ENCLOSURE 3

SHINE TECHNOLOGIES, LLC

SHINE TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE SUPPLEMENT NO. 13 AND RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION
PUBLIC VERSION

The U.S. Nuclear Regulatory Commission (NRC) staff determined that additional information was required (Reference 1) to enable the continued review of the SHINE Technologies, LLC (SHINE) operating license application (Reference 2). The following information is provided by SHINE in response to the NRC staff's request.

Chapter 7 – Instrumentation and Control Systems

RAI 7-20

NUREG-1537, Part 2, Section 7.4, "Reactor Protection System," states, in part, that the safety analysis report (SAR) should describe the protection system, "listing the protective functions performed by the [protection system], and the parameters monitored to detect the need for protective action." Section 7.4 further states that the facility should have "operable protection capability in all operating modes and conditions, as analyzed in the SAR" and "[t]he range of operation of sensor (detector) channels should be sufficient to cover the expected range of variation of the monitored variable during normal and transient…reactor operation." NUREG-1537, Part 2, Section 7.4, states, in part, that the protection system should be "designed to perform its safety function after a single failure and to meet requirements for seismic and environmental qualification, redundancy, diversity, and independence." NUREG-1537, Part 2, Section 7.4, also states that the protection systems should be "designed for reliable operation in the normal range of environmental conditions anticipated within the facility." Therefore, the design of the protection systems should consider features that can ensure the reliability of the system such as independence, redundancy, diversity, maintenance, testing, and quality components.

Similarly, NUREG-1537 Sections 7.1, "Summary Description," and 7.5, "Engineered Safety Features Actuation Systems," state that in the FSAR, the applicant should "describe all the Engineered Safety Features (ESFs) in the facility design and summarize the postulated accidents whose consequences could be unacceptable without mitigation…..These summaries should include the design bases, the performance criteria, and the full range of reactor conditions, including accident conditions, under which the equipment or systems must maintain function." The information to be reviewed should also include the "design criteria of each ESF actuation system, and the design bases and functional requirements for the ESF actuation

systems." Additionally, "[t]he ESF actuation system should be designed not to fail or operate in a mode that would prevent the [protection systems] from performing its designed function, or prevent safe reactor shutdown." The FSAR should also describe "the detector channels that sense the need for mitigation of possible consequences."

The SHINE FSAR does not have sufficient details and analysis of the design for the NRC staff to determine the adequacy of the protection systems and their consideration of features that can ensure the reliability of the system such as independence, redundancy, diversity, maintenance, testing, and quality components. Parts (a) through (g) of this RAI are intended to address topics related to monitored variables, logic, safety functions, functional diversity, terminology, and calculations to obtain the necessary detail and analysis of the SHINE TRPS and ESFAS so that the NRC staff can make the applicable findings in Chapter 7 of NUREG-1537, Part 2.

As SHINE prepares responses to the RAIs below, it may consider uploading supporting reference documentation to its electronic reading room, such as the TRPS and ESFAS system requirement specifications; TRPS and ESFAS system design descriptions; and TRPS and ESFAS system design specifications. Providing such information could be reviewed by the NRC staff to confirm the adequacy of certain design elements and calculations.

The information requested in parts (a) through (f) of RAI 7-20, below, is necessary for the NRC staff to make a reasonable assurance finding of adequate protection based on demonstration of the TRPS and ESFAS compliance to the identified design criteria, as well as the accuracy and completeness of descriptions in the SHINE FSAR. Specifically, the information requested in parts (a) through (f) of RAI 7-20, below, is necessary to support the following evaluation findings in Sections 7.4 and 7.5 of NUREG-1537, Part 2:

- "The design reasonably ensures that the design bases can be achieved, the system will be built of high-quality components using accepted engineering and industrial practices, and the system can be readily tested and maintained in the design operating condition."

- The protection system "is sufficient to provide for all isolation and independence from other…subsystems required…to avoid malfunctions or failures caused by the other systems."

- "The design considerations of the ESF actuation system give reasonable assurance that the system will detect changes in measured parameters as designed and will initiate timely actuation of the applicable ESF."

(a)(1) TRPS Monitored Variables

SHINE Design Criterion 13, "Instrumentation and Controls," requires instrumentation be provided to monitor variables and systems over the anticipated range of variation of the monitored variable during normal and transient conditions. Also, this criterion requires that the information provided be sufficient to verify that individual safety limits are protected by independent channels. SHINE FSAR Sections 7.3.1.1, "Irradiation Unit Systems," and 7.4.3.2, "Mode Transition," describe the modes of operation of the IU systems. The operator uses PICS to change modes of operation; however, the TRPS controls the mode of operation with permissives and interlocks of its assigned IU and provides protection against analyzed events. Furthermore, SHINE FSAR Section 7.4.2.1.4, "Protection System Independence," references manual actuation of the safety functions and manual actuation capabilities via individual push button, in part, to meet

SHINE Design Criterion 16, “Protection System Independence.” Manual actuations must be based on information provided to the operator. Therefore, the TRPS should monitor and display necessary information for all monitored variables during normal operation and transient circumstances. The SHINE FSAR Table 7.4-1, “TRPS Monitored Variables,” lists process variables monitored by the TRPS, associated process analytical limits, safety logic, instrument range, accuracy, and instrument response for the TRPS. However, the SHINE FSAR does not identify what TRPS variables provide information to the operators in the control room (via the control console) to change the IU operation mode and control the IUs. SHINE FSAR Section 7.3.1.1 only describes capabilities provided in the PICS, and SHINE FSAR Section 7.4.3.2 only describes the transition criteria to move from one mode to another.

Update the SHINE FSAR to identify TRPS variables to be displayed to operate and monitor IU operation, including any necessary for operators to perform manual protective actions and to meet SHINE Design Criteria 13 and 16, and to verify that the facility has functional protection capability in all operating modes and conditions, as analyzed in the SHINE FSAR.

(a)(2) ESFAS Monitored Variables

SHINE Design Criterion 13 requires instrumentation be provided to monitor variables and systems over the expected range of variation of the monitored variable during normal and transient operation. Also, this criterion requires that the information provided be sufficient to verify that individual safety limits are protected by independent channels.

SHINE FSAR Section 7.5.2.1.4, “Protection System Independence,” states, in part, “automatic and manual” actuation of the safety functions is used in meeting SHINE Design Criterion 16.

The ESFAS design: (1) should perform the functions necessary to ensure safety, and (2) ensure conformance to the design bases. The ESFAS monitors the IF and the RPF continually throughout the operation of processes within the facility. To perform its function, the ESFAS should monitor the necessary variables to actuate functions whenever an accident could occur for which the SHINE FSAR shows consequence mitigation is necessary. Manual actuations must be based on information provided to the operator. In addition, the ESFAS should include sensors (detectors) sufficient to cover the expected range of variation of the monitored variable during normal and transient operation (e.g., see SHINE Design Criterion 13).

SHINE FSAR Table 7.5-1, “ESFAS Monitored Variables,” lists process variables monitored by the ESFAS, associated process analytical limits, safety logic, instrument range, accuracy, and instrument response for the ESFAS. However, the SHINE FSAR does not identify what ESFAS variables provide information to the operators in the control room (via the control console) to monitor operation and status of the IF and the RPF. Section 7.3.1.1 only describes capabilities provided in the PICS. Update the SHINE FSAR to identify ESFAS variables to be displayed, including any necessary for operators to perform manual protective actions and to meet SHINE Design Criteria 13 and 16, and to verify that the facility has functional protection capability in all operating modes and conditions, as analyzed in the SHINE FSAR.

(b) TRPS and ESFAS Logic

SHINE Design Criterion 15, “Protection System Reliability and Testability,” requires that no single failure results in a loss of the protection function (see also RAI 7-11, ADAMS Accession No. ML21172A195). SHINE FSAR Section 7.4.3.4, “Single Failure,” states that “[e]ach input variable to the TRPS for monitoring and indication only is processed on independent input submodules that are unique to that input.” However, during the May 2021 regulatory audit of SHINE’s Instrumentation and Controls (I&C) (ADAMS Package No. ML21130A312) the NRC staff learned that the TRPS includes remote input sub-modules (RISMs) to gather data from each neutron flux detector system division and transmit it to the associated TRPS division. This information contradicts the statement in SHINE FSAR Section 7.4.3.4. Similarly, SHINE FSAR Section 7.5.3.3, “Single Failure,” states that “[e]ach input variable to the ESFAS for monitoring and indication only is processed on independent input submodules that are unique to that input.” The May 2021 regulatory audit did not identify if any RISMs are being used in the ESFAS or whether multiple inputs use the same RISM.

SHINE FSAR Section 7.4.3.4, “Single Failure,” describes the operational use of the “safety-related enable nonsafety switch” and the logic for this switch is depicted in Figure 7.4-1, “TRPS Logic Diagrams,” Sheets 12 and 13. However, during the May 2021 regulatory audit, SHINE stated that this description and depiction was not accurate and would be revised.

SHINE FSAR Section 7.5.3.3, “Single Failure,” states that “the ESFAS [also] contains a safety-related enable nonsafety switch.” The ESFAS implementation of this switch was not discussed during the May 2021 2021 regulatory audit; however, sheets 22 and 24 of SHINE FSAR Figure 7.5-1, “ESFAS Logic Diagrams,” depict this switch in the same manner as it is depicted in the TRPS. It is not clear to the NRC staff whether SHINE intends to revise this description and depiction of ESFAS logic as it intends to do for the related TRPS logic.

Update the SHINE FSAR to accurately describe the design and operation of the TRPS and ESFAS logic, as necessary, in FSAR Sections 7.4.3.4 and 7.5.3.3, as well as SHINE FSAR Figures 7.4-1 and 7.5-1.

(c) Assignment of monitored variables to each TRPS Division and ESFAS Division

SHINE Design Criterion 15 requires that no single failure results in a loss of the protection function. SHINE FSAR Section 7.4.2.1.3, “Protection System Reliability and Testability,” describes how the TRPS design addresses this criterion. As part of this description, SHINE states that 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. However, SHINE FSAR Section 7.4.3.4, “Single Failure,” describes an exception:

> 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.

The SHINE FSAR does not provide sufficient information for the NRC staff to assess whether this excepted condition is acceptable to prevent a single failure resulting in a loss of the protective function. Further, the SHINE FSAR does not clearly identify what variables or situations are only assigned to Division A.

SHINE Design Criterion 15 requires that no single failure result in a loss of the protection function. In the FSAR, Section 7.5.2.1.3, "Protection System Reliability and Testability," describes how the ESFAS design addresses this criterion. As part of this description, the SHINE FSAR describes that the ESFAS 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. (Note: Since there are several ESFAS functions which are based on two inputs in a one-out-of-two voting configuration, there are several single failures which could generate an unnecessary safety actuation). However, SHINE FSAR Section 7.5.3.3, "Single Failure," describes an exception:

> 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.

The SHINE FSAR does not provide sufficient information for the NRC staff to assess whether this excepted condition is acceptable to prevent a single failure resulting in a loss of the protective function. Further, the SHINE FSAR does not clearly identify what variables or situations are only assigned to Division A.

Update the SHINE FSAR to identify all variables that are only assigned to Division A for TRPS and ESFAS, as appropriate. Also, update the SHINE FSAR to justify how the excepted conditions identified in SHINE FSAR Sections 7.4.3.4 and 7.5.3.3, including use of passive safety components to provide a diverse activation, meet SHINE Design Criterion 15 and will not result in a single failure resulting in a loss of the protective function.

(d) Assignment of safety functions to the TRPS and ESFAS safety function modules (SFM)

The HIPS Topical Report (TR) TR-1015-18653, "Design of the Highly Integrated Protection System Platform," Revision 2 (ADAMS Accession No. ML17256A892) Section 3.3, "Trip Determination," describes how sensor inputs can be assigned to the SFM. Furthermore, HIPS TR Section 4.2, "Safety Function Module," states, in part:

> Each SFM is dedicated to implementing one safety function or function group. An example of a safety function is a reactor trip from low reactor coolant system (RCS) flow generated from an RCS flow sensor signal, where a safety function group would be a pressurizer pressure channel that has multiple trips and actuations (i.e., low pressure reactor trip, high pressure reactor trip, high pressure decay heat removal actuation, etc.). This results in the gate level

implementation of each safety function being different from other safety functions.

SHINE FSAR Section 7.4.5.2.5, “Simplicity,” states, in part:

> 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 SHINE FSAR does not describe how safety signals are assigned to each SFM. Table B-3.2.3, “TRPS Input Variable Allocation,” in the technical specifications (TSs) bases for Liming Condition for Operation (LCO) 3.2.3 describes the allocation of inputs to the TRPS modules. From this table, it appears to the NRC staff that more than one input device provides a signal to each SFM. For example, the signals from wide range neutron flux, power range neutron flux, source range neutron flux, TOGS mainstream flow, TOGS dump tank flow, and TOGS oxygen concentration are assigned to the same SFM. If this is correct, this would contradict the information in SHINE FSAR Section 7.4.5.2.5 since the signals from the neutron flux monitoring system and signals associated with the TOGS are transmitted to the same SFM.

Update the SHINE FSAR to clarify the function allocations within the TRPS and ESFAS, ensuring consistency between the SHINE FSAR and TSs. In particular, as requested in item (c) above, identify the functions only assigned to Division A. Also, update the SHINE FSAR to provide allocation and differences of safety functions to each SFM (which is a TRPS channel) for their implementation at the gate level.

(e)(1) Clarification of Terminology for Monitored Variables

The names and terms for monitored variables used in the SHINE FSAR Chapter 7, “Instrumentation and Control Systems,” are not always consistent with those used in other chapters of the SHINE FSAR and the TSs. For example:

(i) FSAR Table 7.4-1, “TRPS Monitored Variables,” includes “TSV fill isolation valves fully closed.” However, TS Table B-3.2.3, “TRPS Input Variable Allocation,” uses the term “TSV fill valve position indication.” This same terminology issue may apply to other signals as well.

(ii) The SHINE FSAR Table 7.5-1, “ESFAS Monitored Variables,” identifies the ESFAS monitored variables. This table includes the iodine and xenon purification (IXP) upper three-way valve position indication, and its analytical limit to be “active”. However, the SHINE TS uses the term “supplying” as the analytical limit. It is not clear to the NRC staff if the term “active” means the same as “supplying,” which is the defined safe state of the valve, and the state of the solenoid when energized.

Revise the SHINE FSAR and SHINE TSs, as appropriate, to use consistent names and terms for all monitored variables.

(e)(2) Clarification of Terminology

The SHINE FSAR uses the terms “anticipated transient” and “design basis event” in different sections. It is not clear to the NRC staff what the difference is between SHINE’s use of these terms.

Revise the SHINE FSAR to clarify the difference – if any – between the terms “anticipated transient” and “design basis event” and use these terms consistently in the SHINE Design Criteria and ESFAS Criteria.

(f) TRPS and ESFAS Setpoint Methodology and Calculations

NUREG-1537, Part 2, Section 7.4, “Reactor Protection System,” states, that the range of operation of sensor (detector) channels should be sufficient to cover the expected range of variation of the monitored variable during normal and transient (pulsing or square wave) reactor operation. NUREG-1537, Part 2, Sections 7.3, 7.4, and 7.7 also state that sensitivity of each sensor channel should be commensurate with the precision and accuracy to which knowledge of the variable measured is required. NUREG-1537, Part 2, Section 7.5 states that the range and sensitivity of ESF actuation system sensors should be sufficient to ensure timely and accurate signals to the actuation devices.

Regulations in 10 CFR 50.36(c)(1)(ii)(A) state that limiting safety system settings are settings for automatic protective devices related to those variables having significant safety functions. This clause requires that where a limiting safety system setting (LSSS) is specified for a variable on which a safety limit has been placed, the setting must be chosen so that automatic protective action will correct the abnormal situation before a safety limit is exceeded.

Regulations in 10 CFR 50.36(c)(3) state, “Surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met.”

The TRPS is responsible for protecting the individual safety limits (SLs) using independent channels when the facility operates in accordance with the TS LCOs. SHINE TS, Section 2.0, defines SLs to protect the primary system boundary (PSB) and LSSS for safety systems to initiate their protective functions. The SHINE FSAR, Table 7.4-1, identifies the variables monitored by the TRPS. This table also provides instrument range, accuracy for each variable monitored, and its analytical limit (AL). The LSSS should provide margin to the AL of each variable monitored during each mode of operation.

For the TRPS monitored variables, TS Table 3.2.3-a identifies the setpoints for the safety function to protect against analyzed events and conditions. The SHINE FSAR does not describe the methodology used to determine these setpoints and only notes that a setpoint methodology was used to determine setpoints for variables monitored by the TRPS. The setpoints for protective function should be based on a documented analysis methodology that identifies assumptions and accounts for instrument uncertainties, such as environmental allowances and measurement computational errors associated with each element of the instrument channel.

Revise the SHINE FSAR to summarize the setpoint methodology used to establish the setpoints or LSSS from the analytical limits for the variables monitored by the TRPS and ESFAS. The summary of the setpoint methodology should include parameters that typically consider instrument precision, sensitivity, accuracy, loop uncertainties, and computational errors. Also, describe how SHINE determined equipment accuracy identified in SHINE FSAR Tables 7.4-1 and 7.5-1 to bound uncertainties and how the equipment accuracy is used in the setpoint methodology. This information is needed for the NRC staff to verify the safety channels and protective responses are sufficient to ensure that no safety limit, limiting safety system setting, or related limiting condition of operation discussed and analyzed in the SHINE FSAR will be exceeded.

SHINE Response

(a)(1) A description of the information from the target solution vessel (TSV) reactivity protection system (TRPS) and the engineered safety features actuation system (ESFAS) that will be displayed in the facility control room (FCR), including the status and value of the monitored variables from the TRPS and ESFAS identified in Tables 7.4-1 and 7.5-1 of the FSAR, is provided in the SHINE Response to RAI 7-13 (Reference 3). SHINE revised Subsection 7.4.5.2.4 of the FSAR to include a description of the information available to the operators in the FCR via the SHINE Response to RAI 7-13.

