable raceways and are segregated from safety-related inputs and outputs. Spatial separation between cable and raceway groups is in accordance with Section 5.1.1.2, Table 1 of Section 5.1.3.3, and Table 2 of Section 5.1.4 of IEEE 384-2008 (IEEE, 2008).

7.4.3.10 Classification and Identification

Each TRPS cable and component is uniquely identified in accordance with the SHINE component numbering guidelines. The equipment identification includes, but is not limited to, system designation (code), equipment train, and division.

7.4.3.11 Setpoints

Conservative setpoints for the TRPS monitored variables are established based in documented analysis methodology (Subsection 7.2.1). Setpoint analysis parameters typically consider instrument precision, sensitivity, accuracy, loop uncertainties, and computational errors. Adequate margin is required between the setpoints and the associated safety limits to ensure the protective action is initiated prior to the safety limit being exceeded. The setpoint values are derived from approved system design technical reports, design calculations, uncertainty calculations, and technical specifications.

7.4.3.12 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

The manual actuation signals input from the operators in the facility control room is brought directly into 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 signal over any other signals that are present.

7.4.3.13 Design Codes and Standards

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 TRPS Criterion 14.
2) IEEE Standard 379-2000, IEEE Standard Application of Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (IEEE, 2000); invoked as guidance to meet SHINE Design Criterion 15.
3) IEEE Standard 384-2008, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (IEEE, 2008); invoked as guidance for separation of safety-related and nonsafety-related cables and raceways to meet TRPS Criteria 20 and 21, and as described in Subsection 8a2.1.3 and Subsection 8a2.1.5.
4) IEEE Standard 1012-2004, IEEE Standard for Software Verification and Validation (IEEE 2004a); invoked as guidance to meet TRPS Design Criterion 8.
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 meet TRPS Criterion 46 and to support electromagnetic compatibility qualification for digital I&C equipment.
6) 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).

7.4.4 OPERATION AND PERFORMANCE

Subsection 7.4.4 discusses the operation of the TRPS.

The TRPS design basis functions utilize redundant logic to ensure safe and reliable operation and to prevent a single failure from defeating the intended function. Additional information related to the effects of single failure, reliability, redundancy, and independence can be found in Subsection 7.4.2 and Subsection 7.4.5.

7.4.4.1 Monitored Variables and Response

Table 7.4-1 identifies specific variables that provide input into the TRPS and includes the instrument range for covering normal and accident conditions, the accuracy for each variable, the analytical limit, and response time. A discussion of each variable (signal input) and the system response is provided in this section.

7.4.4.1.1 High Source Range Neutron Flux

The high source range neutron flux signal protects against an insertion of excess reactivity during the filling process (Subsection 13a2.1.2, Scenarios 5, 6, and 11). The signal is generated by TRPS when a source range neutron flux input exceeds the high level setpoint. The TRPS bypasses safety actuations based on the high source range neutron flux signal when filling activities cannot be in progress (i.e., Modes 2, 3, and 4), because the fill isolation valves are closed. The signal is transmitted as an analog input to the TRPS from the neutron flux detection system (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.

7.4.4.1.2 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 (Subsection 13a2.1.2, Scenario 4). The signal is generated by TRPS when a power range neutron flux input exceeds the low level setpoint. 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.

7.4.4.1.3 High Time-Averaged Neutron Flux

The high time-averaged neutron flux signal protects against exceeding analyzed TSV power levels during Modes 1 and 2 (Subsection 13a2.1.2, Scenarios 1, 3, 5, and 10; Subsection 13a2.1.6, Scenarios 2 and 5; and Subsection 13a2.1.8). The high time-averaged neutron flux signal is generated by the TRPS, which averages the power range neutron flux input over a set time period, and compares the averaged power to the high level setpoint. 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.

7.4.4.1.4 High Wide Range Neutron Flux

The high wide power range neutron flux signal protects against exceeding solution power density limits during Modes 1 and 2 (Subsection 13a2.1.2, Scenario 4; and Subsection 13a2.1.8). The signal is generated by TRPS when a wide range neutron flux input exceeds the high level setpoint. 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.

7.4.4.1.5 High PCLS Temperature

The high PCLS temperature signal protects against a loss of cooling that could cause target solution heat-up (Subsection 13a2.1.2, Scenarios 2, 3, and 11; Subsection 13a2.1.3, Scenarios 1 and 2; Subsection 13a2.1.6, Scenario 2; and Subsection 13a2.1.11, Scenario 2). The signal is generated by TRPS when a PCLS temperature input exceeds the high level setpoint. The PCLS temperature is measured 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.

7.4.4.1.6 Low PCLS Temperature

The low PCLS temperature signal protects against an overcooling of the target solution that could cause an excess reactivity insertion (Subsection 13a2.1.2.2, Scenarios 2 and 3; and Subsection 13a2.1.11.2, Scenario 2). The signal is generated by TRPS when a PCLS temperature input exceeds the low level setpoint. The PCLS temperature is measured on three different channels, one for each TRPS division. Safety actuations based on PCLS temperature are not bypassed during filling and irradiation of the TSV (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.

7.4.4.1.7 Low PCLS Flow

The low PCLS flow signal protects against a loss of cooling that could cause target solution bulk boiling (Subsection 13a2.1.3.2, Scenarios 1 and 2; Subsection 13a2.1.6.2, Scenario 2; and Subsection 13a2.1.11.2, Scenario 1). The signal is generated by TRPS when a PCLS flow input exceeds the low level setpoint. 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.

7.4.4.1.8 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 (Subsection 13a2.1.2.2, Scenario 5). 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 (Subsection 13a2.1.9.2, Scenario 1). The low-high TSV dump tank level signal is received by the TRPS as a discrete input from level switches associated with three different channels, one for each TRPS division. The low-high TSV dump tank level switches are physically separate from the high-high level switches described in Subsection 7.4.4.1.9. 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.

7.4.4.1.9 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 (Subsection 13a2.1.9.2, Scenario 1). The high-high TSV dump tank level signal is received by the TRPS as a discrete input from level switches on three different channels, one for each TRPS division. The high-high TSV dump tank level switches are physically separate from the low-high level switches described in Subsection 7.4.4.1.8. 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.

7.4.4.1.10 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 (Subsection 13a2.1.9.2, Scenario 1). The signal is generated by TRPS when a TOGS oxygen concentration input exceeds the low level setpoint. 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.

7.4.4.1.11 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 (Subsection 13a2.1.9.2, Scenario 1; and Subsection 13a2.1.11.2, Scenario 1). The signal is generated by TRPS when a TOGS mainstream flow input exceeds the low level setpoint. TOGS mainstream flow is measured independently for both TOGS Train A and TOGS Train B. 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.

7.4.4.1.12 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 (Subsection 13a2.1.9.2, Scenario 1; and Subsection 13a2.1.11.2, Scenario 1). The signal is generated by TRPS when a TOGS dump tank flow input exceeds the low level setpoint. TOGS dump tank flow is only measured for TOGS Train A, which is the only TOGS train that provides sweep gas flow to the TSV dump 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.

7.4.4.1.13 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 (Subsection 13a2.1.9.2, Scenario 1). The signal is generated by TRPS when a TOGS condenser demister outlet temperature input exceeds the high level setpoint. TOGS condenser demister outlet temperature is measured independently for both TOGS Train A and TOGS Train B. 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.

7.4.4.1.14 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 (Subsection 13a2.1.9.2, Scenario 1). The signal is generated by ESFAS and provided to each of the eight TRPS subsystems when ESFAS senses a loss of external (i.e., normal) power being provided to the UPSS as described in Subsection 7.5.4.1.19. 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.

7.4.4.1.15 High RVZ1e IU Cell Radiation

The high RVZ1e radiation signal protects against a breach in the primary system boundary (Subsection 13a2.1.4.2, Scenario 4; and Subsection 13a2.1.9.2, Scenario 2). The signal is generated by TRPS when an RVZ1e IU cell radiation input exceeds the high level setpoint. 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.

7.4.4.1.16 TSV Fill Isolation Valve Fully Closed

A TSV fill isolation valve fully closed signal protects against the inadvertent addition of target solution to the TSV (Subsection 13a2.1.2.2, Scenario 6). The TSV fill isolation valve fully closed position indication is received by the TRPS as a discrete input from redundant position indicating limit switches on two different channels for each valve. When one-out-of-two or more TSV fill isolation valve fully closed signals are no longer active for either of the TSV fill isolation valves, an IU Cell Safety Actuation is initiated. IU Cell Safety Actuation on TSV fill isolation valves fully closed is only active when the IU cell is undergoing irradiation (Mode 2).

7.4.4.1.17 ESFAS IU Cell TPS Actuation

An ESFAS IU Cell TPS Actuation protects against release of tritium events in the TPS (Subsection 13a2.1.6.2, Scenario 3; and Subsection 13a2.1.12.2, Scenario 1). The actuation signal is generated by ESFAS and provided to only the affected TRPS subsystems when the ESFAS initiates a TPS Train A/B/C Isolation as described in Subsections 7.5.3.1.18, 7.5.3.1.19, and 7.5.3.1.20. 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.

7.4.4.1.18 Fill Stop

The nonsafety-related Fill Stop function aids in controlling the rate of fill of the TSV, as described in Subsection 13a2.1.2.2, Scenario 6. 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 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 [ ]$^{PROP/ECI}$ timer is initiated. If the TSV fill isolation valve fully closed position indication is not active before the end of the [ ]$^{PROP/ECI}$ 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 [ ]$^{PROP/ECI}$ duration, then the [ ]$^{PROP/ECI}$ 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 [ ]$^{PROP/ECI}$ and that a 5-minute delay occurs between fill steps.

7.4.4.2 Operational Bypass, Permissiives, and Interlocks

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, an IU Cell TPS Actuation, 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 (Train A) (Train B)
- Low TOGS dump tank flow
- High TOGS condenser demister outlet temperature (Train A) (Train B)
- 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
- Low PCLS flow
- High PCLS temperature

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

- High source range neutron flux

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 [ ]$^{PROP/ECI}$ 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
- 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 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
- 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 fully closed

When a mode of operation changes, the bypasses from the previous mode are automatically removed as they are no longer appropriate. The status of each bypass is provided to the operator through the monitoring and indication bus to the PICS, including any channel placed in maintenance bypass (Subsection 7.4.4.3), which allows the operator to confirm that a function has been bypassed or returned to service.

7.4.4.3 Maintenance Bypass

Each SFM can be placed in maintenance bypass or in a trip state by use of the OOS switch located on the front of the SFM and an associated trip/bypass switch located below the SFM. Details of the physical configuration and operation of the OOS and trip/bypass switches are provided in Sections 2.5.1 and 2.5.2 of Topical Report TR-1015-18653 (NuScale, 2017). Any TRPS channels placed in maintenance bypass for maintenance or testing, or removed from maintenance bypass, will be displayed to the operators in the facility control room through the monitoring and indication bus to the PICS.

An individual SFM within a TRPS division is allowed to be placed in maintenance bypass for up to two hours while the associated input channel(s) is required to be operable, in accordance with the technical specifications, for the purpose of performing required technical specification surveillance testing. A time limit of two hours is acceptable based on the small amount of time the channel could be in bypass, the continual attendance by operations or maintenance personnel during the test, the continued operability of the redundant channel(s), and the low likelihood that an accident would occur during the two hour time period.

An SFM may also be placed in trip by use of the OOS and trip/bypass switches, as described in Sections 2.5.1 and 2.5.2 of Topical Report TR-1015-18653 (NuScale, 2017). Placing an SFM in trip preserves the single failure criterion for variables associated with that SFM where three channels are provided. In cases where only two channels are provided, placing a channel in trip serves to actuate the associated safety function. Inoperable channels are required to be placed in trip, or other actions are required to be taken to mitigate the condition, in accordance with the technical specifications.

7.4.4.4 Testing Capability

Testing of the TRPS consists of the inservice self-testing capabilities of the HIPS platform and periodic surveillance testing.

End-to-end testing of the entire HIPS platform is performed through overlap testing. Individual self-tests in the various components of the TRPS ensure that the entire component is functioning correctly. Self-test features are provided for components that do not have setpoints or tunable parameters. All TRPS components, except the discrete APL of the EIM, have self-testing capabilities that ensure the information passed on to the following step in the signal path is correct.

The discrete logic of the APL of the EIM does not have self-test capability but is instead functionally tested. This functional testing consists of periodic simulated automatic and manual actuations to verify the functionality of the APL and the manual actuation pushbuttons.

Testing of input devices consists of channel checks, channel tests, and channel calibrations. Channel checks are performed while the channel is in service. Channel tests and channel calibrations may be performed while the IU is in a mode where the channel is required to be operable (i.e., inservice) by placing the associated SFM in maintenance bypass (Subsection 7.4.4.3). Channel tests and channel calibrations may also be performed when the channel is not required to be operable.

7.4.4.5 Technical Specifications and Surveillance

Limiting Conditions for Operation and Surveillance Requirements are established for TRPS logic, voting, and actuation divisions and instrumentation monitored by TRPS as input to safety actuations.

7.4.5 HIGHLY INTEGRATED PROTECTION SYSTEM DESIGN

7.4.5.1 HIPS Design Summary

A HIPS platform is used to achieve the desired architecture for system control. The HIPS platform is a generic digital safety-related instrumentation and control platform devoted to the implementation of safety-related applications in nuclear facilities. The platform is a logic-based platform that does not utilize software or microprocessors for operation. It is composed of logic that is implemented using discrete components and FPGA technology. The platform is described in detail in Section 2.0 of Topical Report TR-1015-18653 (NuScale, 2017). The HIPS platform is utilized for the design of the TRPS and ESFAS (Section 7.5).

The TRPS HIPS design is shown in Figure 7.1-2.

7.4.5.2 HIPS Design Attributes

7.4.5.2.1 Independence

The HIPS design incorporates the independence principles outlined in Section 4.0 of Topical Report TR-1015-18653 (NuScale, 2017).

The built-in self-test (BIST) feature in the 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.

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 are located on the opposite side of the facility control room from where Division B is located.

For communications independence, the TRPS platform is designed such that each safety division functions independently of other safety divisions. With the exception of interdivisional voting, communication within a division does not rely on communication outside the respective division to perform the safety function. Safety-related inputs to the TRPS which originate within a specific division of the TRPS are input to, and processed in, only the same division prior to being provided to any other division of the system for voting purposes.

Individual TRPS units are supplied for each of the eight irradiation units.

7.4.5.2.2 Redundancy

The HIPS design incorporates the redundancy principles outlined in Section 5 of Topical Report TR-1015-18653 (NuScale, 2017). The use of the redundancy design principles meets portions of the criteria for redundancy in SHINE Design Criterion 15.

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 main production 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.

Figure 7.1-2 shows typical signal data flow paths in the HIPS platform.

7.4.5.2.3 Predictability and Repeatability

The HIPS design incorporates the predictability and repeatability principles outlined in Section 7 of Topical Report TR-1015-18653 (NuScale, 2017). The use of the predictability and repeatability design principles meets portions of the criteria for ensuring an extremely high probability of accomplishing safety functions as required by SHINE Design Criterion 19.

The information in this section satisfies Application-Specific Action Items (ASAI) numbers 19, 56, and 59 from Topical Report TR-1015-18653 (NuScale, 2017).

Each SBVM 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 APL circuits to actuate the appropriate equipment associated with that division. Manual trip and actuation capability also provides a direct trip or actuation of equipment, as well as input to the automatic portion of the system, to ensure the sequence is maintained.

To meet a response time performance requirement of 500 milliseconds, 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 (Figure 7.4-2). The required response times credited in the safety analysis for systems using the HIPS design (TRPS, ESFAS) cover the process delays through the sensor input to the platform and the delays through the final actuating device.

7.4.5.2.4 Diversity

The APL portions within an EIM support the implementation of different actuation methods. 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.

The APL is implemented using discrete components and is not vulnerable to a software CCF.

The HIPS design incorporates the diversity principles outlined in Section 6 of Topical Report TR1015-18653 (NuScale, 2017). The use of the diversity design principles meets portions of the criteria for diversity in SHINE Design Criterion 16.

The information in this section satisfies the application-specific information requirements for ASAI numbers 62, 63, 64, and 65 from Topical Report TR-1015-18653 (NuScale, 2017).

In order to ensure performance in the presence of a digital CCF, the different divisions of the system (TRPS, ESFAS) use different FPGA architectures (static random access memory, flash, or one-time programmable).

Display of information is available to the operator(s) at various locations in the facility control room. Information from the safety-related control systems is processed through the system (TRPS or ESFAS) and is transmitted to PICS for display on the static display screens of the main control board or at the operator workstation. Other information at the operator workstations or the main control board is aggregated from instruments throughout the facility and displayed to the operator. Section 7.6 provides further detail on the SHINE display systems.

7.4.5.2.5 Simplicity

Simplicity attributes have been considered and incorporated into the design of the I&C system architecture. The I&C system architecture is consistent with proven safety system designs used for nuclear production facilities.

The HIPS technology utilized 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 communication module (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 CCF. These diversity attributes simplify the system 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 CMs) 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 CM use a point-to-point physical layer. Communication between modules is done asynchronously which simplifies implementation by avoiding complex syncing techniques.

7.4.5.3 Access Control and Cyber Security

The secure development operating environment, cyber security requirements, and access control are discussed in this section.

7.4.5.3.1 Secure Development Operating Environment

The developmental process for creating safety-related applications (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 system design information to authorized individuals, and the use of an 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 to 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).

7.4.5.3.2 Cyber Security Design Features

A defensive system architecture is utilized as shown in Figure 7.1-1.

The defensive system architecture has the following characteristics:

- Communication outside of the 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 a maintenance workstation (MWS) to a HIPS chassis is only allowed when the affected module is placed out of service by activating the 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.

7.4.5.3.3 Access Control

Additional access control features include:

- Required use of a physical key at the main control board to prevent unauthorized use.
- Rack mounted equipment is 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 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 technical specifications, including any that establish the minimum number of redundant safety channels that must remain operable for the applicable operating mode and conditions.

7.4.5.4 Software Requirements Development

Safety-related systems 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 systems 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 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 systems has been delegated to SHINE's safety-related control system vendor. Any modifications to the system logic required to be implemented after initial development activities are complete are also delegated to the vendor.

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

The systems 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 systems.

7.4.5.4.1 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 safety-related control systems in accordance with the processes identified in this section.

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

7.4.5.4.2 Programmable Logic Lifecycle Process

The programmable logic lifecycle process is shown in Figure 7.4-3 and 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. The design interfaces include addressing any impacts on the safety system, control console, or display instruments during the lifecycle process.

7.4.5.4.2.1 Planning Phase

SHINE procurement and technical documents (e.g., specifications, drawings, input/output database) are inputs to the planning phase. These documents are reviewed by the vendor to identify design input documents containing system 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 SyRS that defines the system design requirements detail is generated. The SyRS is generated in accordance with the vendor SyRS 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 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.

7.4.5.4.2.2 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 HRS 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 PLRS 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 an 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 is 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.

7.4.5.4.2.3 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 PLDS development procedure and reviewed in accordance with the vendor verification process procedure.

In the case when a PLDS 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 design meets the system requirements in accordance with the vendor verification process procedure. Design tests are performed to validate that the design meets the system requirements in accordance with the vendor test control procedure.

7.4.5.4.2.4 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.

7.4.5.4.2.5 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.

7.4.5.4.2.6 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.

7.4.5.4.3 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 V&V 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.

7.4.5.4.4 Project Requirements Traceability Matrix

A system 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 system 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 is used for bi-directional traceability between model elements and requirements external to the model.

7.4.5.4.5 Verification and Validation

SHINE has delegated V&V activities related to the safety-related control system development to the vendor. The vendor Project V&V 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), 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 safety-related systems are classified as Software Integrity Level 2. The vendor Project V&V Plan for the system development was tailored and adapted for FPGA technology from the guidance in IEEE Standard 1012-2004 (IEEE, 2004a). The V&V activities are commensurate with the expectations for a Software Integrity Level 2 classification. Successful completion of V&V activities is documented.

The V&V activities are performed using an internal V&V team from within the design organization. It is recommended, but not required, that the personnel performing the V&V activities are not the same personnel involved directly in the design. 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 system development lifecycle as described in Subsection 7.4.5.4.2.

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 lifecycle phase, prior to approving the deliverable. Revision control is performed in accordance with the 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 system requirements traceability matrices are used to generate comprehensive validation test procedure(s) that ensure that each requirement is adequately tested and meets the system requirements. Test procedure(s) are generated by V&V personnel.

7.4.5.4.5.1 Management Phase V&V

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

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

7.4.5.4.5.2 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.

7.4.5.4.5.3 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

7.4.5.4.5.4 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.

7.4.5.4.5.5 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.

7.4.5.4.5.6 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.

7.4.5.4.6 Configuration Management

7.4.5.4.6.1 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 system. 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
- SyRS
- System design specifications
- System hardware design specifications
- System hardware components
- Programmable logic requirements documents
- Programmable logic requirements models
- Programmable logic design models
- Programmable logic hardware description language code
- V&V 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 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 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 system requirements traceability matrix.

Any proposed change to a baselined configuration item is subject to the change control and review requirements in the 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 V&V.

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.

7.4.5.4.6.2 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 7.4.5.4.6.1, 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.

7.4.5.4.6.3 Configuration Management Compliance

Versions of software/firmware and documentation of specified hardware components are managed by the configuration management process to ensure the correct version of software/firmware is installed in the correct hardware components.

7.4.5.4.7 Independent Testing

Development, review, and release of V&V generated test documents and execution of tests are performed by the vendor in accordance with the system Test Plan and V&V 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
- System 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 has 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 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 that the system hardware conforms to the system requirements as defined in the SyRS and as documented in the system 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 Configuration Management Plan and are implemented and tested.

There is no process risk associated with either the system 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 system test plan are schedule compliance and satisfaction of test acceptance criteria.

7.4.5.4.8 Project Risk Management

The vendor 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 assess 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.

7.4.5.5 HIPS Performance Analysis

HIPS system performance is addressed in Subsection 7.4.4.

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. Attributes of the system incorporate the diagnostic and maintenance principles outlined in Section 8.0 of Topical Report TR-1015-18653 (NuScale, 2017).

7.4.6 CONCLUSION

The safety-related TRPS is designed to specific and measurable criteria to ensure quality and adequacy in the system design, implementation, and maintenance.

Design basis functions ensure safe operation of the facility and prevent or mitigate consequences of design basis events.

The HIPS platform used in the TRPS design is based on fundamental instrumentation and control principles of independence, redundancy, predictability and repeatability, and diversity and was developed under quality management to provide a simple yet reliable solution for the safety-related TRPS functions.

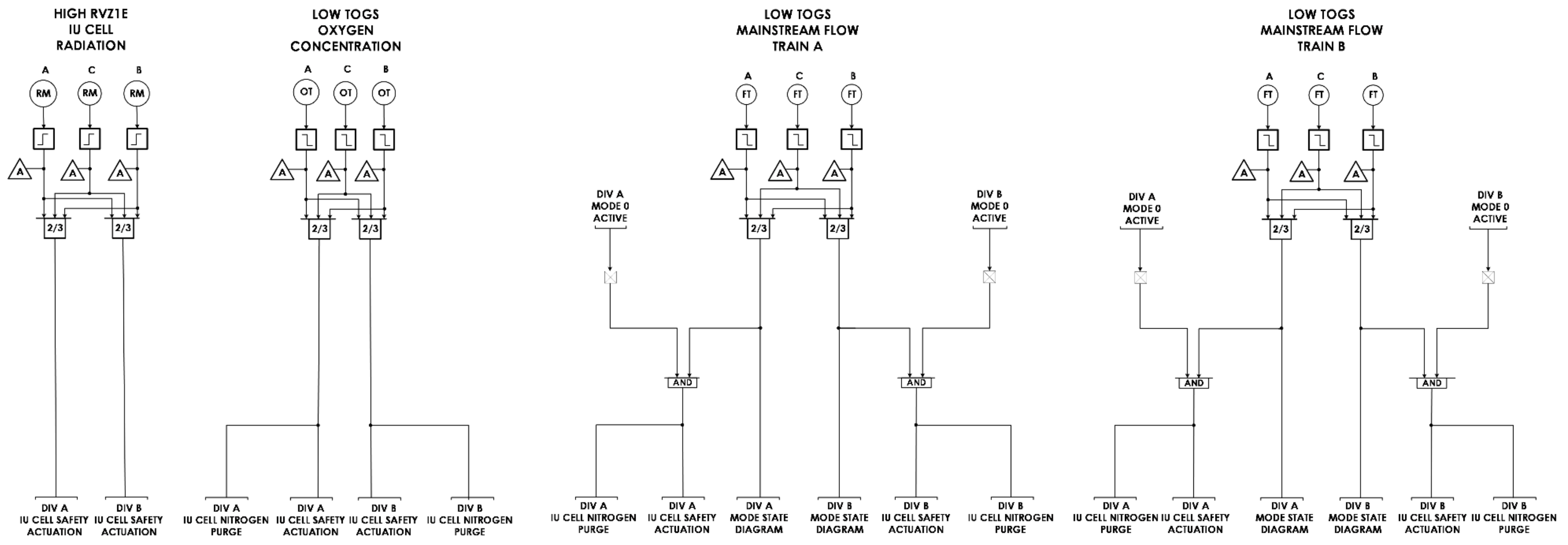
Table 7.4-1 – TRPS Monitored Variables (Sheet 1 of 2)

Variable	Analytical Limit	Logic	Range	Accuracy	Instrument Response Time
Source range neutron flux	2.52 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↑	2.5E-8 to 250 percent	2 percent	450 milliseconds
Power range neutron flux (Low power range limit, driver dropout permissive, and high time-averaged limit)	[ ]$^{PROP/ECI}$	2/3↓	0 to 125 percent	1 percent	1 second
	40 percent	2/3↑			
	104 percent	2/3↑			
RVZ1e IU cell radiation	60x 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	[ ]$^{PROP/ECI}$	2/3↓	[ ]$^{PROP/ECI}$	3 percent	0.5 seconds
TOGS dump tank flow	[ ]$^{PROP/ECI}$	2/3↓	[ ]$^{PROP/ECI}$	3 percent	0.5 seconds
TOGS 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	[ ]$^{PROP/ECI}$	2/3↓	[ ]$^{PROP/ECI}$	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)

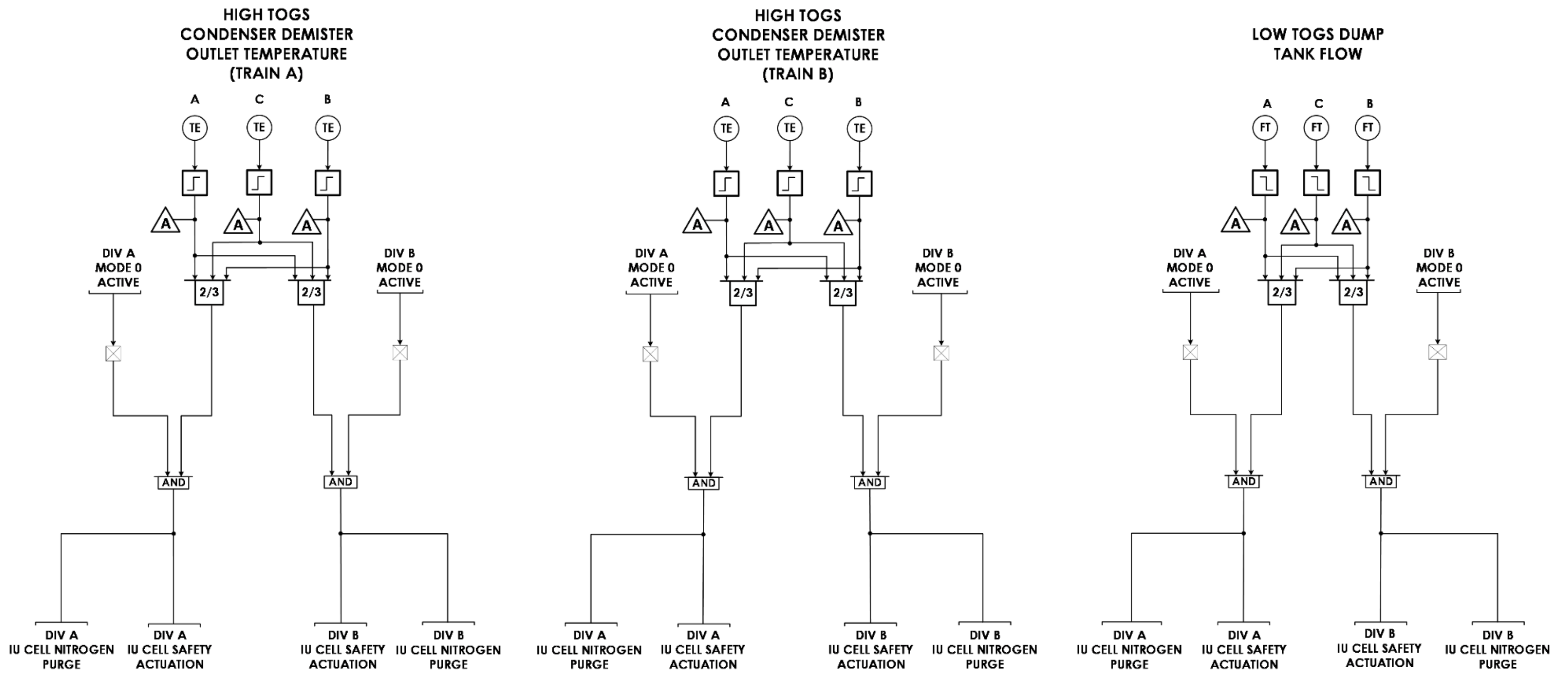
Variable	Analytical Limit	Logic	Range	Accuracy	Instrument Response Time
TSV fill isolation valves fully closed	Inactive full close	1/2↑	Active/inactive	Discrete input signal	0.5 seconds
ESFAS loss of external power	Inactive	1/1↑	Active/inactive	Discrete input signal	0.5 seconds

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


HIGH RVZ1E IU CELL RADIATION
LOW TOGS OXYGEN CONCENTRATION
LOW TOGS MAINSTREAM FLOW TRAIN A
LOW TOGS MAINSTREAM FLOW TRAIN B
A
C
B
RM
OT
FT
2/3
AND
DIV A MODE 0 ACTIVE
DIV B MODE 0 ACTIVE
DIV A IU CELL SAFETY ACTUATION
DIV B IU CELL SAFETY ACTUATION
DIV A IU CELL NITROGEN PURGE
DIV B IU CELL NITROGEN PURGE
DIV A MODE STATE DIAGRAM
DIV B MODE STATE DIAGRAM

