ENCLOSURE 3

SHINE MEDICAL TECHNOLOGIES, LLC

SHINE MEDICAL TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE SUPPLEMENT NO. 8 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 Medical 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 7-9

Section 50.34 of 10 CFR states, in part, that a safety analysis report (SAR) shall include (1) "the principal design criteria for the facility," and (2) "the design bases and the relation of the design bases to the principal design criteria". A definition is provided in 10 CFR 50.2 for what constitutes a design bases:

> Design bases means that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals.

NUREG-1537, Part 2, Section 7.4, "Reactor Protection System," states, in part, that the SAR should include the design bases, acceptance criteria, and guidelines used for design of the protection system, as well as an "analysis of adequacy of the design to perform the functions necessary to ensure safety, and its conformance to the design bases, acceptance criteria, and the guidelines used."

Section 7.2.2, "Design Criteria," of the SHINE FSAR states, in part, that "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)" and are applied in a graded approach to each I&C system. The SHINE FSAR states that Section 3.1, "Design Criteria," shows how the facility design criteria are applied to each ICS The SHINE FSAR also indicates that system-specific criteria are provided in SHINE FSAR Sections 7.4 and 7.5 for TRPS and ESFAS and "additionally describe how the facility design criteria and system-specific design criteria are met or implemented for each I&C system."

The NRC staff reviewed the SHINE design criteria and sampled selected system-specific criteria in Sections 7.4 and 7.5 of the SHINE FSAR that predominantly rely upon the underlying HIPS protective system architecture, communications, and equipment interface that is common in both the TRPS and ESFAS. The SHINE FSAR descriptions of how the TRPS and ESFAS meet applicable design criteria lack sufficient detail on the attributes of the HIPS platform configuration and its operation. Without an adequate description of the specific configuration details and operation, the NRC staff cannot determine if the facility design criteria, TRPS design criteria, and ESFAS design criteria are achieved.

In some cases, the NRC staff has also identified explanations where design or operational descriptions appear to be incomplete, inconsistent with the language and common understanding of the design criterion wording, or inconsistent with the HIPS TR and intent of the associated plant-specific action items.

(a) Re-evaluate the TRPS and ESFAS design criteria in SHINE FSAR Sections 7.4 and 7.5, and provide additional design and operational detail in the SHINE FSAR to explain how the facility design criteria and TRPS and ESFAS criteria are met.

In its re-evaluation, SHINE should verify the applicability of each of its design criteria to the TRPS and ESFAS. SHINE should describe how design features or functions are used to meet each of the criteria applicable to the TRPS and ESFAS. SHINE should consider RAI 7-9 items (b) – (f), below, as examples of inconsistent explanations of the implementation design criteria in the SHINE FSAR that may aid in the preparation of its response to this part of the RAI. However, the NRC staff notes that these are representative examples and not an exhaustive list of all information SHINE may determine to be appropriate to include in its RAI response and any FSAR updates. After assessing the applicability of the design criteria, the relevant SHINE FSAR narratives should be updated to summarize the type of information likely to address how the design criteria are met. The NRC staff notes that key SHINE design documents, such as the TRPS and ESFAS system requirement specifications; TRPS and ESFAS system design descriptions; and TRPS and ESFAS system design specifications could be provided to support this information need[1].

The NRC staff recognizes that the information needs requested in RAIs 7-10 through 7-16 below may address the deficiencies associated with several of the design criteria.

(b) **Maintenance Bypass of Execute Features** - TRPS Criterion 41 contains the design criteria for the maintenance bypass of execute features of the TRPS (ESFAS Criterion 42 contains similar criteria).

Section 7.4.2.2.9, “Operational Bypass, Permissives, and Interlocks,” states, in part, that “[w]here three channels are provided, taking an SFM [safety function module] out of service preserves the single failure criterion for variables associated with that SFM. In cases where only two channels are provided, taking a channel out of service will actuate the associated safety function. For testing purposes, placing a channel in maintenance bypass will be allowed by technical specifications [TSs] for up to two hours to perform required testing. Two hours is considered acceptable due to the continued operability of the redundant channel(s) and the low likelihood that an accident would occur in those two hours (Subsection 7.4.4.3).”

[1] For information that SHINE prefers to share in its electronic reading room rather than through docketed correspondence, a regulatory audit of information may be the most appropriate means for further NRC staff evaluation.