Variables monitored by the TRPS, identified in Table 7.4-1 of the FSAR, are provided to operators in the FCR to change the irradiation unit (IU) operation mode and control the IUs. Variables monitored by the ESFAS, identified in Table 7.5-1 of the FSAR, are provided to operators in the FCR to monitor the operation and status of the irradiation facility (IF) and the radioisotope production facility (RPF). A description of how a mode transition request is processed by the TRPS is provided in the SHINE Response to RAI 7-14 (Reference 3).

The description of how the TRPS and ESFAS satisfy SHINE Design Criterion 13 was enhanced via the SHINE Response to Part (a) of RAI 7-9 (Reference 4).

Manual actuation of safety-related components is not required to mitigate the consequences of a design basis event at SHINE and is not required for the TRPS or the ESFAS to satisfy SHINE Design Criterion 16. A discussion of how manual controls contribute to diversity in the TRPS and ESFAS is provided in the SHINE Response to RAI 7-11 (Reference 3).

SHINE has revised Subsections 7.4.2.1.4 and 7.5.2.1.4 of the FSAR to remove reference to manual actuations in the description of how the TRPS and ESFAS satisfy SHINE Design Criterion 16. SHINE has also revised Subsection 7.4.5.2.4 of the FSAR to clarify manual operation of safety systems and to enhance the description of information displayed in the FCR from the TRPS and ESFAS. A markup of the FSAR incorporating these changes is provided as Attachment 1.

(a)(2) A discussion of the ESFAS variables provided to operators in the FCR to monitor the operation and status of the IF and the RPF is provided in the SHINE Response to Part (a)(1) of RAI 7-20.

(b) The description and depiction of the TRPS and ESFAS logic associated with the enable nonsafety switch were revised as described in Enclosure 1 of Reference 4.

The remote input submodules (RISMs) are described in Section 5.9 of TECRPT-2018-0028, "HIPS Platform Application Specific Action Item Report for the TRPS and ESFAS," provided as Attachment 2 to Enclosure 2 of Reference 4. RISMs are only implemented for the TRPS and are not used in the ESFAS design.

SHINE has revised Subsections 7.4.3.4 and 7.5.3.3 to remove reference to the processing of variables used for monitoring and indication only. The processing of signal inputs is addressed in the SHINE Response to RAI 7-21. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

(c) The following instances exist in the design of the TRPS where a passive check valve is credited as a redundant component to a valve actuated by TRPS Division A:

- During an IU Cell Nitrogen Purge, one TSV off-gas system (TOGS) radioisotope process facility cooling system (RPCS) return isolation valve is designed to close to isolate the RPCS cooling water from the TOGS condensers when actuated by TRPS Division A. The TOGS RPCS return check valve is provided in series with this valve to perform the safety function should a failure in TRPS Division A occur.

- During an IU Cell Safety Actuation, one primary closed loop cooling system (PCLS) supply isolation valve is designed to close to isolate the PCLS supply penetration through the primary confinement boundary when actuated by TRPS Division A. The PCLS supply check valve is provided in series with this valve to perform the safety function should a failure in TRPS Division A occur.

These instances were evaluated as acceptable in the single failure analysis performed for the TRPS and ESFAS. Additionally, these instances support satisfying SHINE Design Criterion 15 because sufficient redundancy is provided by the passive check valve such that no single failure results in the loss of the protection function.

The following instances exist in the design of the ESFAS where a passive check valve is credited as a redundant component to a valve actuated by ESFAS Division A:

- During a Vacuum Transfer System (VTS) Safety Actuation, the following valves close when actuated by ESFAS Division A:

    - Molybdenum extraction and purification system (MEPS) A extraction column wash supply valve
    - MEPS A extraction column eluent valve
    - MEPS A [ ]$^{PROP/ECI}$ wash supply valve
    - MEPS A [ ]$^{PROP/ECI}$ eluent valve
    - MEPS B extraction column wash supply valve
    - MEPS B extraction column eluent valve
    - MEPS B [ ]$^{PROP/ECI}$ wash supply valve
    - MEPS B [ ]$^{PROP/ECI}$ eluent valve
    - MEPS C extraction column wash supply valve
    - MEPS C extraction column eluent valve
    - MEPS C [ ]$^{PROP/ECI}$ wash supply valve
    - MEPS C [ ]$^{PROP/ECI}$ eluent valve

- Iodine and xenon purification (IXP) recovery column wash supply valve
- IXP recovery column eluent valve
- IXP [ ]PROP/ECI wash supply valve
- IXP [ ]PROP/ECI eluent valve
- IXP facility nitrogen handling system (FNHS) supply valve
- IXP liquid nitrogen supply valve

There is a check valve provided in series with each of these valves to perform the safety function should a failure in ESFAS Division A occur.

- During a Tritium Purification System (TPS) Train A/B/C Isolation, there is one TPS train A/B/C helium supply isolation valve that closes when actuated by ESFAS Division A. A TPS helium supply check valve is provided in series with each of these valves to perform the safety function should a failure in ESFAS Division A occur.

- During a RPF Nitrogen Purge, there is one radioactive liquid waste immobilization (RLWI) process vessel vent system (PVVS) isolation valve that closes when actuated by ESFAS Division A. The RLWI PVVS check valve is provided in series with this valve to perform the safety function should a failure in ESFAS Division A occur.

These instances were evaluated as acceptable in the single failure analysis performed for the TRPS and ESFAS. Additionally, these instances support satisfying SHINE Design Criterion 15 because sufficient redundancy is provided by the passive check valve such that no single failure results in the loss of the protection function.

SHINE has revised Subsections 7.4.3.4 and 7.5.3.3 of the FSAR to identify the instances where passive components are provided in conjunction with components actuated by Division A of the TRPS or ESFAS and to provide justification of the excepted instances. A markup of the FSAR incorporating these changes is provided as Attachment 1.

(d) SHINE has revised Figures 7.4-1 and 7.5-1 of the FSAR to depict the allocation of safety functions, via allocation of inputs, to each safety function module (SFM). Revisions to these figures incorporating these changes are provided in Attachment 1.

The functions assigned only to Division A of the TRPS and ESFAS are described in the SHINE Response to Part (c) of RAI 7-20. The acceptability of the allocations of functions to SFMs as described in Subsection 7.4.5.2.5, to include discussion of the results of a diversity and defense-in-depth assessment and a description of functional diversity, was discussed as part of the SHINE Response to Part (e) of RAI 7-9 (Reference 4). The allocation of inputs provided in Table B-3.2.3 of the technical specifications represents the grouping of functions referred to in Subsection 7.4.2.5 of the FSAR; therefore, there is no contradiction between the Subsection 7.4.5.2.5 statement referenced in the request and the allocation of inputs provided in the technical specifications.

SHINE has also revised Subsection 7.4.5.2.5 of the FSAR to clarify that multiple inputs are allocated to each SFM, consistent with the technical specifications. A markup of the FSAR incorporating this change is provided as Attachment 1.

(e)(1) SHINE has revised Subsections 7.4.3.1, 7.4.4.1, 7.4.4.2, 7.5.3.1, 7.5.4.1, and 7.5.4.3 of the FSAR; Tables 7.4-1 and 7.5-1 of the FSAR; and the technical specifications to provide consistent terminology for the variables monitored by the TRPS and ESFAS. A mark-up of the FSAR incorporating these changes is provided as Attachment 1. A mark-up of the technical specifications incorporating these changes is provided as Attachment 2.

(e)(2) SHINE defined the term anticipated transient in the SHINE Response to Part (d) of RAI 7-9 (Reference 4). This response also revised the FSAR to enhance the description of how the TRPS and ESFAS satisfy SHINE Design Criterion 14 as it relates to anticipated transients.

SHINE uses the terms design basis accident and design basis event interchangeably in the FSAR. The identification of design basis accidents is described in Chapter 13 of the FSAR. SHINE has reviewed the SHINE Design Criteria and ESFAS Criteria and determined that the use of the terms anticipated transient and design basis event are appropriate; therefore, no additional revisions to the FSAR are necessary.

(f) SHINE applies an analysis methodology for establishing setpoints for the TRPS and the ESFAS. The methodology applies to the TRPS and ESFAS, and to the instrumentation, including the neutron flux detection system (NFDS) and safety-related radiation monitors, that supply inputs to the TRPS or ESFAS.

The setpoint methodology treats instrument uncertainty as a combination of multiple errors including, but not limited to, instrument reference accuracy, process effects, changes in ambient conditions, and calibration methods. The accuracy of instrument measurement is expressed in terms of statistical probabilities. The setpoint methodology considers uncertainty as reflecting the distribution of possible errors, which is consistent with the treatment of the term contained in International Society of Automation (ISA) recommended practice ISA-RP67.04.02-2010, “Methodologies for the Determination of Setpoints for Nuclear Safety Related Instrumentation,” (Reference 5). The methodology for combining instrument uncertainties is a combination of statistical and algebraic methods. The statistical square-root-sum-of-squares (SRSS) method, which is described in ISA-RP67.04.02-2010, is used to combine uncertainties that are random, normally distributed, and independent. The algebraic method is used to combine uncertainties that are not randomly distributed or are dependent.

The setpoint methodology considers three main categories of uncertainty associated with instrumentation channels: process measurement uncertainties, sensor uncertainties, and protection system processing uncertainties (rack uncertainties). The most significant sources of uncertainty are encountered by the process measurement interface and sensor elements. The instrument channel elements analyzed in the setpoint methodology are process, process interface, sensor, sensor interface and transmission, signal conditioning, and actuation.

In addition to uncertainties associated with these channel elements, the instrument channel environment, both normal and accident, are determined for each instrument channel element, and environmental uncertainties are included in the calculation of setpoint error. The channel uncertainty calculations also include instrument drift allowances. Setpoint drift is measured during surveillance testing required by the technical specifications. The setpoint methodology includes methodology for establishing

performance and test acceptance criteria during surveillance testing and calibration, and calibration uncertainty allowances are incorporated.

Process measurement uncertainties include process measurement errors (PME) uncertainties and primary element accuracy (PEA) uncertainties. PME uncertainties account for errors associated with the process variable monitored by the instrument channel. These uncertainties are independent of sensor uncertainties and include items such as the effect of fluid stratification on temperature measurement, the effect of fluid density changes on differential pressure, and the effect of solution void fraction and solution and pool temperature on neutron flux measurements. PEA uncertainties are included when a process variable depends on a measuring device in addition to the process sensor, such as the use of a venturi, elbow, or orifice plate as the primary element for flow measurements. These uncertainties are independent of sensor uncertainties.

Sensor uncertainties addressed in the setpoint methodology include a set of parameters combined as a group to account for sensor errors. Sensors are generally field-mounted instruments that interface directly with the process and, as a result, the ambient environment may be less controlled than instrument rooms where rack-mounted modules are located. The sensor uncertainties considered are sensor reference accuracy (SRA), sensor drift allowance (SDA), sensor measurement and test equipment (SMTE) uncertainties, sensor calibration accuracy (SCA), sensor temperature effects (STE), sensor pressure effects (SPE), sensor accident environment effects (SAE), and insulation resistance effects (IRE).

SRA is provided by the manufacturer as a limit for measurement errors when the sensor is in operation under specified conditions. SRA includes linearity, hysteresis, dead band, and repeatability.

SDA is included in the calculation of sensor uncertainties to establish a limit for setpoint drift between surveillance intervals. The sensor calibration interval is used to establish the drift allowance, and the frequency of calibration is based upon the technical specification requirements.

A bounding SMTE allowance is used in the setpoint analysis to account for measure and test equipment (M&TE) uncertainties. The methodology for establishing M&TE uncertainty includes the M&TE reference accuracy, the M&TE calibration standard, and uncertainties associated with M&TE readability.

SCA refers to the uncertainties introduced into the sensor during the calibration process. Sensor calibration errors are the result of measurement and test equipment uncertainties and human errors introduced during the calibration process. For the setpoint methodology, SCA is assumed to be equal to the as-left tolerance used in the calibration procedure. The as-left tolerance is typically set equal to the SRA. Therefore, the SCA equals the SRA, and both terms are included in the calculation of total loop uncertainty.

STE accounts for ambient temperature variations which may cause undesired changes in sensor output and is based on the maximum temperature deviation from reference calibration conditions.

SPE accounts for differences between operating pressure and calibration pressure for differential pressure transmitters. To calculate SPE, the maximum pressure variation above and below the operating pressure is determined, and then a static pressure effect supplied by the manufacturer is applied to the operating pressure variation.

SAE effects account for instruments which can be exposed to severe ambient conditions due to an accident and which are required to remain functional during or after the accident. A sensor accident environmental effect term is determined by manufacturers based upon sensor qualification data. The sensor environmental effects analysis is treated as a bias term in the calculation of total loop uncertainty.

IRE accounts for conditions of high temperature and humidity when the leakage current may increase to a level that causes a significant error in the measurement signal. During normal conditions, IRE error is so small that it is negligible. For sensors required to operate during and after accident conditions, IRE is accounted for as a bias error with known sign in the total loop uncertainty calculation.

Rack uncertainties addressed in the setpoint methodology include a set of parameters combined as a group to account for errors associated with rack-mounted equipment. Rack-mounted equipment receives input signals from field-mounted sensors, performs signal conditioning and processing, and actuates protective functions based on predetermined setpoints. The rack uncertainties considered are rack reference accuracy (RRA), rack drift allowance (RDA), rack M&TE uncertainties (RMTE), rack temperature effect (RTE), and rack calibration analysis (RCA).

RRA is provided by the manufacturer as a limit for measurement errors when the module is in operation under specified conditions. RRA includes linearity, hysteresis, dead band, and repeatability. For digital systems, RRA, represents uncertainties associated with calibration of the analog/digital converter providing input to the digital processing functions module.

RDA is included in the calculation of rack module uncertainties to establish a limit for setpoint drift between surveillance intervals. The source of rack module drift allowance may be the manufacturer’s specifications or an analysis of calibration data. The rack module performance test interval is used to establish the drift allowance. Periodic module performance testing frequency is based on technical specification requirements.

A bounding RMTE is used in the setpoint methodology to account for M&TE uncertainties. The methodology for establishing M&TE uncertainty includes the M&TE reference accuracy, the M&TE calibration standard, uncertainties associated with M&TE readability, and any additional uncertainties associated with the module performance test procedure.

RTE accounts for ambient temperature variations which may cause undesired changes in module output and is based on the maximum expected ambient temperature deviation from reference calibration conditions.

RCA refers to the uncertainties introduced into the rack-mounted module during the performance testing process. Module calibration errors are the result of measurement and test equipment uncertainties and human errors introduced during the testing process. For the setpoint methodology, RCA is assumed to be equal to the as-left

tolerance used in the surveillance test procedure. The as-left tolerance is typically set equal to RRA. Therefore, RCA equals RRA, and both terms are included in the calculation of total loop uncertainty.

The total loop uncertainty (TLU) is calculated from the process measurement uncertainties, sensor uncertainties, and rack uncertainties using the SRSS and algebraic methodologies as follows:

$$TLU = \pm [(PEA)^2 + (PME)^2 + (SRA)^2 + (SDA)^2 + (SMTE)^2 + (SCA)^2 + (STE)^2 + (SPE)^2 + (RRA)^2 + (RMTE)^2 + (RDA)^2 + (RCA)^2 + (RTE)^2]^{1/2} + IRE + SAE + Bias$$

The TLU is applied in the determination of setpoints for the TRPS and ESFAS, and to setpoints for the instrumentation, including the NFDS and safety-related radiation monitors, that supply inputs to the TRPS or ESFAS. A description of the application of the TLU in the determination of limiting safety system settings is as follows.

SHINE safety limits will not be exceeded if required actions are initiated before analytical limits are exceeded. Analytical limits are chosen to include a conservative margin between the analytical limit and the safety limit. The limiting safety system setting (LSSS) is the least conservative value that the instrument setpoint can be and still ensure the analytical limits are not exceeded and the safety limits are protected. The LSSS is separated from the analytical limit by an amount not less than the TLU.

The equipment accuracy identified in Tables 7.4-1 and 7.5-1 of the FSAR is the SRA and is determined and applied to the TLU as described above.

SHINE has revised Subsection 7.2.1 of the FSAR to enhance the description of the setpoint methodology used to establish the LSSS from the analytical limits for the variables monitored by the TRPS and ESFAS. A mark-up of the FSAR incorporating these changes in provided as Attachment 1.

RAI 7-21

Section 7.4 of NUREG-1537, Part 2, states, in part, that the FSAR should contain information such as “descriptive information, including system logic and schematic diagrams, showing all instruments, computer hardware and software, electrical, and electromechanical equipment used in detecting reactor conditions requiring scram or other reactor protective action and in initiating the action.” Additionally, “[t]he logic, schematic, and circuit diagrams should be included and should show independence of detector channels and trip circuits.”

Additionally, Section 7.5 of NUREG-1537, Part 2, states, in part, that the FSAR should contain information such as “logic and schematic diagrams[, as well as] description[s] of instruments, computer hardware and software, electromechanical components, detector channels, trip devices and set points.”

The HIPS platform is composed of several modules. One of these modules is the SFM, which performs the logic decision to initiate the required protective trips and actuations. The SHINE FSAR includes logic diagrams for the TRPS and ESFAS to perform their safety functions. However, the logic diagrams in the FSAR don’t identify in which HIPS module each safety function is performed to ensure that specified design limits are not exceeded. Also, the FSAR does not describe nor include logic diagrams for signal conditioning.

Revise the SHINE FSAR to describe the logic used to generate discrete signals from analog signal inputs to the TRPS and ESFAS, as well as the logic used to implement operational and maintenance bypass and permissives. Also, revise the FSAR to describe how monitored signals are input to the TRPS and ESFAS, conditioned, and evaluated against defined setpoints in the safety function module (i.e., the logic to generate safety signals).

The information is necessary for the NRC staff to make a reasonable assurance finding of adequate protection based on demonstration of the ability of the TRPS and ESFAS to perform their intended functions. Specifically, the information requested is necessary to support the following evaluation findings in Sections 7.4 and 7.5 of NUREG-1537, Part 2:

- "The design reasonably ensures that the design bases can be achieved, the system will be built of high-quality components using accepted engineering and industrial practices, and the system can be readily tested and maintained in the design operating condition."