Trip Determination and Bypasses

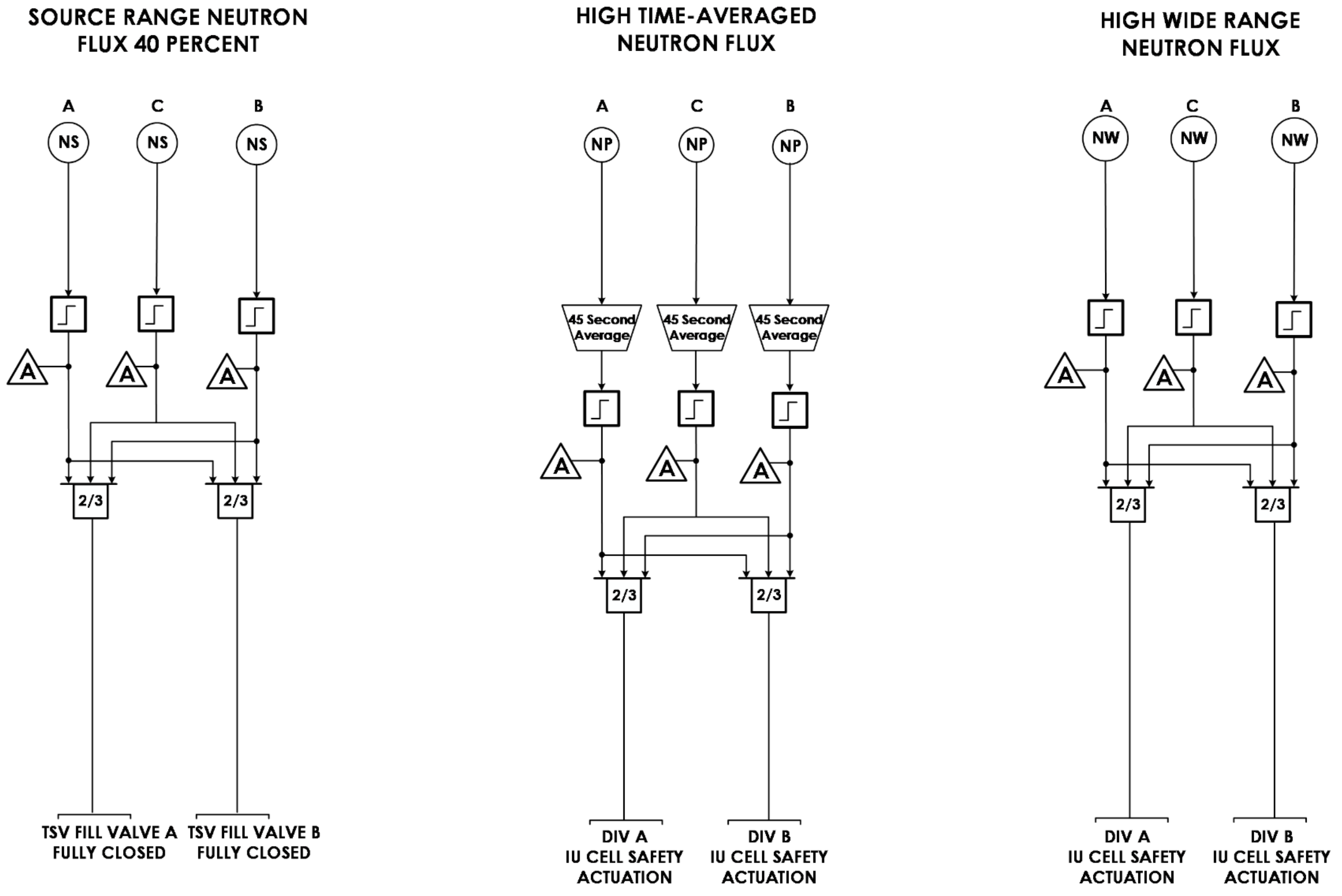
Figure 7.4-1 TRPS Logic Diagrams
(Sheet 2 of 14)


HIGH TOGS CONDENSER DEMISTER OUTLET TEMPERATURE (TRAIN A)
A
C
B
TE
A
DIV A MODE 0 ACTIVE
DIV B MODE 0 ACTIVE
2/3
AND
DIV A IU CELL NITROGEN PURGE
DIV A IU CELL SAFETY ACTUATION
DIV B IU CELL SAFETY ACTUATION
DIV B IU CELL NITROGEN PURGE
HIGH TOGS CONDENSER DEMISTER OUTLET TEMPERATURE (TRAIN B)
LOW TOGS DUMP TANK FLOW
FT

Trip Determination and Bypasses

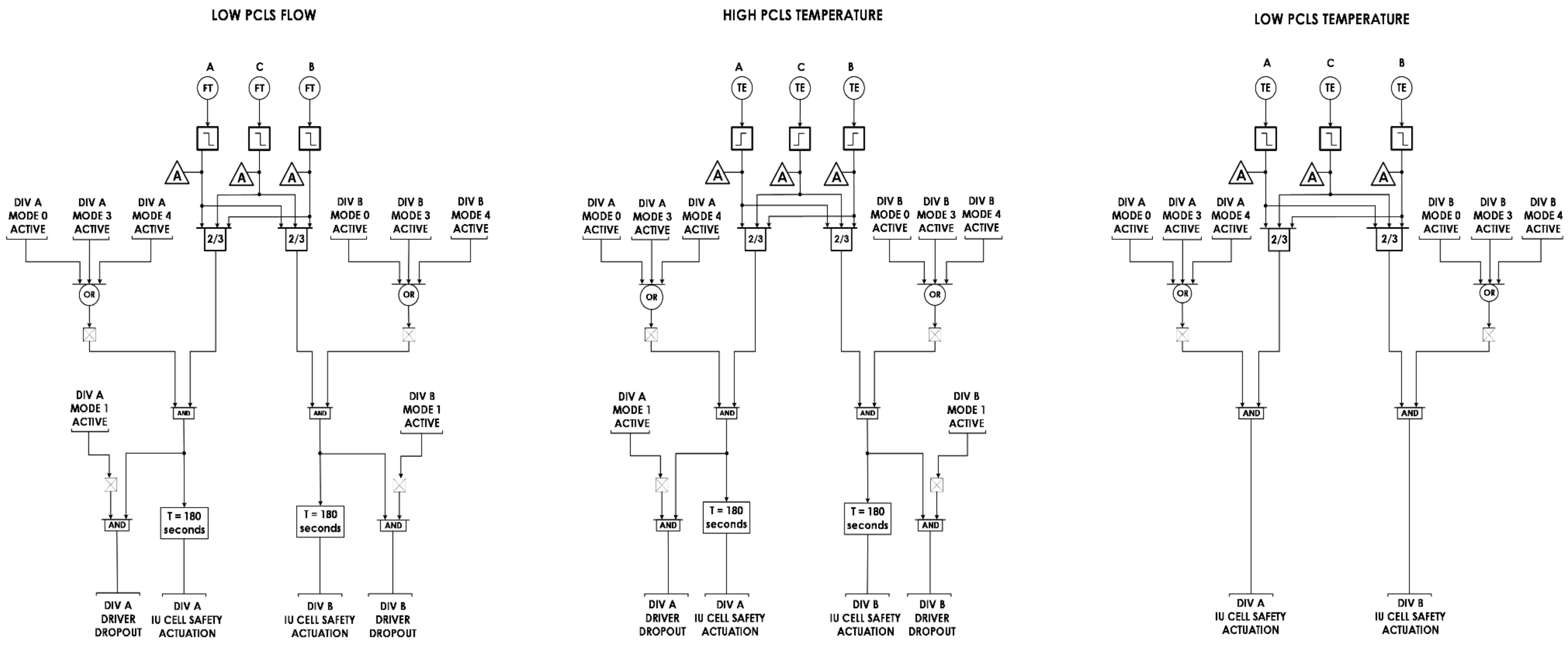
**Figure 7.4-1 TRPS Logic Diagrams
(Sheet 3 of 14)**

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


SOURCE RANGE NEUTRON FLUX 40 PERCENT
A
C
B
NS
NS
NS
A
2/3
2/3
TSV FILL VALVE A FULLY CLOSED
TSV FILL VALVE B FULLY CLOSED
HIGH TIME-AVERAGED NEUTRON FLUX
NP
45 Second Average
DIV A IU CELL SAFETY ACTUATION
DIV B IU CELL SAFETY ACTUATION
HIGH WIDE RANGE NEUTRON FLUX
NW

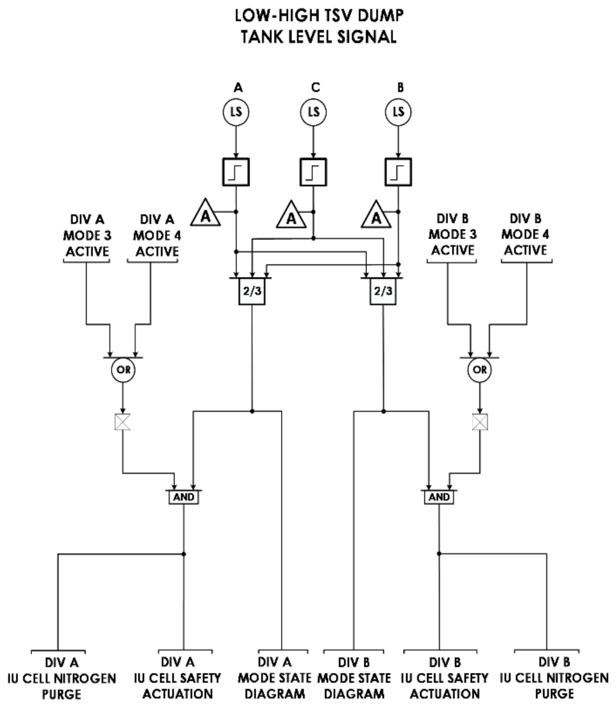
Trip Determination and Bypasses

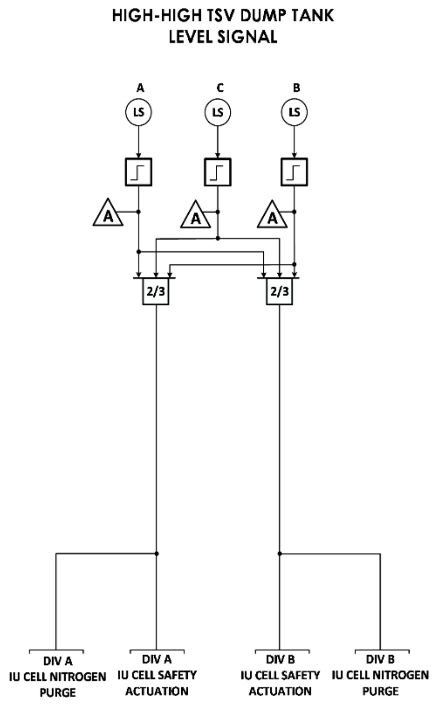
Figure 7.4-1 TRPS Logic Diagrams
(Sheet 5 of 14)

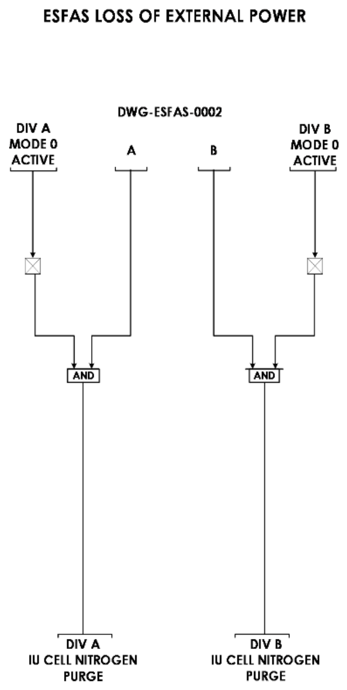


Trip Determination and Bypasses

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



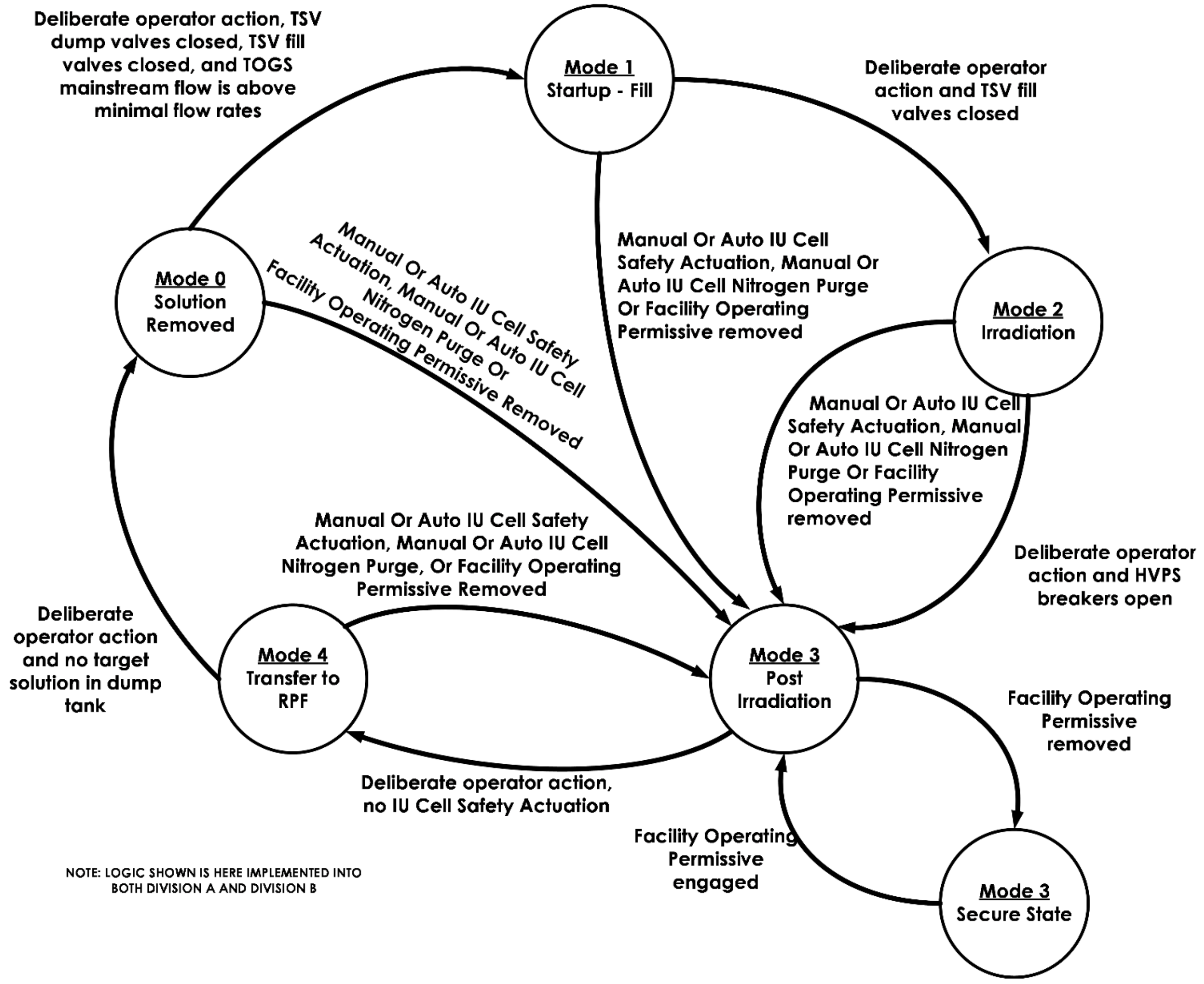

HIGH-HIGH TSV DUMP TANK LEVEL SIGNAL
A
C
B
LS
LS
LS
A
A
A
2/3
2/3
DIV A IU CELL NITROGEN PURGE
DIV A IU CELL SAFETY ACTUATION
DIV B IU CELL SAFETY ACTUATION
DIV B IU CELL NITROGEN PURGE


ESFAS LOSS OF EXTERNAL POWER
DWG-ESFAS-0002
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

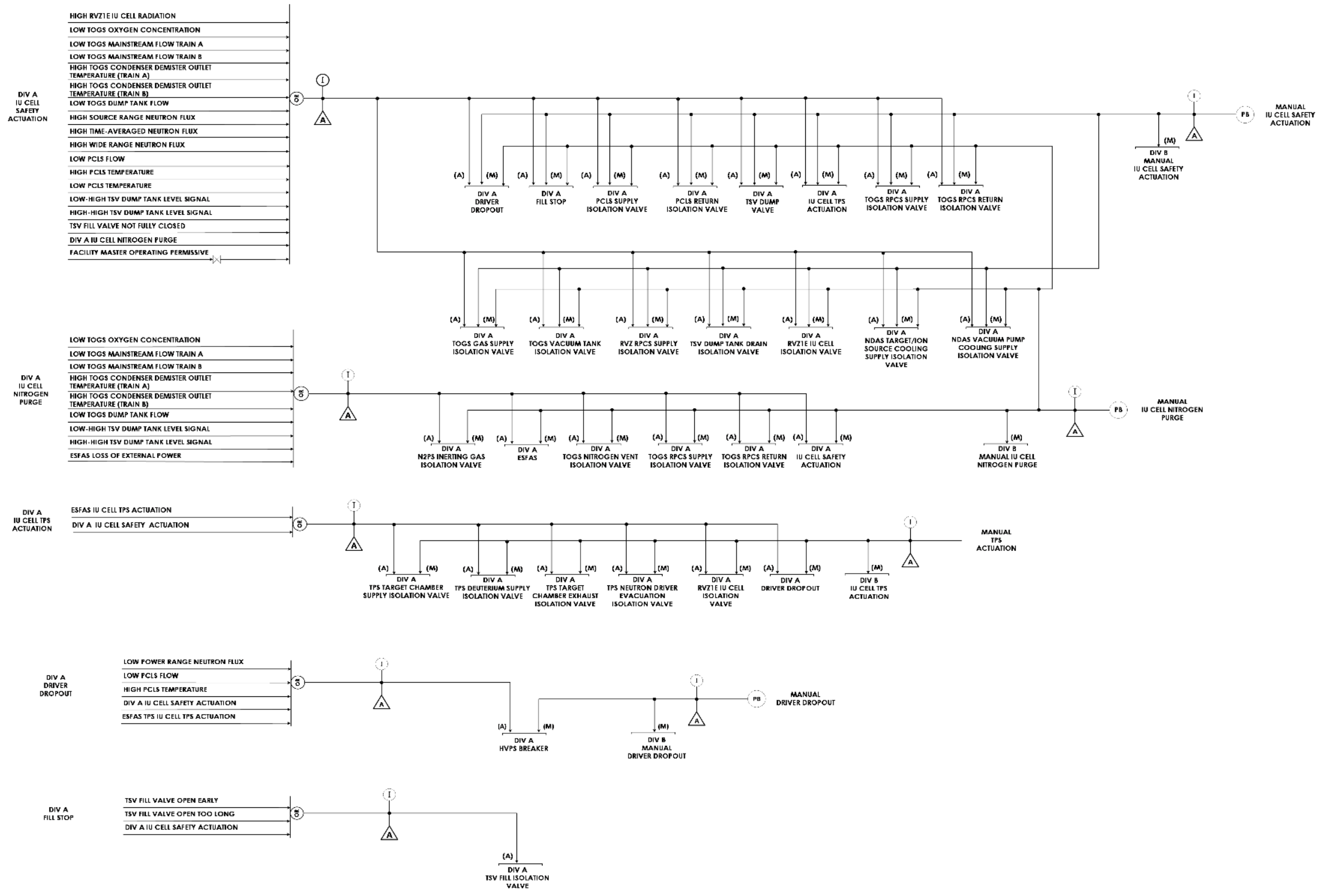
Figure 7.4-1 TRPS Logic Diagrams
(Sheet 7 of 14)

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


Deliberate operator action, TSV dump valves closed, TSV fill valves closed, and TOGS mainstream flow is above minimal flow rates
Mode 1
Startup - Fill
Deliberate operator action and TSV fill valves closed
Mode 0
Solution Removed
Manual Or Auto IU Cell Safety Actuation, Manual Or Auto IU Cell Nitrogen Purge Or Facility Operating Permissive Removed
Manual Or Auto IU Cell Safety Actuation, Manual Or Auto IU Cell Nitrogen Purge Or Facility Operating Permissive removed
Mode 2
Irradiation
Manual Or Auto IU Cell Safety Actuation, Manual Or Auto IU Cell Nitrogen Purge Or Facility Operating Permissive removed
Deliberate operator action and HVPS breakers open
Manual Or Auto IU Cell Safety Actuation, Manual Or Auto IU Cell Nitrogen Purge, Or Facility Operating Permissive Removed
Deliberate operator action and no target solution in dump tank
Mode 4
Transfer to RPF
Mode 3
Post Irradiation
Facility Operating Permissive removed
Deliberate operator action, no IU Cell Safety Actuation
Facility Operating Permissive engaged
NOTE: LOGIC SHOWN IS HERE IMPLEMENTED INTO BOTH DIVISION A AND DIVISION B
Mode 3
Secure State

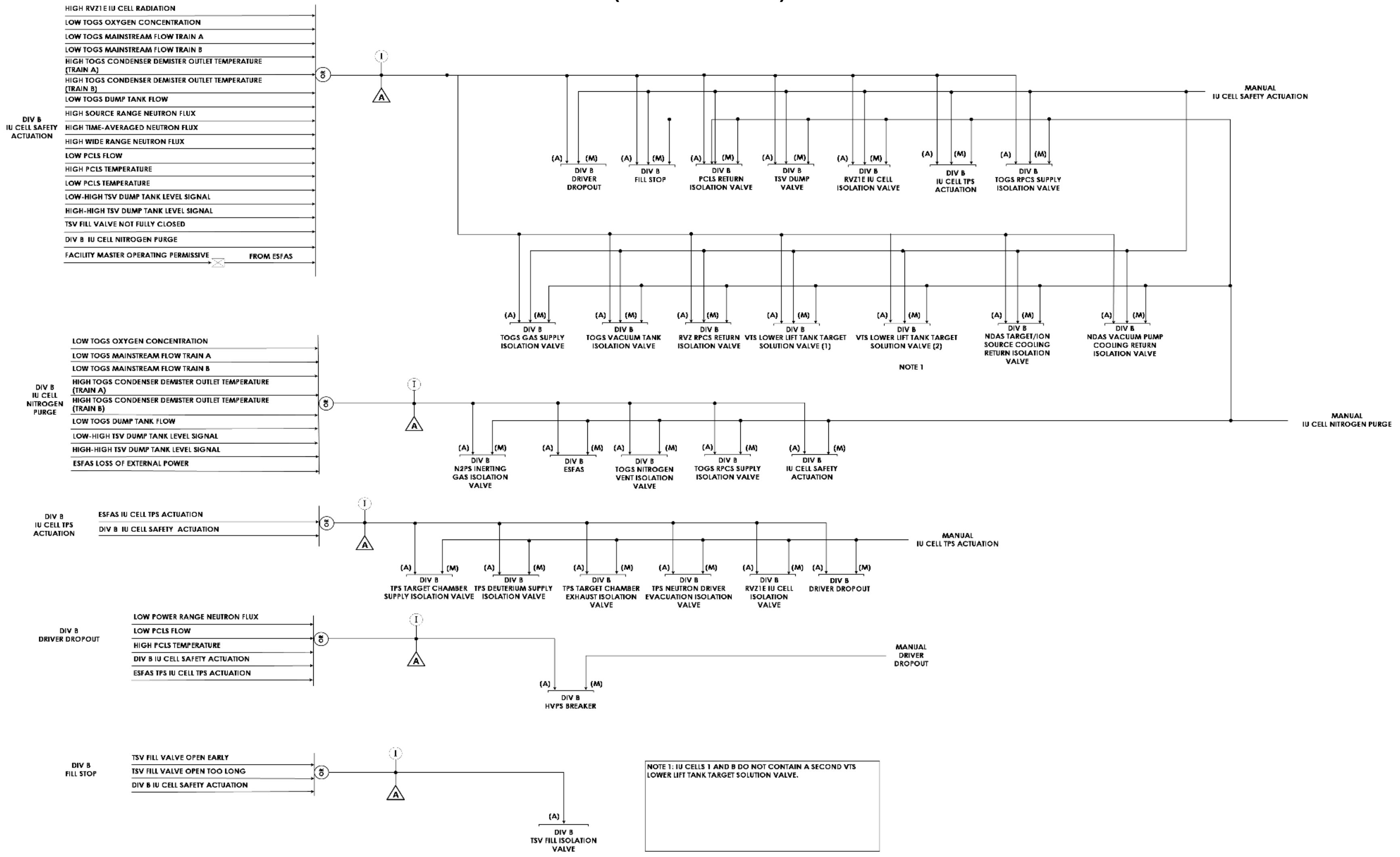
Mode State Machine

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


DIV A IU CELL SAFETY ACTUATION
HIGH RVZ1E IU CELL 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
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
DIV A IU CELL NITROGEN PURGE
FACILITY MASTER OPERATING PERMISSIVE
OR
I
A
(A)
(M)
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 RVZ1E IU CELL ISOLATION VALVE
DIV A NDAS TARGET/ION SOURCE COOLING SUPPLY ISOLATION VALVE
DIV A NDAS VACUUM PUMP COOLING SUPPLY ISOLATION VALVE
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 A IU CELL SAFETY ACTUATION
DIV B MANUAL IU CELL NITROGEN PURGE
MANUAL IU CELL NITROGEN PURGE
DIV A IU CELL TPS ACTUATION
ESFAS 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 RVZ1E IU CELL ISOLATION VALVE
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

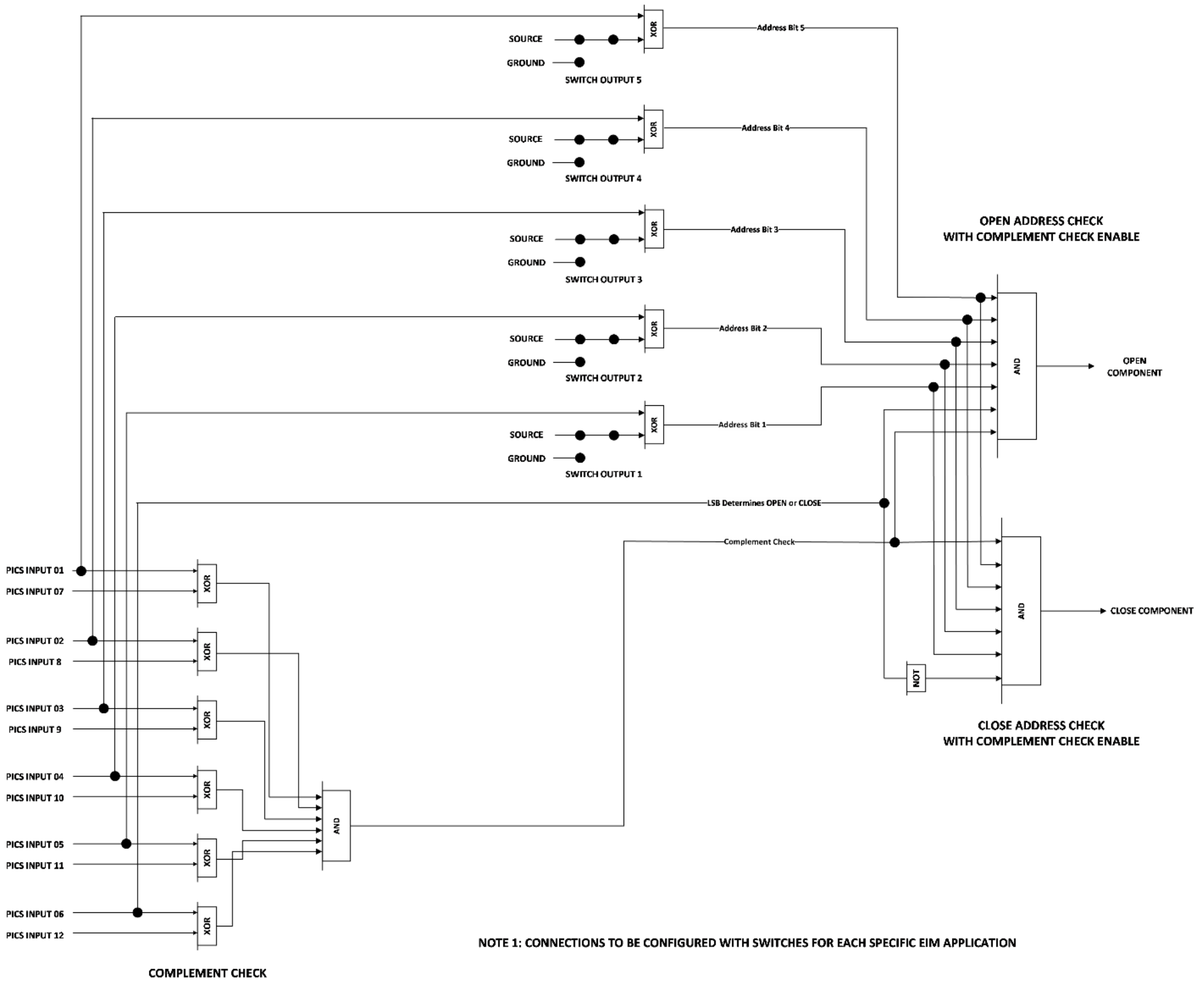
Safety Function

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



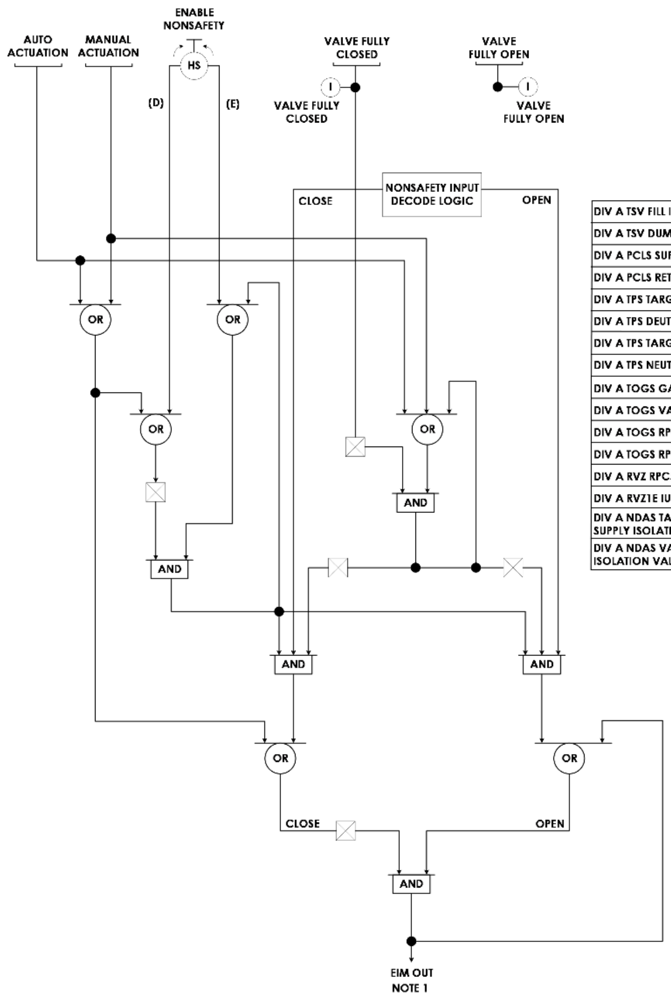
Safety Function

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



Nonsafety Interface Decode

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

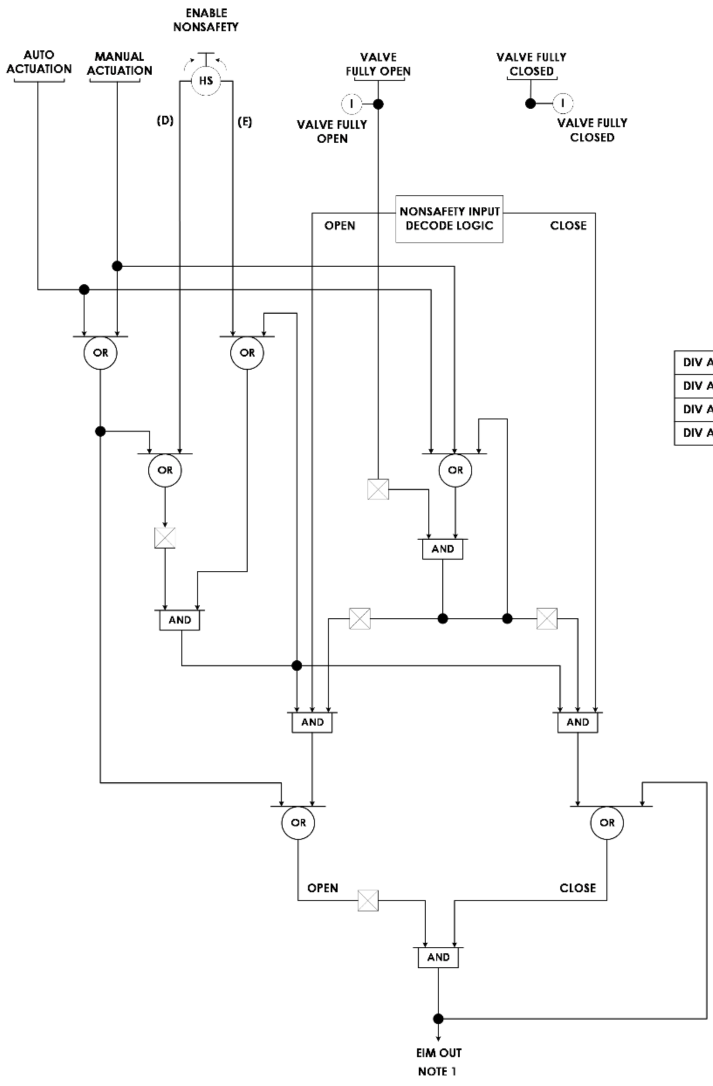


DIV A TSV FILL ISOLATION VALVE	DIV B TSV FILL ISOLATION VALVE
DIV A TSV DUMP TANK DRAIN ISOLATION VALVE	DIV B PCLS RETURN ISOLATION VALVE
DIV A PCLS SUPPLY ISOLATION VALVE	DIV B TPS TARGET CHAMBER SUPPLY ISOLATION VALVE
DIV A PCLS RETURN ISOLATION VALVE	DIV B TPS DEUTERIUM SUPPLY ISOLATION VALVE
DIV 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 RVZ1E IU CELL ISOLATION VALVE
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 RVZ1E IU CELL ISOLATION VALVE	DIV B NDAS TARGET/ION SOURCE COOLING RETURN ISOLATION VALVE
DIV A NDAS TARGET/ION SOURCE COOLING SUPPLY ISOLATION VALVE	DIV B NDAS VACUUM PUMP COOLING RETURN ISOLATION VALVE
DIV A NDAS VACUUM PUMP COOLING SUPPLY 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 13 of 14)