Further, from the NRC audit of the HIPS platform on May 13, 2021, the NRC staff learned that the design and configuration of the HIPS equipment for TRPS is not intended to allow a portion of the execute features to be placed in maintenance bypass.

The explanation provided in the SHINE FSAR describes maintenance bypass features associated with the sense and command features of the HIPS equipment, and does not address the execute functions of the HIPS equipment or the execute features of the TRPS that is specified in TRPS Criterion 41.

For example, there are two options for taking the SFM modules out of service, and only one option is consistent with the description provided. Furthermore, in cases where only two channels are provided[2], the manner of taking a channel out of service is accomplished differently and is not explained.

Revise the SHINE FSAR to include an explanation to clearly reflect the intended design of the TRPS and ESFAS for maintenance bypass of the execute features.

(c) **Separation of Protection and Control Systems** – SHINE Design Criterion 18 contains the design criteria for the separation of the protection system from control systems. This criterion is normally used to address instrumentation and control configurations where the control of a process parameter (e.g., power density) and the protection against an undesirable process parameter value (e.g., exceeding power density limits) are using the same sensors. For example, from the description in the SHINE FSAR, it appears that the SHINE facility protects and controls solution power density using the same set of safety-related sensors. The NRC staff notes that IU power indications (i.e., neutron flux) are common to both protection and control.

This particular type of equipment configuration is vulnerable to a sensor failure causing an undesirable control action and could prevent the protection system from protecting against the undesirable control action due to reliance on the same sensor.

Section 7.4.2.1.6, “Separation of Protection and Control Systems,” of the SHINE FSAR states the following:

> 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).

[2] For the TRPS, there is only one instance where “only two channels are provided.” This is the case for the TSV fill valve position indication. Since this input does not use an SFM, there is no description of how to remove these channels from service. ESFAS, on the other hand, has many “two channel” configurations that use SFMs.

The NRC staff notes that since protection systems are safety-related, then all shared sensors with the PICS should be safety-related. Therefore, the NRC staff does not agree that there are “nonsafety-related inputs into the TRPS.” In addition, the SHINE FSAR description quoted above does not identify what sensors are shared between the protection and control systems. Further, this description does not explain how the TRPS would perform its protection function given a failure of a shared component.

Revise the SHINE FSAR to include a description of how the TRPS design meets SHINE Design Criterion 18 to clearly reflect the intended design of components shared to protect and control certain operations.

(d) **Protection of Specified Acceptable Target Solution Design Limits** – SHINE Design Criterion 14 requires the TRPS to be designed to automatically initiate the operation of appropriate systems to ensure that specified acceptable target solution design limits are not exceeded as a result of anticipated transients.

SHINE FSAR Section 13a2.1.2, “Insertion of Excess Reactivity,” describes accidents analyzed due to insertion of excess reactivity. One identified initiating event and scenario is attributed to high neutron production (and consequently high power) at cold conditions. To protect from these events, Chapter 13 of the SHINE FSAR identifies actions to be performed by the TRPS to terminate IU operation to preserve the safety limits (SLs). The NRC staff considers SHINE Design Criterion 14 to apply to all excess reactivity scenarios.

Chapter 7 of the SHINE FSAR does not appear to 1) provide or reference a description of the “specified acceptable target solution design limits” referenced in SHINE Design Criterion 14 or 2) describe how the TRPS protects against exceeding such limits during all analyzed scenarios. The NRC staff infers that the SHINE TS limiting condition for operation (LCO) 3.1.6 provides acceptable target solution design limits applicable during operation and 3.1.7 design limits only during loss of driver and restart transients. Based on this information, the NRC staff infers that the TRPS protects against the specific design limits identified in LCO 3.1.7 for driver and restart transients above 40 percent power, because the high wide range neutron flux setpoint will initiate an automatic IU Cell Safety Actuation. However, it appears that the TRPS is not identified to protect against the acceptable target solution design limits of LCO 3.1.6 for all other operating conditions. In particular, it is not clear to the NRC staff how TRPS and power range monitors protect against design solution limits for all excess neutron production or excess reactivity scenarios below 120 degrees Fahrenheit.

Revise the SHINE FSAR to identify protection functions credited to maintain the specified acceptable target solution design limits during all modes of operation and the transients specified in Chapter 13 of the SHINE FSAR.

(e) **Protection System Independence and Diversity** – SHINE Design Criterion 16 requires, in part, that 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.