- "The design considerations of the ESF actuation system give reasonable assurance that the system will detect changes in measured parameters as designed and will initiate timely actuation of the applicable ESF."

SHINE Response

As described in Section 2.5.1 of Topical Report TR-1015-18653, "Design of the Highly Integrated Protection System Platform," (Reference 6), analog signal inputs to the TRPS and the ESFAS are input to an SFM, which is composed of three functional areas:

1. Signal Conditioning/Analog to Digital Conversion performed on the input sub-module (ISM)
2. SFM Digital Logic Circuits
3. Communications Engines

The ISM consists of a signal conditioning circuit, analog to digital converter (ADC), and a serial interface to the SFM field programmable gate array (FPGA). The ISM converts the process analog input signal to a raw value in digital format.

The ISM continuously provides the input signal raw value to the SFM and also provides a discrete health signal to the SFM which is used to indicate the following:

- Process input signal is under or over range.
- An ADC internal error.

The ISM provides the process input signal raw value to the SFM where it is compared with a setpoint in raw value.

Setpoints are set by the operator from the maintenance work station (MWS) and stored in raw value on a non-volatile memory (NVM) on the SFM board. Each setpoint is stored in raw value in three different 24-bit registers on the NVM. Each register is provided respectively to triplicated SFM safety function logic. Each of the three SFM safety function logic compares the process input raw value provided by the ISM to the setpoint raw value provided by the NVM.

The SFM uses an FPGA device to contain digital logic circuits, including the safety function algorithm, engineering unit calculations, bus communication logic, and indication and diagnostic information logic circuits.

The SFM logic functions consist of multiple deterministic state-machines. The output of each of the ISMs on an SFM is sent to four signal paths in the FPGA. One of the signal paths is to the monitoring and indication bus (MIB) logic function. The other three signal paths are inputs to core logic functions that:

- Convert the output of the ISM into engineering units
- Perform the safety function algorithm
- Compare the safety function algorithm output to a setpoint and makes a trip/actuation determination
- Communicates the trip/actuation determinations to the scheduling and bypass modules (SBMs) or scheduling, bypass, and voting modules (SBVMs)

The above items are performed by a core logic function logically independent from any other core logic function, which allows for three functionally independent core logic functions and allows for the continuation of three redundant signal paths. The safety function algorithm is processed through three redundant paths to provide error detection and fault tolerance of the safety function.

The logic used to implement operational and maintenance bypasses and permissives is described in the SHINE Response to RAI 7-14 (Reference 3).

SHINE has revised Figures 7.4-1 and 7.5-1 of the FSAR to identify in which highly integrated protection system (HIPS) module each safety function is performed. SHINE has also revised Subsections 7.4.3.11 and 7.5.3.10 of the FSAR to describe how discrete signals are generated from analog signal inputs to the TRPS and ESFAS and to describe how monitored signals are input, conditioned, and evaluated against defined setpoints in the SFM. A markup of the FSAR incorporating these changes is provided as Attachment 1.

RAI 7-22

Sections 7.4 and 7.5 of NUREG-1537, Part 2, state, in part, that hardware and software for computerized systems should meet the guidelines of Institute of Electrical and Electronics Engineers (IEEE) Std. 7-4.3.2-1993, “IEEE Standard Criteria for digital Computers in Safety Systems of Nuclear Power Generating Stations,” Regulatory Guide 1.152, Revision 1, “Criteria for Digital Computers In Safety Systems of Nuclear Power Plants,” and American National Standards Institute/American Nuclear Society (ANSI/ANS)-10.4-1987, “Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry.”

The SHINE FSAR Sections 7.4.2.2.2, “Software Requirements Development,” and 7.5.2.2.2, “Software Requirements Development,” identify TRPS and ESFAS criteria associated with the software requirements development, respectively. SHINE FSAR Section 7.4.5, “Highly Integrated Protection System Design,” provides an overview of the system design process for the HIPS platform for the TRPS. Section 7.5.5 of the FSAR addresses the design for the ESFAS equipment by referencing to Section 7.4.5. Section 7.4.5 states that the development of the HIPS equipment for the TRPS and ESFAS had been delegated to SHINE's safety-related HIPS

vendor. Section 7.4.5.4 of the SHINE FSAR describes the design process for the vendor to follow. However, the SHINE FSAR does not provide information to determine whether the HIPS vendor followed this process for the TRPS and ESFAS and the results obtained.

Revise the SHINE FSAR to summarize how the HIPS vendor implemented the process described in the FSAR for the TRPS and ESFAS. This summary should include development procedures and test results. Also, revise the FSAR to describe how SHINE conforms with the guidelines of IEEE 7-4.3.2 and RG 1.152, as applicable. Note: This RAI is related to RAI 7-17, which asks SHINE to update the FSAR to describe how codes and standards listed in the SHINE FSAR are used to design each of the SHINE I&C systems (ADAMS Accession No. ML21172A195).

The information is necessary for the NRC staff to make a reasonable assurance finding of adequate protection based on demonstration of the ability of the TRPS and ESFAS to perform their intended functions. Specifically, the information requested is necessary to support the following evaluation findings in Sections 7.4 and 7.5 of NUREG-1537, Part 2:

- "The design reasonably ensures that the design bases can be achieved, the system will be built of high-quality components using accepted engineering and industrial practices, and the system can be readily tested and maintained in the design operating condition."

- "The design considerations of the ESF actuation system give reasonable assurance that the system will detect changes in measured parameters as designed and will initiate timely actuation of the applicable ESF."

SHINE Response

SHINE previously revised Subsections 7.4.2.2.2 and 7.5.2.2.2 of the FSAR to enhance the descriptions of how system-specific design criteria for software requirements development are satisfied and revised Subsection 7.4.5.4 of the FSAR to summarize how the HIPS vendor implemented the software requirements development process as part of the SHINE Response to Part (a) of RAI 7-9 (Reference 4).

SHINE has revised Subsection 7.4.5.4 of the FSAR to provide additional description of the implementation of the processes described therein. A markup of the FSAR incorporating these changes is provided as Attachment 1.

In lieu of complying with the nuclear power plant-specific guidance of Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," SHINE complies with applicable portions of Institute of Electrical and Electronics Engineers (IEEE) Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 7). A traceability matrix describing how SHINE conforms with IEEE 7-4.3.2-2003 is provided in TECRPT-2018-0028, "HIPS Platform Application Specific Action Item Report for the TRPS and ESFAS," provided as Attachment 2 to Enclosure 2 of Reference 4. The applicability of additional codes and standards to the design of the TRPS and ESFAS is described in the SHINE Response to RAI 7-17 (Reference 3).

RAI 7-23

NUREG-1537, Part 1, Section 7.2.4, "System Performance Analysis," states, in part, that "[t]he applicant should conduct a performance analysis of the proposed I&C system to ensure the design criteria and design bases are met and license requirements for the performance of the system are specified.

The system performance analysis should encompass…[t]echnical specification LSSSs [limiting safety system settings], LCOs, and surveillance requirements for the I&C system…. These parameters and requirements should include system operability tests, trip or actuation setpoint checks, trip or actuation-setpoint calibrations, and any system response-time tests that are required. Surveillance intervals should be specified and the bases for the intervals, including operating experience, engineering judgment, or vendor recommendation should be discussed."

The information requested in parts (a) through (c) of RAI 7-23, below, is necessary for the NRC staff to make the following evaluation findings in Sections 7.4 and 7.5 of NUREG-1537, Part 2:

- "The protection channels and protective responses are sufficient to ensure that no safety limit, safety system setting, or [protection system]-related limiting condition of operation discussed and analyzed in the SAR will be exceeded."

- "The bases for technical specifications, including surveillance tests and intervals for the ESF actuating system, give reasonable assurance of actuation of ESFs when required."

(a) SHINE FSAR Section 7.4.4.5, "Technical Specifications and Surveillance," states that "[l]imiting 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." SHINE FSAR Section 7.5.4.6, "Technical Specifications and Surveillance," provides a similar statement for the ESFAS.

However, the SHINE FSAR does not include a description or reference to the system performance analysis that encompasses the TS LSSSs, LCOs, and surveillance requirements for the TRPS and ESFAS.

Revise the SHINE FSAR to include a reference to and/or a description of the system performance analysis that addresses the TS LSSSs, LCOs, and surveillance requirements for the TRPS and ESFAS.

(b) SHINE TS LCOs 3.2.3 and 3.2.4 address the input devices and the actuation determination portions of the TRPS and ESFAS. The SHINE TS bases for LCO 3.2.3 and 3.2.4 identify the allocation of inputs to SFMs and hardwired modules (HWMs). This information appears to show that more than one input device provides a signal to each SFM or HWM. However, the TS Basis 3.2.3 notes that one input for TRPS is through an HWM. This could be understood as requiring that one of the 32 possible inputs to HWM must be operable. Therefore, it is not clear to the NRC staff what happens to the other remaining inputs and other modules. Further, it is not clear to the NRC staff how the facility operator would determine operability of an HWM.

Revise the SHINE FSAR to clarify how the HWM is addressed in the TS LCO 3.2.3, including inputs and determination of operability.

(c) SHINE TS Basis 3.2.1 describes operation of the equipment interface module (EIM) and safety actuation logic. This basis also describes requirements for operability of the EIMs. The EIM receives signals from the scheduling, bypass and voting modules (SBVMs) in Divisions A and B and control signals from the PICS. SHINE states that the EIM will give priority to the safety signal from the SBVMs over the non-safety signal from PICS. However, the SHINE FSAR and TS bases do not describe how the PICS can control an output when an EIM becomes inoperable. The TS bases only describe what happens to the actuation logic when an EIM is inoperable.

Revise the SHINE FSAR to describe how the EIM will treat signals from PICS when an EIM is inoperable.

SHINE Response

(a) The analysis that was performed for the purpose of identifying the technical specification LSSSs, limiting conditions of operation (LCOs), and surveillance requirements (SRs) for the instrumentation and controls (I&C) systems is described below:

The SHINE technical specification LSSSs were developed to provide margin to analytical limits as described in the SHINE Response to Part (f) of RAI 7-20. Values for LCOs for parameters that have LSSSs were set at the same value as the LSSS because sufficient margin to analytical limits, and hence safety limits, was provided.

During the development of the technical specifications for I&C systems, LCOs were established for components of the safety-related I&C systems that perform safety functions. This ensures that the safety-related I&C systems will remain available to perform safety functions when required.

Technical specification SRs were defined consistent with American National Standards Institute/American Nuclear Society Standard (ANSI/ANS)-15.1-2007, “The Development of Technical Specifications for Research Reactors” (Reference 8). The frequency of the performance of SRs, which is considered in the instrument uncertainty calculation, was selected ensuring that the margin to analytical limits described in the SHINE Response to Part (f) of RAI 7-20 is maintained.

For I&C systems, SHINE has established technical specification LSSSs, LCOs, SRs to demonstrate operability, and appropriate surveillance requirement frequency to protect LSSSs, consistent with the system performance analysis described in Section 7.2.4 of Part 1 of NUREG-1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Format and Content” (Reference 9).

SHINE has revised Subsections 7.4.4.5 and 7.5.4.6 of the FSAR to enhance the description of the technical specifications and surveillance requirements. A markup of the FSAR incorporating these changes is provided as Attachment 1.

(b) Only technical specification LCO 3.2.3 discusses hardwired modules (HWMs), since the only HWM input that is used to initiate an automatic safety actuation in either the TRPS or the ESFAS is the TSV fill isolation valve position indication, which causes an IU Cell Safety Actuation in the TRPS when the valve is inadvertently opened during Mode 2. Other inputs to an HWM are not addressed in the technical specifications as they are not required to perform safety functions.

Determination of operability for a required individual input (i.e., TSV fill isolation valve position indication) to an HWM is accomplished by performance of a Channel Test of the input. As defined in the technical specifications, this test is performed by manual introduction of a known signal into the channel and verification of the proper input into the associated divisional SBVMs via the monitoring and indication information provided from the SBVMs to the process integrated control system (PICS) for display to the operator.

SHINE has revised Subsection 7.4.4.4 of the FSAR to clarify how determination of operability for safety-related inputs to the TRPS HWM is performed. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

(c) The safety signals from the SBVMs and the non-safety signals from the PICS are inputs to the actuation and priority logic (APL), which is constructed entirely of discrete logic components for implementation of the priority logic.

There are two types of potential failures for an equipment interface module (EIM): failures associated with the FPGA logic and failures of the discrete circuitry of the APL.

Failures of the FPGA which render the EIM inoperable (e.g., unable to actuate in response to automatic signals) will not affect how the APL will treat signals from PICS (i.e., the APL will continue to prioritize automatic actuation signals from the FPGA over PICS inputs, and the APL will still accept PICS inputs and allow for the reset of an actuated component). If this type of failure prevents an automatic actuation signal from being provided to the APL, manual actuation capability by the operator would still be available through the APL from the manual pushbuttons on the control board, the redundant secondary EIM/APL within the same division would still be available for actuation (manual and automatic), and the other division of actuation would be available for those functions which have both Divisions A and B actuation components. For those functions which do not have a Division B actuation component, the redundant passive component would be available to perform the safety function (e.g., check valve).

Failures of the APL which render the EIM inoperable will not defeat APL prioritization of automatic actuation over the PICS signals. A single failure of APL circuitry could disable the capability for manual actuation or disable the capability for reset of an actuated component with PICS inputs. An APL failure will not impact APL prioritization of automatic actuation over the PICS signals because there are two redundant and independent paths for the automatic actuation signal into the APL and a single failure of an APL component can only affect at most one of these two paths. Either automatic actuation path will result in prioritization of the automatic actuation signal over the PICS signals. For this type of failure, automatic actuation from the affected APL would still be available, the redundant secondary EIM/APL within the same division would still be available for actuation (manual and automatic), and the other division of actuation would be available for those functions which have both Divisions A and B actuation components. For those functions which do not have a Division B actuation component, the redundant passive component would be available to perform the safety function (e.g., check valve).

SHINE has revised Subsections 7.4.3.12 and 7.5.3.11 of the FSAR to clarify that failures of the EIM do not defeat APL prioritization of the automatic or manual safety actuations

over the PICS control signals. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

RAI 7-24

SHINE FSAR Sections 7.4.2.2.9, “Operational Bypass, Permissives, and Interlocks,” and 7.5.2.2.9, “Operational Bypass, Permissives, and Interlocks,” describe the operational bypass, permissives, and interlocks for the TRPS and ESFAS. SHINE FSAR Sections 7.4.3.2, “Mode Transition,” and 7.5.2.2.9 describe, in part, how the TRPS and ESFAS incorporate the Facility Master Operating Permissive key switch in the system design. This key switch will be used to select operation in the normal, unsecured mode, or operationally secured. The NRC staff notes the key switch is not identified in the SHINE FSAR Table 7.4-1 or Table 7.5-1. The SHINE FSAR should also identify all inputs used by the TRPS and ESFAS to perform its functions, including non-safety signals.

Revise the SHINE FSAR to describe the design and configuration of the facility master operating permissive. Include all inputs to be used by the TRPS and ESFAS to perform its functions (also see items (a)(1) and (a)(2) for RAI 7-20 above).

The information is necessary for the NRC staff to make a reasonable assurance finding of adequate protection based on demonstration of the ability of the TRPS and ESFAS to perform their intended functions. Specifically, the information requested is necessary to support the following evaluation findings in Sections 7.4 and 7.5 of NUREG-1537, Part 2:

- “The design reasonably ensures that the design bases can be achieved, the system will be built of high-quality components using accepted engineering and industrial practices, and the system can be readily tested and maintained in the design operating condition.”

- “The design considerations of the ESF actuation system give reasonable assurance that the system will detect changes in measured parameters as designed and will initiate timely actuation of the applicable ESF.”

SHINE Response

The facility master operating permissive switch is a single operator controlled key switch located on the main control board that initiates select ESFAS and TRPS actuations and Mode transitions. The facility master operating permissive switch has two positions, Secure and Operate. If the key is placed in the Secure position or is removed from the main control board, the actuations and Mode transitions controlled by the key switch cannot be reset until the key has been inserted and returned to the Operate position.

The key switch engages divisions A and B of the ESFAS and is then transmitted to each of the eight instances of the TRPS when the key is inserted and is in the Operate position. Disengaging the facility master operating permissive switch, which occurs when the key is in the Secure position or is removed, will result in the ESFAS actuation of the following safety functions:

- VTS Safety Actuation
- TPS Process Vent Actuation
- TPS Train A Isolation
- TPS Train B Isolation

- TPS Train C Isolation

Disengaging the facility master operating permissive switch will not result in the ESFAS actuation of the following safety functions:

- Radiologically Controlled Area (RCA) Isolation
- Supercells Area 1 through 10 Isolations
- MEPS A, B, or C Heating Loop Isolations
- IU Cell Nitrogen Purge
- Carbon Delay Bed Group 1, 2, or 3 Isolations
- Extraction Column A, B, or C Alignment Actuations
- IXP Alignment Actuation
- RPF Nitrogen Purge
- Dissolution Tank Isolation

Disengaging the facility master operating permissive switch will result in the TRPS actuation of the following safety functions:

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

Disengaging the facility master operating permissive switch will also result in the TRPS actuation of the Fill Stop.

Disengaging the facility master operating permissive switch will not result in the TRPS actuation of the IU Cell Nitrogen Purge.

Disengaging the facility master operating permissive switch will cause the IUs to transition to Mode 3 as described in Subsections 7.4.3.2 and 7.4.4.2 of the FSAR.

The variables provided in Tables 7.4-1 and 7.5-1 of the FSAR are associated with process parameters. Inputs based upon manual actuation are not included in these tables. The facility master operating permissive switch, inputs associated with process parameters, and other manual inputs (i.e., push buttons) are depicted in Figures 7.4-1 and 7.5-1 of the FSAR.

SHINE has revised Subsections 7.4.3.1.3, 7.4.3.1.4, 7.4.3.2, 7.4.4.1.18, 7.4.4.2, and 7.5.4.3 of the FSAR and Figures 7.4-1 and 7.5-1 of the FSAR to enhance the description of the facility master operating permissive switch. A markup of the FSAR incorporating these changes is provided as Attachment 1.