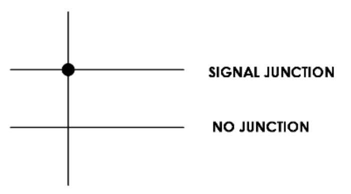
DIV A TSV DUMP VALVE	DIV B TSV DUMP VALVE
DIV A HVPS BREAKER	DIV B HVPS BREAKER
DIV A N2PS INERTING GAS ISOLATION VALVE	DIV B N2PS INERTING GAS ISOLATION VALVE
DIV A TOGS NITROGEN VENT ISOLATION VALVE	DIV B TOGS NITROGEN VENT ISOLATION VALVE

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
NOT OR ⊠	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
LSB – LEAST SIGNIFICANT BIT
NDAS – NEUTRON DRIVER ASSEMBLY SYSTEM

Legend

Figure 7.4-2 – HIPS Platform Timing

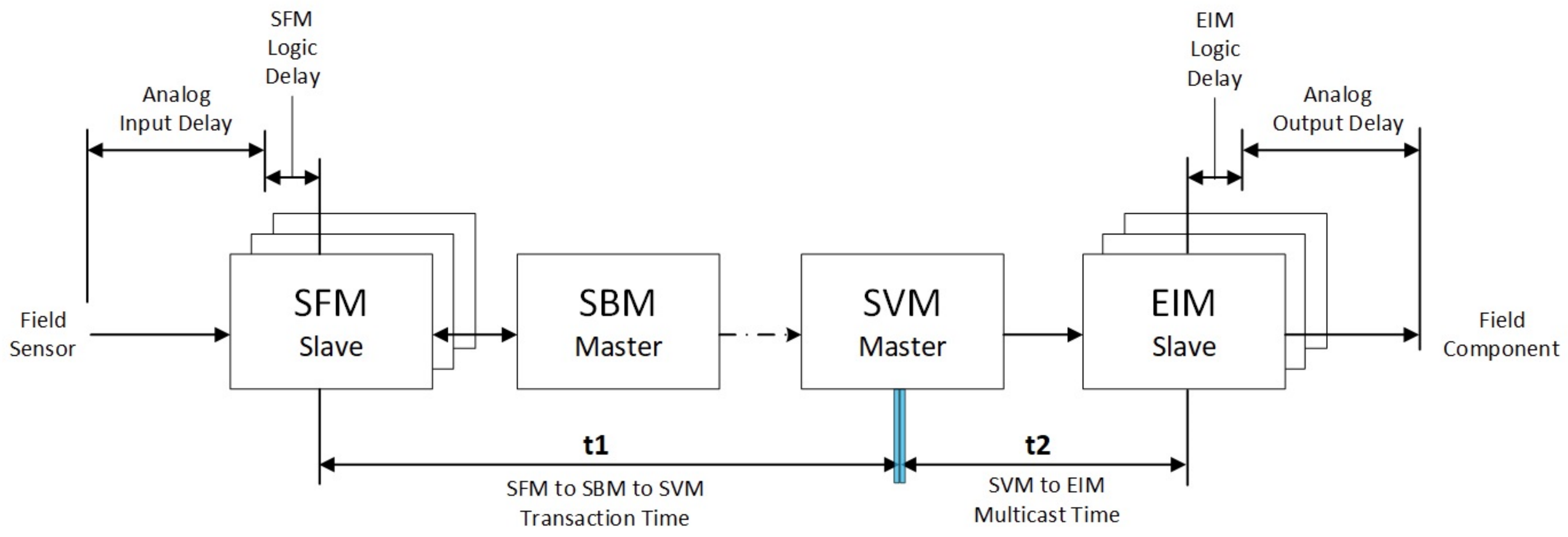
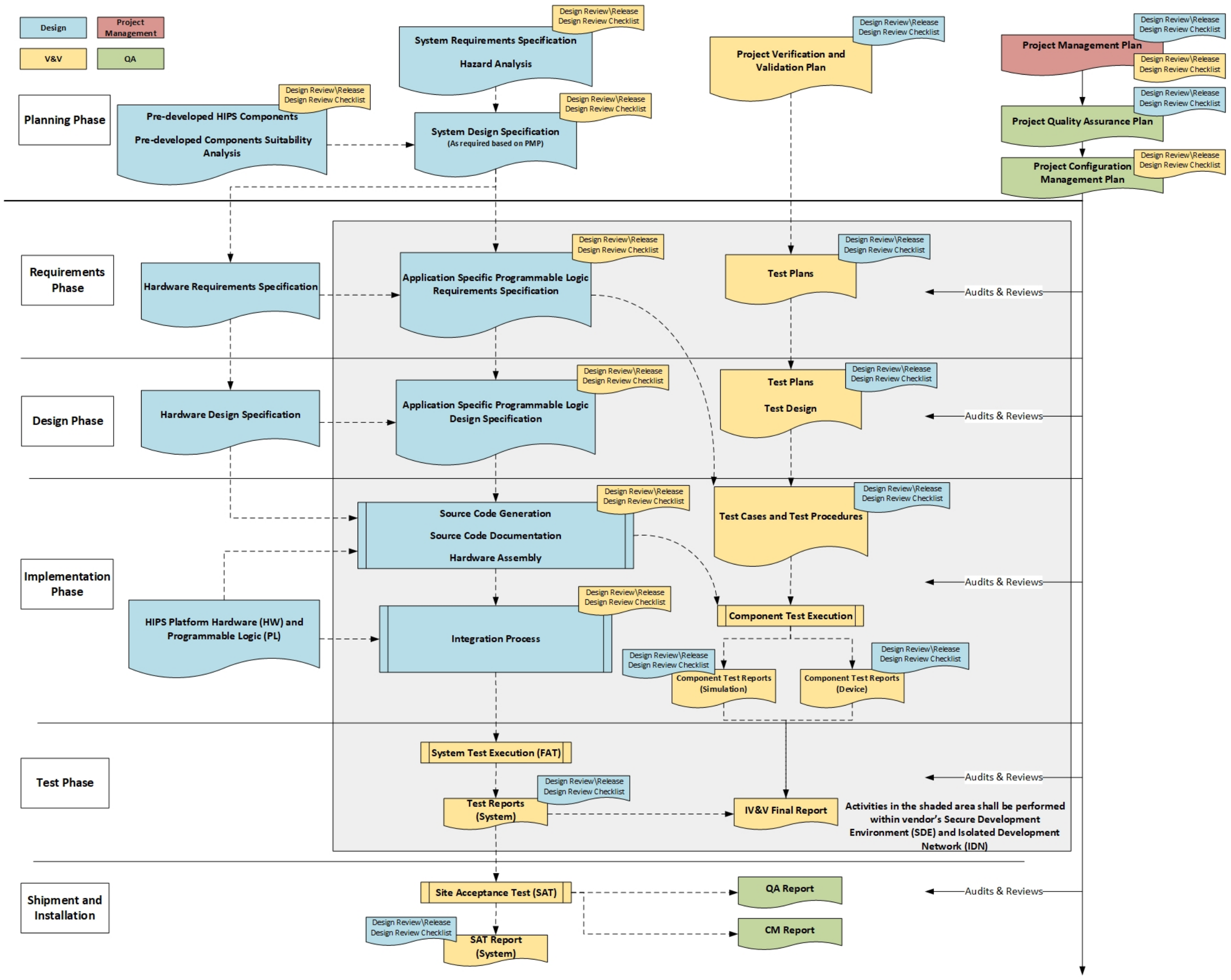


Figure 7.4-3 – TRPS and ESFAS Programmable Logic Lifecycle Process


Design
Project Management
V&V
QA
Planning Phase
Requirements Phase
Design Phase
Implementation Phase
Test Phase
Shipment and Installation
Design Review\Release Design Review Checklist
System Requirements Specification
Hazard Analysis
Pre-developed HIPS Components
Pre-developed Components Suitability Analysis
System Design Specification (As required based on PMP)
Project Verification and Validation Plan
Project Management Plan
Project Quality Assurance Plan
Project Configuration Management Plan
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

7.5 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

7.5.1 SYSTEM DESCRIPTION

The engineered safety features actuation system (ESFAS) is a single, safety-related instrumentation and control (I&C) system that provides monitoring and actuation functions throughout the SHINE main production facility.

The ESFAS performs various detection, logic processing, control, and actuation functions credited by the SHINE safety analysis described in Chapter 13 as required to prevent the occurrence or mitigate the consequences of design basis events within the main production facility. The ESFAS provides sense, command, and execute functions necessary to maintain the facility confinement strategy and provides process actuation functions required to shut down 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.

The ESFAS is built using the highly integrated protection system (HIPS) platform as described in Subsection 7.4.5. ESFAS equipment is separated into three divisions (A, B, and C). The ESFAS redundantly receives safety-related inputs from field instrumentation (input devices) to either two divisions (A and B) or all three divisions, dependent on the input variable. The input signals are provided to the ESFAS safety function modules (SFMs). More than one input device provides a signal to each SFM. The inputs are allocated to the different SFMs within a division as described in the technical specifications. Each SFM can be placed in maintenance bypass or in a trip state by use of the out-of-service (OOS) switch located on the front of the SFM and an associated trip/bypass switch located below the SFM, as described in Subsection 7.5.4.4. Placing an SFM in trip or bypass causes all channels associated with that SFM to be placed in trip or bypass, respectively.

The ESFAS bypass logic is implemented in all three divisions using scheduling, bypass, and voting modules (SBVMs) for divisions A and B, or scheduling and bypass modules (SBMs) for division C. The ESFAS voting and actuation logic is implemented in only divisions A and B. For divisions A and B, the three SBVMs, in each division, generate actuation signals when the SFMs in any two of three (or one of two) divisions determine that an actuation is required. Both ESFAS divisions A and B evaluate the input signals from the SFMs in each of three redundant SBVMs. Each SBVM compares the inputs received from the SFMs and generates an appropriate actuation signal if required by two or more of the three (or one or more of the two) divisions.

The output of the three redundant SBVMs in divisions A and B is communicated via three independent safety data buses to the associated equipment interface modules (EIMs). There are two independent EIMs for each actuation component, associated with each division A and B of ESFAS. The EIMs compare inputs from the three SBVMs and initiate an actuation if two out of three signals agree on the need to actuate. Both EIMs associated with a component are required to be deenergized for the actuation component(s) to fail to their actuated (deenergized) states, with the exception of the process vessel vent system (PVVS) carbon delay bed three-way and outlet isolation valves (Subsections 7.5.3.1.14, 7.5.3.1.15, and 7.5.3.1.16). These valves are energized to actuate.

7.5.2 DESIGN CRITERIA

The SHINE facility design criteria applicable to the ESFAS are stated in Table 3.1-1. The facility design criteria applicable to the ESFAS, and the ESFAS system design criteria, are addressed in this section.

The ESFAS utilizes a HIPS design. The HIPS design is applicable to both the target solution vessel (TSV) reactivity protection system (TRPS) and the ESFAS. The HIPS design is described in Subsection 7.4.5.

7.5.2.1 SHINE Facility Design Criteria

SHINE facility Design Criteria 13 through 19 and 37 through 39 apply to the ESFAS.

7.5.2.1.1 Instrumentation and Controls

> SHINE Design Criterion 13 – Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated transients, and for postulated accidents as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the primary system boundary, the primary confinement and its associated systems, and the process confinement boundary and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating ranges.

The ESFAS monitored variables for performance of design basis functions are presented in Table 7.5-1 and include the instrument range for covering normal and accident conditions, the accuracy for each variable, and the analytical limit. Operation of the ESFAS in response to the analyzed events is presented in Subsection 7.5.4.1.

7.5.2.1.2 Protection System Functions

<u>SHINE Design Criterion 14</u> – The protection systems are designed to: (1) initiate, automatically, the operation of appropriate systems to ensure that specified acceptable target solution design limits are not exceeded as a result of anticipated transients; and (2) sense accident conditions and to initiate the operation of safety-related systems and components.

Operation of the ESFAS in response to the analyzed events is presented in Subsection 7.5.4.1. This section describes the automatic system response to actuation setpoints in monitored variables.

7.5.2.1.3 Protection System Reliability and Testability

<u>SHINE Design Criterion 15</u> – The protection systems are designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection systems are sufficient to ensure that: (1) no single failure results in loss of the protection function, and (2) 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 protection systems are designed to permit periodic testing, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

High functional reliability is addressed in SHINE Design Criterion 19 (Subsection 7.5.2.1.7). The HIPS design incorporates predictability and repeatability principles to ensure an extremely high probability of accomplishing safety functions (Subsection 7.4.5.2.3).

The ESFAS contains capabilities for inservice testing for those functions that cannot be tested while the associated equipment is out of service (Subsection 7.5.4.5).

The ESFAS design utilizes functional independence; 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 (Subsection 7.4.5.2.1).

The ESFAS consists of two or three divisions of input processing and trip determination (dependent on the monitored variable) and two divisions of actuation logic arranged such that no single failure can prevent a safety actuation when required (Subsection 7.5.3.3). A single failure analysis of the ESFAS was performed in accordance with IEEE Standard 379-2000 (IEEE-2000).

The maintenance bypass function allows an individual safety function module to be removed from service for required testing (Subsection 7.5.4.4). Self-test features are provided for components that do not have setpoints or tunable parameters. The discrete logic of the actuation and priority logic (APL) of the EIM does not have self-test capability but is instead functionally tested (Subsection 7.5.4.5). Calibration, testing, and diagnostics is addressed in Section 8.0 of Topical Report TR-1015-18653 (NuScale, 2017).

7.5.2.1.4 Protection System Independence

<u>SHINE Design Criterion 16</u> – The protection systems are designed to ensure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated

accident conditions on redundant channels, do not result in loss of the protection function or are demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, are used to the extent practical to prevent loss of the protection function.

The ESFAS control and logic functions operate inside of the facility control room where the environment is mild, not exposed to the irradiation process, and is protected from earthquakes, tornadoes, and floods (Subsections 7.5.3.4 and 7.5.3.5). The 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, extending from the sensor to the devices actuating the protective function (Subsection 7.4.5.2.1). The architecture provides two diverse methods for an actuation of the safety functions at the division level, automatic and manual, and field programmable gate arrays (FPGAs) in each division are of a different physical architecture to prevent common cause failure (Subsections 7.4.5.2.4 and 7.5.3.6).

7.5.2.1.5 Protection System Failure Modes

> SHINE Design Criterion 17 – The protection systems are designed to fail into a safe state if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments are experienced.

Controlled components associated with safety actuations are designed to go to their safe state when deenergized (Table 7.5-2). The ESFAS equipment is qualified for radiological and environmental hazards present during normal operation and postulated accidents (Subsection 7.5.3.4).

7.5.2.1.6 Separation of Protection and Control Systems

> SHINE Design Criterion 18 – The protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.

Nonsafety-related inputs to the ESFAS from the PICS are designed and controlled so they do not prevent the ESFAS from performing its safety functions (Subsection 7.5.3.2).

7.5.2.1.7 Protection Against Anticipated Transients

> SHINE Design Criterion 19 – The protection systems are designed to ensure an extremely high probability of accomplishing their safety functions in the event of anticipated transients.

The ESFAS design utilizes functional independence; 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 (Subsection 7.4.5.2.1). The ESFAS includes redundancy such that no single failure can prevent a safety actuation when required (Subsection 7.5.3.3). The architecture provides two diverse methods for an actuation of the safety functions at the division level, automatic and manual, and FPGAs in each division are of a different physical architecture to prevent common cause failure (Subsections 7.4.5.2.4 and 7.5.3.6).

7.5.2.1.8 Criticality Control in the Radioisotope Production Facility

SHINE Design Criterion 37 – Criticality in the radioisotope production facility is prevented by physical systems or processes and the use of administrative controls. Use of geometrically safe configurations is preferred. Control of criticality adheres to the double contingency principle. A criticality accident alarm system to detect and alert facility personnel of an inadvertent criticality is provided.

The ESFAS provides two safety functions as required by the SHINE criticality safety program described in Section 6b.3. The VTS Safety Actuation safety function stops the transfer of target solution or other radioactive solutions upon indication of potential upset conditions (Subsection 7.5.3.1.17). Actuation on a VTS vacuum header liquid detection switch signal protects against an overflow of the vacuum lift tanks and potential criticality event (Subsection 7.5.4.1.8). The Dissolution Tank Isolation safety function protects against a criticality event due to excess fissile material in a non-favorable geometry system (Subsection 7.5.4.1.18) and prevents overflow of the dissolution tank into the uranium handling glovebox or ventilation system.

7.5.2.1.9 Monitoring Radioactivity Releases

SHINE Design Criterion 38 – Means are provided for monitoring the primary confinement boundary, hot cell, and glovebox atmospheres to detect potential leakage of gaseous or other airborne radioactive material. Potential effluent discharge paths and the plant environs are monitored for radioactivity that may be released from normal operations, including anticipated transients, and from postulated accidents.

The ESFAS monitors for potential radioactivity releases from various areas of the SHINE main production facility. The ESFAS monitors radiation in the radiological ventilation zone 1 (RVZ1) or radiological ventilation zone 2 (RVZ2) facility exhaust (Subsection 7.5.3.1.24), radiation from the outlet of each cell of the supercell (Subsections 7.5.3.1.1 through 7.5.3.1.10), and tritium from the tritium purification system glovebox (SSubsections 7.5.3.1.18, 7.5.3.1.19, and 7.5.3.1.20). Additional radioactivity release monitoring is provided by the TRPS (Section 7.4) and by nonsafety-related radiation monitoring systems (Section 7.7).

7.5.2.1.10 Hydrogen Mitigation

SHINE Design Criterion 39 – Systems to control the buildup of hydrogen that is released into the primary system boundary and tanks or other volumes that contain fission products and produce significant quantities of hydrogen are provided to ensure that the integrity of the system and confinement boundaries is maintained.

The ESFAS monitors variables and provides actuations to prevent and mitigate hydrogen deflagration in various areas in the SHINE main production facility. The TRPS IU cell nitrogen purge signal protects against a loss of hydrogen mitigation capabilities in the IUs (Subsection 7.5.4.1.14). The low PVVS flow signal protects against a loss of hydrogen mitigation capabilities in the RPF (Subsection 7.5.4.1.15). The uninterruptible electrical power supply system (UPSS) loss of external power signal protects against an anticipatory loss of hydrogen mitigation in the IU cell (Subsection 7.5.4.1.19).

7.5.2.2 ESFAS System Design Criteria

7.5.2.2.1 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.

The ESFAS utilizes a HIPS design which is described in Subsection 7.4.5. Unauthorized use of the ESFAS is prevented by required use of a physical key as described in the HIPS design (Subsection 7.4.5.3.3).

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

The ESFAS development design uses a defensive system architecture described in Subsection 7.4.5.3.2 that prevents unauthorized physical and electronic access.

<u>ESFAS Criterion 3</u> – 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.

Access control features prevent unauthorized physical and electronic access to CDAs during the operational phase and during transition from development to operations. Access control, cyber security, and the secure development operating environment are described in Subsection 7.4.4.1.3. Subsection 7.4.4.1.3 also describes prevention of unauthorized access during the development and operational phases. Post-development installation and testing is performed and controlled by the safety-related control system vendor as described in Subsections 7.4.4.1.4 and 7.4.5.4.2.6.

7.5.2.2.2 Software Requirements Development

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

The system design requirements are specified in the system requirements specification which is generated in accordance with the vendor system requirements specification development procedure (Subsection 7.4.5.4.2.1). A system design description is generated to define the system design details. Software requirements development is addressed in Subsection 7.4.4.1.4.

<u>ESFAS Criterion 5</u> – Development of ESFAS software shall follow a formally defined lifecycle process and address potential security vulnerabilities in each phase of the lifecycle.

The programmable logic lifecycle process is described in Subsection 7.4.5.4.2. The lifecycle process includes a Project Security Plan as stated in Subsection 7.4.5.4.2.1. The development process addresses security vulnerabilities (physical and electronic) in the developmental phases of the software and addresses controls to prevent unauthorized physical and electronic access. Programmable logic lifecycle activities are performed within a secure development environment using an isolated development network (Subsections 7.4.5.3.1 and 7.4.5.4.2.2).

> ESFAS Criterion 6 – ESFAS development lifecycle 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.

Programmable logic lifecycle activities necessitate use of a secure development environment using an isolated development network from the Requirements Phase forward (Subsection 7.4.5.4.2.2). Software requirements development, including lifecycle phase-specific security requirements, is addressed in ESFAS Criterion 5.

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

Design basis requirements are specified in the system requirements specification and system design description (Subsection 7.4.5.4.2.1). The lifecycle process includes development of a V&V Plan and Configuration Management Plan to control V&V and configuration management activities (Subsection 7.4.5.4.2.1).

> 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 lifecycle activity group shall be documented.

SHINE has delegated V&V activities related to the safety-related control system development, including V&V documentation, to the vendor. The vendor Project V&V Plan for the system development was tailored and adapted for FPGA technology from the guidance in IEEE Standard 1012-2004 (IEEE, 2004a). The V&V activities are performed using an internal V&V team from within the design organization, as defined in IEEE Standard 1012-2004 (IEEE, 2004a), Annex C.4.4, and is independent of the design team (Subsection 7.4.5.4.5).

> ESFAS Criterion 9 – The ESFAS software lifecycle 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.

The programmable logic lifecycle process addresses design interfaces, which includes addressing any impacts on the safety system, control console, or display instruments during the lifecycle process, as stated in Subsection 7.4.5.4.2.

> 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.

Subsection 7.4.5.4.6.3 addresses compliance with ESFAS Criterion 10 and ensures the correct version of software/firmware is installed in the correct hardware components. The development phase configuration management process is described in Subsection 7.4.5.4.6.1 and states that components of the system (hardware) and programmable logic and its development process data (software) are controlled by the Project Configuration Management Plan. Post-installation phase configuration management is addressed in Subsection 7.4.5.4.6.2.

> 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.

Implementation phase V&V activities (Subsection 7.4.5.4.5.5) verify the design accuracy to accomplish safety functions and include functional verification and timing verification activities. Test phase V&V (Subsection 7.4.5.4.5.6) includes system functional, interface, and performance testing.

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

The vendor utilizes a Project Risk Management Plan for development of the ESFAS, as described in Subsection 7.4.5.4.8. Risk identification activities occur throughout the project lifecycle. Identified risks are documented in a project risk register and actions are developed to address identified risks or vulnerabilities.

> 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.

The developmental process for creating the safety-related ESFAS has been delegated to SHINE's safety-related control system vendor (Subsection 7.4.5.3.1), including any modifications to the system logic after initial development (Subsection 7.4.4.1.4). 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 (Subsection 7.4.5.4.1).

7.5.2.2.3 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.

The ESFAS equipment is installed in the seismically qualified portion of the main production facility where it is protected from earthquakes, tornadoes, and floods. The ESFAS equipment is Seismic Category I, designed in accordance with Section 8 of IEEE Standard 344-2013 (IEEE, 2013) (Subsections 7.5.3.4 and 7.5.3.5). The ESFAS control and logic equipment is located in a mild operating environment inside the facility control room, protected from radiological and environmental hazards during normal operation, maintenance, testing, and postulated accidents, and cables and sensors outside the facility control room are designed for their respective environments (Subsection 7.5.3.4).

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

The ESFAS logic diagrams (Figure 7.5-1) display where the manual actuation is brought into the logic. Manual controls and nonsafety control system inputs come individually into the APL and are downstream of the programmable logic portion of the ESFAS architecture shown in Figure 7.1-3 (Subsection 7.4.5.2.4).

7.5.2.2.4 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.

The ESFAS consists of three divisions of input processing and trip determination and two divisions of actuation logic arranged such that no single failure within the ESFAS results in the loss of the protective function. Redundancy is addressed in Subsection 7.4.5.2.2. Nonsafety-related inputs into the ESFAS are designed and controlled so they do not prevent the ESFAS from performing its safety functions. Single failure is additionally addressed in Subsection 7.5.3.3.

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

The ESFAS is comprised of three divisions of signal conditioning and trip determination, and two divisions of voting and actuation. This configuration allows for the architecture to handle a single failure of a field input, signal conditioning circuit, or trip determination and still maintain the ability to provide the needed number of valid inputs to the voting circuitry. A single failure of the voting logic or the actuation logic is also acceptable within the configuration as the redundant division of voting logic and actuation logic is capable of performing the safety function. Functional independence is addressed in Subsection 7.4.5.2.1 and redundancy is addressed in Subsection 7.4.5.2.2.

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.

The ESFAS provides separate communication paths to the PICS display systems from each of the three ESFAS divisions. ESFAS divisions A and B are powered from a separate division of the UPSS; ESFAS division C receives auctioneered power from both UPSS divisions A and B. This redundancy in communication paths and power sources ensures no single failure concurrent with a design basis event prevents operators from being presented necessary information (Subsection 7.5.3.3). Loss of external power to the PICS is described in Subsection 7.3.3.6.

7.5.2.2.5 Independence

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

Safety-related inputs to the ESFAS which originate within a specific division of the ESFAS are input to, and processed in, only the same division prior to being provided to any other division of the system for voting purposes (Subsection 7.4.5.2.1).

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

The APL, which is constructed of discrete components and part of the equipment interface module, is designed to provide priority to safety-related signals over nonsafety-related signals. Division A and division B priority logic of the ESFAS prioritizes the following ESFAS 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 Actuation, and (2) PICS nonsafety control signals (Subsection 7.5.3.11). When the enable nonsafety control is not active, the nonsafety-related control signals are ignored. If the enable nonsafety control is active, and no automatic safety actuation or manual actuation command is present, the nonsafety control signal can control the component (Subsection 7.5.3.2).

> 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.

The 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 (Subsection 7.4.5.2.1) and nonsafety-related ESFAS inputs and outputs are routed in non-divisional cable raceways and are segregated from safety-related inputs and outputs (Subsection 7.5.3.8). Wiring for redundant divisions uses physical separation and isolation to provide independence for circuits (Subsection 7.4.5.2.1) in accordance with IEEE Standard 384-2008 (IEEE, 2008). HIPS communication paths are designed such that a single failure does not cause all safety functions of a division to be inoperable (Subsection 7.4.4.1.2).

> 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.

The 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 (Subsection 7.4.5.2.1) and nonsafety-related ESFAS inputs and outputs are routed in non-divisional cable raceways and are segregated from safety-related inputs and outputs (Subsection 7.5.3.8). Wiring for redundant divisions uses physical separation and isolation to provide independence for circuits (Subsection 7.4.5.2.1) in accordance with IEEE Standard 384-2008 (IEEE, 2008).

> 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.

HIPS communication paths are designed with simplicity such that a single failure does not cause all safety functions of a division to be inoperable. The design uses triple redundant communication paths. A single failure does not cause all safety functions of that division to be inoperable (Subsection 7.4.4.1.2). Communication ports that are for communication outside of a HIPS chassis implement the one-way communication with hardware (Subsection 7.4.5.3.2).

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

ESFAS data communications protocol is detailed in Section 7.5.1 of Topical Report TR-1015-18653 (NuScale, 2017). The protocol is used on the safety buses as a simple master-slave communication protocol and employs a cyclic redundancy checksum feature to ensure the integrity of the communicated information between modules. Data communications is discussed in Subsection 7.4.5.2.5.

<u>ESFAS Criterion 25</u> – The timing of ESFAS data communications shall be deterministic.

The maximum response time of the ESFAS components from when an input signal exceeds a predetermined setpoint to the time that the ESFAS deenergizes the equipment interface module output switching for actuated components is conservatively set to a maximum of 500 milliseconds (Subsection 7.4.5.2.3).

<u>ESFAS Criterion 26</u> – 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 communication protocols are verified as conforming to the validated protocol specifications by the Project V&V Plan (Subsection 7.4.5.4.5).

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

For communications independence, the ESFAS platform is designed such that each safety division functions independently of other safety divisions. With the exception of interdivisional voting, communication within a division does not rely on communication outside the respective division to perform the safety function. Safety-related inputs to the ESFAS which originate within a specific division of the ESFAS are input to, and processed in, only the same division prior to being provided to any other division of the system for voting purposes (Subsection 7.4.5.2.1).

7.5.2.2.6 Prioritization of Functions

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

Priority is provided to automatic and manual safety-related actuation signals over nonsafety-related signals as described in Subsection 7.5.3.11.

7.5.2.2.7 Fail-Safe

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

Controlled components associated with safety actuations are designed to go to their safe state when deenergized (Table 7.5-2).

7.5.2.2.8 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, facility design, and expected maintenance practices.

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 further described in Subsections 7.2.1 and 7.5.3.10.

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

Setpoints in the ESFAS are based on a documented methodology that ensures adequate margin exists between setpoints and analytical limits or safety limits. The setpoint methodology is further described in Subsections 7.2.1 and 7.5.3.10.

> 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.

There are no safety functions in the ESFAS that use multiple setpoints.

> 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.

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 further described in Subsections 7.2.1 and 7.5.3.10. Setpoint analysis parameters typically consider instrument precision, sensitivity, accuracy, loop uncertainties, and computational errors.

7.5.2.2.9 Operational Bypass, Permissives and Interlocks

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

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2). The ESFAS incorporates the Facility Master Operating Permissive key switch in the system design to select operation in the normal, unsecured mode or operationally secured (Subsection 7.5.4.3).

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.

The ESFAS has no operational bypasses included in the design, and therefore no interlocks are required to prevent operator actions from defeating an automatic safety function (Subsection 7.5.4.2).

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

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2). PICS inputs may be bypassed with the enable nonsafety switch, as described in Subsection 7.5.3.2.

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

Manual safety actuations are shown in the logic diagrams (Figure 7.5-1). There are no conditions that allow manually initiated ESFAS safety functions to be bypassed.

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.

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2). Use of the maintenance bypass either preserves the single failure criterion where three channels are provided or is performed in accordance with technical specification requirements (Subsection 7.5.4.4).

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.

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2). A maintenance bypass is provided and utilized for maintenance and testing purposes (Subsection 7.5.4.4).

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.

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2).

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)

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2).

> <u>ESFAS Criterion 42</u> – 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.

Where three channels are provided, taking a SFM out of service preserves the single failure criterion for variables associated with that SFM. In cases where only two channels are provided, taking a channel out of service will actuate the associated safety function. For testing purposes, placing a channel in maintenance bypass will be allowed by technical specifications for up to two hours to perform required testing. Two hours is considered acceptable due to the continued operability of the redundant channel(s) and the low likelihood that an accident would occur in those two hours (Subsection 7.5.4.4).

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

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2). Any ESFAS channels placed in maintenance bypass for maintenance or testing, or removed from maintenance bypass, will be displayed to the operators in the facility control room through the monitoring and indication bus to the PICS (Subsection 7.5.4.4). The PICS is described in Section 7.3 and operator displays and human factors considerations are addressed in Section 7.6.

7.5.2.2.10 Completion of Protective Actions

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

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. Completion of protective actions is described in Subsection 7.5.3.2.

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

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. Completion of protective actions is described in Subsection 7.5.3.2.

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

A safety-related enable nonsafety switch (when enabled) allows a facility operator to control the output state of the ESFAS with a hardwired binary control signal from the nonsafety-related controls. 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 (Subsection 7.5.3.2). Additionally, safety-related signals are prioritized over nonsafety-related signals (Subsection 7.5.3.11).

7.5.2.2.11 Equipment Qualification

> <u>ESFAS Criterion 47</u> – 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.

ESFAS rack mounted equipment is installed in a mild operating environment and is designed to meet the environmental conditions described in Subsection 7.5.3.4. 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 IEEE Standard 1050-2004 (IEEE, 2004b).

7.5.2.2.12 Surveillance

> <u>ESFAS Criterion 48</u> – 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.

The ESFAS design supports testing, maintenance, and calibration to ensure operability as described in Subsections 7.5.4.4 and 7.5.4.5. Testing performed during operation is controlled in accordance with the technical specifications to ensure that at least one division of the ESFAS is capable of performing its safety functions when required.