RAI 7-25

(a) SHINE FSAR Section 7.5.2.1.8, “Criticality Control in the Radioisotope Production Facility,” states, in part, that “[t]he ESFAS provides two safety functions as required by the SHINE criticality safety program described in Section 6b.3.” These two safety functions include 1) the vacuum transfer system (VTS) Safety Actuation, as described in SHINE FSAR Section 7.5.3.1.17, “VTS Safety Actuation,” and 2) the Dissolution Tank Isolation, as described in SHINE FSAR Section 7.5.4.1.18, “TSPS Dissolution Tank Level Switch.”

The VTS Safety Actuation includes an “[a]ctuation on a VTS vacuum header liquid detection switch signal [to protect] against on overflow of the vacuum lift tanks and potential criticality

event," as described in SHINE FSAR Section 7.5.4.1.8, "VTS Vacuum Header Liquid Detection Switch." Additional details on the VTS are included in SHINE FSAR Section 6b.3.2.5, "Vacuum Transfer System," including references to certain signals used by the ESFAS to initiate safety functions and components. Specifically, FSAR Section 6b.3.2.5 states that the "vacuum headers are equipped with liquid detection that stops transfers upon detection of liquid."

Further, SHINE FSAR Section 7.5.3.1.17 identifies safety functions initiated by the VTS Safety Actuation Isolation, including the deenergizing of VTS "vacuum break valves." While SHINE FSAR Section 6b.3.2.5 identifies "valves," a "three-way valve," and a "ball-check valve," there is no reference to the vacuum break valves identified in SHINE FSAR Section 7.5.3.1.17.

The Dissolution Tank Isolation safety function includes the "TSPS [target solution preparation system] dissolution tank level switch signal [to protect] against a criticality event due to excess fissile material in a non-favorable geometry," as described in SHINE FSAR Section 7.5.4.1.18. Additional details on the TSPS and associated signals are included in SHINE FSAR 6b.3.2.4, "Target Solution Preparation System," which states that "high level within the dissolution tanks requires application of the DCP [double contingency principle] to prevent criticality accidents. The dissolution tanks are equipped with high level controls that are interlocked with isolation valves."

The NRC staff seeks clarification on the relationship between descriptions of signals and equipment associated with the two safety functions provided by the ESFAS, as required by the SHINE criticality safety program.

(1) Confirm that "VTS vacuum header liquid detection switch signal" described in SHINE FSAR Section 7.5.4.1.8 is the same signal as "liquid detection" described in SHINE FSAR Section 6b.3.2.5.

(2) Confirm which valves identified in SHINE FSAR Section 6b.3.2.5 correspond with the "vacuum break valves" identified in SHINE FSAR Section 7.5.3.1.17.

(3) Confirm that the "TSPS dissolution tank level switch signal" described in SHINE FSAR Section 7.5.4.1.18 is the same signal as the "high level controls" described in SHINE FSAR Section 6b.3.2.4.

(b) SHINE FSAR Section 7.5.1, "System Description," states that the ESFAS monitors variables for criticality safety to actuate the dissolution tank isolation safety function, actuate on a vacuum transfer system (VTS) vacuum header liquid detection, and actuate the VTS safety function. Further, FSAR Section 7.5.2.1.8 defines SHINE Design Criterion 37 associated with criticality control in the RPF. In the description provided on how the ESFAS design meets this criterion, the NRC staff could not identify descriptions of the safety functions to be performed by the ESFAS.

Provide a description and details of how ESFAS implements SHINE Design Criterion 37.

(c) By letter dated January 21, 2021 (ADAMS Accession No. ML21029A038), SHINE requested exemption from the monitoring requirements of paragraph (a) of 10 CFR 70.24, "Criticality Accident Requirements," for the irradiation unit cells and the material staging building. SHINE FSAR Section 7.5.2.1.8, "Criticality Control in the Radioisotope Production Facility,"

provides SHINE Design Criterion 37, which describes criterion for criticality control and alarming. It is not clear if SHINE Design Criterion 37 and associated FSAR descriptions related to the SHINE criticality monitoring system in SHINE FSAR Chapter 7 are impacted by the January 2021 exemption request.

Confirm whether the SHINE Design Criterion 37 and associated FSAR criticality control and alarming descriptions in Chapter 7 are expected to be impacted by the January 2021 exemption request and associated configuration of the criticality monitoring system. Update the SHINE FSAR Chapter 7, as appropriate, to reflect the current SHINE Design Criterion 37 and associated configuration of the criticality monitoring system.

The information requested in parts (a) through (c) of RAI 7-25, above, is necessary for the NRC staff to make a reasonable assurance finding of adequate protection based on demonstration of the ESFAS compliance to the identified design criteria, as well as the accuracy and completeness of descriptions in the SHINE FSAR. Specifically, the information requested in parts (a) through (c) of RAI 7-25, above, is necessary to support the following evaluation findings in Section 7.5 of NUREG-1537, Part 2:

- "The applicant has analyzed the scenarios for all postulated accidents at the facility, including all accidents for which consequence mitigation by engineered safety features (ESFs) is required or planned. The staff evaluated the ESFs and has determined that the designs of their actuation systems give reasonable assurance of reliable operation if required."

- "The applicant has considered the environments in which the ESFs are expected to operate, and the applicable actuation systems have been designed accordingly to function as required."

- "The design considerations of the ESF actuation system give reasonable assurance that the system will detect changes in measured parameters as designed and will initiate timely actuation of the applicable ESF."

SHINE Response

(a)(1) The VTS vacuum header liquid detection switch signal described in Subsection 7.5.4.1.8 of the FSAR is the same signal as the liquid detection described in Subsection 6b.3.2.5 of the FSAR.

(a)(2) The vacuum break valves identified in Subsection 7.5.3.1.17 of the FSAR are associated with the vacuum buffer tank, also referred to as the VTS knockout pot, and are described in Subsection 9b.2.5.3 of the FSAR. The vacuum break valves are not specifically mentioned in Subsection 6b.3.2.5 of the FSAR. Rather, the vacuum break valves will be deenergized as part of the VTS Safety Actuation that will occur as the result of the VTS vacuum header liquid detection signal discussed in (1) above.

The three-way valve used to break vacuum in the vacuum lift tanks that is discussed in Subsection 6b.3.2.5 is associated with normal operation of the tank as described in Subsection 9b.2.5.2 of the FSAR. The ball-check valve that is described in Subsection 6b.3.2.5 is strictly a mechanical component and is not operated by signals from the ESFAS. Other references in Subsection 6b.3.2.5 to valves used to supply

vacuum lift tanks are generic references to valves used in the normal operation of the system as described in Subsection 9b.2.5.2 of the FSAR.

(a)(3) The target solution preparation system (TSPS) dissolution tank level switch signal described in Subsection 7.5.4.1.18 of the FSAR is the same signal as the high level controls described in Subsection 6b.3.2.4 of the FSAR.

(b) The ESFAS contributes to satisfying SHINE Design Criterion 37 by providing two safety functions, VTS Safety Actuation and Dissolution Tank Isolation, that help to satisfy the double contingency principle for the VTS and the TSPS, respectively.

The VTS Safety Actuation actuates on a VTS vacuum header liquid detection signal as described in Subsection 7.5.4.1.8 of the FSAR. This signal is relied upon to prevent a criticality accident in the VTS by preventing overflow of fissile material into non-favorable geometry portions of the system due to overflow of a vacuum lift tank. The criticality safety basis of the VTS is further described in Subsection 6b.3.2.5 of the FSAR.

The Dissolution Tank Isolation actuates on a TSPS dissolution tank level switch signal as described in Subsection 7.5.4.1.18. This signal is relied upon to prevent a criticality accident in the TSPS by ensuring a high level in the dissolution tank is identified, water sources are isolated (RPCS supply and return valves), and the tank is isolated before a spill occurs or solution enters the ventilation. The criticality safety basis of the TSPS is further described in Subsection 6b.3.2.4 of the FSAR.

(c) SHINE Design Criterion 37 and the associated FSAR descriptions related to the SHINE criticality monitoring system in Chapter 7 of the FSAR are not impacted by the requested exemption from the monitoring requirements of paragraph (a) of 10 CFR 70.24 (Reference 10). The current SHINE Design Criterion 37 and associated configuration of the criticality monitoring system is as stated in Subsection 7.5.2.1.8 of the FSAR.

RAI 7-26

Note 2 of SHINE FSAR Chapter 3, “Design of Structures, Systems, and Components,” states that “[t]he generally-applicable design criteria 1 - 8 from Table 3.1-3 are not specifically listed even though they are generally applicable to most SSCs.” However, it is not clear to the NRC staff whether these design criteria are applicable to the TRPS and ESFAS.

Confirm whether SHINE Design Criteria 1 - 8 are applicable to the TRPS and ESFAS. Update the SHINE FSAR to describe the relation of the TRPS and ESFAS design bases to the applicable SHINE Design Criteria 1-8.

This information is necessary for the NRC staff to understand the relation of the design bases to the principle design criteria of facility, as required by 10 CFR 50.34.

SHINE Response

SHINE Design Criteria 1 through 6 are applicable to the TRPS and ESFAS. SHINE does not rely on the TRPS or ESFAS to satisfy SHINE Design Criteria 7 or 8.

SHINE has revised Subsections 7.4.2.1 and 7.5.2.1 of the FSAR to describe the relationship of the TRPS and ESFAS design bases to SHINE Design Criteria 1 through 6. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

References

1. NRC letter to SHINE Medical Technologies, LLC, “SHINE Medical Technologies, LLC – Request for Additional Information Related to Instrumentation and Control Systems (EPID No. L 2019-NEW-0004),” dated September 27, 2021 (ML21252A753)

2. SHINE Medical Technologies, LLC letter to the NRC, “SHINE Medical Technologies, LLC Application for an Operating License,” dated July 17, 2019 (ML19211C143)

3. SHINE Medical Technologies, LLC letter to NRC, “SHINE Medical Technologies, LLC Application for an Operating License Response to Request for Additional Information,” dated August 27, 2021 (ML21239A049)

4. SHINE Medical Technologies, LLC letter to NRC, “SHINE Medical Technologies, LLC Application for an Operating License Supplement No. 8 and Response to Request for Additional Information,” dated September 29, 2021 (ML21272A341)

5. International Society of Automation, “Methodologies for the Determination of Setpoints for Nuclear Safety Related Instrumentation,” ISA-RP67.04.02-2010, Research Triangle Park, NC

6. NuScale Power, LLC letter to NRC, “NuScale Power, LLC Submittal of the Approved Version of NuScale Topical Report TR-1015018653, ‘Design of the Highly Integrated Protection System Platform,” Revision 2 (CAC No. RQ6005), NuScale Power, LLC, September 13, 2017 (ML17256A892)

7. Institute of Electrical and Electronics Engineers, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” IEEE Standard 7-4.3.2-2003, New York, NY

8. American National Standards Institute/American Nuclear Society, “The Development of Technical Specifications for Research Reactors” ANSI/ANS-15.1-2007, La Grange Park, IL

9. U.S. Nuclear Regulatory Commission, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Format and Content,” NUREG-1537, Part 1, February 1996 (ML042430055)

10. SHINE Medical Technologies, LLC letter to the NRC, “SHINE Medical Technologies, LLC Request for Exemption from Criticality Accident Alarm System Monitoring Requirements for the SHINE Irradiation Unit Cells and Material Staging Building,” dated January 21, 2021 (ML21029A038)

ENCLOSURE 3
ATTACHMENT 1

SHINE TECHNOLOGIES, LLC

SHINE TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE
SUPPLEMENT NO. 13 AND RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

FINAL SAFETY ANALYSIS REPORT CHANGES
PUBLIC VERSION
(MARK-UP)

111 pages follow

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

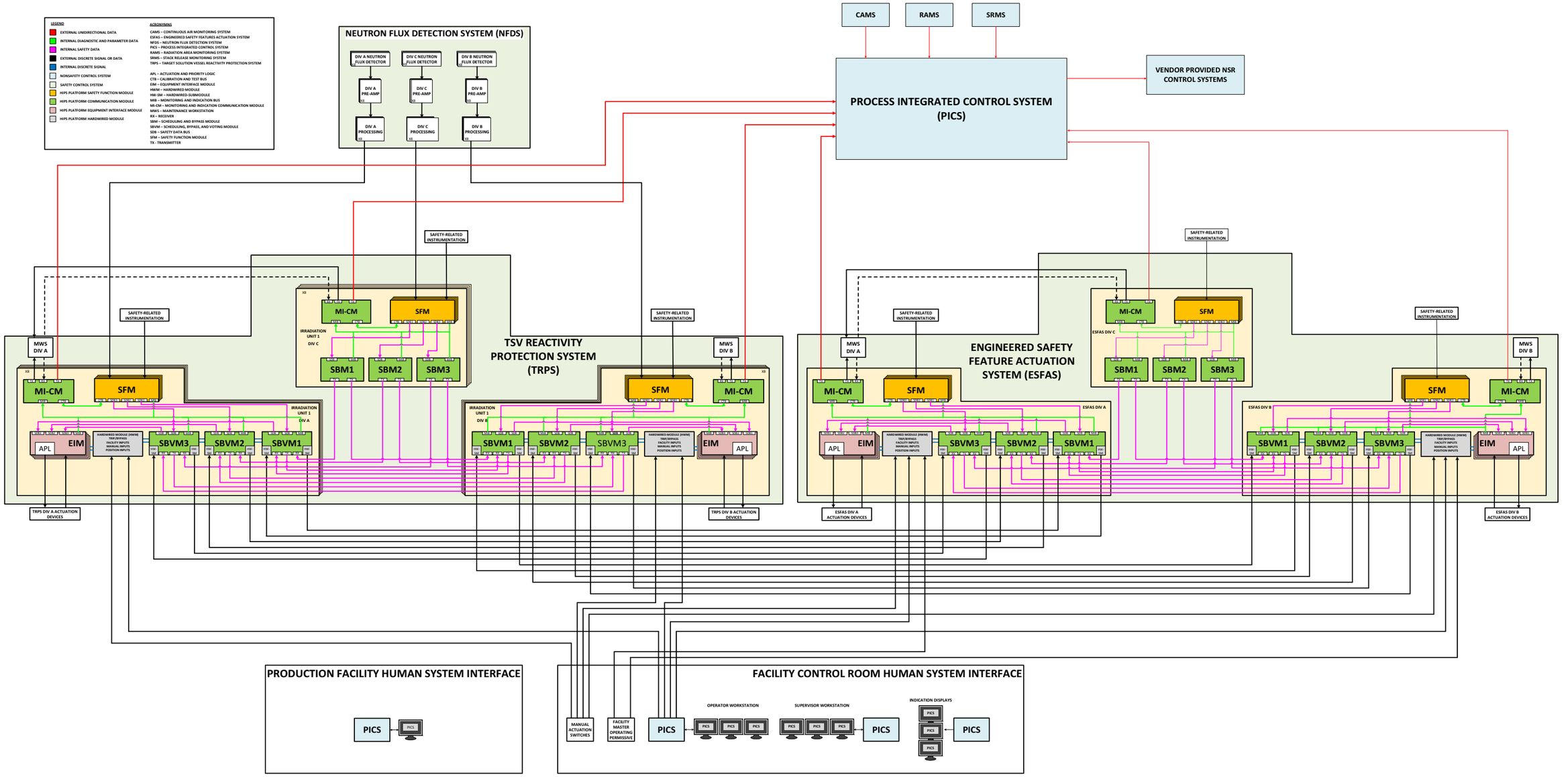
The NFDS is used for monitoring the reactivity and power of the subcritical assembly system in the IU. The NFDS is a safety-related system with redundant channels of neutron flux detectors. The NFDS detects and provides remote indication of the neutron flux levels during TSV filling and irradiation to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



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.~~

SHINE safety limits will not be exceeded if required actions are initiated before analytical limits are exceeded. Analytical limits are chosen to include a conservative margin between the analytical limit and the safety limit. The limiting safety system setting (LSSS) is the least conservative value that the instrument setpoint can be and still ensure the analytical limits are not exceeded and the safety limits are protected. The LSSS is separated from the analytical limit by an amount not less than the total loop uncertainty for the setpoint determined by the methodology discussed above.

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

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 indirectly 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

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

The generally-applicable SHINE facility design criteria 1 through 6 apply to the TRPS. The TRPS is designed, fabricated, and erected to quality standards commensurate to the safety functions to be performed; will perform these safety functions during external events; will perform these safety functions within the environmental conditions associated with normal operation, maintenance, and testing; does not share components between irradiation units; and is able to be manually initiated from the facility control room. These elements of the TRPS design contribute to satisfying SHINE facility design criteria 1 through 6.

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

7.4.2.1.1 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 range.

~~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 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 7.4.3.5 and 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. This d~~D~~ivision independence is maintained throughout the design, extending from the sensor to the devices actuating the protective function (Subsection 7.4.5.2.1).

Functional diversity and diversity in component design are used to prevent loss of the protection function. Functional diversity is discussed in Subsection 7.4.5.2.5. ~~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 f~~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). A failure modes and effects analysis (FMEA) was performed which verified that there are no single failures or non-detectable failures that can prevent the TRPS from performing its required safety function (Subsection 7.4.5.2.2).

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).~~ Sensors with an output used to determine TRPS protective actions are safety-related and input directly to the TRPS. The TRPS provides these sensor inputs to the PICS through redundant outputs. After receiving the input from the TRPS, the PICS performs its control function, if one is associated with the input. There are no inputs to the TRPS from the PICS that are used in the determination of protective actions. Since there are no inputs from the PICS that impact a safety function in the TRPS, and sensors that provide a safety-related protection function and a nonsafety-related control function are routed directly to the TRPS, a 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 the reliability, redundancy, and independence requirements of the TRPS as described in Subsections 7.4.3.4, 7.4.4.3, 7.4.5.2.1, 7.4.5.2.2, and 7.4.5.2.3.

Identified risks are documented in a project risk register and actions are developed to address identified risks or vulnerabilities.

TRPS Criterion 13 – 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

TRPS Criterion 14 – 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 RPF, irradiation facility (IF), and the facility control room, protected from radiological and environmental hazards during normal operation, maintenance, testing, and postulated accidents, and cables and sensors outside of these ~~facility control room~~areas are designed for their respective environments (Subsection 7.4.3.5). The TRPS is qualified for a mild operating environment by applying the guidance of Sections 4.1, 5.1, 6.1, and 7 of IEEE Standard 323-2003 (IEEE, 2003b).

TRPS Criterion 15 – 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

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

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-

- 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 valve~~s~~ position indication 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~~Subcritical assembly system (SCAS) nitrogen purge 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
- Facility master operating permissive

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
- Facility master operating permissive

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 [ ]$^{PROP/ECI}$ 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.

Mode 0 to Mode 1 Transition Criteria

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

Mode 0 to Mode 3 Transition Criteria

Transition from Mode 0 to Mode 3 is initiated automatically by TRPS or manually by an operator via manual actuation or the facility master operating permissive (Subsection 7.4.4.2). 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 (Subsection 7.4.4.2). 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 (Subsection 7.4.4.2). 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 (Subsection 7.4.4.2). 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 (Subsection 7.4.4.2). 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 (Subsection 7.5.4.3). 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~~n 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~~n 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~~The following instances 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 is 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.~~:

- A TOGS RPCS return check valve is provided in series with the TOGS RPCS return isolation valve to support isolation during an IU Cell Nitrogen Purge.
- A PCLS supply check valve is provided in series with the PCLS supply isolation valve to support isolation during an IU Cell Safety Actuation.

In each of the above instances, sufficient redundancy is provided by the passive check valve such that no single failure results in the loss of the protection function.

~~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.~~

TRPS division A is powered from division A of the uninterruptible electrical power supply system (UPSS). TRPS division B is powered from division B of the UPSS. TRPS division C receives auctioneered power from division A and division B of the UPSS. The UPSS provides safety-related 125-volt direct current (VDC) and 208Y/120-volt alternating current (VAC) power to system loads, including the TRPS, as described in Subsection 8a2.2.3.

Each division of the TRPS contains three redundant 125 VDC to 24 VDC converters. The 24 VDC power is distributed to each of three chassis mounting bays, where it is then used to power two redundant 24 VDC to 5 VDC converters located beneath each chassis bay. These provide independent +5-volt (V) A and +5V B power channels to each chassis. This configuration allows for the architecture to handle a single failure of a power supply.

7.4.3.5 Operating Conditions

The TRPS control and logic functions are located inside ~~of~~ the RPF, IF, and 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 radiation qualification of the affected components is based upon the total integrated dose (TID) identified in Table 7.2-1 being less than the threshold values identified in industry studies.

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.

Analog signals are input into the input sub-module (ISM) of an SFM. The ISM consists of a signal conditioning circuit, analog to digital converter, and a serial interface to the SFM FPGA. The ISM converts the process analog input signal to a raw value in digital format, which is provided to the SFM where it is compared with a setpoint in raw value.

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. Failures of the EIM do not defeat APL prioritization of the automatic or manual safety actuations over the PICS control signals.

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) IEEE Standard 323-2003, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations (IEEE, 2003b), invoked as guidance to meet TRPS Criterion 14.

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 TSV 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

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 indicates power has been lost~~is active~~, the division receiving the discrete signal initiates an IU Cell Nitrogen Purge.

7.4.4.1.15 High RVZ1e IU Cell Exhaust Radiation

The high RVZ1e IU cell exhaust 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 high RVZ1e IU cell exhaust radiation is measured on the exhaust of the PCLS expansion tank located in each IU cell. The signal is generated by TRPS when an RVZ1e IU cell exhaust radiation input exceeds the high level setpoint. The RVZ1e IU cell radiation is measured with an analog interface on three different channels, one for each division of TRPS. When two-out-of-three or more RVZ1e IU cell exhaust radiation channels exceed the allowable limit, an IU Cell Safety Actuation is initiated.

7.4.4.1.16 TSV Fill Isolation Valve Position Indication ~~Fully~~Not Closed

A TSV fill isolation valve position indication not~~fully~~ closed signal protects against the inadvertent addition of target solution to the TSV (Subsection 13a2.1.2.2, Scenario 6) via an inappropriately opened TSV fill isolation valve. 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~~ position indication signals ~~are no longer active~~ indicate the associated valve is not closed for either of the TSV fill isolation valves, an IU Cell Safety Actuation is initiated. IU Cell Safety Actuation on TSV fill isolation valve position indication~~s fully closed~~ is only ~~active~~applicable 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~~signal indicates that an actuation is required, 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~~signal indicates the two in-series valves are not closed, then a [ ]$^{PROP/ECI}$ timer is initiated. If the TSV fill isolation valve ~~fully closed~~ position indication ~~is not active~~ signal indicates that both valves remain not closed at~~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~~ signal indicates that the valve(s) is (are) closed 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~~signal indicates the valve(s) is (are) closed, a 5-minute timer is initiated. If the TSV fill isolation valve ~~fully closed~~ position indication signal indicates both valves are not closed~~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.

A Fill Stop is initiated when the facility master operating permissive key switch is disengaged, as described in Subsection 7.5.4.3.

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.

Operational bypasses for the TRPS are based upon the mode of operation and are automatically implemented within the SBVMs to bypass safety actuations that are not required for each mode. 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. A mode transition request occurs via separate discrete inputs from PICS to each of the Division A and B HWMs, which then converts the mode transition input to a logic level signal and makes the signal available to the associated SBVMs within the division. When associated permissives are satisfied and the manual operator action for mode transition occurs, the TRPS progresses to the next mode and the SBVMs will: (1) automatically bypass the final trip determinations for safety actuations that are not required for that particular mode of operation, and (2) will automatically remove any bypasses of the final trip determinations for safety actuations that are required for that particular mode of operation. See the TRPS mode state diagram in the TRPS logic diagrams (Figure 7.4-1) for the transitional sequence of the TRPS.

If the permissive conditions are not met for transitioning to the next mode and the operator action occurs, the TRPS will not advance to the next mode of operation. 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 position 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 position indication 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 position indication not~~fully~~ closed

The TRPS includes the ability for the operator to transition the system from Mode 3 operation to a secure state of operation. While in the secure state, an interlock is maintained preventing the TRPS from transitioning to the next sequential mode. The control key, via use of a facility master operating permissive, is used to place the TRPS into and out of the secure state. Should the system be operating in a Mode other than Mode 3 when the facility master operating permissive key switch (Subsection 7.5.4.3) is taken to Secure, the IU will transition to Mode 3 as described in Subsection 7.4.3.2 and will be in 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~~position indication not 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.~~With the OOS switch in the OOS position, the trip/bypass switch is used to activate maintenance trips and maintenance bypasses. The trip/bypass switch signal is input first to an HWM, which then converts the trip/bypass discrete input to a logic level signal and makes the signal available to the associated SBMs or SBVMs within the same division as the trip/bypass switch. When the OOS switch is in the Operate position and the SFM is functioning normally, the SBMs or SBVMs associated with the SFM will ignore the associated trip/bypass switch input.

The SFMs continually provide the status of their OOS switch to the associated divisional SBMs or SBVMs along with their partial trip information. With an SFM's OOS switch in the OOS position and the associated trip/bypass switch in the trip position, the associated divisional SBMs or SBVMs will then assert all partial trip information associated with the SFM to the trip state for input to coincident logic voting in the SBVMs. All of the partial trip information associated with all inputs for this SFM would be in a maintenance trip condition for this case. For those safety functions that use two-out-of-three coincident voting, a single failure of the same SFM in another division would not defeat the safety function because the third remaining divisional SFM is available to complete a two-out-of-three vote if required. For those safety functions that only use one-out-of-two coincident voting, the safety functions would be actuated when the OOS switch is placed into the OOS position with the associated trip/bypass switch in the trip position.

With an SFM's OOS switch in the OOS position and the associated trip/bypass switch in the bypass position, the associated divisional SBMs or SBVMs will then assert all partial trip information associated with the SFM to the bypassed state (not tripped) for input to coincident logic voting in the SBVMs. All of the partial trip information associated with all inputs for this SFM would be in a maintenance bypass condition for this case. For safety functions that use either one-out-of-two or two-out-of-three coincident voting, a single failure of the same SFM in another division would defeat the safety function. Placing a single SFM in maintenance bypass is allowed by the technical specifications for up to two hours for the purpose of performing required technical specification surveillance testing.

With an SFM's OOS switch in the OOS position and the associated trip/bypass switch in either the trip or bypass position, the input channels associated with the SFM are inoperable.

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 for inputs provided to an SFM may also be performed when the channel is not required to be operable. Channel tests of inputs provided to an HWM are performed when the channel is not required to be operable, since HWMs are not provided with maintenance bypass capabilities.

7.4.4.5 Technical Specifications and Surveillance

Limiting ~~C~~conditions for ~~O~~operation and ~~S~~surveillance ~~R~~requirements are established for TRPS logic, voting, and actuation divisions and instrumentation monitored by TRPS as input to safety actuations. Limiting conditions for operation are established for components of the safety-related I&C systems that perform safety functions to ensure that the system will remain available to perform safety functions when required. Surveillance requirements are performed at a frequency to ensure that limiting safety system settings (Subsection 7.2.1) are not exceeded.

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 generic HIPS 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)~~. Modifications to the generic HIPS platform made during the design of the TRPS and ESFAS were reviewed, evaluated, and documented.

The HIPS platform Topical Report TR-1015-18653 included a representative architecture to illustrate how the HIPS platform meets the fundamental digital I&C principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth. The architectures of the TRPS and ESFAS are described in Subsections 7.4.1 and 7.5.1, respectively. Approval of Topical Report TR-1015-18653 included identification of 65 Application Specific Action Items (ASAIs). SHINE has evaluated the ASAIs and determined each has been satisfactorily addressed for the HIPS implementation in the TRPS and ESFAS designs.

The SHINE application of the HIPS platform conforms to IEEE Standard 7-4.3.2-2003 (IEEE, 2003a) for the TRPS and ESFAS, as described in Appendix B of Topical Report TR-1015-18653. Consistent with Appendix B of TR-1015-18653, the TRPS and ESFAS conforms to Section 5.5.1, Section 5.5.2, Section 5.5.3, and Section 5.6 of IEEE Standard 7-4.3.2-2003.

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.

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). A diversity and defense-in-depth (D3) assessment of the TRPS and ESFAS was performed using the guidance of NUREG/CR-6303 (USNRC, 1994) to identify potential vulnerabilities to digital CCFs. The D3 assessment concluded:

- Potential digital CCFs associated with the TRPS and ESFAS would not lead to a failure to initiate protective actions when required.
- Potential digital CCFs associated with the TRPS, ESFAS, and certain detectors could lead to spurious actuations without adverse impacts on safety.
- Potential digital CCFs associated with most detectors would not lead to a failure to initiate protective actions when required; however, in each instance where a potential digital CCF could cause a failure to initiate protective actions, there exists either an alternate automatic means of mitigating events or an alternate means for the operator to identify, initiate, and assess protective actions.

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. This monitoring and indication information provided to PICS from TRPS and ESFAS includes the status and values of the monitored variables identified in Table 7.4-1 and Table 7.5-1 as well as the status of the TRPS and ESFAS systems themselves. Display of this monitoring and indication information in the facility control room provides the information operators require to determine if manual actuation of a safety system is appropriate. Variables monitored by the TRPS are provided to operators in the facility control room to change the IU operation mode and control the IUs. Variables monitored by the ESFAS are provided to operators in the facility control room to monitor the operation and status of the IF and RPF. 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 inputs 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 allocation of inputs to SFMs is depicted in Figures 7.4-1 and 7.5-1.

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. In the D3 assessment (Subsection 7.4.5.2.4), functional diversity was applied to the TRPS and ESFAS as monitoring different input process parameters on different SFMs. 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.

The systems are developed using the vendor's ~~Project Management Plan~~PLDP, which describes a planned and systematic approach to design, implement, test, and deliver the safety-related ~~systems (TRPS, ESFAS)~~programmable logic for the TRPS and 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.

The vendor's PLDP identifies the tasks and associated documentation for the process described in Subsections 7.4.5.4.1 through 7.4.5.4.8. Results documented for the process, which demonstrate compliance with SHINE vendor specifications, are submitted upon completion by the vendor to SHINE for review and acceptance.

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.

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 exhaust 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~~1.5 seconds
TOGS dump tank flow	[ ]PROP/ECI	2/3↓	[ ]PROP/ECI	3 percent	~~0~~1.5 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~~High level	2/3↑	~~Active/inactive~~High level/ not high level	Discrete input signal	1.5 seconds
High-high TSV dump tank level ~~signal~~	~~Active~~High level	2/3↑	~~Active/inactive~~High level/ not high level	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 valve~~s fully closed~~ position indication	~~Inactive full close~~Not closed	1/2↑	~~Active/inactive~~Closed/not closed	Discrete input signal	0.5 seconds
ESFAS loss of external power	~~Inactive~~Loss of power	1/1↑	~~Active/inactive~~Power/loss of power	Discrete input signal	0.5 seconds

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

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

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

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

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

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

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

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

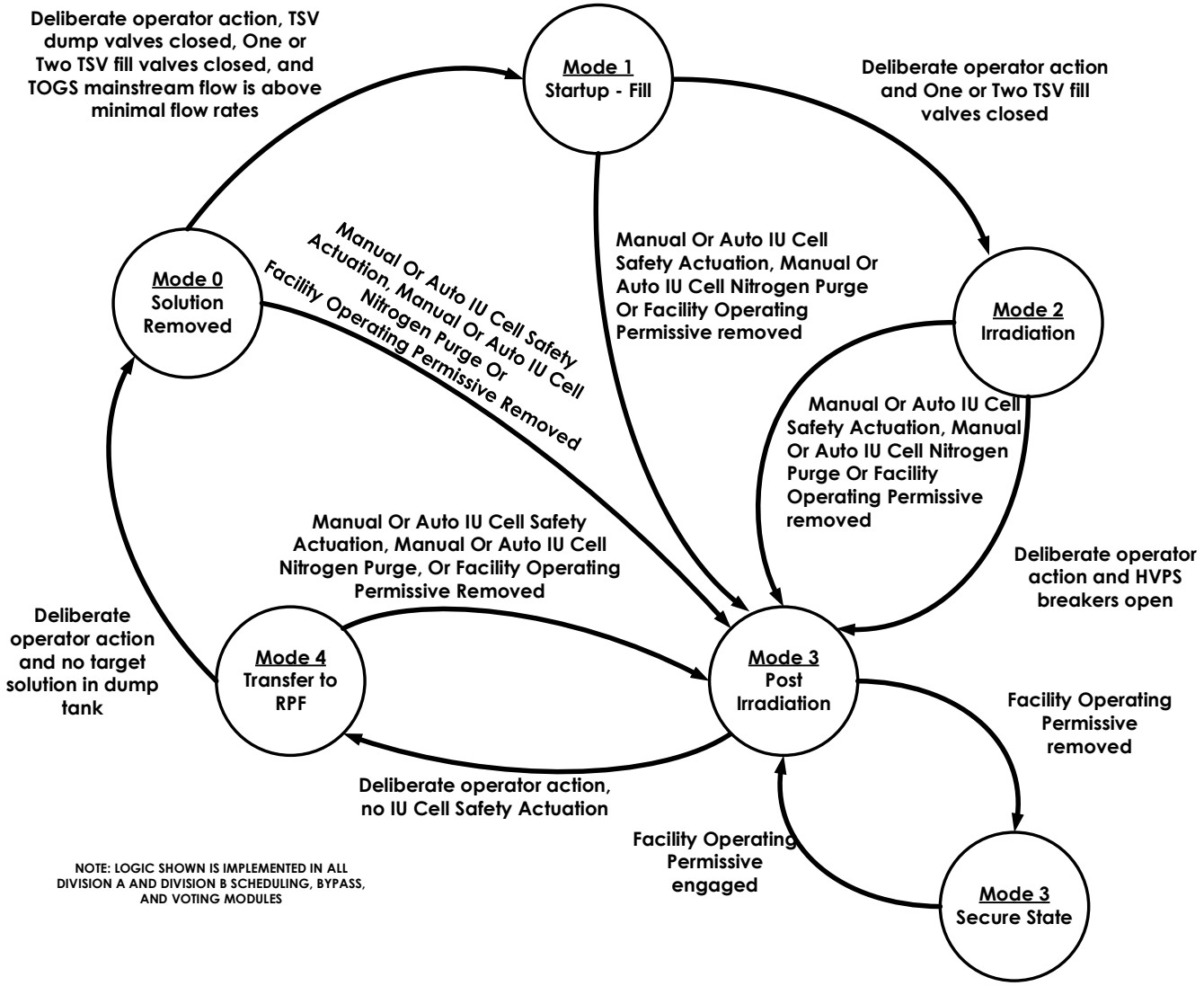


Figure 7.4-1 TRPS Logic Diagrams
(Sheet 9 of 14)

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

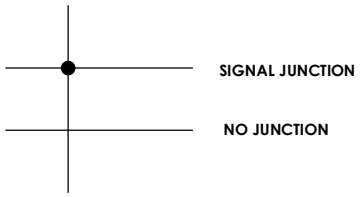
Figure 7.4-1 TRPS Logic Diagrams
(Sheet 11 of 14)