> <u>ESFAS Criterion 49</u> – 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.

The ESFAS design supports testing, maintenance, and calibration, as described in Subsections 7.5.4.4 and 7.5.4.5. End-to-end testing of the entire ESFAS platform can be performed through overlap testing. ESFAS components have self-testing capabilities, except the discrete APL of the EIM which is functionally tested.

> <u>ESFAS Criterion 50</u> – 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.

The ESFAS design supports testing, maintenance, and calibration, as described in Subsections 7.5.4.4 and 7.5.4.5. Testing intervals are established in the technical specifications (Subsection 7.5.4.6).

7.5.2.2.13 Classification and Identification

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

Each ESFAS cable and component is uniquely identified in accordance with SHINE component numbering guidelines. The unique identification number indicates the applicable system and division (Subsection 7.5.3.9).

7.5.2.2.14 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.

Human factors is a design consideration for development of the ESFAS. Changes to the design throughout the lifecycle process include human factors considerations (Subsection 7.4.5.4.2). Human factors design is described in Subsection 7.5.3.6.

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

The ESFAS provides manual safety actuation capability as shown in the logic diagrams. Figure 7.5-1 displays where the manual actuation is brought into the logic. Human factors design in support of manual initiation is described in Subsection 7.5.3.6.

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.

To support the use of manual safety actuations, the ESFAS includes isolated outputs for each safety-related instrument channel to provide monitoring and indication information to the PICS (Subsection 7.5.3.6). See also ESFAS Criterion 45 regarding manual operator reset in Subsection 7.5.2.2.10.

7.5.2.2.15 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.

The safety-related ESFAS is designed, fabricated, erected, and tested by SHINE's safety-related control system vendor in accordance with the vendor's Project Quality Assurance Plan (Subsection 7.4.4.1.4). SHINE is responsible for oversight of the vendor and maintaining the vendor as an approved supplier on the SHINE approved supplier list (Subsection 7.4.5.4.1).

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).

The ESFAS design conforms to the guidance of ANSI/ANS 15.8-1995 (ANSI/ANS, 1995) as endorsed by Regulatory Guide 2.5 (USNRC, 2010) (Subsection 7.5.3.12).

7.5.3 DESIGN BASIS

The ESFAS monitors process variables and provides automatic initiating signals in response to off-normal conditions, providing protection against unsafe conditions in the main production facility.

Subsection 7.5.4 addresses the specific variables that provide input into the ESFAS, the instrument range for covering normal and accident conditions, the accuracy for each variable, the analytical limit, and response time. The conditions or operating modes applicable to each variable monitored by the ESFAS are described in the technical specifications.

7.5.3.1 Safety Functions

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 facility operating conditions applicable to each automatic ESFAS safety function listed in this subsection are specified in the technical specifications.

7.5.3.1.1 Supercell Area 1 (PVVS Area) Isolation

Supercell Area 1 (PVVS Area) Isolation is relied upon as a safety-related control for radioactivity release scenarios similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3), and to provide for a consistent confinement strategy for all ten cells of the supercell.

A Supercell Area 1 (PVVS Area) Isolation initiates the following safety functions:

- Deenergize RVZ2 supercell area 1 (PVVS area) inlet isolation dampers
- Deenergize 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenarios 1, 2, 3, and 13).

A 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 [ ]$^{PROP/ECI}$ 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

7.5.3.1.3 Supercell Area 3 (Purification Area A) Isolation

Supercell Area 3 (Purification Area A) Isolation is relied upon as a safety-related control for radioactivity release scenarios similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3), and to provide for a consistent confinement strategy for all ten cells of the supercell.

A 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 is relied upon as a safety-related control for radioactivity release scenarios similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3), and to provide for a consistent confinement strategy for all ten cells of the supercell.

A 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 is relied upon as a safety-related control for radioactivity release scenarios similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3), and to provide for a consistent confinement strategy for all ten cells of the supercell.

A 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenarios 1, 2, 3, and 13).

A 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 [ ]$^{PROP/ECI}$ 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenarios 1, 2, 3, and 13).

A 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 [ ]$^{PROP/ECI}$ 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 is relied upon as a safety-related control for radioactivity release scenarios similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3), and to provide for a consistent confinement strategy for all ten cells of the supercell.

A 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 is relied upon as a safety-related control for radioactivity release scenarios similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3), and to provide for a consistent confinement strategy for all ten cells of the supercell.

A 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenarios 4, 5, 6, and 7).

A 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 [ ]$^{\text{PROP/ECI}}$ Isolation

MEPS A [ ]$^{\text{PROP/ECI}}$ Isolation is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenario 14).

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

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

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

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

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

MEPS B [ ]$^{\text{PROP/ECI}}$ Isolation is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenario 14).

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

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

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

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

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

MEPS C [ ]$^{\text{PROP/ECI}}$ Isolation is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenario 14).

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

- Deenergize MEPS [ ]$^{\text{PROP/ECI}}$ C inlet isolation valves
- Deenergize MEPS [ ]$^{\text{PROP/ECI}}$ 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF fire events (Subsection 13b.1.2.5, Scenario 1).

A 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF fire events (Subsection 13b.1.2.5, Scenario 1).

A 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF fire events (Subsection 13b.1.2.5, Scenario 1).

A 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenarios 8, 10, 11, 12, and 16), and for criticality safety requirements (Subsection 6b.3.2.5).

A 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 break valves
- Deenergize MEPS A extraction column wash supply valve
- Deenergize MEPS A extraction column eluent valve
- Deenergize MEPS A [ ]PROP/ECI wash supply valve
- Deenergize MEPS A [ ]PROP/ECI eluent valve
- Deenergize MEPS B extraction column wash supply valve
- Deenergize MEPS B extraction column eluent valve
- Deenergize MEPS B [ ]PROP/ECI wash supply valve
- Deenergize MEPS B [ ]PROP/ECI eluent valve
- Deenergize MEPS C extraction column wash supply valve
- Deenergize MEPS C extraction column eluent valve
- Deenergize MEPS C [ ]PROP/ECI wash supply valve
- Deenergize MEPS C [ ]PROP/ECI eluent valve
- Deenergize IXP recovery column wash supply valve
- Deenergize IXP recovery column eluent valve
- Deenergize IXP [ ]PROP/ECI wash supply valve
- Deenergize IXP [ ]PROP/ECI eluent valve
- Deenergize IXP FNHS supply valve
- Deenergize 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

7.5.3.1.18 TPS Train A Isolation

TPS Train A Isolation is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for external events (Subsection 13a2.1.6, Scenario 3), and for facility specific tritium purification system events (Subsection 13a2.1.12, TPS Scenario 1).

A TPS Train A Isolation initiates the following safety functions:

- Deenergize TPS train A glovebox pressure control exhaust isolation valve
- Deenergize vacuum/impurity treatment subsystem (VAC/ITS) train A process vent ITS isolation valves (TPS train A ITS isolation valves)
- Deenergize TPS train A helium air operated valve (AOV) supply isolation valve
- Deenergize TPS train A helium solenoid operated valve (SOV) supply isolation valve
- Deenergize RVZ2 TPS room supply isolation dampers
- Deenergize RVZ2 TPS room exhaust isolation dampers
- Deenergize VAC/ITS train A process vent vacuum isolation valves (TPS train A vacuum isolation valves)
- Deenergize IU Cell 1 TPS Actuation
- Deenergize 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for external events (Subsection 13a2.1.6, Scenario 3), and for facility specific tritium purification system events (Subsection 13a2.1.12, TPS Scenario 1).

A TPS Train B Isolation initiates the following safety functions:

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

- TRPS IU Cell 4 TPS Actuation
- TRPS 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for external events (Subsection 13a2.1.6, Scenario 3), and for facility specific tritium purification system events (Subsection 13a2.1.12, TPS Scenario 1).

A TPS Train C Isolation initiates the following safety functions:

- Deenergize TPS train C glovebox pressure control exhaust isolation valve
- Deenergize VAC/ITS train C process vent ITS isolation valves (TPS train C ITS isolation valves)
- Deenergize TPS train C helium AOV supply isolation valve
- Deenergize TPS train C helium SOV supply isolation valve
- Deenergize RVZ2 TPS room supply isolation dampers
- Deenergize RVZ2 TPS room exhaust isolation dampers
- Deenergize VAC/ITS train C process vent vacuum isolation valves (TPS train C vacuum isolation valves)
- TRPS IU Cell 6 TPS Actuation
- TRPS IU Cell 7 TPS Actuation
- TRPS 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 is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for facility specific tritium purification system events (Subsection 13a2.1.12, TPS Scenario 3 and TPS Scenario 4).

A TPS Process Vent Actuation initiates the following safety functions:

- Deenergize TPS train A vacuum isolation valves
- Deenergize TPS train A ITS isolation valves
- Deenergize TPS train B vacuum isolation valves
- Deenergize TPS train B ITS isolation valves
- Deenergize TPS train C vacuum isolation valves
- Deenergize TPS train C ITS isolation valves
- TRPS IU Cell 1 TPS Actuation
- TRPS IU Cell 2 TPS Actuation
- TRPS IU Cell 3 TPS Actuation
- TRPS IU Cell 4 TPS Actuation
- TRPS IU Cell 5 TPS Actuation
- TRPS IU Cell 6 TPS Actuation
- TRPS IU Cell 7 TPS Actuation
- TRPS 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 an ESFAS loss of external power actuation signal to the TRPS subsystem associated with each IU cell upon receipt of a UPSS loss of external power signal to initiate an IU Cell Nitrogen Purge within the TRPS (Subsection 7.4.3.1.2).

An IU Cell Nitrogen Purge is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for insertion of excess reactivity events (Subsection 13a2.1.12, Scenario 5), and detonation and deflagration in the primary system boundary (Subsection 13a2.1.9, Scenario 1).

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

An RPF Nitrogen Purge is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for external events (Subsection 13a2.1.6, Scenario 7).

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 PVVS north header valves
- Deenergize N2PS PVVS 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

An RCA Isolation is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenarios 8, 10, 11, 12, and 16).

RCA Isolation initiates the following safety functions:

- Deenergize RVZ1 RCA exhaust isolation dampers
- Deenergize RVZ2 RCA exhaust isolation dampers
- Deenergize RVZ2 RCA supply isolation dampers
- Deenergize RVZ2 TPS room supply isolation dampers
- Deenergize RVZ2 TPS room exhaust isolation dampers
- Deenergize RVZ3 transfer isolation dampers shipping/receiving IF
- Deenergize RVZ3 transfer isolation dampers shipping/receiving RPF
- Deenergize RVZ3 transfer isolation dampers main RCA ingress/egress
- Deenergize RVZ3 transfer isolation dampers RPF emergency exit
- Deenergize RVZ3 transfer isolation dampers IF emergency exit
- Deenergize RVZ3 transfer isolation dampers mezzanine 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
- TPS Process Vent Actuation

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

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

7.5.3.1.25 Extraction Column A Alignment Actuation

Extraction Column A Alignment Actuation is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenario 15).

An Extraction Column A Alignment Actuation initiates the following safety functions:

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

7.5.3.1.26 Extraction Column B Alignment Actuation

Extraction Column B Alignment Actuation is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenario 15).

An Extraction Column B Alignment Actuation initiates the following safety functions:

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

7.5.3.1.27 Extraction Column C Alignment Actuation

Extraction Column C Alignment Actuation is relied upon as a safety-related control in accordance with the SHINE safety analysis described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenario 15).

An Extraction Column C Alignment Actuation initiates the following safety functions:

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

7.5.3.1.28 IXP Alignment Actuation

An IXP Alignment Actuation is relied upon as a safety-related control for column misalignment scenarios similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3, Scenario 15).

An 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 is relied upon as a safety-related control for preventing criticality events (Subsection 6b.3.2.4).

A 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 TSPS air inlet isolation valve
- Deenergize TSPS RVZ1 exhaust isolation valve

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

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

7.5.3.2 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.

7.5.3.3 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.

Nonsafety-related inputs into the ESFAS are designed and controlled so they do not prevent the ESFAS from performing its safety functions. The only nonsafety inputs into the ESFAS are those from the PICS for controls and monitoring/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 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.

Situations exist in the design where the ESFAS only actuates a Division A component and there is no corresponding Division B component, or there is a passive check valve credited as a redundant component. These situations are considered acceptable since the safety function includes a separate, redundant and passive component (i.e., check valve) which does not need to be monitored or manipulated by the ESFAS.

Each input variable to the ESFAS 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 or the variable is used only for actuated component position indication), 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.

The ESFAS provides separate communication paths to the PICS display systems from each of the three ESFAS divisions. ESFAS divisions A and B are powered from a separate division of the UPSS; ESFAS division C receives auctioneered power from both UPSS divisions A and B.

7.5.3.4 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, and is not subject to operational cycling. 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.

7.5.3.5 Seismic, Tornado, Flood

The ESFAS equipment is installed in the seismically qualified portion of the main production facility where it is protected from earthquakes, tornadoes, and floods. The ESFAS equipment is Seismic Category I, designed in accordance with Section 8 of IEEE Standard 344-2013 (IEEE, 2013) (Subsection 7.5.3.12).

7.5.3.6 Human Factors

The ESFAS provides manual actuation capabilities for the safety functions identified in Subsection 7.5.3.1, except for the IU Cell Nitrogen Purge signal which originates in the TRPS, via the following manual push buttons located on the main control board:

- RCA Isolation
- Supercell Isolation (performs Supercell Areas 1 through 10 Isolations and MEPS A/B/C [ ]PROP/ECI Isolations)
- VTS Actuation
- TPS Isolation (performs TPS Train A/B/C Isolation and TPS Process Vent Isolation)
- Carbon Delay Bed Group 1 Isolation
- Carbon Delay Bed Group 2 Isolation
- Carbon Delay Bed Group 3 Isolation
- Extraction Column A Alignment Actuation
- Extraction Column B Alignment Actuation
- Extraction Column C Alignment Actuation
- IXP Alignment Actuation
- RPF Nitrogen Purge
- Dissolution Tank Isolation

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

Operator display criteria and design are addressed in Section 7.6.

7.5.3.7 Loss of External Power

The ESFAS is powered from the 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.

Controlled components associated with safety actuations are designed to go to their safe state when deenergized. On a loss of power to the ESFAS, the ESFAS deenergizes actuation components to the positions defined in Table 7.5-2.

ESFAS response to a loss of external power signal is discussed in Subsection 7.5.4.1.19.

7.5.3.8 Fire Protection

The ESFAS design utilizes physical separation to minimize the effects from fire or explosion. Safety-related ESFAS equipment in different divisions is located in separate fire areas when practical. Exceptions include components for all three divisions located in the facility control room and in other locations where end devices are installed.

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 cables are routed along the south side of the RPF to the facility control room and Division B cables are routed on the north side of the RPF. Where possible, conduit is routed subgrade to provide additional separation. Instrument transmitters are located in separate areas: A and C instrumentation is located primarily on the east side of the G-line wall, while Division B is located along the west side of the wall.

Division A and C ESFAS cabinets are separated by a minimum of four feet and are located on the opposite side of the facility control room from where Division B cabinets are located. Portable Class A and Class C fire extinguishers are located in the control room to extinguish fires originating within a cabinet, console, or connecting cables. Wet sprinklers are not used in the facility control room to avoid potentially impairing the ability of the ESFAS to perform its safety functions.

Noncombustible and heat resistant materials are used whenever practical in the ESFAS design, particularly in locations such as confinement boundaries and the facility control room. Use of materials that release toxic or corrosive gases under combustion is minimized.

Nonsafety-related ESFAS inputs and outputs are routed in non-divisional cable raceways and are segregated from safety-related inputs and outputs. Spatial separation between cable and raceway groups is in accordance with Section 5.1.1.2, Table 1 of Section 5.1.3.3, and Table 2 of Section 5.1.4 of IEEE Standard 384-2008 (IEEE, 2008) (Subsection 7.5.3.12).

7.5.3.9 Classification and Identification

Each ESFAS cable and component is uniquely identified in accordance with the SHINE component numbering guideline. The unique identification number includes, but is not limited to, system designation (code), equipment train, and division.

7.5.3.10 Setpoints

Conservative setpoints for the ESFAS monitored variables are established based on documented analysis methodology (Subsection 7.2.1). Setpoint analysis parameters typically consider instrument precision, sensitivity, accuracy, loop uncertainties, and computational errors. Adequate margin is required between the setpoints and the associated safety limits to ensure the protective action is initiated prior to the safety limit being exceeded. The setpoint values are derived from approved system design technical reports, design calculations, uncertainty calculations, and technical specifications.

7.5.3.11 Prioritization of Functions

The APL (which is constructed of discrete components and part of the equipment interface module) is designed to provide priority to safety-related signals over nonsafety-related signals. Division A and Division B priority logic of the ESFAS prioritizes the following ESFAS 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

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.

7.5.3.12 Design 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 ESFAS Criterion 14.
2) IEEE Standard 379-2000, IEEE Standard Application of Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (IEEE, 2000); invoked as guidance to meet SHINE Design Criterion 15.
3) IEEE Standard 384-2008, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (IEEE, 2008); invoked as guidance for separation of safety-related and nonsafety-related cables and raceways to meet ESFAS Design Criteria 21 and 22, and 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 meet ESFAS Design Criterion 47 and 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).
6) IEEE Standard 1012-2004, IEEE Standard for Software Verification and Validation (IEEE 2004a); invoked as guidance to meet ESFAS Design Criterion 8.

7.5.4 OPERATION AND PERFORMANCE

Subsection 7.5.4 discusses the operation of the ESFAS.

The ESFAS design basis functions utilize redundant logic to ensure safe and reliable operation and to prevent a single failure from defeating the intended function. Additional information related to the effects of single failure, reliability, redundancy, and independence can be found in Subsection 7.5.2.

7.5.4.1 Monitored Variables and Response

Table 7.5-1 identifies specific variables that provide input into the ESFAS and includes the instrument range for covering normal and accident conditions, the accuracy for each variable, the analytical limit, and response time. A discussion of each variable (signal input) and the system response is provided in this section.

7.5.4.1.1 High RVZ1/2 RCA Exhaust Radiation

The high RVZ1/2 RCA exhaust radiation signal protects against confinement leakage or accidents that could potentially result in excess radiation doses to the workers or to the public (Subsection 13b.1.2.3, Scenarios 8, 10, 11, 12, and 16). The signal is generated by ESFAS when an RVZ1/2 RCA exhaust radiation input exceeds the high level setpoint. The RZV1/2 RCA exhaust radiation is measured by an analog interface on three different channels in RVZ1 and three different channels in RVZ2, one channel of each type for each division of ESFAS. When two-out-of-three or more high RVZ1 or two-out-of-three or more high RVZ2 RCA exhaust radiation channels are active, then an RCA Isolation is initiated.

7.5.4.1.2 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 signal is used to indicate potential radioactivity releases in the PVVS cell similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3). The signal is generated by ESFAS when a PVVS cell radiation input exceeds the high level setpoint. 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.

7.5.4.1.3 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 (Subsection 13b.1.2.3, Scenarios 1, 2, 3, and 13). The signal is generated by ESFAS when a MEPS extraction cell radiation input exceeds the high level setpoint. 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.

7.5.4.1.4 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 (Subsection 13b.1.2.3, Scenarios 4, 5, 6, and 7). The signal is generated by ESFAS when an IXP extraction cell radiation input exceeds the high level setpoint. 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.

7.5.4.1.5 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 signal is used to indicate potential radioactivity releases in the purification or packaging cells similar to those described in Chapter 13 for RPF critical equipment malfunction events (Subsection 13b.1.2.3). The signal is generated by ESFAS when a purification or packaging cell radiation input exceeds the high level setpoint. 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.

7.5.4.1.6 High MEPS [ ]$^{\text{PROP/ECI}}$ Conductivity

The high MEPS [ ]$^{\text{PROP/ECI}}$ conductivity signal protects against leakage of high radiation solutions into the [ ]$^{\text{PROP/ECI}}$, which is partially located outside the supercell shielding and could potentially result in an excess dose to the workers (Subsection 13b.1.2.3, Scenario 14). The signal is generated by ESFAS when a MEPS [ ]$^{\text{PROP/ECI}}$ conductivity input exceeds the high level setpoint. The MEPS [ ]$^{\text{PROP/ECI}}$ conductivity is measured by an analog interface on two different channels, one for each Division A and Division B of ESFAS. MEPS [ ]$^{\text{PROP/ECI}}$ conductivity is measured in three locations (MEPS A, B, and C). When one-out-of-two or more high MEPS [ ]$^{\text{PROP/ECI}}$ conductivity channels are active in a given [ ]$^{\text{PROP/ECI}}$ (A, B, or C), then a MEPS [ ]$^{\text{PROP/ECI}}$ Isolation is initiated for that [ ]$^{\text{PROP/ECI}}$.

7.5.4.1.7 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 (Subsection 13b.1.2.5, Scenario 1). The signal is generated by ESFAS for the associated carbon delay bed group (Group 1, 2, or 3) when a carbon delay bed exhaust carbon monoxide input exceeds the high level setpoint. 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.

7.5.4.1.8 VTS Vacuum Header Liquid Detection Switch

The VTS vacuum header liquid detection switch signal protects against an overflow of the vacuum lift tanks to prevent a potential criticality event as described in Subsection 6b.3.2.5. The VTS vacuum header liquid detection switch signal is received by the ESFAS as a discrete input from a liquid detection switch on two different channels, one for each Division A and Division B of ESFAS. When one-out-of-two or more (Division A and Division B) VTS vacuum header liquid detection switch signals are active, then a VTS Safety Actuation is initiated.

7.5.4.1.9 RDS Liquid Detection Switch

The RDS liquid detection switch signal detects leakage or overflow from other tanks and piping (Subsection 13b.1.2.3, Scenarios 8, 10, 11, 12, and 16). The RDS liquid detection switch signal is received by the ESFAS as a discrete input from a liquid detection switch 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.

7.5.4.1.10 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 (Subsection 13a2.1.6.2, Scenario 3 and Subsection 13a2.1.12.2, TPS Scenario 3). The signal is generated by ESFAS when a target chamber exhaust pressure input exceeds the high level setpoint. 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.

7.5.4.1.11 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 (Subsection 13a2.1.6.2, Scenario 3 and Subsection 13a2.1.12.2, TPS Scenario 3). The signal is generated by ESFAS when a target chamber supply pressure input exceeds the high level setpoint. 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.

7.5.4.1.12 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 (Subsection 13a2.1.12.2, TPS Scenario 3 and TPS Scenario 4). The signal is generated by ESFAS when a TPS exhaust to facility stack tritium input exceeds the high level setpoint. 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.

7.5.4.1.13 High TPS Confinement Tritium

The high TPS confinement tritium signal protects against a release of tritium from TPS equipment into the TPS glovebox (Subsection 13a2.1.12.2, TPS Scenario 1). The signal is generated by ESFAS when a TPS confinement tritium input exceeds the high level setpoint. 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.

7.5.4.1.14 TRPS IU Cell Nitrogen Purge

The TRPS IU cell nitrogen purge signal protects against a loss of hydrogen mitigation capabilities in the irradiation units (Subsection 13a2.1.2.2, Scenario 5 and Subsection 13a2.1.9.2, Scenario 1). The signal is generated by an affected TRPS subsystem and provided to the ESFAS when the TRPS initiates an IU Cell Nitrogen Purge, as described in Subsection 7.4.3.1.2. The TRPS IU cell nitrogen purge signal is transmitted as 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.

7.5.4.1.15 Low PVVS Flow

The PVVS flow signal protects against loss of hydrogen mitigation capabilities in the RPF (Subsection 13a2.1.6.2, Scenario 7). The signal is generated by ESFAS when a PVVS flow input exceeds the low level setpoint. 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 low PVVS flow channels are active, then an RPF Nitrogen Purge is initiated.

7.5.4.1.16 MEPS Extraction Column Three-Way Valves Misaligned

The MEPS extraction column three-way valves misalignment signal protects against a misalignment of the extraction column upper and lower three-way valves, degrading one of the barriers preventing misdirection of chemical reagents or target solution (Subsection 13b.1.2.3, Scenario 15). The MEPS extraction column upper and lower three-way valve position indication is received by the ESFAS as a discrete input from redundant position indicating limit switches on two different channels, one for each Division A and Division B of ESFAS, for each three-way valve. When two-out-of-two MEPS extraction column upper and lower three-way valve position indications indicate they are energized, then an Extraction Column Alignment Actuation for that area is initiated.

7.5.4.1.17 IXP Three-Way Valves Misaligned

The IXP 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 signal is used to detect scenarios similar to a MEPS extraction column three-way valve misalignment as described in Subsection 13b.1.2.3, Scenario 15.The IXP three-way valve position indication is received by the ESFAS as a discrete input from redundant position indicating limit switches on two different channels, one for each Division A and Division B of ESFAS, for each three-way valve. When two-out-of-two IXP three-way valve position indications indicate they are energized, then an IXP Alignment Actuation is initiated.

7.5.4.1.18 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 (Subsection 6b.3.2.4). The TSPS dissolution tank level switch signal is received by the ESFAS as a discrete input from level switches 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.

7.5.4.1.19 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), as described in Subsection 13a2.1.9.2, Scenario 1. The UPSS loss of external power signal is received by the ESFAS as 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. While the timer is running, if fewer 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. The ESFAS initiated IU Cell Nitrogen Purge signal is provided to each of the eight TRPS as an ESFAS loss of external power signal as described in Subsection 7.4.4.1.14.

7.5.4.2 Operational Bypass, Permissives, and Interlocks

The ESFAS has no operational bypasses included in the design, and therefore no interlocks are required to prevent operator actions from defeating an automatic safety function.

After an ESFAS actuation, the ESFAS system must receive feedback signals from each impacted actuated device that each device has indeed reached its fail-safe position. Only then can the operator, through deliberate action with the manual enable nonsafety switch, be allowed to enable the PICS to reset the components.

7.5.4.3 Facility Master Operating Permissive

The ESFAS incorporates the Facility Master Operating Permissive key switch in the system design. The key switch has two positions, Operating and Secure (Subsection 7.6.1.1). When the Facility Master Operating Permissive key switch is active (operating), the ESFAS operates in the normal, nonsecure mode.

7.5.4.4 Maintenance Bypass

Each SFM can be placed in maintenance bypass or in a trip state by use of the OOS switch located on the front of the SFM and an associated trip/bypass switch located below the SFM. Details of the physical configuration and operation of the OOS and trip/bypass switches are provided in Sections 2.5.1 and 2.5.2 of Topical Report TR-1015-18653 (NuScale, 2017). Any ESFAS channels placed in maintenance bypass for maintenance or testing, or removed from maintenance bypass, will be displayed to the operators in the facility control room through the monitoring and indication bus to the PICS.

An individual SFM within an ESFAS division is allowed to be placed in maintenance bypass for up to two hours while the associated input channel(s) is required to be operable, in accordance with the technical specifications, for the purpose of performing required technical specification surveillance testing. A time limit of two hours is acceptable based on the small amount of time the channel could be in bypass, the continual attendance by operations or maintenance personnel during the test, the continued operability of the redundant channel(s), and the low likelihood that an accident would occur during the two-hour time period.

An SFM may also be placed in trip by use of the OOS and trip/bypass switches, as described in Sections 2.5.1 and 2.5.2 of Topical Report TR-1015-18653 (NuScale, 2017). Placing an SFM in trip preserves the single failure criterion for variables associated with that SFM where three channels are provided. In cases where only two channels are provided, placing a channel in trip serves to actuate the associated safety function. Inoperable channels are required to be placed in trip, or other actions are required to be taken to mitigate the condition, in accordance with the technical specifications.

7.5.4.5 Testing Capability

Testing of the ESFAS consists of the inservice self-testing capabilities of the HIPS platform and periodic surveillance testing.

End-to-end testing of the entire HIPS platform can be performed through overlap testing. Individual self-tests in the various components of the ESFAS ensure that the entire component is functioning correctly. Self-test features are provided for components that do not have setpoints or tunable parameters. ESFAS components, except the discrete APL of the EIM, have self-testing capabilities that ensure the information passed on to the following step in the signal path is correct.

The discrete logic of the APL of the EIM does not have self-test capability but is instead functionally tested. This functional testing consists of periodic simulated automatic and manual actuations to verify the functionality of the APL and the manual actuation pushbuttons.

Testing of input devices consists of channel checks, channel tests, and channel calibrations. Channel checks are performed while the channel is in service. Channel tests and channel calibrations may be performed while the associated equipment is in a condition where the channel is required to be operable (i.e., inservice), by placing the associated SFM in maintenance bypass (Subsection 7.5.4.4). Channel tests and channel calibrations may also be performed when the channel is not required to be operable.

7.5.4.6 Technical Specifications and Surveillance

Limiting Conditions for Operation and Surveillance Requirements are established for ESFAS logic, voting, and actuation divisions and instrumentation monitored by ESFAS as input to safety actuations.

7.5.5 HIGHLY INTEGRATED PROTECTION SYSTEM (HIPS) DESIGN

The ESFAS utilizes a HIPS platform to achieve the desired architecture for ESFAS system control. The HIPS platform used to support both the TRPS and the ESFAS is described in Subsection 7.4.5. The HIPS design described in Subsection 7.4.5 addresses HIPS design attributes, access control and cyber security, software development requirements, and HIPS performance analysis.

The ESFAS HIPS architecture is shown in Figure 7.1-3.

7.5.6 CONCLUSION

The safety-related ESFAS is designed to specific and measurable criteria to ensure quality and adequacy in the system design, implementation, and maintenance.

Design basis functions ensure safe operation of the facility and prevent or mitigate the consequences of design basis events.

The HIPS platform used in the ESFAS design is based on fundamental instrumentation and control principles of independence, redundancy, predictability and repeatability, and diversity and was developed under quality management to provide a simple yet reliable solution for the safety-related ESFAS functions.