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

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

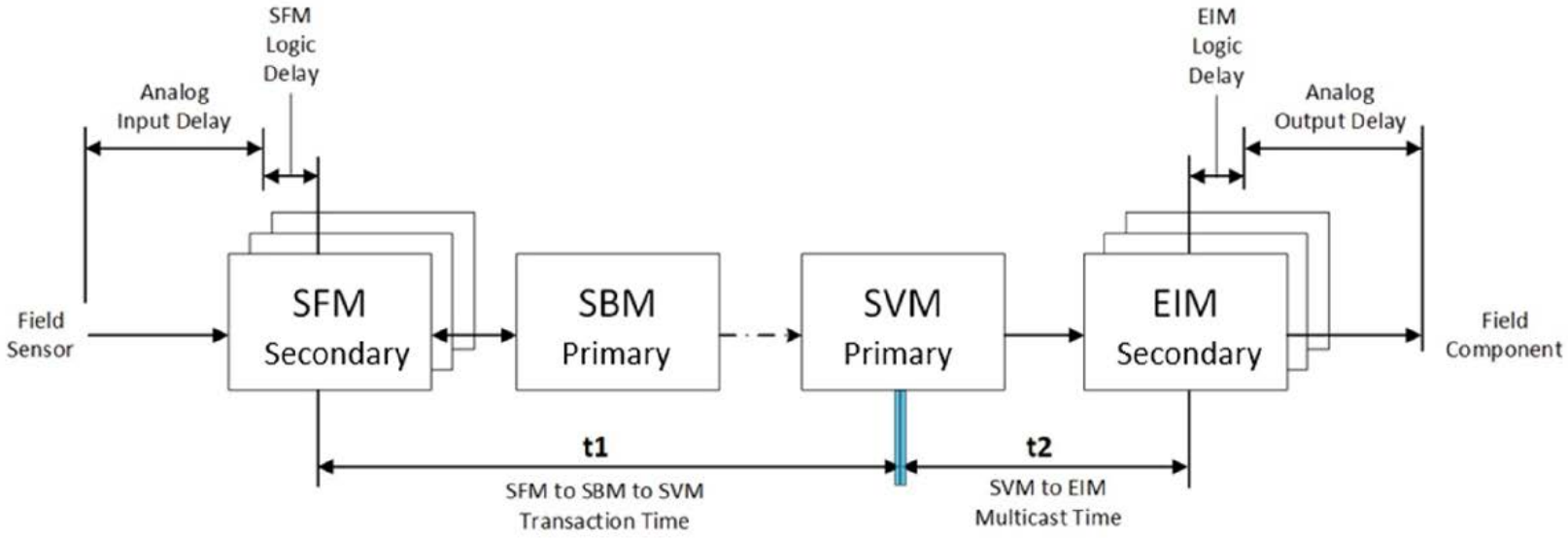
Figure 7.4-1 TRPS Logic Diagrams
(Sheet 14 of 14)

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
XNOR	LOGICAL "XNOR" GATE	TT	TRITIUM TRANSMITTER
2/3	TWO-OUT-OF-THREE VOTING GATE	FT	FLOW TRANSMITTER
2/2	TWO-OUT-OF-TWO VOTING GATE	TE	TEMPERATURE ELEMENT
⎍	BISTABLE – INCREASING SETPOINT OR DISCRETE ACTIVE	PT	PRESSURE TRANSMITTER
⎍	BISTABLE – DECREASING SETPOINT OR DISCRETE INACTIVE	ZI	DISCREET POSITION INDICATION
PB	PUSH BUTTON	RM	RADIATION MONITOR
HS	TWO POSITION HAND SWITCH	DI	DISCRETE INPUT
T = XX seconds	TIMER THAT INITIATES ON A LOGIC "1", RESETS ON LOGIC "0" AND OUTPUTS A LOGIC "1" IF TIMER HAS EXPIRED	CF	COMPENSATED FLOW
Xs Timer Logic	UNIQUE TIMER LOGIC, SEE NOTES	(A)	AUTOMATIC ACTUATION
XX Second Average	AVERAGE OPERATOR OVER XX AMOUNT OF TIME	(M)	MANUAL ACTUATION
(E)	ENABLE NONSAFETY "ENABLED"		
(D)	ENABLE NONSAFETY "DISABLED"		



ACRONYMS
APL – ACTUATION AND PRIORITY LOGIC
DIV – DIVISION
EIM – EQUIPMENT INTERFACE MODULE
HVPS – HIGH VOLTAGE POWER SUPPLY
HWMI – HARDWIRED MODULE INPUT
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
SBM – SCHEDULING AND BYPASS MODULE
SBVM – SCHEDULING, BYPASS, AND VOTING MODULE
SFM – SAFETY FUNCTION MODULE
TOGS – TSV OFF-GAS SYSTEM
TPS – TRITIUM PURIFICATION SYSTEM
TSV – TARGET SOLUTION VESSEL
LSB – LEAST SIGNIFICANT BIT
NDAS – NEUTRON DRIVER ASSEMBLY SYSTEM

Figure 7.4-2 – HIPS Platform Timing



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

The generally-applicable SHINE facility design criteria 1 through 6 apply to the ESFAS. The ESFAS is designed, fabricated, and erected to quality standards commensurate to the safety functions to be performed; will perform these safety functions during external events; will perform these safety functions within the environmental conditions associated with normal operation, maintenance, and testing; does not share components between irradiation units unless that sharing will not significantly impair the ability to perform the required safety functions; and is able to be manually initiated from the facility control room. These elements of the ESFAS design contribute to satisfying SHINE facility design criteria 1 through 6.

SHINE facility Design Criteria 13 through 19 and 37 through 39 also 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

is maintained throughout, extending from the sensor to the devices actuating the protective function (Subsection 7.4.5.2.1).

Functional diversity and diversity in component design are used to prevent loss of the protection function. Functional diversity is discussed in Subsection 7.4.5.2.5. ~~The architecture provides two diverse methods for an actuation of the safety functions at the division level, automatic and manual, and f~~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~~Subsection 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). A failure modes and effects analysis (FMEA) was performed which verified that there are no single failures or non-detectable failures that can prevent the ESFAS from performing its required safety function (Subsection 7.4.5.2.2).

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).~~There are no sensor outputs that have both an ESFAS safety-related protection function and a nonsafety-related control function. There are no inputs to the ESFAS from the PICS that are used in the determination of protective actions. Since there are no inputs from the PICS that impact a safety function in the ESFAS, and no sensors that provide both a safety-related protection function and a nonsafety-related control function, a failure or removal from service of any single protection system component or channel leaves intact a system satisfying the reliability, redundancy, and independence requirements of the ESFAS as described in Subsections 7.4.5.2.1, 7.4.5.2.2, 7.4.5.2.3, 7.5.3.3, and 7.5.4.4.

Nonsafety-related inputs to the ESFAS from the PICS are limited to those for controls and monitoring and indication only variables and are further described in Subsection 7.5.3.3. A failure of these nonsafety inputs will not impede the ESFAS from performing its safety function because the safety function is prioritized over the nonsafety input as described in Subsection 7.5.3.11. This limitation of inputs and prioritization of the safety function ensures that interconnection of the ESFAS and PICS is limited to assure that safety is not significantly impaired.

The ESFAS design, fabrication, installation, and modification is performed in accordance with a quality assurance program which 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) exhaust ventilation 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 Heating Loop 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 A) exhaust ventilation 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 A) exhaust ventilation 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 1) exhaust ventilation 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 B) exhaust ventilation 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 Heating Loop 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 B) exhaust ventilation 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 Heating Loop 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 C) exhaust ventilation 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 C) exhaust ventilation 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 2) exhaust ventilation 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) exhaust ventilation radiation
- RCA Isolation

7.5.3.1.11 MEPS A Heating Loop Isolation

MEPS A Heating Loop 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 Heating Loop Isolation initiates the following safety functions:

- Deenergize MEPS heating loop A inlet isolation valves
- Deenergize MEPS heating loop A discharge isolation valves
- Deenergize MEPS A extraction feed pump breakers

The ESFAS initiates a MEPS A Heating Loop Isolation based on the following variables or safety actuation:

- High MEPS heating loop conductivity extraction area A
- Radioactive drain system (RDS) liquid detection ~~switch signal~~
- Supercell Area 2 Isolation

7.5.3.1.12 MEPS B Heating Loop Isolation

MEPS B Heating Loop 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 Heating Loop Isolation initiates the following safety functions:

- Deenergize MEPS heating loop B inlet isolation valves
- Deenergize MEPS heating loop B discharge isolation valves
- Deenergize MEPS B extraction feed pump breakers

The ESFAS initiates a MEPS B Heating Loop Isolation based on the following variables or safety actuation:

- High MEPS heating loop conductivity extraction area B
- RDS liquid detection ~~switch signal~~
- Supercell Area 6 Isolation

7.5.3.1.13 MEPS C Heating Loop Isolation

MEPS C Heating Loop 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 Heating Loop Isolation initiates the following safety functions:

- Deenergize MEPS heating loop C inlet isolation valves
- Deenergize MEPS heating loop C discharge isolation valves
- Deenergize MEPS C extraction feed pump breakers

The ESFAS initiates a MEPS C Heating Loop Isolation based on the following variables or safety actuation:

- High MEPS heating loop 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 variable~~s~~:

- 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 variable~~s~~:

- 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 variable~~s~~:

- 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 facility nitrogen handing system (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 valves
- 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 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).

- 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 when~~based on~~ both of the following ~~inputs being active~~conditions are met:

- MEPS area A extraction column upper three-way valve ~~supplying~~ position indication in "supplying"
- MEPS area A extraction column lower three-way valve ~~supplying~~ position indication in "supplying"

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~~ when both of the following ~~inputs being active~~ conditions are met:

- MEPS area B extraction column upper three-way valve ~~supplying~~ position indication in "supplying"
- MEPS area B extraction column lower three-way valve ~~supplying~~ position indication in "supplying"

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~~ when both of the following ~~inputs being active~~conditions are met:

- MEPS area C extraction column upper three-way valve ~~supplying~~ position indication in "supplying"
- MEPS area C extraction column lower three-way valve ~~supplying~~ position indication in "supplying"

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~~ when both of the following conditions are met~~inputs being active~~:

- IXP upper three-way valve ~~supplying~~ position indication in "supplying"
- IXP lower three-way valve ~~supplying~~ position indication in "supplying"

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~~variables:

- 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~~n 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~~n 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~~The following instances 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 is 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~~.:

- A check valve is provided in series with each of the following components to support isolation during a VTS Safety Actuation:
  - MEPS A/B/C extraction column wash supply valve
  - MEPS A/B/C extraction column eluent valve
  - MEPS A/B/C [ ]$^{PROP/ECI}$ wash supply valve
  - MEPS A/B/C [ ]$^{PROP/ECI}$ eluent valve
  - IXP recovery column wash supply valve
  - IXP recovery column eluent valve
  - IXP [ ]$^{PROP/ECI}$ wash supply valve
  - IXP [ ]$^{PROP/ECI}$ eluent valve
  - IXP FNHS supply valve
  - IXP liquid nitrogen supply valve
- A TPS helium supply check valve is provided in series with the TPS train A/B/C helium supply isolation valve to support isolation during a TPS Train A/B/C Isolation.
- An RLWI PVVS check valve is provided in series with the RLWI PVVS isolation valve to support isolation during an RPF Nitrogen Purge.

In each of the above instances, sufficient redundancy is provided such that no single failure results in the loss of the protective function.

~~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.~~

ESFAS division A is powered from division A of the UPSS. ESFAS division B is powered from division B of the UPSS. ESFAS division C receives auctioneered power from division A and division B of the UPSS. The UPSS provides safety-related 125-volt direct current (VDC) and 208Y/120-volt alternating current (VAC) power to system loads, including the ESFAS, as described in Subsection 8a2.2.3.

Each division of the ESFAS contains three redundant 125 VDC to 24 VDC converters. The 24 VDC power is distributed to each of three chassis mounting bays, where it is then used to power two redundant 24 VDC to 5 VDC converters located beneath each chassis bay. These provide independent +5-volt (V) A and +5V B power channels to each chassis. This configuration allows for the architecture to handle a single failure of a power supply.

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 radiation qualification of the affected components is based upon the total integrated dose (TID) identified in Table 7.2-1 being less than the threshold values identified in industry studies.

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~~tested using biaxial excitation testing and triaxial excitation testing, in accordance with Section 8 of IEEE Standard 344-2013 (IEEE, 2013) (Subsection 7.5.3.12).

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.

Analog signals are input into the input sub-module (ISM) of an SFM. The ISM consists of a signal conditioning circuit, analog to digital converter, and a serial interface to the SFM FPGA. The ISM

converts the process analog input signal to a raw value in digital format, which is provided to the SFM where it is compared with a setpoint in raw value.

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. Failures of the EIM do not defeat APL prioritization of the automatic or manual safety actuations over the PICS control signals.

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) IEEE Standard 323-2003, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations (IEEE, 2003b), invoked as guidance to meet ESFAS Criterion 14.

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 and RVZ2 RCA exhaust radiation signals protect 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). A signal is generated by ESFAS when an RVZ1 or RVZ2 RCA exhaust radiation input exceeds its high level setpoint. RVZ1 and RVZ2 RCA exhaust radiation is measured using 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~~exceed their setpoint, then an RCA Isolation is initiated.

7.5.4.1.2 High RVZ1 Supercell Exhaust Ventilation Radiation (PVVS Hot Cell)

The high RVZ1 supercell area 1 (PVVS) exhaust ventilation 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 hot 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 an RVZ1 supercell area- 1 (PVVS) exhaust ventilation radiation input exceeds the high level setpoint. RVZ1 supercell area- 1 (PVVS) exhaust ventilation radiation is measured using an analog interface on three different channels, one for each division of ESFAS. When two-out-of-three or more ~~high~~ RVZ1 supercell area -1 (PVVS) exhaust ventilation radiation channels exceed their setpoint~~are active~~, then a Supercell Isolation for area 1 and a VTS Safety Actuation are initiated.

7.5.4.1.3 High RVZ1 Supercell Exhaust Ventilation Radiation (MEPS Extraction Hot Cells)

The high RVZ1 supercell area 2/6/7 (extraction A/B/C) exhaust ventilation radiation signals protect 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) for their respective hot cells. A signal is generated by ESFAS when an RVZ1 supercell area 2/6/7 (extraction A/B/C) exhaust ventilation radiation input exceeds its high level setpoint. RVZ1 supercell area 2/6/7 (extraction A/B/C) exhaust ventilation radiation is measured using an analog interface on two different channels per area, one for each Division A and Division B of ESFAS. When one-out-of-two or more ~~high~~ RVZ1 supercell area 2/6/7 (extraction A/B/C) exhaust

ventilation radiation channels exceed their setpoint~~are active~~ (for a single area), then a Supercell Isolation for that area, MEPS Heating Loop Isolation, and VTS Safety Actuation are initiated.

7.5.4.1.4 High RVZ1 Supercell Exhaust Ventilation Radiation (IXP ~~Extraction~~Hot Cell)

The high RVZ1 supercell area 10 (IXP) exhaust ventilation 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 RVZ1 supercell area 10 (IXP) exhaust ventilation radiation input exceeds the high level setpoint. RVZ1 supercell area 10 (IXP) exhaust ventilation radiation is measured using 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 area 10 (IXP) exhaust ventilation radiation channels exceed their setpoint~~are active~~, then a Supercell Isolation for area 10 and a VTS Safety Actuation are initiated.

7.5.4.1.5 High RVZ1 Supercell Exhaust Ventilation Radiation (Purification and Packaging Hot Cells)

The high RVZ1 supercell area 3/4/5/8/9 (purification A/B/C and packaging 1/2) exhaust ventilation radiation signals protect against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public for their respective hot cells. The signals are 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). A signal is generated by ESFAS when an RVZ1 supercell area 3/4/5/8/9 (purification A/B/C or packaging 1/2) exhaust ventilation radiation input exceeds its high level setpoint. RVZ1 supercell area 3/4/5/8/9 (purification A/B/C and packaging 1/2) exhaust ventilation radiation is measured using an analog interface on two different channels per area, one for each Division A and Division B of ESFAS. When one-out-of-two or more ~~high~~ RVZ1 supercell area 3/4/5/8/9 (purification A/B/C and packaging 1/2) exhaust ventilation radiation channels exceed their setpoint~~are active~~ (for a single area), then a Supercell Isolation for that area is initiated.

7.5.4.1.6 High MEPS Heating Loop Conductivity

The high MEPS heating loop conductivity extraction area A/B/C signal~~s~~ protect~~s~~ against leakage of high radiation solutions into the heating water loop, 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 heating loop conductivity extraction area A/B/C input exceeds the high level setpoint. The MEPS heating loop conductivity extraction area A/B/C is measured by an analog interface on two different channels, one for each Division A and Division B of ESFAS. MEPS heating loop conductivity is measured in three locations (MEPS extraction hot cells A, B, and C). When one-out-of-two or more ~~high~~ MEPS heating loop conductivity extraction area A/B/C channels ~~are active~~exceed their setpoint in a given heating loop (A, B, or C), then a MEPS Heating Loop Isolation is initiated for that heating loop.

7.5.4.1.7 High PVVS Carbon Delay Bed Exhaust Carbon Monoxide

The high PVVS carbon delay bed group 1/2/3 exhaust carbon monoxide signal~~s~~ protect~~s~~ 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 group 1/2/3 exhaust carbon monoxide input exceeds the high level setpoint. The PVVS carbon delay bed group 1/2/3 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 group 1/2/3 exhaust carbon monoxide channels ~~are active~~exceed their setpoint, 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~~channels indicate liquid is detected ~~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~~indicate liquid is detected, 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~~exceed their setpoint, then a TPS Process Vent Actuation is initiated.

7.5.4.1.13 High TPS Confinement Tritium

The high TPS confinement A/B/C tritium signals protect against a release of tritium from TPS equipment into the associated TPS glovebox (Subsection 13a2.1.12.2, TPS Scenario 1). A signal is generated by ESFAS when a TPS confinement A/B/C tritium input exceeds its high level setpoint. There is an independent and separate tritium measurement for each of the three TPS trains. TPS confinement tritium concentration is measured using an analog interface on two different channels per glovebox, one for each Division A and Division B of ESFAS. When one-out-of-two or more ~~high~~ TPS confinement A/B/C tritium channels ~~are active~~exceed their setpoint (for a particular glovebox), 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 1/2/3/4/5/6/7/8 Nitrogen Purge

The TRPS IU cell 1/2/3/4/5/6/7/8 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 1/2/3/4/5/6/7/8 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 1/2/3/4/5/6/7/8 nitrogen purge ~~signal is active~~indicates purging, 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~~exceed their setpoint, then an RPF Nitrogen Purge is initiated.

7.5.4.1.16 MEPS Area A/B/C~~Extraction Column~~ Three-Way Valve~~s Misaligned~~Position Indication

The MEPS ~~extraction column~~area A/B/C three-way valve ~~s misalignment~~position indication signal~~s~~ protect~~s~~ 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 area A/B/C extraction column upper and lower three-way valve position indications indicate they are in the "supplying" position (i.e., energized), then an Extraction Column Alignment Actuation for that area is initiated.