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

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
RVZ1 RCA exhaust radiation	60x background radiation	2/3↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
RVZ2 RCA exhaust radiation	60x background radiation	2/3↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 1 (PVVS area) radiation	60x background radiation	2/3↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 2 (extraction area A) radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 3 (purification area A) radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 4 (packaging area 1) radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 5 (purification area B) radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 6 (extraction area B) radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 7 (extraction area C) radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 8 (purification area C) radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 9 (packaging area 2) radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} μCi/cc	20 percent	15 seconds
Supercell area 10 (IXP area) radiation	60x 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	500 micromho/cm	1/2↑	0.2 to 500 micromho/cm	3 percent	5 seconds
MEPS [ ]$^{PROP/ECI}$ conductivity extraction area B	500 micromho/cm	1/2↑	0.2 to 500 micromho/cm	3 percent	5 seconds
MEPS [ ]$^{PROP/ECI}$ conductivity extraction area C	500 micromho/cm	1/2↑	0.2 to 500 micromho/cm	3 percent	5 seconds
Carbon delay bed group 1 exhaust carbon monoxide	50 ppm	1/2↑	1 to 100 ppm	10 percent	15 seconds
Carbon delay bed group 2 exhaust carbon monoxide	50 ppm	1/2↑	1 to 100 ppm	10 percent	15 seconds
Carbon delay bed group 3 exhaust carbon monoxide	50 ppm	1/2↑	1 to 100 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	1 Ci/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

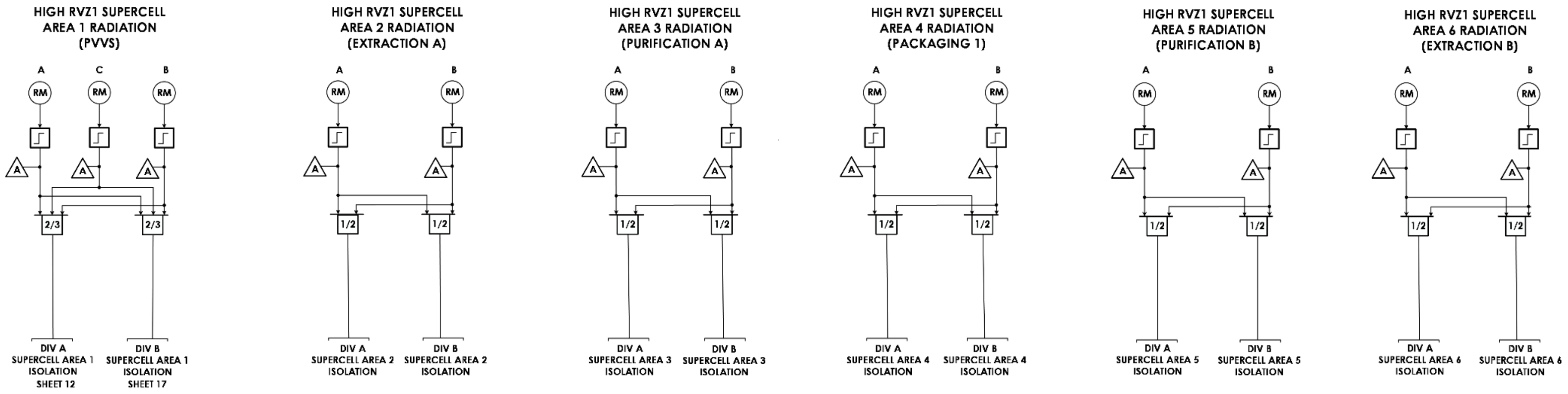
RVZ1 RCA exhaust isolation dampers	RVZ1 supercell area 9 (packaging area 2) outlet isolation dampers
RVZ2 RCA exhaust isolation dampers	RVZ2 supercell area 10 (IXP area) inlet isolation dampers
RVZ2 RCA supply isolation dampers	RVZ1 supercell area 10 (IXP area) outlet isolation dampers
RVZ3 transfer isolation dampers shipping/receiving IF	RVZ2 TPS room supply isolation dampers
RVZ3 transfer isolation dampers shipping/receiving RPF	RVZ2 TP S room exhaust isolation dampers
RVZ3 transfer isolation dampers main RCA ingress/egress	RLWI PVVS isolation valve
RVZ3 transfer isolation dampers RPF emergency exit	MEPS [ ]$^{PROP/ECI}$ A inlet isolation valve
RVZ3 transfer isolation dampers IF emergency exit	MEPS [ ]$^{PROP/ECI}$ B inlet isolation valve
RVZ3 transfer isolation dampers mezzanine emergency exit	MEPS [ ]$^{PROP/ECI}$ C inlet isolation valve
TSPS air inlet isolative valve	MEPS [ ]$^{PROP/ECI}$ A discharge isolation valve
TSPS RVZ1 exhaust valve	MEPS [ ]$^{PROP/ECI}$ B discharge isolation valve
RVZ2 supercell area 1 (PVVS area) inlet isolation dampers	MEPS [ ]$^{PROP/ECI}$ C discharge isolation valve
RVZ1 supercell area 1 (PVVS area) outlet isolation dampers	MEPS A extraction column wash supply valve
RVZ2 supercell area 2 (extraction area A) inlet isolation dampers	MEPS A extraction column eluent valve
RVZ1 supercell area 2 (extraction area A) outlet isolation dampers	MEPS A [ ]$^{PROP/ECI}$ wash supply valve
RVZ2 supercell area 3 (purification area A) inlet isolation dampers	MEPS A [ ]$^{PROP/ECI}$ eluent valve
RVZ1 supercell area 3 (purification area A) outlet isolation dampers	MEPS B extraction column wash supply valve
RVZ2 supercell area 4 (packaging area 1) inlet isolation dampers	MEPS B extraction column eluent valve
RVZ1 supercell area 4 (packaging area 1) outlet isolation dampers	MEPS B [ ]$^{PROP/ECI}$ wash supply valve
RVZ2 supercell area 5 (purification area B) inlet isolation dampers	MEPS B [ ]$^{PROP/ECI}$ eluent valve
RVZ1 supercell area 5 (purification area B) outlet isolation dampers	MEPS C extraction column wash supply valve
RVZ2 supercell area 6 (extraction area B) inlet isolation dampers	MEPS C extraction column eluent valve
RVZ1 supercell area 6 (extraction area B) outlet isolation dampers	MEPS C [ ]$^{PROP/ECI}$ wash supply valve
RVZ2 supercell area 7 (extraction area C) inlet isolation dampers	MEPS C [ ]$^{PROP/ECI}$ eluent valve
RVZ1 supercell area 7 (extraction area C) outlet isolation dampers	IXP recovery column wash supply valve
RVZ2 supercell area 8 (purification area C) inlet isolation dampers	IXP recovery column eluent valve
RVZ1 supercell area 8 (purification area C) outlet isolation dampers	IXP [ ]$^{PROP/ECI}$ wash supply valve
RVZ2 supercell area 9 (packaging area 2) inlet isolation dampers	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	TPS train B vacuum isolation valves
IXP liquid nitrogen supply valve	TPS train C glovebox pressure control exhaust isolation valve
TPS train A glovebox pressure control exhaust isolation valve	TPS train C ITS isolation valves
TPS train A ITS isolation valves	TPS train C helium AOV supply valve
TPS train A helium AOV supply valve	TPS train C helium SOV supply valve
TPS train A helium SOV supply valve	TPS train C vacuum isolation valves
TPS train A vacuum isolation valves	N2PS PVVS north header valves
TPS train B glovebox pressure control exhaust isolation valve	N2PS PVVS south header valves
TPS train B ITS isolation valves	TSPS RPCS supply cooling valves
TPS train B helium AOV supply valve	TSPS RPCS return cooling valve
TPS train B helium SOV supply valve	
FAIL-SAFE POSITION: OPEN	
RVZ1 exhaust train 1 blower breakers	PVVS blower bypass valves
RVZ1 exhaust train 2 blower breakers	PVVS carbon guard bed bypass valves
RVZ2 exhaust train 1 blower breakers	PVVS carbon delay bed group 1 outlet isolation valves
RVZ2 exhaust train 2 blower breakers	PVVS carbon delay bed group 2 outlet isolation valves
RVZ2 supply train 1 blower breakers	PVVS carbon delay bed group 3 outlet isolation valves
RVZ2 supply train 2 blower breakers	MEPS A extraction feed pump breakers
VTS vacuum transfer pump 1 breakers	MEPS B extraction feed pump breakers
VTS vacuum transfer pump 2 breakers	MEPS C extraction feed pump breakers
VTS vacuum break valves	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 C lower three-way isolation valve
MEPS area A upper three-way valve	MEPS area C upper three-way isolation valve
MEPS area B lower three-way valve	IXP upper three-way valve
MEPS area B upper three-way valve	IXP lower three-way valve

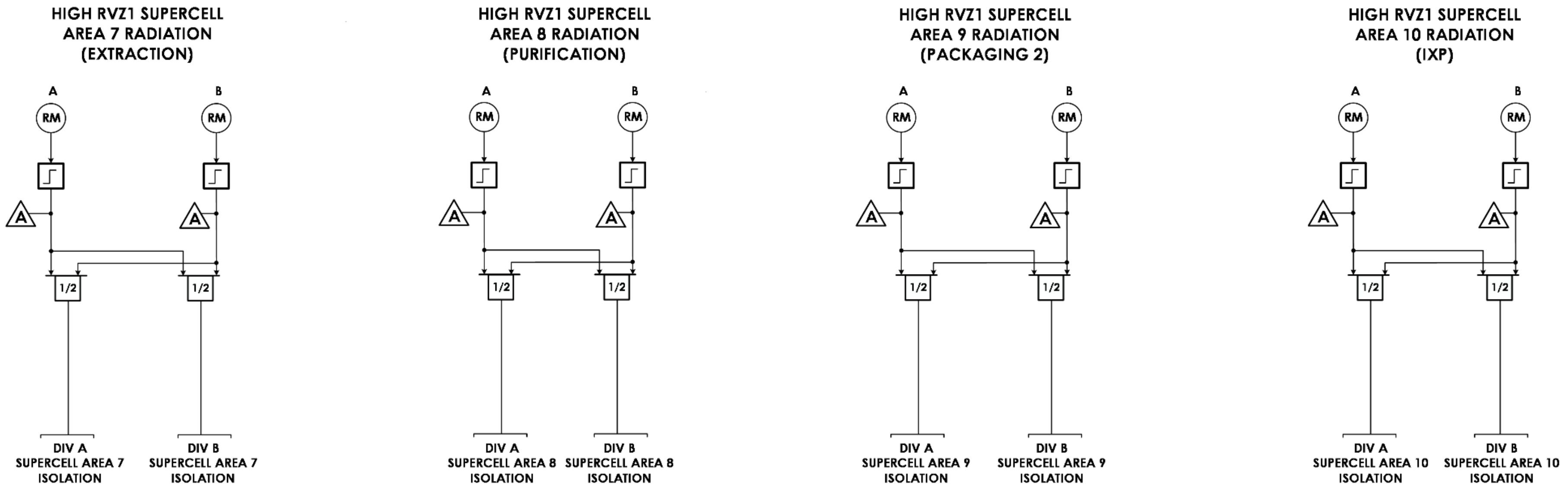
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 1 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 2 of 27)


HIGH RVZ1 SUPERCELL AREA 1 RADIATION (PVVS)
A
C
B
RM
A
2/3
DIV A SUPERCELL AREA 1 ISOLATION SHEET 12
DIV B SUPERCELL AREA 1 ISOLATION SHEET 17
HIGH RVZ1 SUPERCELL AREA 2 RADIATION (EXTRACTION A)
1/2
DIV A SUPERCELL AREA 2 ISOLATION
DIV B SUPERCELL AREA 2 ISOLATION
HIGH RVZ1 SUPERCELL AREA 3 RADIATION (PURIFICATION A)
DIV A SUPERCELL AREA 3 ISOLATION
DIV B SUPERCELL AREA 3 ISOLATION
HIGH RVZ1 SUPERCELL AREA 4 RADIATION (PACKAGING 1)
DIV A SUPERCELL AREA 4 ISOLATION
DIV B SUPERCELL AREA 4 ISOLATION
HIGH RVZ1 SUPERCELL AREA 5 RADIATION (PURIFICATION B)
DIV A SUPERCELL AREA 5 ISOLATION
DIV B SUPERCELL AREA 5 ISOLATION
HIGH RVZ1 SUPERCELL AREA 6 RADIATION (EXTRACTION B)
DIV A SUPERCELL AREA 6 ISOLATION
DIV B SUPERCELL AREA 6 ISOLATION

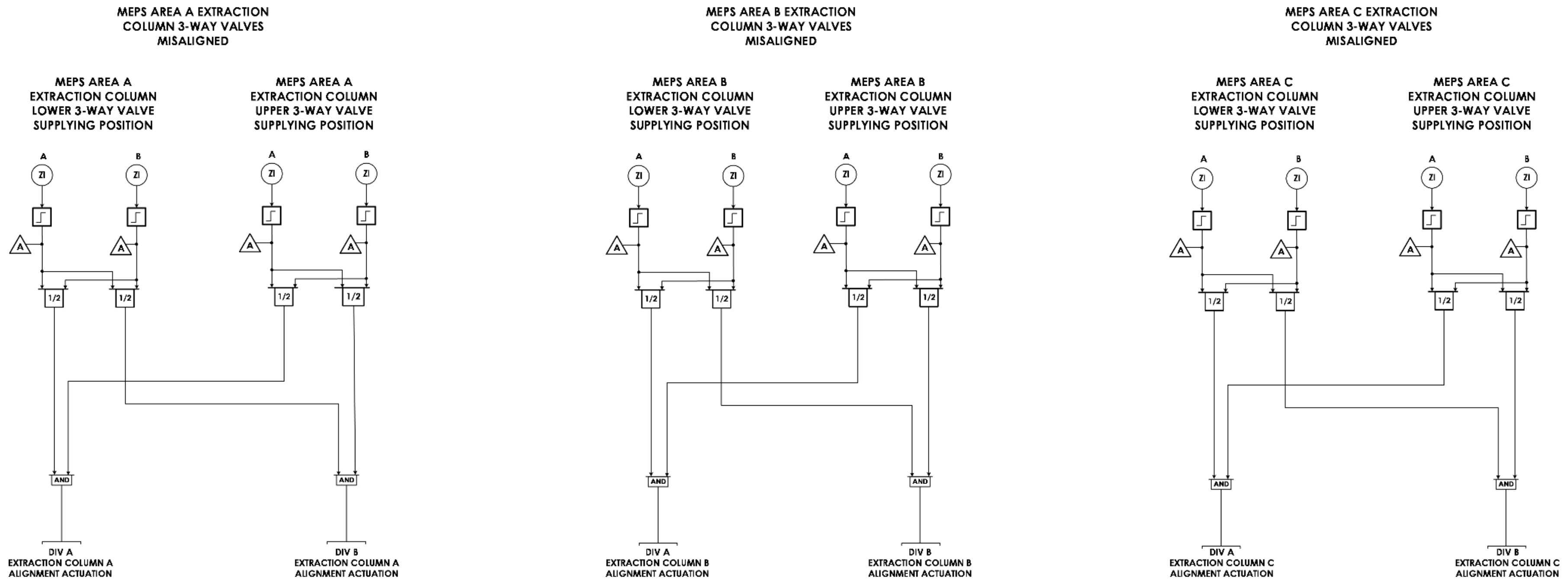
Trip Determination

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 3 of 27)



Trip Determination

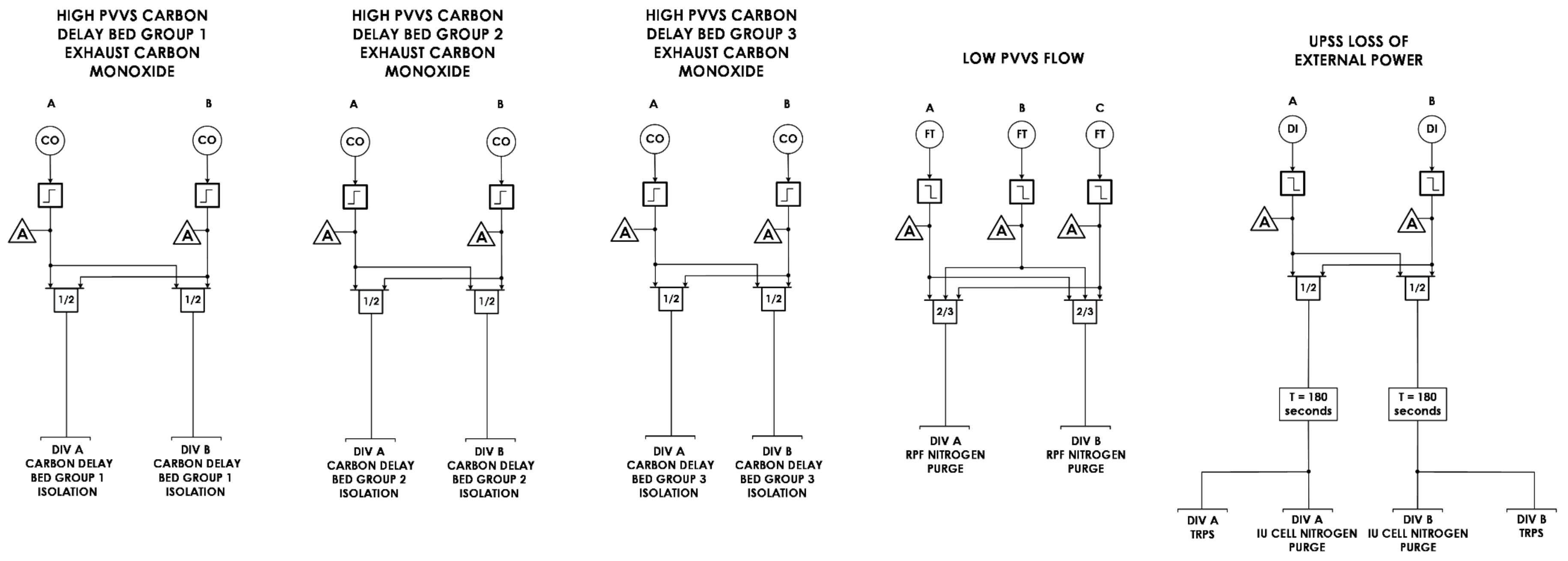
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 4 of 27)


MEPS AREA A 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
DIV A EXTRACTION COLUMN A ALIGNMENT ACTUATION
DIV B EXTRACTION COLUMN A ALIGNMENT ACTUATION
MEPS AREA B EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
MEPS AREA B EXTRACTION COLUMN LOWER 3-WAY VALVE SUPPLYING POSITION
MEPS AREA B EXTRACTION COLUMN UPPER 3-WAY VALVE SUPPLYING POSITION
DIV A EXTRACTION COLUMN B ALIGNMENT ACTUATION
DIV B EXTRACTION COLUMN B ALIGNMENT ACTUATION
MEPS AREA C EXTRACTION COLUMN 3-WAY VALVES MISALIGNED
MEPS AREA C EXTRACTION COLUMN LOWER 3-WAY VALVE SUPPLYING POSITION
MEPS AREA C EXTRACTION COLUMN UPPER 3-WAY VALVE SUPPLYING POSITION
DIV A EXTRACTION COLUMN C ALIGNMENT ACTUATION
DIV B EXTRACTION COLUMN C ALIGNMENT ACTUATION
A
B
ZI
1/2
AND

Trip Determination

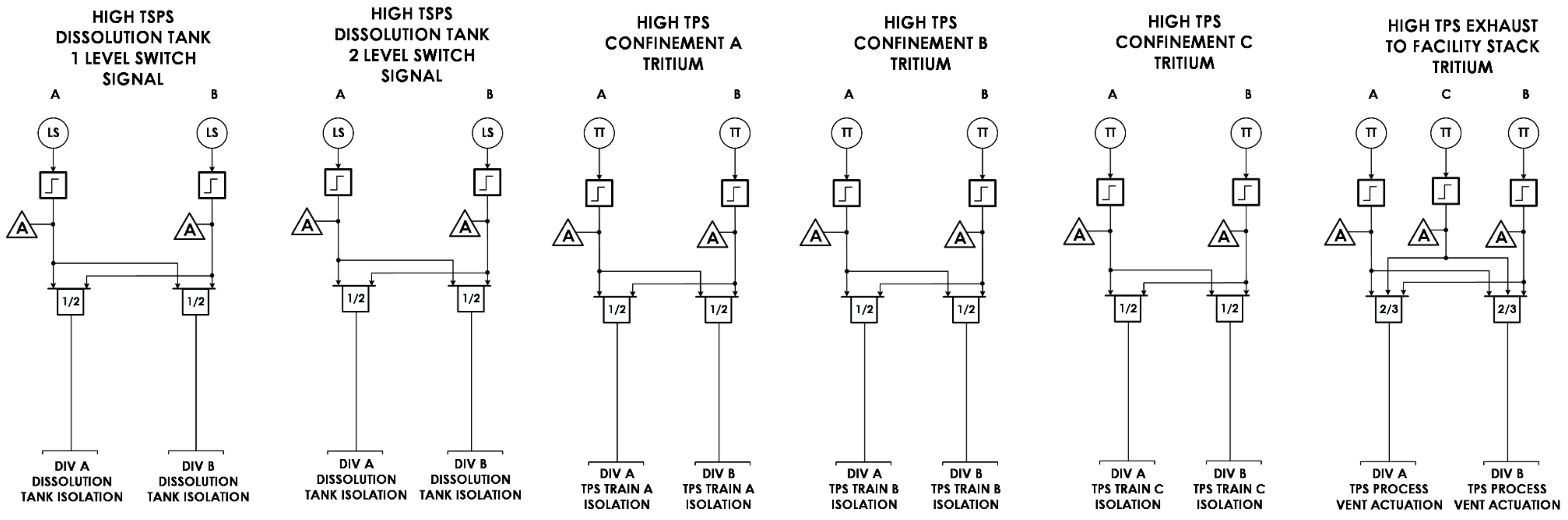
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 5 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 6 of 27)


HIGH PVVS CARBON DELAY BED GROUP 1 EXHAUST CARBON MONOXIDE
A
B
CO
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
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
DIV A CARBON DELAY BED GROUP 3 ISOLATION
DIV B CARBON DELAY BED GROUP 3 ISOLATION
LOW PVVS FLOW
C
FT
2/3
DIV A RPF NITROGEN PURGE
DIV B RPF NITROGEN PURGE
UPSS LOSS OF EXTERNAL POWER
DI
T = 180 seconds
DIV A TRPS
DIV A IU CELL NITROGEN PURGE
DIV B IU CELL NITROGEN PURGE
DIV B TRPS

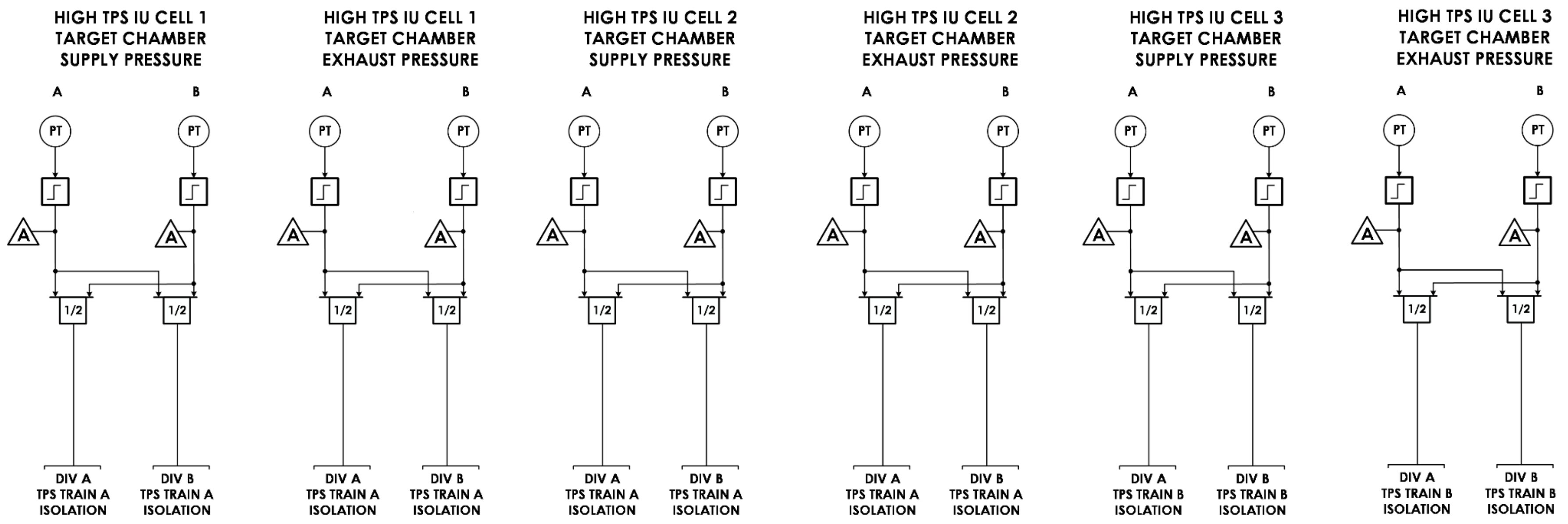
Trip Determination

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
DIV B DISSOLUTION TANK ISOLATION
HIGH TSPS DISSOLUTION TANK 2 LEVEL SWITCH SIGNAL
A
B
LS
LS
1/2
1/2
DIV A DISSOLUTION TANK ISOLATION
DIV B DISSOLUTION TANK ISOLATION
HIGH TPS CONFINEMENT A TRITIUM
A
B
TT
TT
1/2
1/2
DIV A TPS TRAIN A ISOLATION
DIV B TPS TRAIN A ISOLATION
HIGH TPS CONFINEMENT B TRITIUM
A
B
TT
TT
1/2
1/2
DIV A TPS TRAIN B ISOLATION
DIV B TPS TRAIN B ISOLATION
HIGH TPS CONFINEMENT C TRITIUM
A
B
TT
TT
1/2
1/2
DIV A TPS TRAIN C ISOLATION
DIV B TPS TRAIN C ISOLATION
HIGH TPS EXHAUST TO FACILITY STACK TRITIUM
A
C
B
TT
TT
TT
2/3
2/3
DIV A TPS PROCESS VENT ACTUATION
DIV B TPS PROCESS VENT ACTUATION

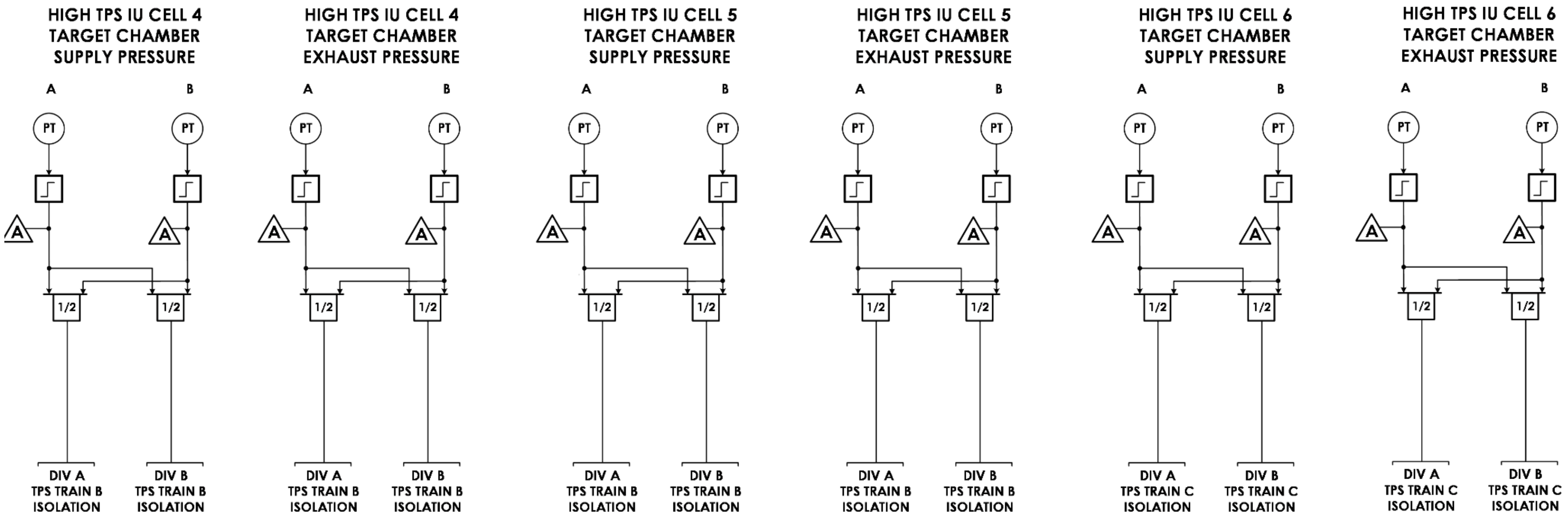
Trip Determination

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 8 of 27)


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 IU CELL 3 TARGET CHAMBER SUPPLY PRESSURE
HIGH TPS IU CELL 3 TARGET CHAMBER EXHAUST PRESSURE
A
B
PT
A
1/2
DIV A TPS TRAIN A ISOLATION
DIV B TPS TRAIN A ISOLATION
DIV A TPS TRAIN B ISOLATION
DIV B TPS TRAIN B ISOLATION

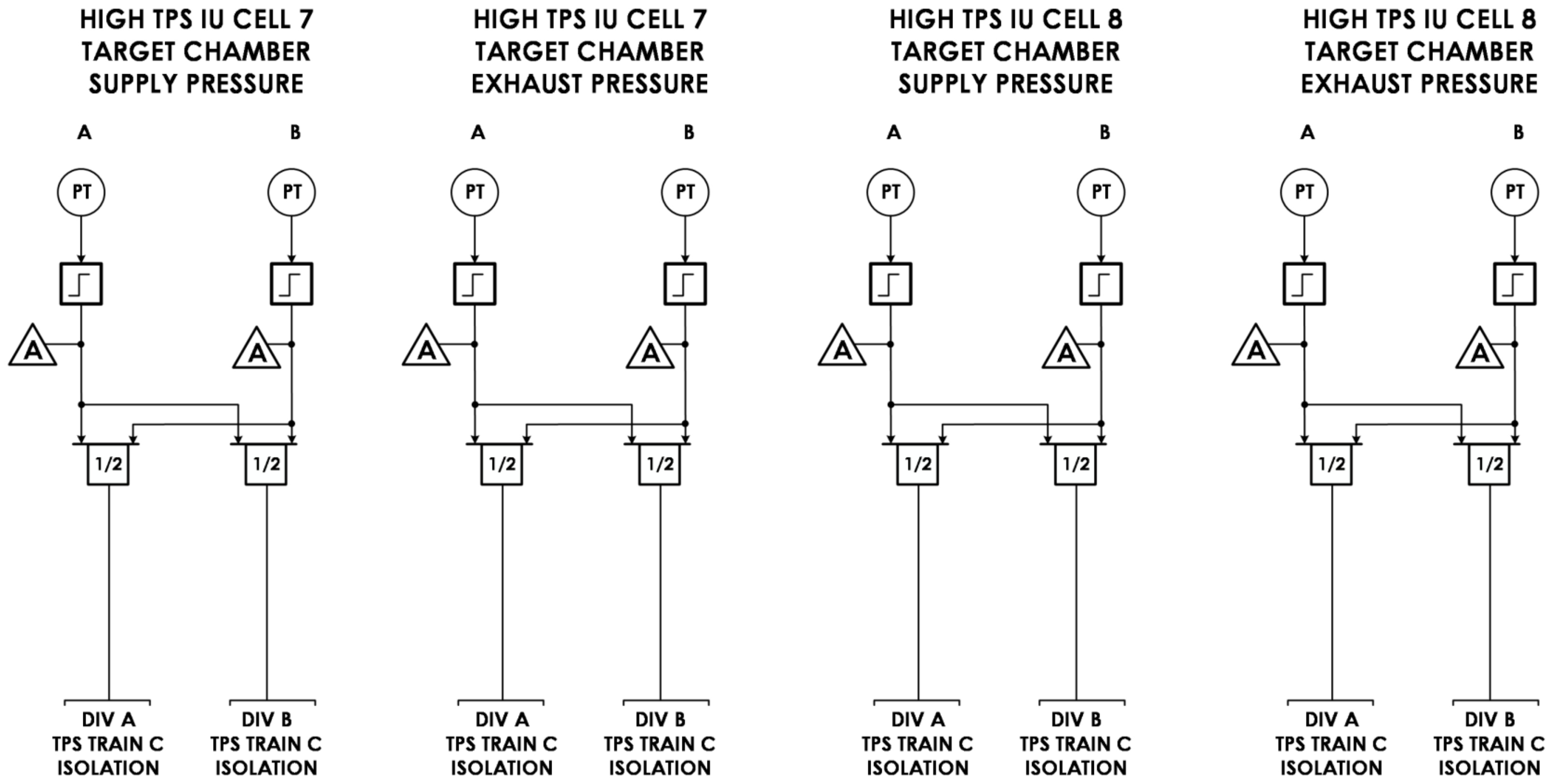
Trip Determination

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
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)


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
A
B
PT
A
1/2
DIV A TPS TRAIN C ISOLATION
DIV B TPS TRAIN C ISOLATION

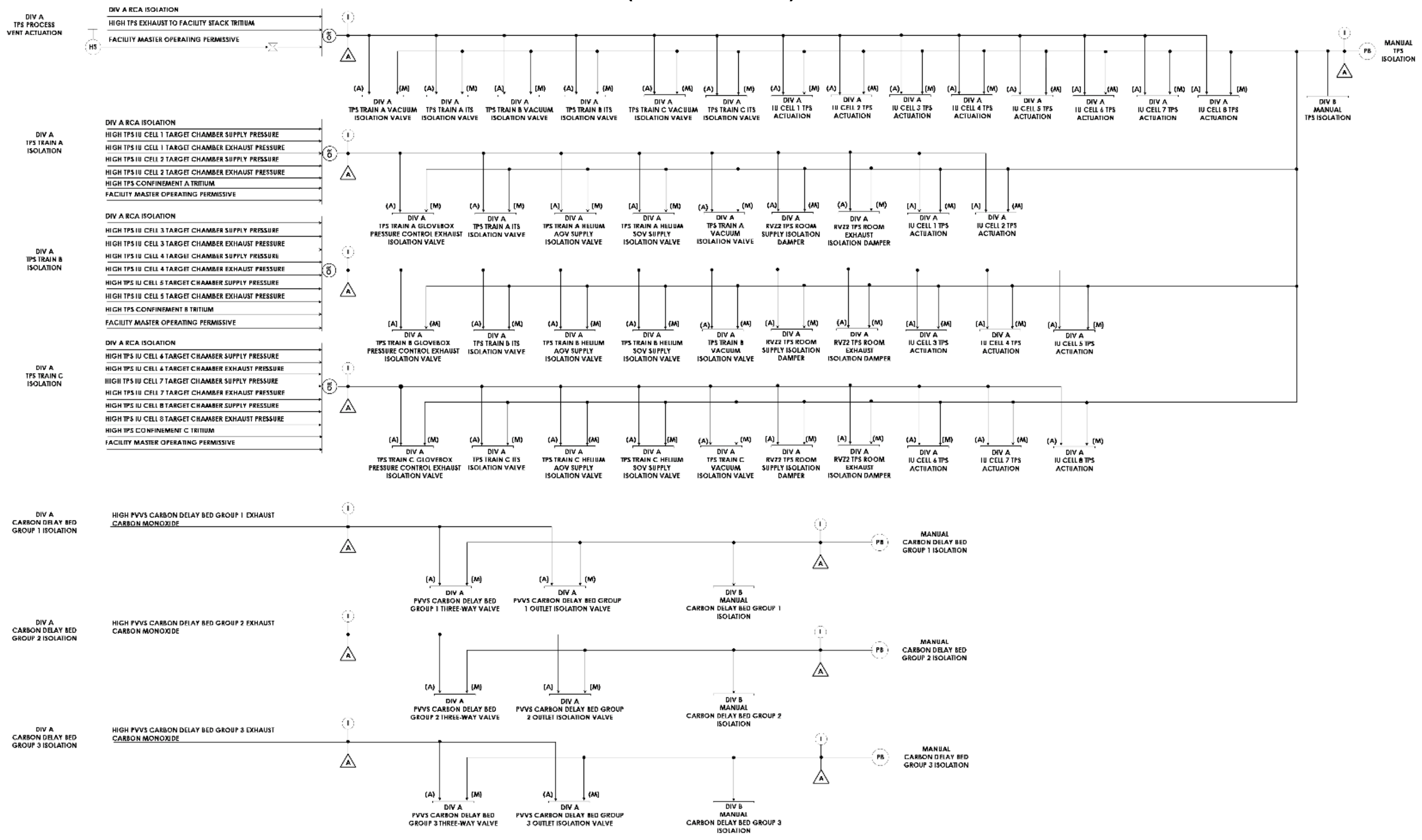
Trip Determination

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 11 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 12 of 27)

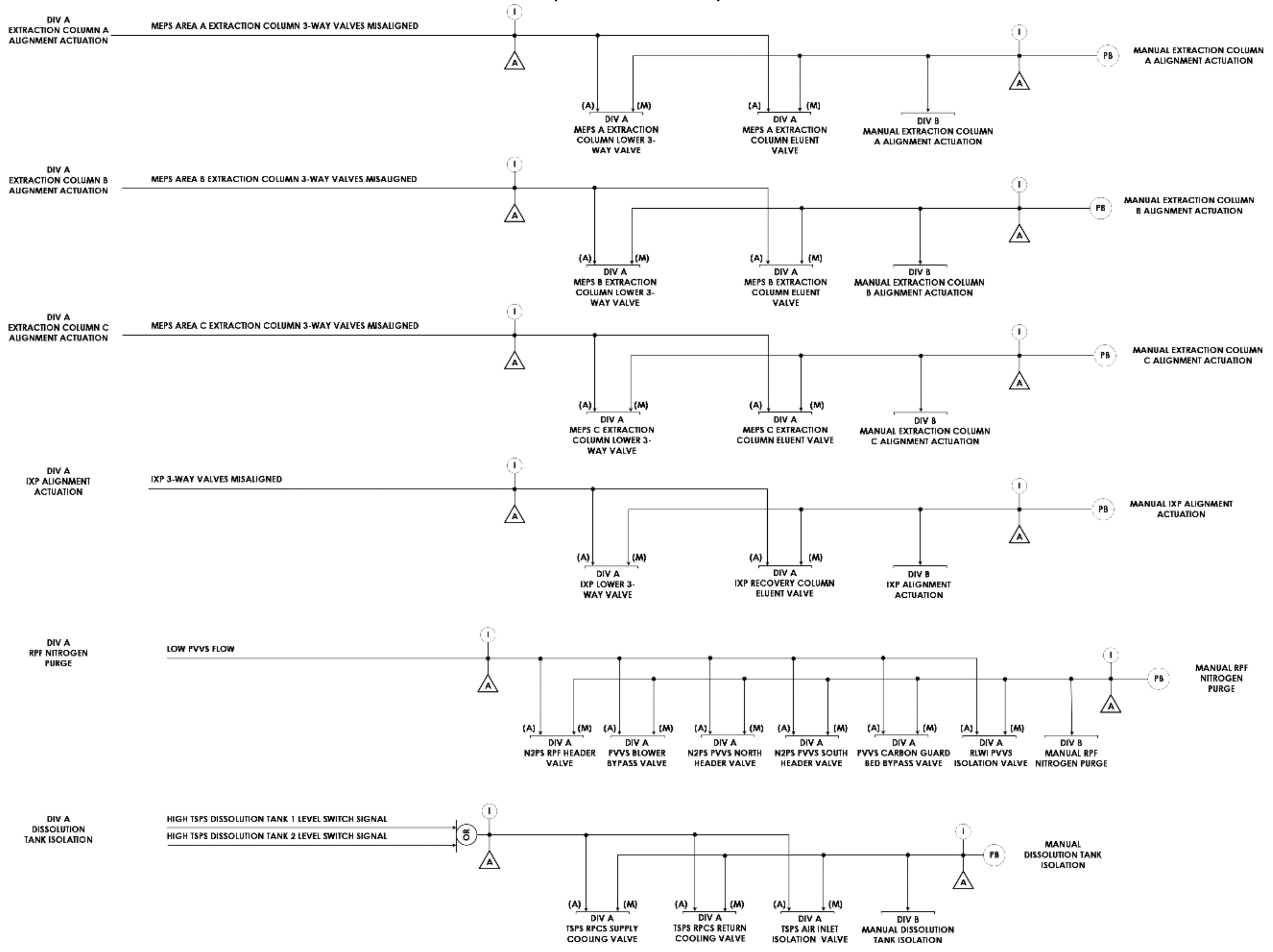
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 13 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 14 of 27)


DIV A TPS PROCESS VENT ACTUATION
DIV A RCA ISOLATION
HIGH TPS EXHAUST TO FACILITY STACK TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
HS
I
OR
A
(A)
(M)
DIV A TPS TRAIN A VACUUM ISOLATION VALVE
DIV A TPS TRAIN A ITS ISOLATION VALVE
DIV A TPS TRAIN B VACUUM ISOLATION VALVE
DIV A TPS TRAIN B ITS ISOLATION VALVE
DIV A TPS TRAIN C VACUUM ISOLATION VALVE
DIV A TPS TRAIN C ITS ISOLATION VALVE
DIV A IU CELL 1 TPS ACTUATION
DIV A IU CELL 2 TPS ACTUATION
DIV A IU CELL 3 TPS ACTUATION
DIV A IU CELL 4 TPS ACTUATION
DIV A IU CELL 5 TPS ACTUATION
DIV A IU CELL 6 TPS ACTUATION
DIV A IU CELL 7 TPS ACTUATION
DIV A IU CELL 8 TPS ACTUATION
DIV B MANUAL TPS ISOLATION
PB
MANUAL TPS ISOLATION
DIV A TPS TRAIN A ISOLATION
DIV A 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 A TPS TRAIN A GLOVEBOX PRESSURE CONTROL EXHAUST ISOLATION VALVE
DIV A TPS TRAIN A ITS ISOLATION VALVE
DIV A TPS TRAIN A HELIUM AOV SUPPLY ISOLATION VALVE
DIV A TPS TRAIN A HELIUM SOV SUPPLY ISOLATION VALVE
DIV A TPS TRAIN A VACUUM ISOLATION VALVE
DIV A RVZ2 TPS ROOM SUPPLY ISOLATION DAMPER
DIV A RVZ2 TPS ROOM EXHAUST ISOLATION DAMPER
DIV A IU CELL 1 TPS ACTUATION
DIV A IU CELL 2 TPS ACTUATION
DIV A TPS TRAIN B ISOLATION
DIV A 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 B TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
DIV A TPS TRAIN B GLOVEBOX PRESSURE CONTROL EXHAUST ISOLATION VALVE
DIV A TPS TRAIN B ITS ISOLATION VALVE
DIV A TPS TRAIN B HELIUM AOV SUPPLY ISOLATION VALVE
DIV A TPS TRAIN B HELIUM SOV SUPPLY ISOLATION VALVE
DIV A TPS TRAIN B VACUUM ISOLATION VALVE
DIV A RVZ2 TPS ROOM SUPPLY ISOLATION DAMPER
DIV A RVZ2 TPS ROOM EXHAUST ISOLATION DAMPER
DIV A IU CELL 3 TPS ACTUATION
DIV A IU CELL 4 TPS ACTUATION
DIV A IU CELL 5 TPS ACTUATION
DIV A TPS TRAIN C ISOLATION
DIV A 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 C TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
DIV A TPS TRAIN C GLOVEBOX PRESSURE CONTROL EXHAUST ISOLATION VALVE
DIV A TPS TRAIN C ITS ISOLATION VALVE
DIV A TPS TRAIN C HELIUM AOV SUPPLY ISOLATION VALVE
DIV A TPS TRAIN C HELIUM SOV SUPPLY ISOLATION VALVE
DIV A TPS TRAIN C VACUUM ISOLATION VALVE
DIV A RVZ2 TPS ROOM SUPPLY ISOLATION DAMPER
DIV A RVZ2 TPS ROOM EXHAUST ISOLATION DAMPER
DIV A IU CELL 6 TPS ACTUATION
DIV A IU CELL 7 TPS ACTUATION
DIV A IU CELL 8 TPS ACTUATION
DIV A CARBON DELAY BED GROUP 1 ISOLATION
HIGH PVVS CARBON DELAY BED GROUP 1 EXHAUST CARBON MONOXIDE
DIV A PVVS CARBON DELAY BED GROUP 1 THREE-WAY VALVE
DIV A PVVS CARBON DELAY BED GROUP 1 OUTLET ISOLATION VALVE
DIV B MANUAL CARBON DELAY BED GROUP 1 ISOLATION
MANUAL CARBON DELAY BED GROUP 1 ISOLATION
DIV A CARBON DELAY BED GROUP 2 ISOLATION
HIGH PVVS CARBON DELAY BED GROUP 2 EXHAUST CARBON MONOXIDE
DIV A PVVS CARBON DELAY BED GROUP 2 THREE-WAY VALVE
DIV A PVVS CARBON DELAY BED GROUP 2 OUTLET ISOLATION VALVE
DIV B MANUAL CARBON DELAY BED GROUP 2 ISOLATION
MANUAL CARBON DELAY BED GROUP 2 ISOLATION
DIV A CARBON DELAY BED GROUP 3 ISOLATION
HIGH PVVS CARBON DELAY BED GROUP 3 EXHAUST CARBON MONOXIDE
DIV A PVVS CARBON DELAY BED GROUP 3 THREE-WAY VALVE
DIV A PVVS CARBON DELAY BED GROUP 3 OUTLET ISOLATION VALVE
DIV B MANUAL CARBON DELAY BED GROUP 3 ISOLATION
MANUAL CARBON DELAY BED GROUP 3 ISOLATION

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
LOW PVVS FLOW
DIV A N2PS RPF HEADER VALVE
DIV A PVVS BLOWER BYPASS VALVE
DIV A N2PS PVVS NORTH HEADER VALVE
DIV A N2PS PVVS 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 TSPS AIR INLET ISOLATION VALVE
DIV B MANUAL DISSOLUTION TANK ISOLATION
MANUAL DISSOLUTION TANK ISOLATION

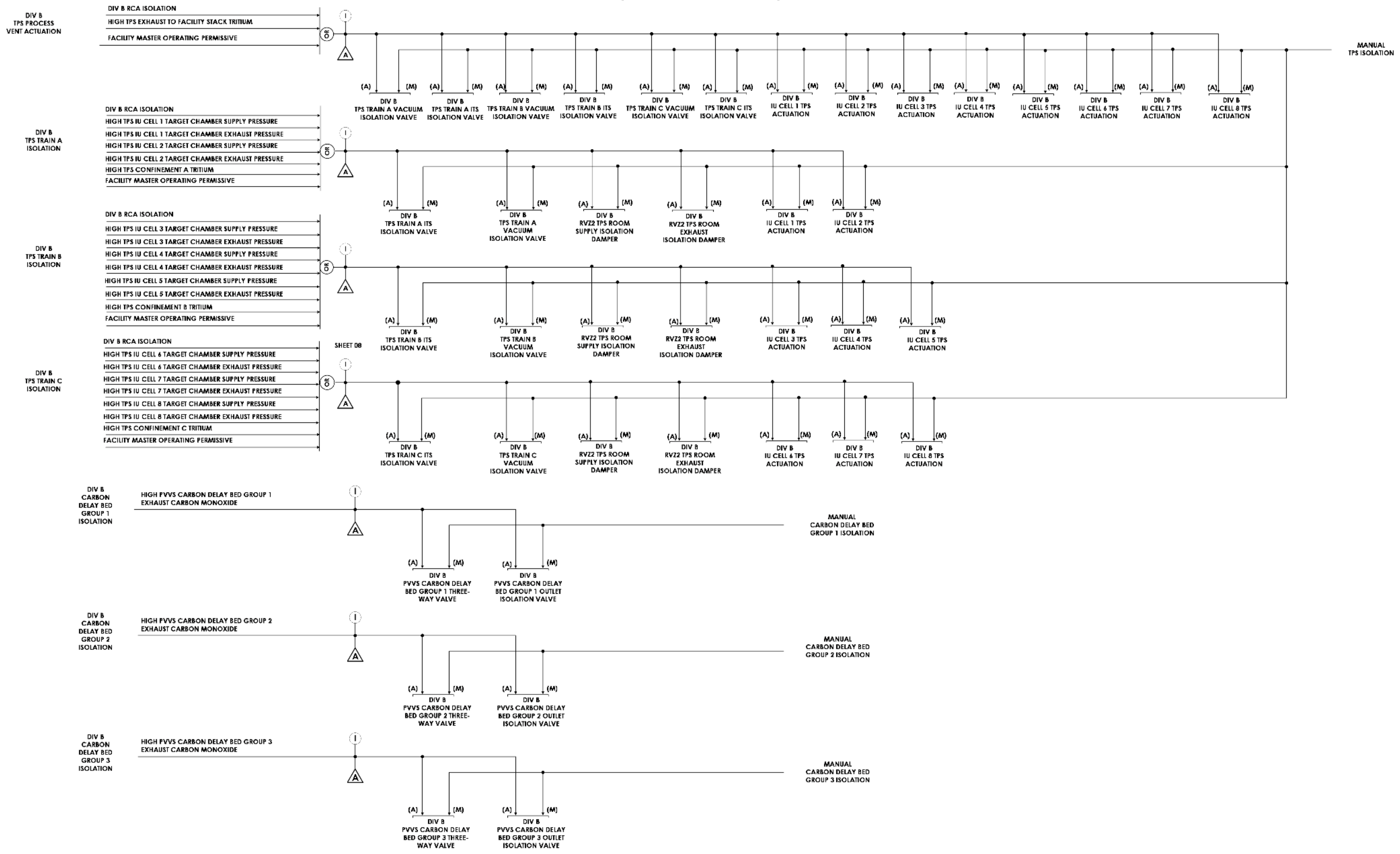
Safety Actuation

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 16 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 17 of 27)

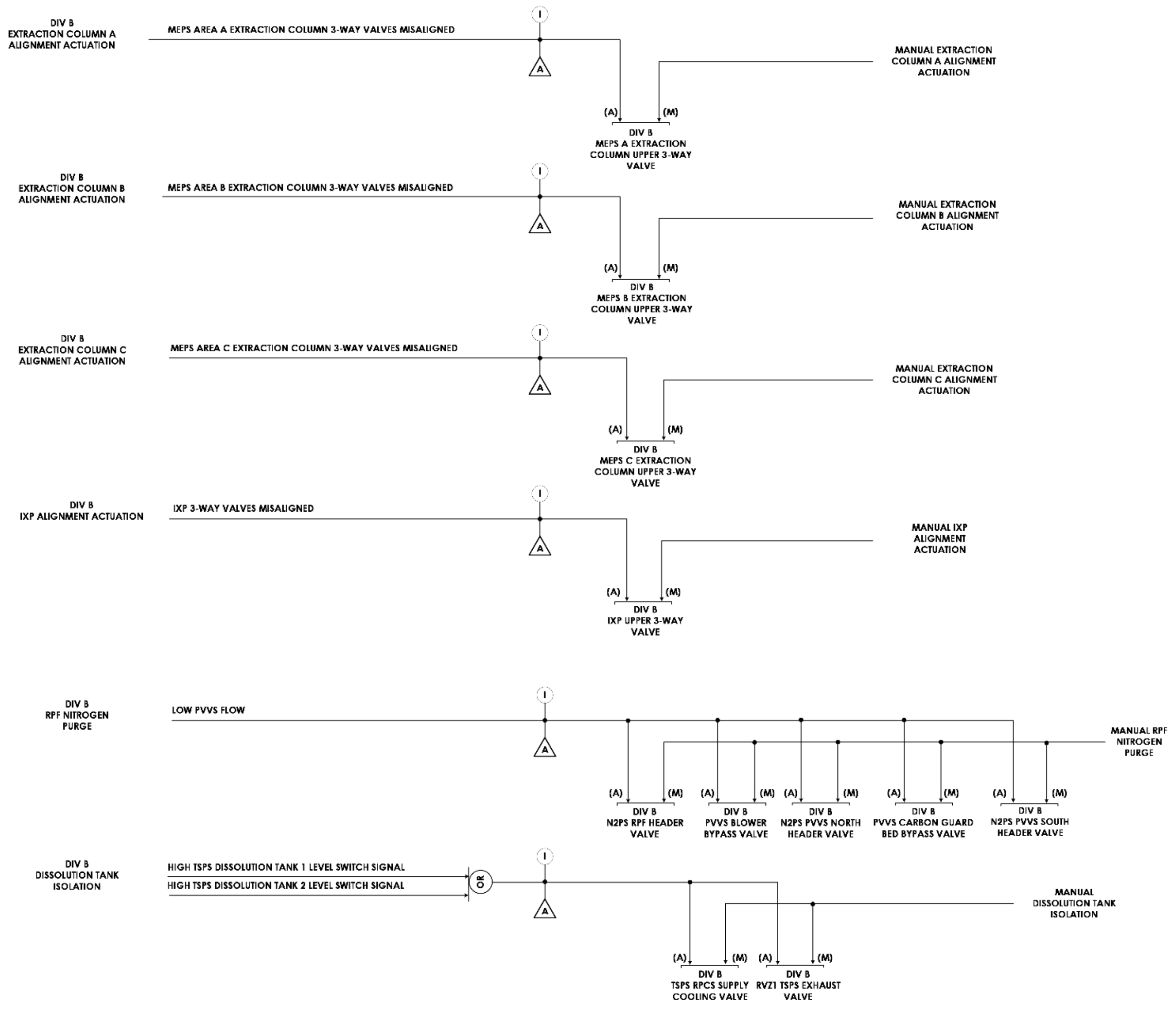
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 18 of 27)

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 VALVE
DIV B TPS TRAIN A ITS ISOLATION VALVE
DIV B TPS TRAIN B VACUUM ISOLATION VALVE
DIV B TPS TRAIN B ITS ISOLATION VALVE
DIV B TPS TRAIN C VACUUM ISOLATION VALVE
DIV B TPS TRAIN C ITS ISOLATION VALVE
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 VALVE
DIV B RVZ2 TPS ROOM SUPPLY ISOLATION DAMPER
DIV B RVZ2 TPS ROOM EXHAUST ISOLATION DAMPER
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 B TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
DIV B TPS TRAIN B ITS ISOLATION VALVE
DIV B TPS TRAIN B VACUUM ISOLATION VALVE
DIV B RVZ2 TPS ROOM SUPPLY ISOLATION DAMPER
DIV B RVZ2 TPS ROOM EXHAUST ISOLATION DAMPER
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
SHEET 08
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 C TRITIUM
FACILITY MASTER OPERATING PERMISSIVE
DIV B TPS TRAIN C ITS ISOLATION VALVE
DIV B TPS TRAIN C VACUUM ISOLATION VALVE
DIV B RVZ2 TPS ROOM SUPPLY ISOLATION DAMPER
DIV B RVZ2 TPS ROOM EXHAUST ISOLATION DAMPER
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

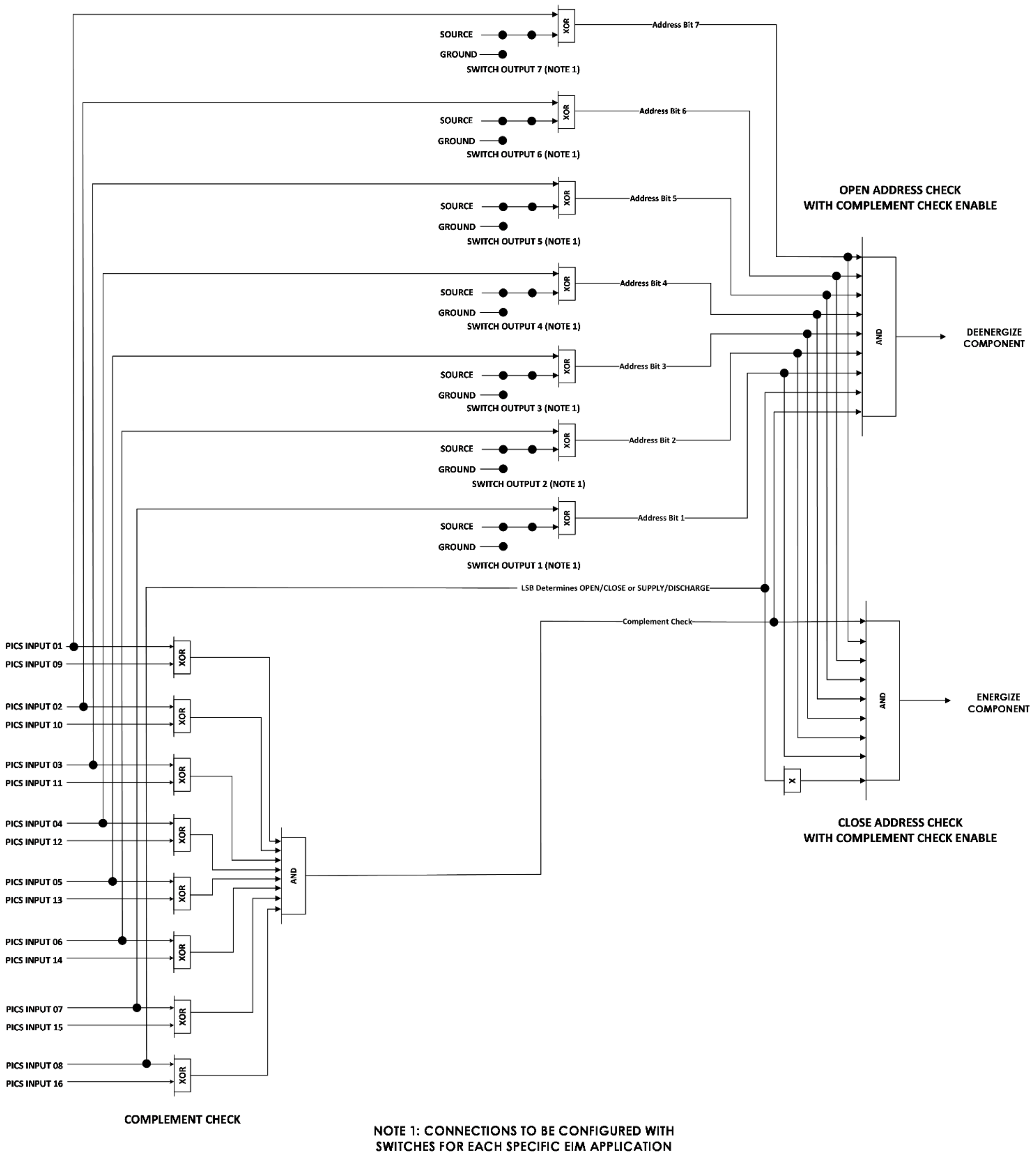
Safety Actuation

Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 20 of 27)



Safety Actuation

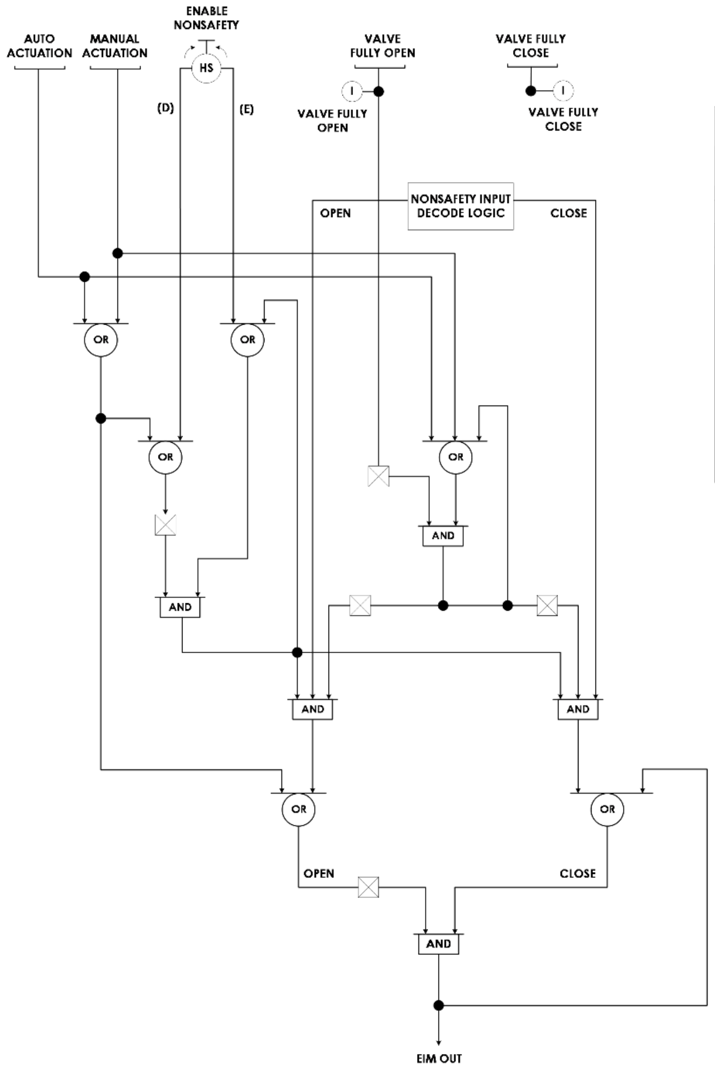
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 21 of 27)



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)

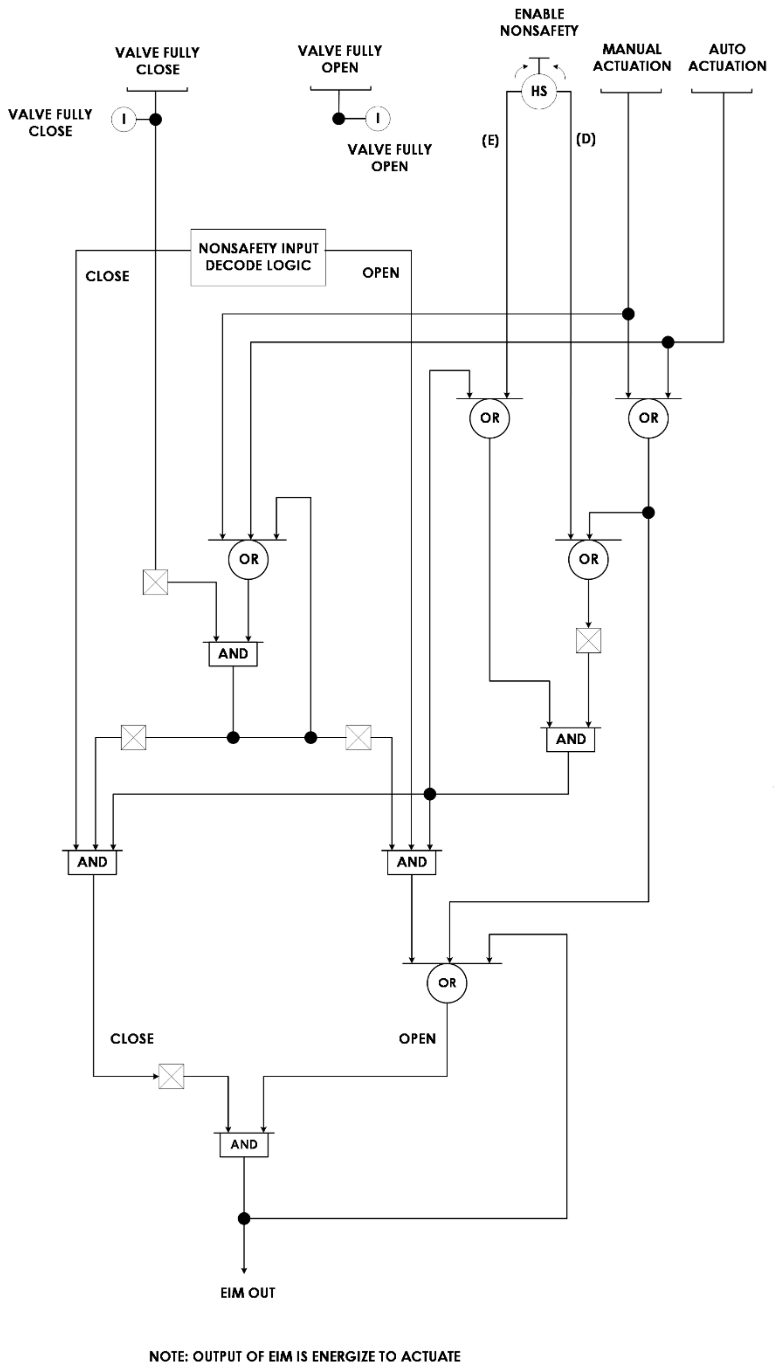


NOTE: OUTPUT OF EIM IS DEENERGIZE TO ACTUATE TO POSITION DEFINED FOR LOSS OF POWER

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 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 PVVS CARBON GUARD BED BYPASS VALVE	DIV B PVVS CARBON GUARD BED 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

Priority Logic

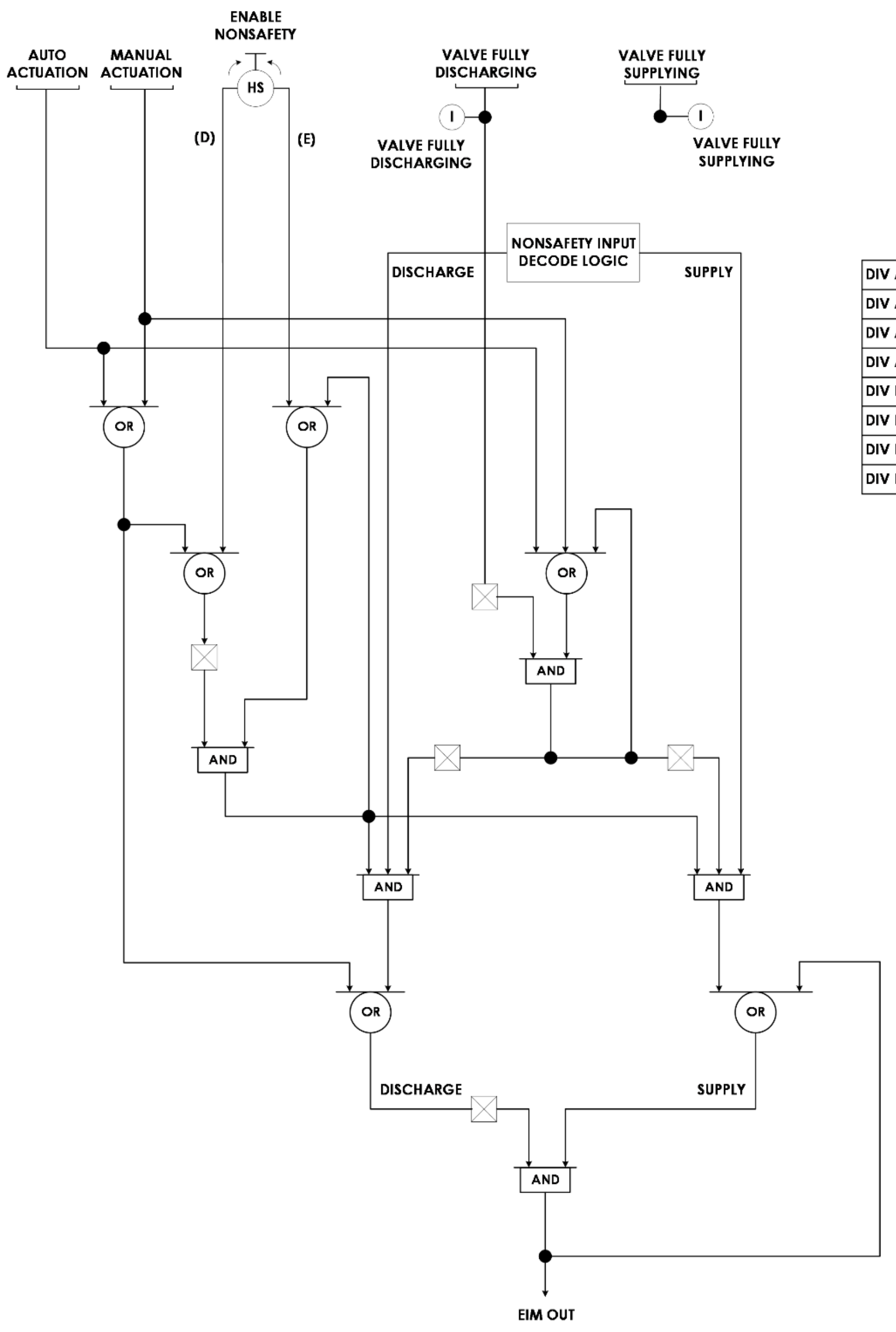
Figure 7.5-1 – ESFAS Logic Diagrams (Sheet 24 of 27)