7.5.4.1.17 IXP Three-Way Valves Position Indication ~~Misaligned~~

The IXP three-way valves ~~misalignment~~position indication signals 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 in the "supplying" position (i.e., energized), then an IXP Alignment Actuation is initiated.

7.5.4.1.18 TSPS Dissolution Tank 1/2 Level ~~Switch~~

The TSPS dissolution tank 1/2 level ~~switch~~ signals 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 1/2 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 1/2 level ~~switch~~ signals ~~are active~~indicate "high level" 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~~indicate "loss of power,"~~,~~ 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 indicate "loss of power,"~~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 subsystems 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 ~~F~~facility ~~M~~master ~~O~~operating ~~P~~permissive key switch in the system design. The key switch has two positions, Operating and Secure (Subsection 7.6.1.1). When the ~~F~~facility ~~M~~master ~~O~~operating ~~P~~permissive key switch is active (operating), the ESFAS operates in the normal, nonsecure mode. When the facility master operating permissive key switch is placed in the Secure position or removed from the main control board, the actuations and Mode transitions controlled by the key switch cannot be reset until the key has been inserted and returned to the Operate position.

The key switch engages divisions A and B of the ESFAS and is then transmitted to each of the eight instances of the TRPS when the key is inserted and is in the Operate position. Disengaging the facility master operating permissive switch, which occurs when the key is in the Secure position or is removed, initiates select TRPS and ESFAS functions (Subsections 7.4.3.1, 7.4.4.1.18, and 7.5.3.1) and initiates Mode transitions as described in Subsection 7.4.3.2.

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.~~ With the OOS switch in the OOS position, the trip/bypass switch is used to activate maintenance trips and maintenance bypasses. The trip/bypass switch signal is input first to a hardwired module (HWM), which then converts the trip/bypass discrete input to a logic level signal and makes the signal available to the associated SBMs or SBVMs within the same division as the trip/bypass switch. When the OOS switch is in the Operate position and the SFM is functioning normally, the SBMs or SBVMs associated with the SFM will ignore the associated trip/bypass switch input.

7.5.4.6 Technical Specifications and Surveillance

Limiting ~~C~~conditions for ~~O~~operation and ~~S~~surveillance ~~R~~requirements are established for ESFAS logic, voting, and actuation divisions and instrumentation monitored by ESFAS as input to safety actuations. Limiting conditions for operation are established for components of the safety-related I&C systems that perform safety functions to ensure that the system will remain available to perform safety functions when required. Surveillance requirements are performed at a frequency to ensure that limiting safety system settings (Subsection 7.2.1) are not exceeded.

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
RVZ1 supercell area 1 (PVVS) exhaust ventilation radiation	60x background radiation	2/3↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
RVZ1 supercell area 2 (extraction A) exhaust ventilation radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
RVZ1 supercell area 3 (purification A) exhaust ventilation radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
RVZ1 supercell area 4 (packaging 1) exhaust ventilation radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
RVZ1 supercell area 5 (purification B) exhaust ventilation radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
RVZ1 supercell area 6 (extraction B) exhaust ventilation radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
RVZ1 supercell area 7 (extraction C) exhaust ventilation 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
RVZ1 supercell area 8 (purification C) exhaust ventilation radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
RVZ1 supercell area 9 (packaging 2) exhaust ventilation radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
RVZ1 supercell area 10 (IXP) exhaust ventilation radiation	60x background radiation	1/2↑	10^{-7} to 10^{-1} µCi/cc	20 percent	15 seconds
MEPS heating loop conductivity extraction area A	500 micromho/cm	1/2↑	0.2 to 500 micromho/cm	3 percent	5 seconds
MEPS heating loop conductivity extraction area B	500 micromho/cm	1/2↑	0.2 to 500 micromho/cm	3 percent	5 seconds
MEPS heating loop conductivity extraction area C	500 micromho/cm	1/2↑	0.2 to 500 micromho/cm	3 percent	5 seconds
PVVS c~~C~~arbon delay bed group 1 exhaust carbon monoxide	50 ppm	1/2↑	1 to 100 ppm	10 percent	15 seconds
PVVS c~~C~~arbon delay bed group 2 exhaust carbon monoxide	50 ppm	1/2↑	1 to 100 ppm	10 percent	15 seconds
PVVS c~~C~~arbon 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~~Liquid detected	1/2↑	~~Active/Inactive~~Liquid detected/liquid not detected	Discrete input signal	5.5 seconds
RDS liquid detection ~~switch signal~~	~~Active~~Liquid detected	1/2↑	~~Active/Inactive~~Liquid detected/liquid not detected	Discrete input signal	5.5 seconds

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

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
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
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↑	1 to 50,000 Ci/m^3	10 percent	5 seconds
TPS confinement B tritium	1000 Ci/m^3	1/2↑	1 to 50,000 Ci/m^3	10 percent	5 seconds
TPS confinement C tritium	1000 Ci/m^3	1/2↑	1 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~~High level	1/2↑	~~Active/Inactive~~High level/not high level	Discrete input signal	1 second
TSPS dissolution tank 2 level ~~switch signal~~	~~Active~~High level	1/2↑	~~Active/Inactive~~High level/not high level	Discrete input signal	1 second
TRPS IU cell 1 nitrogen purge ~~signal~~	~~Active~~Purging	1/1↑	~~Active/ Inactive~~Purging/not purging	Discrete input signal	500 ms
TRPS IU cell 2 nitrogen purge ~~signal~~	~~Active~~Purging	1/1↑	~~Active/ Inactive~~Purging/not purging	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 3 nitrogen purge ~~signal~~	~~Active~~Purging	1/1↑	~~Active/ Inactive~~Purging/not purging	Discrete input signal	500 ms
TRPS IU cell 4 nitrogen purge ~~signal~~	~~Active~~Purging	1/1↑	~~Active/ Inactive~~Purging/not purging	Discrete input signal	500 ms
TRPS IU cell 5 nitrogen purge ~~signal~~	~~Active~~Purging	1/1↑	~~Active/Inactiv~~Purging/ not purging~~e~~	Discrete input signal	500 ms
TRPS IU cell 6 nitrogen purge ~~signal~~	~~Active~~Purging	1/1↑	~~Active/ Inactive~~Purging/not purging	Discrete input signal	500 ms
TRPS IU cell 7 nitrogen purge ~~signal~~	~~Active~~Purging	1/1↑	~~Active/ Inactive~~Purging/not purging	Discrete input signal	500 ms
TRPS IU cell 8 nitrogen purge ~~signal~~	~~Active~~Purging	1/1↑	~~Active/ Inactive~~Purging/not purging	Discrete input signal	500 ms
MEPS area A lower three-way valve ~~supplying~~ position indication[(a)]	~~Active~~Supplying	1/2↑ & 1/2↑	~~Active/ Inactive~~Supplying/not supplying	Discrete input signal	1 second
MEPS area A upper three-way valve ~~supplying~~ position indication[(a)]	~~Active~~Supplying	1/2↑ & 1/2↑	~~Active/ Inactive~~Supplying/not supplying	Discrete input signal	1 second
MEPS area B lower three-way valve ~~supplying~~ position indication[(a)]	~~Active~~Supplying	1/2↑ & 1/2↑	~~Active/ Inactive~~Supplying/not supplying	Discrete input signal	1 second

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

Variable	Analytical Limit	Logic	Range	Accuracy	Response Time
MEPS area B upper three-way valve ~~supplying~~ position indication[(a)]	~~Active~~Supplying	1/2↑ & 1/2↑	~~Active/ Inactive~~Supplying/not supplying	Discrete input signal	1 second
MEPS area C lower three-way valve ~~supplying~~ position indication[(a)]	~~Active~~Supplying	1/2↑ & 1/2↑	~~Active/ Inactive~~Supplying/not supplying	Discrete input signal	1 second
MEPS area C upper three-way valve ~~supplying~~ position indication[(a)]	~~Active~~Supplying	1/2↑ & 1/2↑	~~Active/ Inactive~~Supplying/not supplying	Discrete input signal	1 second
IXP lower three-way valve ~~supplying~~ position indication[(a)]	~~Active~~Supplying	1/2↑ & 1/2↑	~~Active/ Inactive~~Supplying/not supplying	Discrete input signal	1 second
IXP upper three-way valve ~~supplying~~ position indication[(a)]	~~Active~~Supplying	1/2↑ & 1/2↑	~~Active/ Inactive~~Supplying/not supplying	Discrete input signal	1 second
UPSS loss of external power	~~Active~~Loss of power	1/2↓	~~Active/Inactive~~Power/ loss of power	Discrete input signal	1 second

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

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

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

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 3 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 4 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 5 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 6 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 7 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 8 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 9 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 10 of 27)

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)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 15 of 27)

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)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 20 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 21 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 22 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 23 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 24 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 25 of 27)

Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 26 of 27)

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

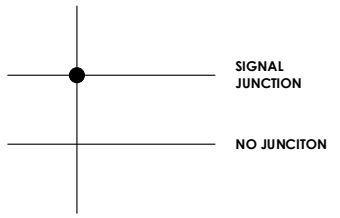
A – ALARM PROVIDED TO PROCESS INTEGRATED CONTROL SYSTEM	RM – RADIATION MONITOR	
I – INDICATION PROVIDED TO PROCESS INTEGRATED CONTROL SYSTEM	LS – LEVEL SWITCH	SIGNAL JUNCTION
OR – LOGICAL "OR" GATE	ZI – DISCREET POSITION INDICATION	NO JUNCITON
AND – LOGICAL "AND" GATE	CT – CONDUCTIVITY TRANSMITTER	
LOGICAL "NOT" OR INVERTER GATE	PT – PRESSURE TRANSMITTER	ACRONYMS
XNOR – LOGICAL "XNOR" GATE	TT – TRITIUM TRANSMITTER	APL – ACTUATION AND PRIORITY LOGIC
		DIV – DIVISION
XOR – LOGICAL "XOR" GATE	TE – TEMPERATURE ELEMENT	EIM – EQUIPMENT INTERFACE MODULE
		FNHS – FACILITY NITROGEN HANDLING SYSTEM
2/3 – TWO-OUT-OF-THREE VOTING GATE	CO – CARBON MONOXIDE TRANSMITTER	HWMI – HARDWIRED MODULE INPUT
		IU – IRRADIATION UNIT
1/2 – ONE-OUT-OF-TWO VOTING GATE	FT – FLOW TRANSMITTER	IXP – IODINE AND XENON PURIFICATION SYSTEM
		MEPS – MOLYBDENUM EXTRACTION AND PURIFICATION SYSTEM
BISTABLE – INCREASING SETPOINT OR DISCREET ACTIVE	DI – DISCRETE INPUT	N2PS – NITROGEN PURGE SYSTEM
		PICS – PROCESS INTEGRATED CONTROL SYSTEM
BISTABLE – DECREASING SETPOINT OR DISCREET INACTIVE	CF – CALCULATED FLOW	PVVS – PROCESS VESSEL VENTILATION SYSTEM
		RCA – RADIOLOGICAL CONTROLLED AREA
PB – PUSH BUTTON	(A) – AUTOMATIC ACTUATION	RLWI – RADIOLOGICAL LIQUID WASTE IMMOBILIZATION
		RVZ1 – RADIOLOGICAL VENTILATION ZONE 1
HS – TWO POSITION HAND SWITCH	(M) – MANUAL ACTUATION	RVZ2 – RADIOLOGICAL VENTILATION ZONE 2
		RVZ3 – RADIOLOGICAL VENTILATION ZONE 3
T = XX Seconds – TIMER THAT INITIATES ON A LOGIC "1", RESETS ON LOGIC "0" AND OUTPUTS A LOGIC "1" IF TIMER HAS EXPIRED	(E) – ENABLE NONSAFETY "ENABLED"	SBM – SCHEDULING AND BYPASS MODULE
		SBVM – SCHEDULING, BYPASS, AND VOTING MODULE
	(D) – ENABLE NONSAFETY "DISABLED"	SFM – SAFETY FUNCTION MODULE
		TPS – TRITIUM PURIFICATION SYSTEM
		TSPS – TARGET SOLUTION PREPARATION SYSTEM
		VTS – VACUUM TRANSFER SYSTEM

Figure 7.6-1 – Facility Control Room Layout

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 outputs of ~~the~~each pre-amplifier ~~is transmitted to cabinets in the facility control room where the signal processing units~~ are ~~located. The signal processing units~~used to 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~~which will then be transmitted to 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.

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~~,~~ and the irradiation facility (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 (Subsections 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 (via TRPS) 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.

NFDS Criterion 5 – 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).

NFDS Criterion 6 – The location and sensitivity of at least one NFDS detector in the source range channel, along with the location and emission rate of the subcritical multiplication source, shall be designed to ensure that changes in reactivity will be reliably indicated even with the TSV shut down.

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.

NFDS Criterion 7 – The NFDS shall have at least one detector in the power range channel to provide reliable readings to a predetermined power level above the licensed maximum power level.

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).

NFDS Criterion 8 – The NFDS shall be separated from the PICS to the extent that any removal of a component or channel common to both the NFDS and the PICS preserves the reliability, redundancy, and independence of the NFDS.

Communications from the NFDS to the TRPS and PICS (via TRPS) 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 9 – The NFDS detectors shall be qualified for continuous submerged operation within the light water pool. The NFDS detector housings shall be watertight and supported by a sleeve structure, mounted to the SASS, at specific locations surrounding the SASS.

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).

NFDS Criterion 10 – 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 (via TRPS) 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~~TRPS electronics in physically separated ~~cable trays and raceways~~electronics enclosures (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 (via TRPS 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).

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 (via TRPS) 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~~TRPS electronics in physically separated ~~cable trays and raceways~~electronics enclosures.

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 in~~side~~ the ~~facility control room~~RPF and IF 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~~,~~ and the IF~~, and facility control room. The facility control room is located in a non-radiologically controlled seismic area~~. The RPF~~,~~ and 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 f~~Fault detection ~~normally available is~~for the "source range missing" and "power range missing" discrete signals is provided to the PICS (via TRPS).

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 (via TRPS) 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.

event. Single failure-proof features are included such that any credible failure of a single component will not result in the loss of capability to stop and hold the critical load.

Radioisotope Production Facility Overhead Crane

The RPF overhead crane is a 15-ton, double girder, bridge style crane designed for the handling of shield cover plugs and equipment in the RPF. The RPF overhead crane is designed to span the width of the RPF and travel the length of the RPF.

The RPF overhead crane employs the use of mechanical stops, electrical-interlocks, and predetermined safe load paths to minimize the movement of loads in proximity to redundant or dual safe shutdown equipment. These safeguards ensures that off-normal load events from loads containing radioactive materials or safety-related SSCs that are beneath, or directly adjacent to a potential travel load path of the RPF overhead crane, could not result in the complete loss of a safe shutdown function or the release of radioactivity in excess of 10 CFR 20 limits.

The RPF overhead crane is designed and constructed following the seismic requirements for an ASME NOG-1, Type II crane so that it will remain in place with or without a load during a design basis earthquake. The crane is not required to support the critical load nor remain operational during and after such an event.

9b.7.2.3 Operational Analysis and Safety Function

The IF overhead crane removes irradiation unit (IU) cell plugs, the target solution vessel (TSV) off-gas system (TOGS) cell plugs, primary cooling room plugs, and neutron driver transport to and from IU cells and the neutron driver assembly system (NDAS) service cell. The IF overhead crane is used for lifting, repositioning, and landing operations associated with major components of the subcritical assembly system (SCAS), the primary closed loop cooling system (PCLS), the TOGS, and the tritium purification system (TPS) as well as various planned maintenance activities throughout the IF.

The RPF overhead crane is utilized for lifts including the removal of tank vault, valve pit, and pipe trench plugs, removal of carbon delay bed vault plugs, supercell ~~slave~~ manipulator replacements, and the removal of column waste drums and post cooldown shielding/packaging. The RPF overhead crane is used for various planned maintenance activities. In addition, the crane performs lifting of empty tanks in the RPF, immobilized waste drums and the associated shielding/packaging hardware, and other major components within the RPF.

The IF and RPF overhead cranes are inspected, tested, and maintained in accordance with ASME B30.2 (ASME, 2011a). The inspection requirements reduce the probability of a load drop that could result in a release of radioactive materials or damage to essential safe shutdown equipment that could cause unacceptable radiation exposures. Inspection and testing of special lifting devices are performed in accordance with American National Standards Institute (ANSI) N14.6, Radioactive Materials - Special Lifting Devices for Shipping Containers Weighing 10,000 Pounds (4500 kg) or More (ANSI, 1993). Inspection and testing of lifting devices not specially designed are in accordance with ASME B30.9, Slings (ASME, 2018).

With respect to the SHINE facility, a heavy load is defined as a load that, if dropped, may cause radiological consequences that challenge 10 CFR 20 limits. For cranes operating in the vicinity of

- RLWI system flushing;
- VTS flushing and adjustment of target solution in the TSSS;
- PVVS condensate pH adjustment and flush; and
- PSB flushing.

Reagents in laboratory containers are manually introduced into the MEPS purification hot cells through hot cell pass-throughs. Hot cell ~~master-slave~~ manipulators are used to add chemicals to the laboratory scale purification processes performed in the hot cells.

Compressed oxygen cylinders are stored inside the IF to service the TOGS. Compressed oxygen is routed through dry particulate filters, regulated, and distributed to the TOGS.

Table 9b.7-6 identifies the systems which interface with the FCRS.

9b.7.10.3 Operational Analysis and Safety Function

Bulk liquid and solid chemicals and chemical reagents are received, stored, maintained, and used in accordance with the chemical hygiene plan and are stored per their applicable safety data sheets.

The FDWS provides demineralized water to both the storage building and the chemical storage and preparation room for chemical reagent preparation. Individual acid, base, and organic waste containers are provided for disposal of chemicals.

Reagents from FCRS process delivery tanks are pumped directly into the respective process tie-in points at controlled flow rates and temperatures in accordance with the process requirements. Administrative and engineered controls, including accurate identification of reagents inside process delivery tanks and containers, and color-coded and size specific connections, ensure that reagents are not inadvertently supplied at incorrect process tie-in points. The FCRS process delivery tanks are volume limited, thereby setting maximum volume of reagents that can be supplied to respective production-related processes.