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

Priority Logic

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 25 of 27)

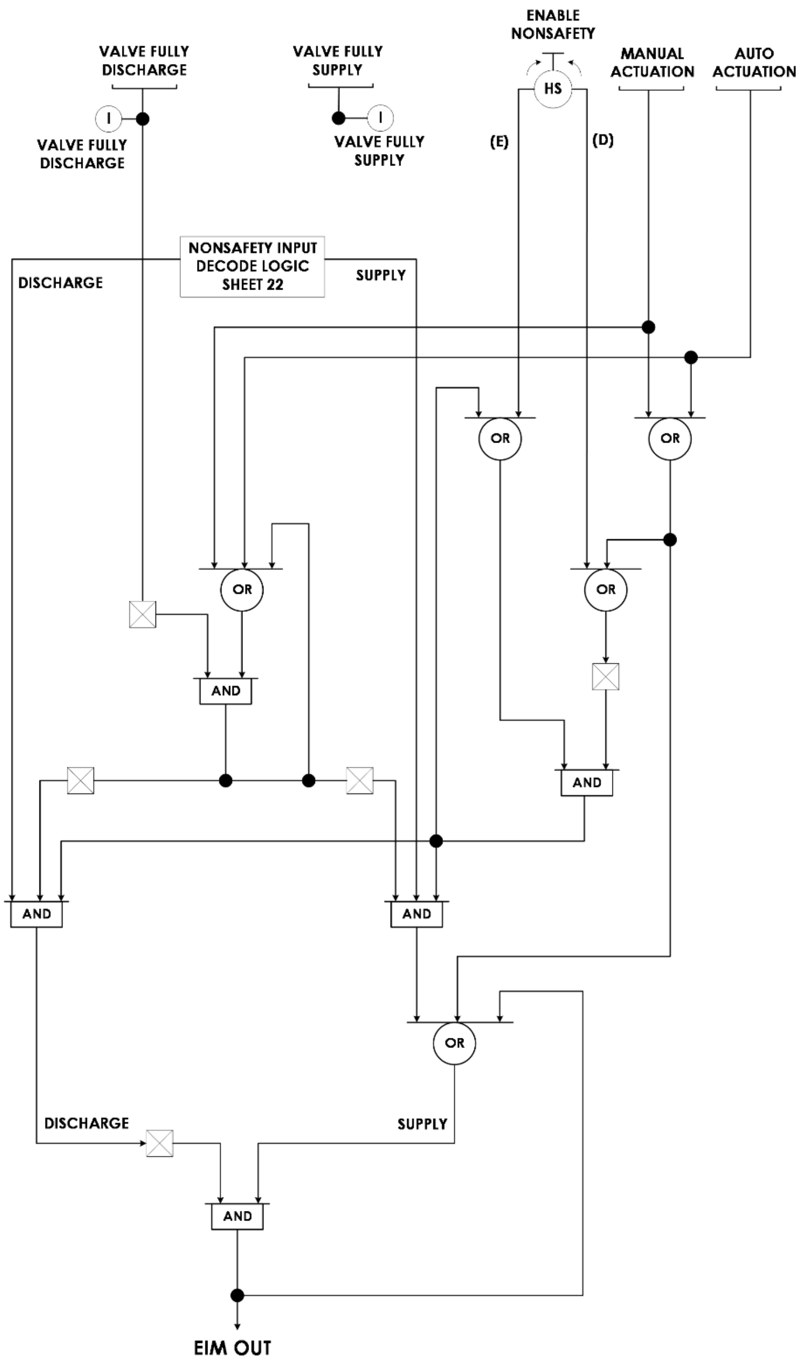


DIV A MEPS A EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A MEPS B EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A MEPS C EXTRACTION COLUMN LOWER 3-WAY VALVE
DIV A IXP LOWER 3-WAY VALVE
DIV B MEPS A EXTRACTION COLUMN UPPER 3-WAY VALVE
DIV B MEPS B EXTRACTION COLUMN UPPER 3-WAY VALVE
DIV B MEPS C EXTRACTION COLUMN 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)



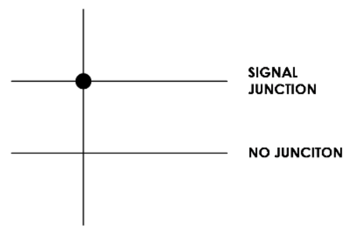
DIV A PVVS CARBON DELAY BED GROUP 1 THREE-WAY VALVE
DIV A PVVS CARBON DELAY BED GROUP 2 THREE-WAY VALVE
DIV A PVVS CARBON DELAY BED GROUP 3 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 1 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 2 THREE-WAY VALVE
DIV B PVVS CARBON DELAY BED GROUP 3 THREE-WAY VALVE

NOTE: OUTPUT OF EIM IS ENERGIZE TO ACTUATE

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

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 main production facility. The facility control room is located in the non-radiologically controlled area of the main production facility.

Within the facility control room, there is a main control board, two process integrated control system (PICS) operator workstations, two neutron driver assembly system (NDAS) workstations, and a supervisor workstation. The operator workstations consist of display screens and human interface equipment, and the main control board consists of a console, static display screens, and manual actuation interfaces. The supervisor workstation is similar to the PICS operator workstations, but is typically used for monitoring purposes only, and is not normally assigned any control functions. The main control board, PICS operator and supervisor workstations, and associated control equipment are considered part of the PICS. The PICS provides nonsafety-related system status and measured process variable values for viewing, recording, and trending in the facility control room (Subsection 7.3.3.1). The main control board, PICS and NDAS 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.

The SHINE facility additionally contains local control stations with limited functionality used for performing specific local tasks.

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 is approximately 25 feet wide and contains eight sections each containing one column of displays dedicated to a single irradiation unit (IU), and a ninth section containing two columns of displays dedicated to other processes within the facility. The ninth section, for the facility generally, is located between the fourth and fifth IU sections.

The static display screens, which show the variables important to the safety functions of the IUs and other facility processes, are located on the upper half of the main control board, aligned in three rows of displays. The configuration of the main control board, 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 main production facility. The current mode of operation for each IU is displayed on a static display screen associated with that IU.

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 main control board section, 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”) for each IU section and for the facility process section, which allows operators to enable the PICS ability to manipulate equipment that can also be actuated 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.

7.6.1.2 Operator Workstation

There are four desks that make up the main operator workstations, centrally located within the facility control room, aligned end-to-end in front of the main control board. The two outermost desks are designated as PICS workstations and the two inner desks are NDAS control stations. Each workstation contains multiple display screens. Configuration of the operator workstations is shown in Figure 7.6-1.

Either PICS workstation can display any of the available PICS display screens for monitoring purposes. PICS controls are designed such that they can only be manipulated by a single station at any given time to prevent two operators from inputting conflicting commands. While control of each IU or process is normally assigned to a particular workstation, control can also be transferred between workstations for operational flexibility. Control of a process or IU may also be transferred to the supervisor workstation if necessary (e.g., to perform maintenance on an operator workstation, or to accommodate additional workload). A limited set of control functions can be transferred to local control stations as described in Subsection 7.6.1.6. Only one workstation (operator, supervisor, or local) is allowed to input control commands to a particular component at any time.

One of the screens at the PICS workstation is used to display the alarms present in the facility. This screen 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 for the IUs are advanced by the operator at the PICS 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 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.

The two NDAS control stations allow operators to monitor and make adjustments to any of the eight neutron drivers in the eight IU cells. The NDAS control stations are only allowed to provide control signals to the NDAS when a permissive provided by the PICS is satisfied. The NDAS control stations are used to interface with the vendor provided NDAS control system described in Subsection 4a2.3.4.

7.6.1.3 Supervisor Workstation

The supervisor workstation is located on an elevated platform on the west side of the facility control room facing the operator workstations and the main control board. The supervisor workstation is similar to the PICS operator workstations, and may be used to control a process or IU, but is normally used for monitoring facility status only. The supervisor station does not have any NDAS control capabilities.

7.6.1.4 Maintenance Workstation

The TRPS/ESFAS maintenance workstations receive diagnostic and indication information from the TRPS and the ESFAS. Any module failure or warning is shown at the maintenance workstation and a log of each failure or warning is maintained at the maintenance workstation for use. The maintenance workstation is also used to update setpoints within the safety function module in the chassis. This update is done through a temporary connection to the monitoring and indication communication module of the associated division, as described in Subsection 7.4.5.

Two TRPS/ESFAS maintenance workstations are provided in the facility control room. Maintenance workstations are integrated into two of the TRPS cabinets, for use by both TRPS and ESFAS. The Division A maintenance workstation is located in a Division A TRPS cabinet, and the Division B maintenance workstation is located in a Division B TRPS cabinet. The Division A maintenance workstation can also be used for performing maintenance on Division C cabinets. The typical arrangement of the maintenance workstation in a TRPS cabinet is shown in Figure 7.6-3.

7.6.1.5 Other Control Room Interface Equipment

The SHINE facility control room also contains the following equipment used for monitoring or interfacing with facility systems:

A criticality accident alarm system (CAAS) panel is located along the east wall of the control room, north of the main control board. The CAAS panel contains a logical unit for processing alarms and is used to monitor the status of the CAAS. The CAAS is described in Subsection 6b.3.3.

A fire control panel is located along the west wall of the control room, north of the supervisor station. The fire control panel is used to monitor for facility fire alarms provided by the facility fire protection system. The facility fire protection system is described in Subsection 9a2.3.7.

7.6.1.6 Local Control Stations

The SHINE main production facility contains eight local PICS control stations:

- Target solution preparation
- Radioactive liquid waste immobilization
- Supercell A
- Supercell B
- Supercell C
- Tritium purification system (TPS) Train A
- TPS Train B
- TPS Train C

A specific, limited set of control functions associated with each local control station can be transferred from the control room to the specified local control station with authorization of a control room supervisor. The local control stations can also be used for monitoring only for PICS displays not associated with the function of the local control station. The local control stations each contain display and human system interface capabilities.

Although not a control station, the PICS is provided with an engineering workstation located in the PICS server room, which is used to perform system administrator functions.

The SHINE facility additionally contains local control stations for vendor provided nonsafety-related control systems. The vendor provided nonsafety-related control systems are further described in Subsection 7.3.2.

The building automation system contains two control stations, one located in the resource building and the other located in the main production facility mezzanine. The control stations are used for periodic adjustments and maintenance on systems served by the building automation system and is not used for normal operation.

The supercell contains an operator interface for the supercell control system used for controlling hot cell functions.

The radioactive liquid waste immobilization (RLWI) system contains an operator interface for the RLWI control system for controlling RLWI equipment functions.

A portable NDAS local control station is provided for controlling one NDAS unit at a time during maintenance and commissioning. The station performs the same functions as the control room NDAS control station, but is not normally connected to an NDAS unit, and is not used for normal operation. The NDAS local control station is also used for controlling an NDAS unit located in the NDAS service cell.

7.6.2 DESIGN CRITERIA

There are no SHINE facility design criteria that are uniquely applicable to the control console and display instruments (other than criteria 1-8 identified in Section 3.1, Tables 3.1-1 and 3.1-2, which are generically applicable to the facility as a whole). The system design criteria applicable to the control console and display instruments are addressed in this section.

7.6.2.1 SHINE Facility Design Criteria

There are no SHINE facility design criteria that are uniquely applicable to the control console and display instruments.

7.6.2.2 System Design Criteria

7.6.2.2.1 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.

Physical access to the control room and access to the equipment within is controlled as described in Subsection 7.6.3.4. The PICS does not allow remote access and includes the capability to disable unneeded networks, communication ports and removable media drives or provide engineered barriers (Subsection 7.3.3.5).

7.6.2.2.2 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.

The development of software for the PICS, which includes the PICS operator workstations and the main control board, follows a structured process as described in Subsection 7.3.3.4. The development of software for the NDAS workstation follows the structured process described in Subsection 7.3.3.4.

PICS Criterion 12 – The operator workstation and main control board development lifecycle 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.

The security requirements imposed on the PICS, which includes the PICS operator workstations and the main control board, are described in Subsection 7.3.3.5. Security requirements imposed during the development of NDAS controls are also described in Subsection 7.3.3.5.

PICS Criterion 13 – The operator workstation and main control board software development lifecycle process requirements shall be described and documented in appropriate plans which shall address verification and validation (V&V) and configuration control activities.

The PICS software, including the operator workstation and main control board software, is developed in accordance with the PICS validation master plan, which addresses V&V and configuration control activities, as described in Subsection 7.3.3.4.

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.

The PICS validation master plan assures that the required PICS hardware and software are installed in the appropriate system configuration and ensures that the correct version of the hardware/firmware is installed in the correct hardware components as described in Subsection 7.3.3.4. Configuration control of the NDAS control system is also described in Subsection 7.3.3.4.

7.6.2.2.3 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.

There are no time constrained operator-required responses. The main control board is readily accessible by operators normally located at either PICS operator workstation.

> 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.

Loss of power, power surges, or power interruption to the operator workstations does not result in a change of position of any controlled components nor does it result in the loss of displaying required parameters from TRPS (Table 7.4-1) or ESFAS (Table 7.5-1) on the main control board.

> 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.

Parameters required to be displayed per TRPS (Table 7.4-1) and ESFAS (Table 7.5-1) are displayed on the main control board and are accessible from the operator and supervisor workstations. Display and control functions are further described in Subsection 7.6.3.1.

7.6.2.2.4 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.

The PICS outputs to TRPS and ESFAS will not impede on the ability of the safety systems to execute their safety functions due to the prioritization of safety signals in the TRPS and ESFAS (Subsections 7.4.3.12 and 7.5.3.11) and the use of the enable nonsafety switch (Subsections 7.4.3.3 and 7.5.3.2).

> 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.

The PICS communication to displays external to the PICS is controlled through one-way data diodes such that no communication outside of the PICS can have an impact on the operation of the PICS (Subsection 7.6.4.5)

7.6.2.2.5 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.

Loss of power to the operator workstations or main control board does not result in a change of position for any controlled components. The control room is not an adverse environment and is maintained at an acceptable temperature for continued equipment operation for at least two hours following a loss of ventilation (Subsection 7.6.3.2).

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.

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 backup power to the PICS if normal power is interrupted (Subsection 7.6.3.5).

7.6.2.2.6 Surveillance

PICS Criterion 22 – The operator workstations and main control board shall be readily testable.

The operator workstations and main control board are part of the PICS. In-service self-testing capabilities of the PICS are described in Subsection 7.6.4.5.

7.6.2.2.7 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.

The design of the facility control room, display screens, and operator interfaces incorporates human factors engineering principles (Subsection 7.1.5). 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 (Subsection 7.6.3.3).

7.6.2.2.8 Annunciators

PICS Criterion 24 – Alarms and annunciators shall clearly show the status of the operating systems, interlocks, engineered safety feature initiations, confinement status, and radiation fields and concentration.

Alarm indication is provided on both the operator workstations and the main control board as described in Subsection 7.6.4.2. The types of alarms provided, including the status of operating systems, interlocks, engineered safety feature initiations, confinement status, and radiation fields and concentration, are described in Subsection 7.3.2.

PICS Criterion 25 – Hardware and software failures shall be assessed in reliability analyses of the annunciators used to support normal and emergency operations.

The annunciators are integral to the PICS and are not designed as a separate system. Operational qualification testing of the PICS is performed as described in Subsection 7.3.3.4. Hardware testing of the PICS is performed as described in Subsection 7.3.4.2.

7.6.2.2.9 Quality

<u>PICS Criterion 26</u> – Controls over the design, fabrication, installation, and modification of the operator workstations and main control board shall conform to commercial quality standards following accepted engineering and industrial practices..

The PICS operator workstations and main control board are part of the PICS and are designed, fabricated, and installed in accordance with the PICS validation master plan, which includes provisions for operational qualification testing as described in Subsection 7.3.3.4. The NDAS control stations are designed, fabricated, and installed in accordance with vendor procedures approved by SHINE. During facility operation, modifications to either the PICS or NDAS controls are controlled in accordance with SHINE work control processes.

7.6.3 DESIGN BASIS

7.6.3.1 Display and Control Functions

Each IU-specific set of static display screens on the main control board indicates variables important for verifying proper operation of safety systems following automatic actuation of the TRPS. The facility process set of static display screens 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 main control board 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 PICS operator workstations have multiple equipment control display screens available to support normal control functions and provide indication of alarms. The PICS 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 displays so that the supervisor can select and monitor the appropriate screen applicable to the current tasks being performed by the operator. Control of select processes or IUs may be transferred to the supervisor workstation at the discretion of the control room supervisor.

The NDAS control stations display variables associated with the neutron drivers located in each IU. The NDAS interface is used by operators to monitor and make adjustments to the neutron drivers in the eight IU cells. Each NDAS control station has the ability to monitor and control any of the eight neutron drivers, but the NDAS control station is only allowed to provide control signals to an NDAS unit when a permissive provided by the PICS is satisfied. The NDAS control station permissive is enabled or disabled using the PICS operator (or supervisor) workstation. Selectively enabling this control permissive is used to prevent both NDAS control stations from providing conflicting commands to a single NDAS unit.

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 equipment is 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

The resultant temperature is within the temperature indicated in Table 7.2-2 for at least two hours, which is sufficient time to ensure that safety-related equipment is able to perform its safety function if required. 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 incorporates human factors engineering principles. The layout of screens presenting the same set of information at multiple locations is identical for each (i.e., PICS operator workstation, supervisor workstation, local control station, or main control board). The displays and controls are generally grouped by system to aid the operator in the recognition and operation of the controls.

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 main control board static display screens are directly in front of the operator workstation.

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 ensures consistency in look and function. These push buttons also include a positive position indication and a protective guard to prevent inadvertent actuation.

7.6.3.4 Access Control

Access is administratively controlled to both the facility control room and the facility control systems. The facility control room is located within the main production facility, and personnel access to the control room and the main production facility is controlled in accordance with facility procedures. The PICS does not allow remote access and does not use any wireless interface capabilities for control functions, as described in Subsection 7.3.3.5. Access control for safety-related control systems is described in Subsection 7.4.4.1.3.

Use of the PICS, including use of the local control stations, requires the user to log in using a personal username and password. Additionally, the use of a local control station is required to be authorized via PICS permissions by a control room supervisor to prevent unauthorized use.

The usage of portable storage devices or other personal electronic equipment is controlled by facility procedures.

7.6.3.5 Loss of External Power

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 SGS provides backup power to the PICS if normal power is interrupted.

7.6.4 OPERATION AND PERFORMANCE

7.6.4.1 Displays

Displays of information related to the operation of the main production 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 is 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 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 PICS operator workstation 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 PICS operator workstation displays, the following variables used in determining and assessing the magnitude of radioactive material release are provided for display at the operator workstations:

- Stack release monitor emissions
- Carbon delay bed effluent monitor emissions
- Radiological ventilation zone 1 (RVZ1) radiologically control area (RCA) exhaust radiation detectors emissions
- Radiological ventilation zone 2 (RVZ2) RCA exhaust radiation detectors emissions

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.

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 (Subsection 7.6.1.6).

7.6.4.2 Alarms

Alarms are integrated into the PICS display systems. The operator workstations provide 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. Indication of alarms present is also provided for each IU and for the facility process systems at the main control board. Alarms are provided to inform the operator of off-normal operating system status, interlocks, engineered safety feature initiations, confinement status, and radiation fields and concentration. Alarms for facility systems are further described in Subsection 7.3.2.

7.6.4.3 Controls

Manual controls are provided on both of the PICS operator workstations, via input to the PICS, and on the main control board.

Manual controls for the safety-related TRPS and ESAFS protective functions are located at the main control board. 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 associated IU or for the facility process section. A safety-related enable nonsafety switch is located in each main control board section next to the manual push buttons to allow the operator 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, a single manual key switch is located at the facility process section of the main control board below the static display screens. The switch has two positions of operation, Secured and Operating.

Manual actuation inputs from the main control board are connected downstream of the safety-related control system programmable logic functions as described in Subsection 7.4.5.2.4.

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 (or NDAS) 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 PICS operator workstations, the supervisor workstation, and the local PICS control stations is provided, such that each PICS operator workstation is normally assigned a specific set of IUs or processes for which the PICS displays provide control functions. The supervisor workstation is not normally assigned control functions, and the local PICS control stations are only assigned limited control functions when approved by a control room supervisor. For PICS display screens where the station has not been assigned a control function, the PICS displays provide monitoring capabilities only. Limiting control capabilities for each IU or facility system or process to a single workstation at a given time prevent two operators from entering conflicting commands to a single component or process. On a failure of one PICS operator workstation, control functions assigned to that station can be transferred to the remaining PICS operator workstation or the supervisor workstation.

The NDAS control stations can each provide control of any of the eight neutron drivers, but each NDAS control station can only provide control commands to one neutron driver at any given time.

7.6.4.4 Information Retrieval

The variables monitored by each of the safety systems, radiation monitoring systems, and the PICS are 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. The data historian provides the ability to retrieve post-event data logging. 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.

7.6.4.5 Reliability

Local batteries are provided for PICS servers, the operator workstations, and the main control board to ensure the PICS continues to operate for at least 10 minutes after a loss of external power event and the SGS provides backup power to the PICS if normal power is interrupted (Subsection 7.6.3.5).

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.

The PICS has in-service self-testing capabilities such that the system will alarm if individual points or an entire rack or cabinet loses communications or faults.

7.6.4.6 Technical Specifications and Surveillance

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 in, the bases that are described in the technical specifications.

7.6.5 CONCLUSION

The SHINE facility control room is located in the non-radiologically controlled area of the main production facility and contains the necessary workstations, displays, and control cabinets needed for the operation of the main production facility. The main control board, PICS operator and supervisor workstations, and associated control cabinets are considered part of the 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. The PICS interfaces with the safety-related TRPS, ESFAS, NFDS, and safety-related radiation monitors to provide nonsafety-related system status and measured process variable values for viewing, recording, and trending.

Control interfaces are also provided both in the control room and locally in the SHINE facility for other vendor provided nonsafety-related control systems that interface with the PICS.

The control console and display instruments are designed for functionality and high reliability.

The control console and display instruments are designed for the normal environment and for specified time intervals following a design basis event or loss of ventilation. No safety-related ventilation or cooling systems are required for the facility control room.

Figure 7.6-1 – Facility Control Room Layout

Figure 7.6-2 – Main Control Board Sections

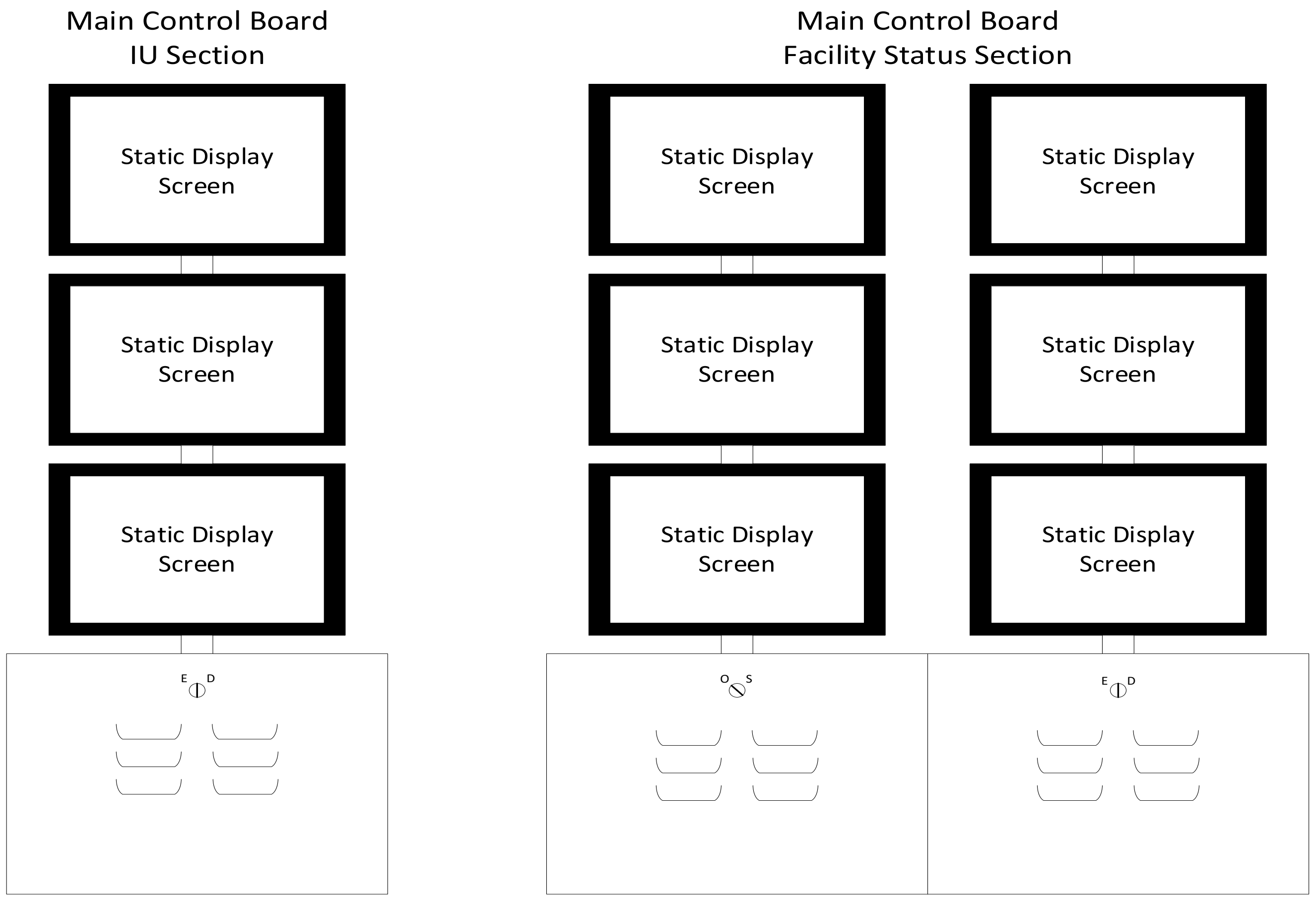
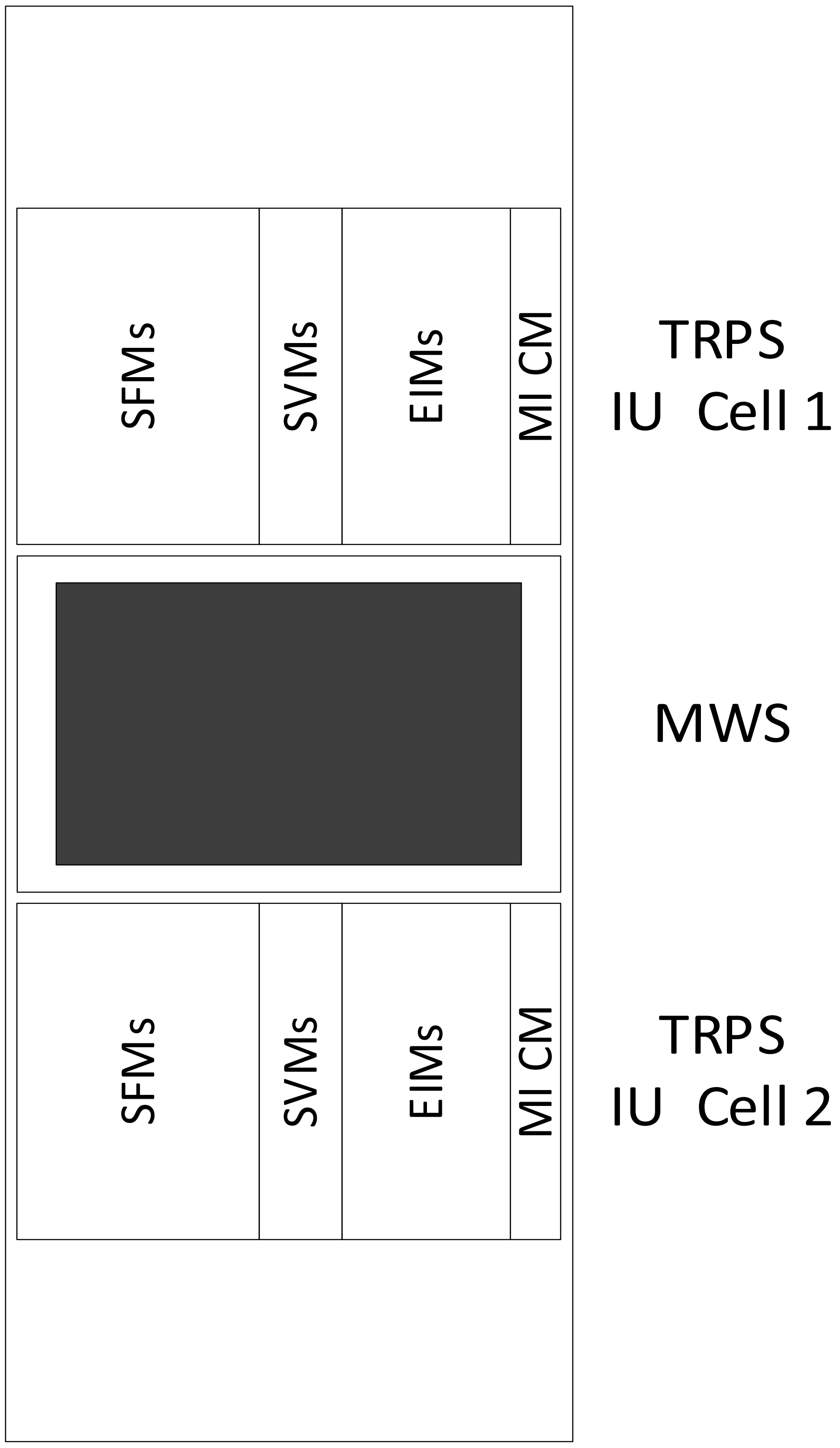


Figure 7.6-3 – Maintenance Workstation



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); and
- effluent monitoring consisting of the stack release monitoring system (SRMS).

The objective of the radiation monitoring systems is to:

- provide 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 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 TRPS and ESFAS are provided in Figure 7.4-1 and Figure 7.5-1, respectively.

7.7.1.2 Design Criteria

The SHINE facility design criteria applicable to the safety-related process radiation monitors are addressed in this section. SHINE facility design criteria 13 and 38 apply to the safety related radiation monitors.

7.7.1.2.1 Instrumentation and Controls

> SHINE Design Criterion 13 – Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated transients, and for postulated accidents as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the primary system boundary, the primary confinement and its associated systems, and the process confinement boundary and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating ranges.

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 (Subsection 7.7.1.3.1). Setpoints are selected based on analytical limits and calculated to account for known uncertainties in accordance with the setpoint determination methodology and the monitors are periodically functionally tested and maintained (Subsection 7.7.1.4.3).

7.7.1.2.2 Monitoring Radioactivity Releases

> SHINE Design Criterion 38 – Means are provided for monitoring the primary confinement boundary, hot cell, and glovebox atmospheres to detect potential leakage of gaseous or other airborne radioactive material. Potential effluent discharge paths and the plant environs are monitored for radioactivity that may be released from normal operations, including anticipated transients, and from postulated accidents.

The safety-related process radiation monitors provide radiation monitoring for the primary confinement boundary, hot cell, and glovebox atmospheres and monitor effluent release paths (Subsection 7.7.1.4.1). The monitors are designed to operate during normal conditions, anticipated transients and design basis accidents (Subsection 7.7.1.4).

7.7.1.3 Design Bases

7.7.1.3.1 Design Bases Functions

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 is provided in Section 7.4 and Section 7.5, respectively.

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 (channels) is 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.

A list of safety-related process radiation monitors, specifying the monitored location, number of sensing channels 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 7.4-1 and Table 7.5-1. Instrument accuracies are appropriate for the associated setpoints. Signal processing time for the ESFAS and TRPS is provided in Subsection 7.4.5.2.3.

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.

7.7.1.3.2 Operating Conditions

During normal operation, the process radiation monitors are designed to operate in the normal environmental conditions (temperature, pressure, relative humidity) identified in Tables 7.2-2 through 7.2-5 for an expected 20-year lifetime of the equipment.

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.

7.7.1.3.3 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 ensures that a failure of one monitor will not prevent the control system from performing its safety function.

The Channel A process radiation monitors receive power from Division A of the uninterruptible power supply system (UPSS), and Channel B monitors receive power from UPSS Division B. Channel 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.

7.7.1.3.4 Independence

Safety-related process radiation monitors provide analog communication to the ESFAS and TRPS controls. Channel 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.

7.7.1.3.5 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 Channels 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.

7.7.1.3.6 Human Factors, Display and Recording

Selection and display of process radiation monitor variables are designed with consideration of human factors engineering principles.

See Section 7.6 for additional discussion of information presented to facility operators and recorded for future use.

7.7.1.3.7 Fire Protection

Safety-related monitors in different channels are located in separate fire areas when practical. Physical separation is used to achieve separation of redundant sensors. Wiring for redundant channels uses physical separation and isolation to provide independence for circuits. Separation of wiring is achieved using separate wireways and cable trays for each channel. Spatial separation between cable and raceway groups is in accordance with IEEE 384-2008 (IEEE, 2008), Section 5.1.1.2, Section 5.1.3.3 Table 1, and Section 5.1.4 Table 2.

Cable, wire, and electrical connectors utilized to connect radiation monitoring components to the ESFAS or TRPS have certifications that demonstrate the ability to inhibit the propagation of flame in the event of a fire. The certifications use recognized industry standards or guidance.

Noncombustible and heat resistant materials are used where practical in the design.

7.7.1.3.8 Natural Phenomena Hazards and Dynamic Effects

The process radiation monitors are installed in the seismically qualified portion of the main production facility where they are protected from earthquakes, tornadoes, and floods (Subsections 7.4.3.6 and 7.5.3.5). The process radiation monitors are Seismic Category I, designed in accordance with Section 8 of IEEE Standard 344-2013 (IEEE, 2013)

(Subsection 7.7.1.3.8). Hurricanes, tsunamis, and seiches are not credible events at the SHINE facility (Subsections 2.4.5.1, 2.4.2.7, and 2.4.5.2).

7.7.1.3.9 Quality

The safety-related process radiation monitors are designed, procured, fabricated, erected, and tested in accordance with the SHINE Quality Program Description (QAPD). Quality records applicable to the design , procurement, fabrication, erection, and testing are maintained.

The following codes and standards are applied to the design of the safety-related process radiation monitors:

- IEEE 344-2013, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations (IEEE, 2013), Section 8.
- IEEE 384-2008, IEEE Standard Criteria for Independence of Class1E 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.

7.7.1.4 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.

7.7.1.4.1 Functionality

TRPS process radiation monitors monitor the ventilation line from the primary closed loop cooling system (PCLS) expansion tanks (i.e., radiological ventilation zone 1 exhaust subsystem [RVZ1e] irradiation unit [IU] cell radiation monitors). 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.

7.7.1.4.2 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 channel (Channel C) is provided for two-out-of-three voting capability.

Instrument ranges and response times are provided in Tables 7.4-1 and 7.5-1.

7.7.1.4.3 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 7.2.1.

Monitors are periodically functionally tested and maintained in accordance with the SHINE 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).

7.7.1.4.4 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 serves as the primary means of alerting individuals of the need to evacuate those areas 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 the operator workstations (via the PICS).

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 facility design criteria applicable to the RAMS are stated in Chapter 3, Table 3.1-2. The SHINE facility design criteria applicable to the RAMS are addressed in this section.

7.7.3.2.1 Applicable Design Criteria

> <u>SHINE Design Criterion 13</u> – Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated transients, and for postulated accidents as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the primary system boundary, the primary confinement and its associated systems, and the process confinement boundary and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating ranges.

The RAMS monitors gamma radiation levels as described in Subsection 7.7.3.3.1, which cover a range from low normal background (below the definition of a radiation area) to 100 times the definition of a high radiation area (100 mrem/hour), in order to monitor radiation during normal operations, anticipated transients, and postulated accidents.

> <u>SHINE Design Criterion 38</u> – Means are provided for monitoring the primary confinement boundary, hot cell, and glovebox atmospheres to detect potential leakage of gaseous or other airborne radioactive material. Potential effluent discharge paths and the plant environs are monitored for radioactivity that may be released from normal operations, including anticipated transients, and from postulated accidents.

The RAMS monitors the general areas of the plant environs for radioactivity as described in Subsection 7.7.3.1.

7.7.3.3 Design Bases

7.7.3.3.1 Design Bases Functions

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.

Each RAMS unit is designed to detect direct radiation from 0.1 mrem/hr up to 10 rem/hr. RAMS units have an accuracy of at least 25 percent of the measured value.

7.7.3.3.2 Operating Conditions

RAMS units are designed to operate in the normal environmental conditions presented in Tables 7.2-1 and 7.2-3.

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.

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 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.

7.7.3.4.1 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 facility design criteria applicable to the CAMS are stated in Chapter 3, Table 3.1-2. The SHINE facility design criteria applicable to the CAMS are addressed in this section.

7.7.4.2.1 Applicable Design Criteria

> <u>SHINE Design Criterion 13</u> – Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated transients, and for postulated accidents as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the primary system boundary, the primary confinement and its associated systems, and the process confinement boundary and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating ranges.

The CAMS units monitor alpha and beta airborne activity concentration and tritium airborne activity concentration as described in Subsection 7.7.4.3.1. For alpha and beta airborne activity concentration detection, the design range is 10 percent DAC up to 1,000,000 DAC. For tritium airborne activity concentration detection, the design range is 5 percent DAC up to 50,000 DAC.

> <u>SHINE Design Criterion 38</u> – Means are provided for monitoring the primary confinement boundary, hot cell, and glovebox atmospheres to detect potential leakage of gaseous or other airborne radioactive material. Potential effluent discharge paths and the plant environs are monitored for radioactivity that may be released from normal operations, including anticipated transients, and from postulated accidents.

The CAMS monitors the facility environment where personnel are normally present and where contamination levels could become significant. The CAMS provides real time sampling for alpha, beta, and tritium. The CAMS is provided with backup power from the SGS (Subsection 7.7.4.1). The monitor locations are shown in Table 7.7-3.

7.7.4.3 Design Bases

7.7.4.3.1 Design Bases Functions

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.

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 $\mu Ci/m^3$, with a span of at least four decades of monitoring capability.

7.7.4.3.2 Operating Conditions

CAMS units are designed to operate in the normal environmental conditions presented in Table 7.2-3.

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.

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.

7.7.4.4.1 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 main production facility are within regulatory limits and do 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 main production 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 do 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 facility design criteria are described in Section 3.1. The SHINE facility design criteria applicable to the SRMS are provided in Table 3.1-2.

7.7.5.2.1 Applicable Design Criteria

> SHINE Design Criterion 13 – Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated transients, and for postulated accidents as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the primary system boundary, the primary confinement and its associated systems, and the process confinement boundary and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating ranges.

The SRMS continuously monitors noble gases that are present in facility effluent streams and allows for the collection and analysis of particulate, iodine, and tritium (Subsection 7.7.5.3.1). 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 (Subsection 7.7.5.4). The SRM and CDBEM instrument ranges are provided in Subsection 7.7.5.3.1.

> SHINE Design Criterion 38 – Means are provided for monitoring the primary confinement boundary, hot cell, and glovebox atmospheres to detect potential leakage of gaseous or other airborne radioactive material. Potential effluent discharge paths and the plant environs are monitored for radioactivity that may be released from normal operations, including anticipated transients, and from postulated accidents.

The SRMS continuously monitors noble gases that are present in facility effluent streams and allows for the collection and analysis of particulate, iodine, and tritium (Subsection 7.7.5.3.1). 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 (Subsection 7.7.5.4).

7.7.5.3 Design Bases

7.7.5.3.1 Design Basis Functions

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.

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 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.

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.

7.7.5.3.2 Operating Conditions

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.

7.7.5.3.3 Quality

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)

7.7.5.4 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. 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 initial channel calibration for the SRM and CDBEM noble gas detectors is performed using standards traceable to NIST.

7.7.5.4.1 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.

7.7.6 CONCLUSION

Radiation monitoring within the SHINE facility is performed by multiple radiation monitoring processes. The radiation monitoring supports facility control room operations, provides information and alarms for personnel within the facility, provides input to safety-related control systems to actuate safety systems, and provides the ability to monitor radioactive releases to the environment.

The radiation monitoring systems and equipment are designed to applicable SHINE facility design criteria and applicable quality standards to support reliable operation in performing the radiation monitoring functions.

Table 7.7-1 – Safety-Related Process Radiation Monitors (Sheet 1 of 4)

Unit	Monitored Material	Monitored Location	Unit Location	Function	Total Available Channels	Minimum Required Channels	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 Channels	Minimum Required Channels	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 Channels	Minimum Required Channels	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 Channels	Minimum Required Channels	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

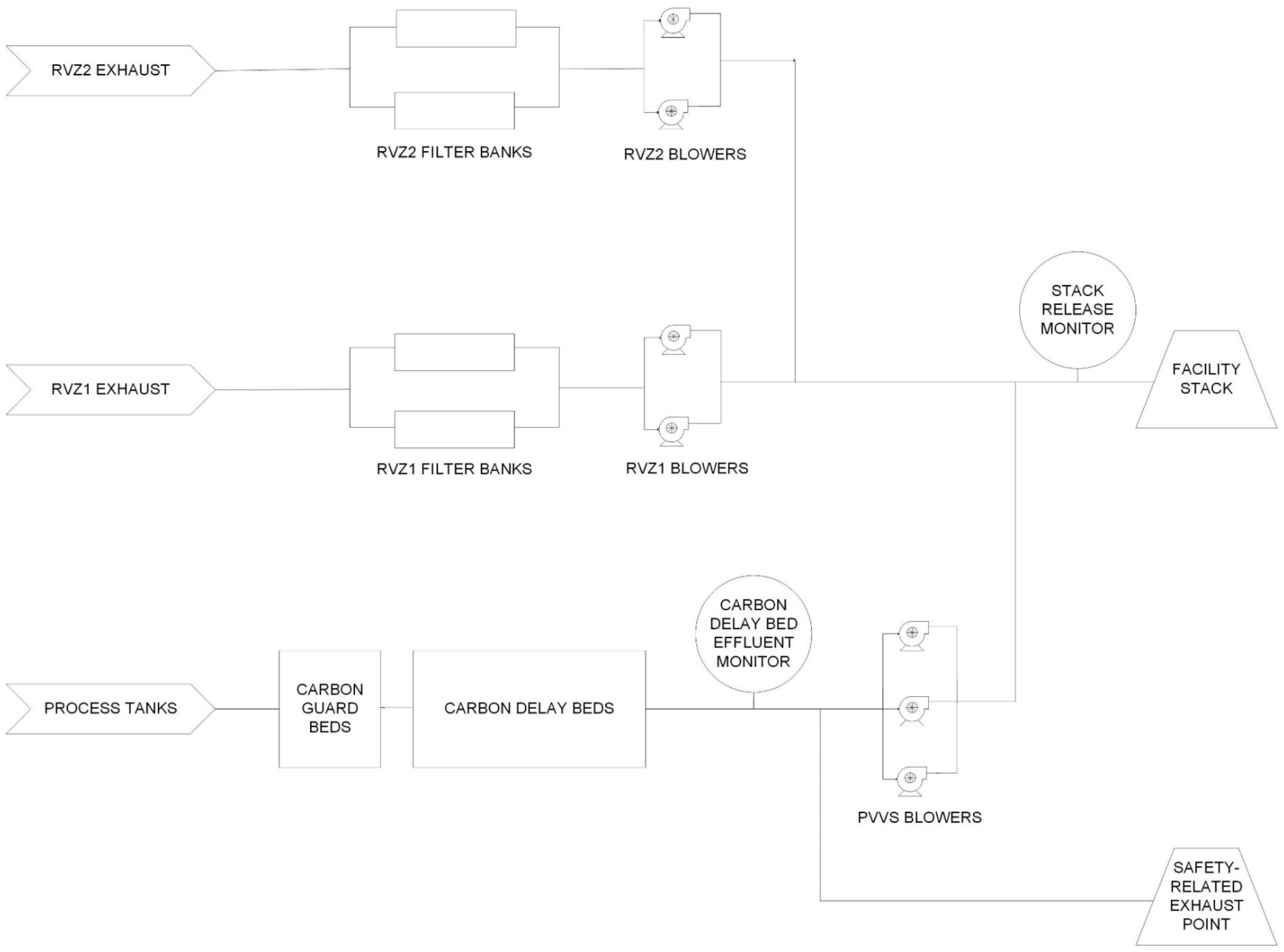
Table 7.7-2 – Radiation Area Monitor Locations

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

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
Airborne Monitor 7	Alert personnel of high contamination levels from filter banks	Safety-related area mezzanine, facility mezzanine
Airborne Monitor 8	Alert laboratory personnel of high contamination levels	North laboratory, ground floor
Airborne Monitor 9	Alert laboratory personnel of high contamination levels	South laboratory, ground floor
Airborne Monitor 10	Alert personnel of high contamination levels from target solution preparation activities	Target solution preparation room, ground floor
Airborne Monitor 11	Alert personnel of high contamination levels from target solution preparation activities	Uranium storage room, ground floor
Tritium Monitor 12	Alert personnel of high tritium levels from the TPS glovebox	TPS room, ground floor
Tritium Monitor 13	Alert personnel of high tritium levels in the main IF corridor	Main IF corridor, ground floor

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 where the signal processing units are located. The signal processing units perform measurement of the neutron flux signal from the pre-amplifier, signal processing, 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 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.

The NFDS is a three-division system with three detectors positioned around the subcritical assembly support structure (SASS) at approximately 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 facility control room. 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 filling with the target solution.

7.8.2 DESIGN CRITERIA

The SHINE facility design criteria applicable to the NFDS are as stated in Chapter 3, Table 3.1-1. The facility design criteria applicable to the NFDS, and the NFDS system design criteria, are addressed in this section.

7.8.2.1 SHINE Facility Design Criteria

SHINE facility design criteria 13 through 19 apply to the NFDS.

7.8.2.1.1 Instrumentation and Controls

<u>SHINE Design Criterion 13</u> – Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated transients, and for postulated accidents as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the primary system boundary, the primary confinement and its associated systems, and the process confinement boundary and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating ranges.

The NFDS provides continuous indication of the neutron flux during operation, from filling through maximum power during irradiation (Subsection 7.8.1). The neutron flux detector setpoints bound normal operations and accident conditions and provide margin to analytical limits (Subsection 7.8.4.3). Setpoints are established based on a documented methodology and accounts for uncertainties in each instrument channel (Subsection 7.8.2.2.5). The NFDS supports maintenance and testing to ensure operability as required by the technical specifications (Subsection 7.8.3.10).

7.8.2.1.2 Protection System Functions

<u>SHINE Design Criterion 14</u> – The protection systems are designed to:

1) initiate, automatically, the operation of appropriate systems to ensure that specified acceptable target solution design limits are not exceeded as a result of anticipated transients; and
2) sense accident conditions and to initiate the operation of safety-related systems and components.

Neutron flux detector setpoints bound normal operations and accident conditions and provide margin to analytical limits (Subsection 7.8.4.3). Upon reaching the neutron flux signal setpoints (Table 7.4-1), automatic safety actuations are initiated by the TRPS, as described in Subsection 7.4.4.1.

7.8.2.1.3 Protection System Reliability and Testability

<u>SHINE Design Criterion 15</u> – The protection systems are designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection systems are sufficient to ensure that:

1) no single failure results in loss of the protection function, and
2) 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 protection systems are designed to permit periodic testing, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

The NFDS is comprised of three redundant divisions of detectors, preamplifiers, and processing circuits for single failure protection. Interfacing systems with the NFDS are downstream of the NFDS such that a failure of an interfacing nonsafety system will not impact the NFDS (Subsection 7.8.3.3 and Figure 7.4-1). The NFDS supports maintenance and testing 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 (Subsection 7.8.3.10). The independent NFDS divisions interface with TRPS, which has been analyzed for single failure in accordance with IEEE Standard 379-2000 (IEEE, 2000) for all inputs, including NFDS.

7.8.2.1.4 Protection System Independence

SHINE Design Criterion 16 – The protection systems are designed to ensure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function or are demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, are used to the extent practical to prevent loss of the protection function.

The NFDS is qualified for operation during and after a seismic design basis event using the guidance in IEEE Standard 344-2013 (IEEE, 2013) (Subsection 7.8.3.8). The NFDS components are located in the RPF, the IF, and facility control room and are protected from seismic events, tornado wind, tornado missile and external flooding (Subsection 7.8.3.8). Hurricanes, tsunamis, and seiches are not credible events at the SHINE facility (Subsection 2.4.5.1, 2.4.2.7, and 2.4.5.2). Physical and electrical independence (Subsection 7.8.3.4), redundancy (Subsection 7.8.3.3), equipment qualification (Subsection 7.8.3.7) and quality in design (Subsection 7.8.3.11) are applied in the NFDS design to prevent loss of the protective function.

7.8.2.1.5 Protection System Failure Modes

SHINE Design Criterion 17 – The protection systems are designed to fail into a safe state if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments are experienced.

The NFDS is designed so that a failure due to loss of power to the NFDS or a removal of an NFDS channel presents to TRPS as zero current on the analog outputs to allow TRPS to treat the condition as a positive trip determination . The interaction between NFDS and TRPS is shown in Figure 7.4-1 (Subsection 7.8.3.5).

7.8.2.1.6 Separation of Protection and Control Systems

SHINE Design Criterion 18 – The protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.

The NFDS is comprised of three redundant divisions of detectors, preamplifiers, and processing circuits for single failure protection (Subsection 7.8.3.3). Communications from the NFDS to the

TRPS and PICS are continuous through isolated outputs that only allow the data to be transmitted out of the system so that no failure from an interfacing system can affect the functions of the NFDS (Subsection 7.8.3.2).

7.8.2.1.7 Protection Against Anticipated Transients

SHINE Design Criterion 19 – The protection systems are designed to ensure an extremely high probability of accomplishing their safety functions in the event of anticipated transients.

The NFDS is comprised of three redundant divisions of detectors, preamplifiers, and processing circuits for single failure protection (Subsection 7.8.3.3). The three divisions of the NFDS are physically and electrically independent of each other (Subsection 7.8.3.4) and the NFDS equipment is qualified for normal and transient conditions (Subsections 7.8.3.6 and 7.8.3.7).

7.8.2.2 NFDS System Design Criteria

7.8.2.2.1 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.

The neutron flux detector setpoints bound normal operations and accident conditions and provide margin to analytical limits (Subsection 7.8.4.3).

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.

The NFDS provides continuous indication of the neutron flux from zero counts per second to at least 250 percent power with two decades of overlap (Subsection 7.8.3.1).

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.

The NFDS power range provides a signal proportional to TSV power level from 0 to 125 percent of the licensed power limit. The source range provides a current signal proportional to count rate for all expected startup count rates (Subsection 7.8.3.1).

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.

Each NFDS division includes a fission chamber detector and a Boron Trifluoride (BF_3) detector pair. These detector types are primarily sensitive to thermal neutrons with excellent gamma rejection.

> <u>NFDS Criterion 5</u> – The NFDS shall provide redundant TSV power level indication through the licensed maximum power range.

The NFDS is comprised of three redundant divisions of detectors, preamplifiers, and processing circuits for single failure protection (Subsection 7.8.3.3). The wide range neutron flux monitors percent power up to 250 percent of the licensed power limit (Subsection 7.8.3.1.3). The power range neutron flux signal has a range of 0 percent to 125 percent of the licensed power limit (Subsection 7.8.3.1.2).

> <u>NFDS Criterion 6</u> – 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.

The positioning of the NFDS source range detectors, and the location, and emission rate of the subcritical multiplication source, is designed so that all three channels are on scale throughout filling. This includes while the TSV is empty of solution. NFDS source range signal increases with increasing target solution volume, and in this way, increasing reactivity will always produce an increase in count rate.

> <u>NFDS Criterion 7</u> – 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.

The wide range neutron flux monitors percent power up to 250 percent of the licensed power limit (Subsection 7.8.3.1.3). The power range neutron flux signal has a range of 0 percent to 125 percent of the licensed power limit (Subsection 7.8.3.1.2).

> <u>NFDS Criterion 8</u> – 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.

Communications from the NFDS to the TRPS and PICS are continuous through isolated outputs that only allow the data to be transmitted out of the system so that no failure from an interfacing system can affect the functions of the NFDS (Subsection 7.8.3.2).

> <u>NFDS Criterion 9</u> – 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.

The NFDS detectors are housed in a watertight assembly qualified for submergence to a depth of up to 16 feet (Subsection 7.8.3.7). The detector housings are supported using brackets attached to the outer shell of the SASS (Subsection 7.8.1). The detectors are installed approximately 120 degrees equidistant around the SASS in relation to the target solution vessel (Subsection 7.8.3.4).

> <u>NFDS Criterion 10</u> – The timing of NFDS communications shall be deterministic.

The timing of NFDS communications is deterministic.

7.8.2.2.2 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.

The NFDS is comprised of three redundant divisions of detectors, preamplifiers, and processing circuits for single failure protection. Interfacing systems with the NFDS are downstream of the NFDS such that a failure of an interfacing nonsafety system will not impact the NFDS (Subsection 7.8.3.3 and Figure 7.4-1). Communications from the NFDS to the TRPS and PICS are continuous through isolated outputs that only allow the data to be transmitted out of the system so that no failure from an interfacing system can affect the functions of the NFDS (Subsection 7.8.3.2).

NFDS Criterion 12 – The NFDS shall be designed such that no single failure can cause the failure of more than one redundant component.

The NFDS is comprised of three redundant divisions of detectors, preamplifiers, and processing circuits for single failure protection (Subsection 7.8.3.3). The three divisions of the NFDS are physically and electrically independent of each other (Subsection 7.8.3.4).

7.8.2.2.3 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.

The three divisions of the NFDS are physically and electrically independent of each other (Subsection 7.8.3.4). The NFDS detector cables are routed back to the control room in physically separated cable trays and raceways (Subsection 7.8.3.4) in accordance with IEEE Standard 384-2008 (IEEE, 2008) (Subsection 7.8.3.11). Interfacing systems with the NFDS are downstream of the NFDS such that a failure of an interfacing nonsafety system will not impact the NFDS (Subsection 7.8.3.3).

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.

The three divisions of the NFDS are physically and electrically independent of each other (Subsection 7.8.3.4). Interfacing systems with the NFDS are downstream of the NFDS such that a failure of an interfacing nonsafety system will not impact the NFDS (Subsection 7.8.3.3). 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 (Subsection 7.8.3.2).

7.8.2.2.4 Fail Safe

> NFDS Criterion 15 – The NFDS and associated components shall be designed to assume a safe state on loss of electrical power.

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. 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 (Subsection 7.8.3.5).

> 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.

The NFDS utilizes a fault-tolerant, triple redundant architecture. This design identifies and compensates for failed system elements. Because of the triple redundant architecture of the NFDS platform, failure mechanisms that affect a single function have no effect on plant operation.

7.8.2.2.5 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.

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 7.2.1.

> NFDS Criterion 18 – Adequate margin shall exist between setpoints and safety limits so that the TRPS initiates protective actions before safety limits are exceeded.

Setpoints applicable to 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 7.2.1.

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.

The source range neutron flux measurement supports filling of the IU cell prior to irradiation of the target solution. The power range neutron flux measurement supports operations when the neutron driver is operating and irradiating the target solution, and the wide range neutron flux measurement overlaps the source range and power range and is usable during both source and power range levels. The instrument ranges and accuracies support the design functions for each range and are provided in Subsection 7.8.3.1 and Table 7.4-1.

7.8.2.2.6 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.

Rack mounted NFDS equipment is tested to appropriate standards to show that the effects of EMI/RFI and power surges are adequately addressed (Subsection 7.8.3.7). The codes and standards applicable to the NFDS design are stated in Subsection 7.8.3.11.

7.8.2.2.7 Surveillance

NFDS Criterion 21 – The NFDS shall provide the capability for calibration, inspection, and testing to validate the desired functionality of the NFDS.

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 (Subsection 7.8.3.10).

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.

The NFDS design 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 (Subsection 7.8.3.10).

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.

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 (Subsection 7.8.3.10).

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.

Limiting Conditions for Operation and Surveillance Requirements are established for the NFDS in the technical specifications (Subsection 7.8.4.3). The NFDS design supports testing and calibration to ensure operability as required by the technical specifications (Subsection 7.8.3.10).

7.8.2.2.8 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.

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

7.8.2.2.9 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.

NFDS input to TRPS safety functions are communicated to the PICS to alert the operators. The I&C system architecture is shown in Figure 7.1-1.

7.8.2.2.10 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 (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5 (USNRC, 2010).

ANSI/ANS 15.8-1995 (ANSI/ANS, 1995) is applied to the NFDS by the SHINE Quality Assurance Program (Subsection 7.8.3.11). The SHINE Quality Assurance Program controls activities related to the system design, fabrication, installation, and modification.

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.

Industry codes and standards are applied to the design of the NFDS to ensure quality in the design of this safety-related system (Subsection 7.8.3.11). The NFDS is also designed for the normal and transient operating environments, as described in Subsections 7.8.3.6 and 7.8.3.7.

7.8.3 DESIGN BASES

7.8.3.1 Design Bases Functions

The NFDS measures the neutron flux in the TSV over three separate ranges: source range, power range, and wide range.

7.8.3.1.1 Source Range

The source range measures low flux levels common to what would be expected during the filling of the IU cell prior to irradiation of the target solution.

The NFDS provides TRPS a count rate signal for TRPS to perform a trip determination upon reaching the source range setpoint. The TRPS initiates an IU Cell Safety Actuation when two-out-of-three or more high source range neutron flux signals from NFDS are above their setpoint (Subsection 7.4.4).

The NFDS transmits the following source range analog signal to the TRPS:

- NFDS source range

The analytical limit for the high source range trip determination is:

- Increasing at 2.52 times the nominal flux at 95 percent volume of the critical fill height

The source range neutron flux signal has an accuracy of less than or equal to 2 percent of the full linear scale.

7.8.3.1.2 Power Range

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 NFDS transmits the following power range analog signal to the TRPS:

- NFDS power range

The power range neutron flux signal is input to the safety-related trip determination by the TRPS. The TRPS initiates a Driver Dropout on low power range neutron flux, as described in Subsection 7.4.4 and initiates an IU Cell Safety Actuation on high (power range) time-averaged neutron flux, as described in Subsection 7.4.4.

The power range neutron flux signal has a range of 0 percent to 125 percent of the licensed power limit and has an accuracy of less than or equal to 1 percent of the full linear scale.

7.8.3.1.3 Wide Range

The wide range neutron flux connects the gap between the source range and the power range with overlap and is usable during both source and power range levels. The wide range neutron flux monitors percent power up to 250 percent of the licensed power limit.

The NFDS transmits the following wide range analog signals to the TRPS:

- NFDS wide range

The NFDS wide range neutron flux signal is input to the safety-related trip determination by the TRPS. The TRPS initiates an IU Cell Safety Actuation on high wide range neutron flux, as described in Subsection 7.4.4.

The wide range neutron flux signal has an accuracy of less than or equal to 1 percent of the full logarithmic scale.

7.8.3.2 Simplicity

The NFDS is an analog system with no digital communications for simplicity. 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.

7.8.3.3 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 ensuring the required safety functions perform as designed during a design basis event. Interfacing systems with the NFDS are downstream of the NFDS such that a failure of an interfacing nonsafety system will not impact the NFDS.

7.8.3.4 Independence

The three divisions of the NFDS are physically and electrically independent of each other. Detectors are installed approximately 120 degrees equidistant around the SASS in relation to the target solution vessel. The detector cables are routed back to the control room in physically separated cable trays and raceways.

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.

7.8.3.5 Loss of External Power

The NFDS is supplied power from the UPSS upon a loss of off-site power. The UPSS battery backup supplies power to the NFDS for a minimum of 10 minutes following a loss of off-site power.

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 in TRPS. The interaction between NFDS and TRPS is shown in Figure 7.4-1.

7.8.3.6 Operating Conditions

The NFDS control and logic functions are located inside the facility control room 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 3.5E+05 rad/hour) and are qualified to survive that environment.

The normal and transient environmental conditions present in areas where NFDS is located are provided in Table 7.2-2 through Table 7.2-4. The main production facility heating, ventilation, and air conditioning (HVAC) systems are relied upon to maintain the temperature and humidity parameters in these areas. The main production 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.

7.8.3.7 Equipment Qualification

The NFDS detectors are housed in a watertight assembly qualified for submergence to a depth up to 16 feet.

NFDS rack mounted equipment is installed in a mild operating environment and is designed to meet the normal and transient environmental conditions described in Subsection 7.8.3.6. Rack mounted NFDS 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 IEEE Standard 1050-2004 (IEEE, 2004b).

7.8.3.8 Natural Phenomena

The NFDS is qualified for operation during and after a seismic design basis event. The NFDS is qualified using the guidance in IEEE Standard 344-2013 (IEEE, 2013) (Subsection 7.8.3.11).

The NFDS components are located in the RPF, the IF, and facility control room. The facility control room is located in a non-radiologically controlled seismic area. The RPF, IF, and the non-radiologically controlled seismic area are classified as Seismic Class I structures (Section 3.4) that provide protection from tornado and tornado missiles (Subsection 3.2.2.3). The main production facility is protected from an external flood (Subsection 3.3.1.1.1).

7.8.3.9 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
- Wide range neutron flux
- Power range neutron flux

Operator display criteria and design are addressed in Section 7.6.

7.8.3.10 Maintenance and Testing

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.

7.8.3.11 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 16.
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).

7.8.4 OPERATION AND PERFORMANCE

The NFDS supports safe and reliable operation of the SHINE facility and prevents a single failure from defeating the intended NFDS functions.

7.8.4.1 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 2.5E-08 percent up to 250 percent covering the irradiation cycle both during deuterium-deuterium reactions and deuterium-tritium reactions.

7.8.4.2 Logic Processing Functions

The NFDS provides the following analog signals to the TRPS:

- NFDS source range
- NFDS wide range
- 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.

The TRPS transmits the analog signals as nonsafety-related signals to the PICS to display for operator use when monitoring conditions in the IU cells.

7.8.4.3 Technical Specifications and Surveillance

Limiting Conditions for Operation and Surveillance Requirements are established for the NFDS in the technical specifications. The neutron flux detector setpoints bound normal operations and accident conditions and provide margin to analytical limits.

7.8.5 CONCLUSION

The NFDS monitors neutron flux levels inside the target solution vessel to support safe operation of the SHINE facility. The system design includes a high source range neutron flux trip determination and neutron flux variables that are input to the TRPS for safety actuations. The NFDS also transmits signals to TRPS (Section 7.4) that are transmitted by TRPS as nonsafety-related neutron flux values to the PICS for display to the operators.

The system design incorporates independence and redundancy to ensure no single failure prevents the NFDS from fulfilling its intended safety functions.

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.

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, 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, 2017. Safety Evaluation by the Office of New Reactors, Licensing Topical Report (TR) 1015-18653-P (Revision 2), "Design of the Highly Integrated Protection System Platform," NuScale Power, LLC, U.S. Nuclear Regulatory Commission, May 2017.