Mixing of acids and bases could cause a highly exothermic reaction. As such, bulk quantities of acids are stored separately from the bases and hydrogen peroxide in segregated storage spaces within the storage building. Small volumes of chemicals to be used in laboratory settings and in processes are stored and labeled in accordance with their applicable safety data sheets. Table 13b.3-1 provides a list of chemicals within the SHINE facility.

The storage and delivery of oxygen gas inside the RCA complies with fire hazard analysis (FHA), as described in Section 9a2.3, and applicable Occupational Safety and Health Administration (OSHA) requirements.

FCRS operations are performed in accordance with the requirements of the radiation protection program, described in Section 11.1.

The FCRS contains no SNM; however, the addition of basic chemical reagents to interfacing systems may result in uranium precipitation. Therefore, chemical additions to process tanks are evaluated under the nuclear criticality safety program, as described in Section 6b.3.

ENCLOSURE 3
ATTACHMENT 2

SHINE TECHNOLOGIES, LLC

SHINE TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE
SUPPLEMENT NO. 13 AND RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

TECHNICAL SPECIFICATIONS MARK-UPS
PUBLIC VERSION

9 pages follow

Table 3.2.3 TRPS Input Channel Actions

	Action	Completion Time
1.	If one channel is inoperable, Place the SFM for the associated channel in trip AND Restore the channel to Operable.	 2 hours 30 days
2.	If two redundant channels are inoperable, Place the associated IU in Mode 3.	 6 hours
3.	If two redundant channels are inoperable, OR Action and associated completion time of Condition 1 not met, Place the associated IU in Mode 3 AND Place the associated IU in Mode 0.	 6 hours [ ]PROP/ECI
4.	If two redundant channels are inoperable, Close at least one TSV fill valve.	 6 hours
5.	If one or more channel is inoperable, Close at least one TSV fill isolation valve OR Place the associated IU in Mode 3.	 6 hours 6 hours
6.	If three redundant channels are inoperable, Place the associated IU in Mode 3.	 1 hour
7.	If three redundant channels are inoperable, Place the associated IU in Mode 3 AND Place the associated IU in Mode 0.	 1 hour [ ]PROP/ECI

Table 3.2.3-a TRPS Instrumentation

	Variable	Setpoint	Required Channels	Applicability (per IU)	Action	SR
a.	Wide range neutron flux	≤ 176% power	3	Modes 1 and 2	1, 2, 6	1, 4
b.	Power range neutron flux	≤ 85% power; averaged over ≤ 45 seconds [ ]PROP/ECI	3	Modes 1 and 2	1, 2, 6	1, 4
c.	Source range neutron flux	≤ 1.5 times the nominal flux at 95% volume of the critical fill height	3	Mode 1	1, 4, 6	1, 4
d.	TSV fill isolation valve position indication	Not Closed	2	Mode 2	5	3
e.	PCLS flow	[ ]PROP/ECI; IU Cell Safety Actuation delayed by ≤ 180 seconds	3	Modes 1 and 2	1, 2, 6	2, 4
f.	PCLS temperature	≤ 72.9°F; IU Cell Safety Actuation delayed by ≤ 180 seconds ≥ 63.5°F	3	Modes 1 and 2	1, 2, 6	2, 4
g.	Low-high TSV dump tank level	~~≤ 3%~~High level	3	Modes 1 and 2	1, 2, 6	3
h.	High-high TSV dump tank level	~~≤ 85%~~High level	3	Modes 1, 2, 3, and 4	1, 3, 7	3
i.	TOGS mainstream flow	[ ]PROP/ECI	3 (per train)	Modes 1, 2, 3, and 4	1, 3, 7	2, 4

	Action	Completion Time
14.	If both required channels are inoperable, Place the associated Alignment Actuation components in the actuated state.	1 hour
15.	If one required channel is inoperable, Close at least one associated TPS target chamber supply line valve per associated IU.	12 hours
16.	If both required channels are inoperable, Close at least one associated TPS target chamber supply line valve per associated IU.	1 hours

Table 3.2.4-a ESFAS Process Instrumentation

	Variable	Setpoint	Required Channels	Applicability	Action	SR
a.	MEPS heating loop conductivity	≤ 478 µmho/cm	2 (per hot cell)	Target solution or radioactive process fluids present in the associated hot cell	3, 4	1, 2
b.	PVVS carbon delay bed exhaust carbon monoxide	≤ 42 ppm	2 (per delay bed group)	Associated carbon delay bed group Operating	7, 8	1, 2
c.	VTS vacuum header liquid detection	~~Active~~Liquid detected	2	Solution transfers using VTS in-progress	5, 6	3
d.	RDS liquid detection	~~Active~~Liquid detected	2	Solution transfers using VTS in-progress	5, 6	3
e.	PVVS flow	≥ 7.1 SCFM	3	Facility not Secured	1, 2	3
f.	~~TSSS~~ TSPS dissolution tank level	~~Active~~High level	2	Dissolution tank or TSPS glovebox contains uranium	9, 10	3
g.	Uninterruptible electrical power supply system (UPSS) loss of external power	Loss of Power; actuation delayed by ≤ 180 seconds	2	Any IU in Mode 1, 2, 3, or 4	11, 12	3

Table B-3.2.3 TRPS Input Variable Allocation

	Variable	Division A	Division B	Division C
a.	Wide range neutron flux	[		
b.	Power range neutron flux			
c.	Source range neutron flux			
d.	TSV fill isolation valve position indication			
e.	PCLS flow			
f.	PCLS temperature			
g.	Low-high TSV dump tank level			
h.	High-high TSV dump tank level			
i.	TOGS mainstream flow			
j.	TOGS dump tank flow			
k.	TOGS oxygen concentration			
l.	TOGS condenser demister outlet temperature			]PROP/ECI

Three TRPS process variable instrumentation channels are provided for each of the variables in Table 3.2.3-a, one channel for each of Divisions A, B, and C, with the exception of TSV fill valve position indication (item d.) for which only two channels are provided. Only two channels of any process variable instrumentation are required to be Operable to provide redundancy to protect against a single failure.

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 FSAR 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.

When all three channels are Operable for a variable provided with three Divisions, actuation of the safety function occurs on 2-out-of-3 voting logic. When any single channel is inoperable for variables provided with three Divisions, the

density limit (see LCO 3.1.6). The [ ]PROP/ECI power setpoint is based on an analytical limit of [ ]PROP/ECI power, which is set such that it is above a flux level expected to be caused by delayed neutrons continuing to be produced after the neutron driver has stopped Operating.

With one channel inoperable, the SFM for the associated channel is placed in trip within 2 hours and the associated channel is restored to operable within 30 days. With two redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 6 hours. With three redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 1 hour. Transition to Mode 3 may be accomplished by initiating a manual IU Cell Safety Actuation, or by cycling the IU Mode to Mode 3 to perform a normal shutdown.

c. During the filling process, the NFDS measures the counts per second, up to 1E+05 cps. The three source range neutron flux channels are required to be Operable to ensure the TSV neutron flux is measured during Mode 1, the only Mode where TSV filling is allowed. The high source range neutron flux limit protect against an insertion of excess positive reactivity during the filling process, as discussed in FSAR Subsection 7.4.4.1.1. The high source range neutron flux setpoint of 1.5 times the nominal flux at 95% volume of the critical fill height is set to ensure an IU Cell Safety Actuation occurs prior to exceeding a percentage above the normal startup flux as measured by the NFDS, as described in FSAR Subsection 4a2.6.2.7. The setpoint provides margin to an analytical limit of [ ]PROP/ECI times the nominal flux at 95% volume of the critical fill height. This analytical limit provides protection against positive reactivity insertions that could challenge the PSB integrity from an uncontrolled fill at [ ]PROP/ECI, the physical limit of the TSV fill system. Exceeding the high source range neutron flux setpoint results in an IU Cell Safety Actuation.
With one channel inoperable, the SFM for the associated channel is placed in trip within 2 hours and the associated channel is restored to operable within 30 days. With two channels inoperable, at least one TSV fill valve is required to be closed within 6 hours to prevent addition of target solution to the TSV. With three redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 1 hour.

d. The TSV fill isolation valve position indication protects against an inadvertent addition of target solution to the TSV during irradiation. Two position indication channels are provided per valve. At least one TSV fill isolation valve must be closed in Mode 2; opening both TSV fill isolation valves in Mode 2 results in an IU Cell Safety Actuation. The TSV fill isolation valve position indication also provides an input to the Fill Stop function. The TSV fill valves being opened early, or opened too long, while the IU is in Mode 1 results in a Fill Stop actuation, which automatically closes both TSV fill valves.
With one or more channels inoperable, at least one TSV fill isolation valve is required to be closed within 6 hours or the associated IU must be placed in Mode 3 within 6 hours.

of the target solution that could cause an excess positive reactivity insertion, as described in FSAR Subsection 7.4.4.1.6. This parameter also ensures the temperature of solution during the fill of the TSV during Mode 1 is within

analyzed limits, as described in FSAR Subsection 7.4.4.1.6. Falling below this setpoint results in an IU Cell Safety Actuation.

With one channel of PCLS temperature inoperable, the SFM for the associated channel is placed in trip within 2 hours and the associated channel is restored to operable within 30 days. With two redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 6 hours, during which PCLS cooling is not required and target solution is drained to the favorable geometry TSV dump tank. With three redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 1 hour.

g. The TSV dump tank low-high level is a discrete signal provided by a level switch. The level switch is installed at a height ~~limit~~ of 3% of the vertical span of the annular tank and is based on an analytical limit of [ ]$^{PROP/ECI}$, which equates to 6.2% of the [ ]$^{PROP/ECI}$ vertical span of the annular tank. The TSV dump tank low-high level protects against a leak of liquid into the TSV dump tank when the tank is expected to be empty, ensuring there is enough capacity in the TSV dump tank to receive a full TSV solution batch, as described in FSAR Subsections 4a2.2.1.10 and 7.4.4.1.8. Exceeding this ~~setpoint~~ high level results in an IU Cell Safety Actuation and an IU Cell Nitrogen Purge.
With one channel inoperable, the SFM for the associated channel is placed in trip within 2 hours and the associated channel is restored to operable within 30 days. With two redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 6 hours. With three redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 1 hour. Leak indication in Mode 3 is provided by the high-high TSV dump tank level.

h. The TSV dump tank high-high ~~limit~~ level is a discrete signal provided by a level switch. The level switch is installed at a height of 85% of the vertical span of the annular tank and is based on an analytical limit of [ ]$^{PROP/ECI}$, which equates to 87.9% of the [ ]$^{PROP/ECI}$ vertical span of the annular tank. The TSV dump tank high-high level ensures the TSV dump tank solution height does not interfere with TOGS operation, as described in FSAR Subsection 7.4.4.1.9. Exceeding this ~~setpoint~~ high level results in an IU Cell Safety Actuation and an IU Cell Nitrogen Purge.
With one channel inoperable, the SFM for the associated channel is placed in trip within 2 hours and the associated channel is restored to operable within 30 days. With two redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 6 hours and Mode 0 within [ ]$^{PROP/ECI}$. With three redundant channels inoperable, the associated IU is required to be placed in Mode 3 within 1 hour and Mode 0 within [ ]$^{PROP/ECI}$. Transfer of target solution out of the IU to achieve Mode 0 requires the target solution to be held in the TSV dump tank for at least the minimum period of time specified in LCO 3.1.8 prior to transfer.

SBVMs or SBMs. Radiation monitors that provide inputs to ESFAS are addressed in LCO 3.7.1.

More than one input device provides a signal to each SFM. The following table describes the allocation of inputs to the ESFAS modules:

Table B-3.2.4 ESFAS Input Variable Allocation

	Variable	Division A	Division B	Division C
a.	MEPS area A heating loop conductivity	[		
	MEPS area B heating loop conductivity			
	MEPS area C heating loop conductivity			
b.	PVVS carbon delay bed group 1 exhaust carbon monoxide			
	PVVS carbon delay bed group 2 exhaust carbon monoxide			
	PVVS carbon delay bed group 3 exhaust carbon monoxide			
c.	VTS vacuum header liquid detection			
d.	RDS liquid detection			
e.	PVVS flow			
f.	TSPS ~~D~~dissolution tank level			
g.	UPSS loss of external power			
h.	MEPS ~~Area~~ area A three-way valve position indication			
	MEPS ~~Area~~ area B three-way valve position indication			
	MEPS ~~Area~~ area C three-way valve position indication			]PROP/ECI

maintenance. At least seven of the eight carbon delay beds are required to be Operating to provide the design noble gas residence time. If only five or six carbon delay beds are Operating, the noble gas residence time is reduced, affecting the total curies released from the facility. The total curies released from the facility are managed in accordance with LCO 3.7.2.

c. The ESFAS monitors for the presence of liquid in the VTS vacuum header to protect against an overflow of liquid out of the VTS lift tanks, as described in FSAR Subsections 6b.3.1.5, 7.5.4.1.8, and 9b.2.5.3. The liquid detection instrumentation provides a discrete signal indicating the presence or absence of liquid. Two Divisions of liquid detection are located in the VTS vacuum header serving all lift tanks that may contain target solution. The detection of liquid results in a VTS Safety Actuation to stop any in-progress transfers of fluid. The function is required to prevent degrading one of the controls to prevent a criticality, by preventing target solution entering non-favorable geometry locations in the VTS system, as described in FSAR Subsection 6b.3.2.5.

   With one channel inoperable, the VTS vacuum pump breakers and VTS vacuum break valves are required to be opened within 12 hours to stop the transfer of solution within the facility. A completion time of 12 hours allows for the performance of minor repairs and is acceptable based on the continued availability of the redundant channel. With both channels inoperable, the VTS vacuum pump breakers and VTS vacuum break valves are required to be opened within 1 hour to stop the transfer of solution within the facility. A completion time of 1 hour recognizes the importance of taking prompt action when equipment credited for the prevention of an unintended criticality is unable to perform its required function. The completion time is acceptable based on the low likelihood of an event during the limited time.

d. The ESFAS monitors for the presence of liquid in the RDS to protect against overflow of high radiation liquids into the RDS sump tanks, as described in FSAR Subsections 7.5.4.1.9 and 9b.2.5.3. The detection of liquid in the RDS sump tanks results in a VTS Safety Actuation to stop any in-progress transfers of liquid. A filled RDS sump tank prevents that tank from accepting leakage in the event of a leak of target solution into a tank vault, valve pit, pipe trench or in the supercell. The VTS Safety Actuation signal is allowed to be bypassed to restart the VTS and remove solution from the RDS sump tanks as part of the recovery from an instance where liquid has entered the tank. The liquid detection instrumentation provides a discrete signal indicating the presence or absence of liquid.

   With one channel inoperable, the VTS vacuum pump breakers and VTS vacuum break valves are required to be opened within 12 hours to stop the transfer of target solution and radioactive liquid wastes within the facility. A completion time of 12 hours allows for the performance of minor repairs and is acceptable based on the continued availability of the redundant channel. With both channels inoperable, the VTS vacuum pump breakers and VTS vacuum break valves are required to be opened within 1 hour to stop the transfer of target solution and radioactive liquid wastes within the facility. A completion time of 1 hour recognizes the importance of taking prompt action when the safety function has been lost. The completion time is acceptable based on the low likelihood of an event during the limited time.

e. PVVS blowers are required to dilute radiolytic hydrogen generated from irradiated target solution and radioactive liquid waste located in tanks in the RPF, as described in FSAR Subsection 6b.2.3. The low PVVS flow limit of 7.1 SCFM is based on an analytical limit of 5.0 SCFM and is indicative of a loss of the PVVS function. Low PVVS flow results in an RPF Nitrogen Purge Actuation, as described in FSAR Subsection 7.5.4.1.15. Three channels of PVVS flow are provided.

With one channel inoperable, the SFM for the associated channel is placed in trip within 2 hours and must be restored to Operable within 30 days. With two or more channels inoperable, or when the required action and completion time for one inoperable channel is not met, the nitrogen purge system is actuated within 1 hour to provide hydrogen mitigation for RPF tanks. A completion time of 1 hour recognizes the importance of taking prompt action when the safety function has been lost. The completion time is acceptable based on the low likelihood of an event during the limited time.

f. Level in the TSPS dissolution tank is monitored to prevent overflow of the tank and protect against a criticality event in a non-favorable geometry location, as described in FSAR Subsections 6b.3.1.4 and 7.5.4.1.18. The indication is a discrete signal provided by a level switch. The setpoint of "~~Active~~high level" indicates that the level switch, installed at approximately 98% of the full volume of the tank, which provides margin to an analytical limit of 100%, has been actuated by rising tank level. Exceeding the ~~setpoint~~ level results in a Dissolution Tank Isolation.

With one channel inoperable, the Dissolution Tank Isolation components (i.e., RPCS supply cooling valves and the TSPS air inlet and RVZ1 exhaust isolation valves) are required to be closed within 12 hours. A completion time of 12 hours allows for the performance of minor repairs and is acceptable based on the continued availability of the redundant channel. With both channels inoperable, the Dissolution Tank Isolation components (i.e., RPCS supply cooling valves and the supply and exhaust ventilation dampers) are required to be closed within 1 hour. A completion time of 1 hour recognizes the importance of taking prompt action when equipment credited for the prevention of an unintended criticality is unable to perform its required function. The completion time is acceptable based on the low likelihood of an event during the limited time.

g. The ESFAS monitors for a loss of external power to the UPSS to protect against an impending loss of hydrogen mitigation via the TOGS in any IU in Modes 1 through 4, as described in FSAR Section 4a2.8 and Subsection 7.5.4.1.19. The ESFAS implements a 180 second timer prior to sending a signal to TRPS to provide margin to the five-minute UPSS runtime for the TOGS blowers and recombiners, as described in FSAR Subsection 8a2.2.3. Two channels are provided; one signal is received from each Division of the UPSS. This signal results in an IU Cell Nitrogen Purge.

With one channel inoperable, the channel is required to be restored within 72 hours. A completion time of 72 hours allows for the performance of repairs, including issues that affect operability of the UPSS (see LCO 3.8.1), while minimizing the time that the reliability of the ESFAS is reduced. The completion time is acceptable based on the continued availability of the