Section 7.4.2.1.4, “Protection System Independence,” of the SHINE FSAR notes that the architecture provides diverse methods for actuation of the safety functions at the division level, automatic and manual, and FPGAs in each division are of a different physical architecture to prevent common cause failure (CCF) (e.g. equipment diversity). In addition,

SHINE FSAR Section 7.4.5.2.4, “Diversity,” does not include a discussion on diversity features, such as the type of FPGA technologies used, logic development tools, signals, built-in equipment diversity, segregation of safety functions, or diverse protection logic on a safety function module for each safety function. Instead, the SHINE FSAR refers back to the approved HIPS TR. However, application specific action item (ASAI) 10 of the HIPS TR requires that an applicant verify that diversity attributes conform to those described in the approved TR, which SHINE has not done.

Further, Section 7.4.5.2.5, “Simplicity,” of the SHINE FSAR states that the HIPS design uses segmentation to provide functional diversity. However, the SHINE FSAR description does not include any description of functional diversity. The NRC staff considers functional diversity to be when two different plant process parameters are sensed to initiate protective actions against the same event.

Revise the SHINE FSAR to describe diversity features included in the HIPS for the TRPS and ESFAS. Also, describe whether and how functional diversity is applied to prevent loss of function, including CCFs.

(f) **Interlocks** – TRPS Criterion 34 requires that interlocks ensure operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required.

The NRC staff considers TRPS Criterion 34 to apply to all operating conditions, including both operational bypass and maintenance bypass conditions.

Section 7.4.2.2.9 of the SHINE FSAR describes how Criterion 34 is achieved for only operational bypass. This section does not describe if there are other ways the operator can defeat an automatic safety function.

Section 7.4.4.3, “Maintenance Bypass,” of the SHINE FSAR describes administrative controls for maintenance bypass, which are in the proposed TSs. However, the SHINE FSAR does not describe whether interlocks are implemented to prevent an operator from putting all instrument channels in maintenance bypass (i.e., not in tripped mode) concurrently.

Confirm the intent of the TRPS Design Criterion 34 by clearly describing how interlocks are implemented to prevent operators from defeating automatic safety functions during all operating conditions.

The information requested in parts (a) through (f) above is necessary to support the evaluation findings in Section 7.4 of NUREG-1537, Part 2, including that “[t]he 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.”

SHINE Response

(a) SHINE has re-evaluated the design criteria provided in Sections 7.4 and 7.5 of the FSAR. Where determined to be appropriate as a result of the re-evaluation, SHINE has provided additional design and operational detail describing how the target solution vessel (TSV) reactivity protection system (TRPS) and engineered safety features actuation system

(ESFAS) meet certain SHINE design criteria, TRPS design criteria, and ESFAS design criteria. For those design criteria where additional detail is not provided, SHINE assessed the description provided in the FSAR on how the TRPS and ESFAS meet the design criteria and determined the description to be sufficient.

The SHINE design criteria, TRPS design criteria, and ESFAS design criteria provided in the FSAR are applicable to TRPS and ESFAS and are met as described in the FSAR. SHINE did not remove any design criteria from the licensing basis as a result of the re-evaluation.

A summary of the results of the re-evaluation is provided below. A mark-up of the FSAR incorporating the below-described changes is provided as Attachment 1.

SHINE Design Criteria

SHINE has revised Subsections 7.4.2.1.1 and 7.5.2.1.1 of the FSAR to enhance the description of how the TRPS and ESFAS meet SHINE Design Criterion 13.

SHINE has revised Subsections 7.4.2.1.2 and 7.5.2.1.2 of the FSAR to enhance the description of how the TRPS and ESFAS meet SHINE Design Criterion 14.

SHINE has revised Subsections 7.4.2.1.3 and 7.5.2.1.3 of the FSAR to enhance the description of how the TRPS and ESFAS meet SHINE Design Criterion 15. Subsections 7.4.2.1.3 and 7.5.2.1.3 were previously revised to enhance the description of the implementation of the maintenance bypass capabilities and self-testing features via the SHINE Response to RAI 7-14 (Reference 3).

SHINE has revised Subsections 7.4.2.1.4 and 7.5.2.1.4 of the FSAR to enhance the description of how the TRPS and ESFAS meet SHINE Design Criterion 16.

SHINE has revised Subsections 7.4.2.1.5 and 7.5.2.1.5 of the FSAR to enhance the description of how the TRPS and ESFAS meet SHINE Design Criterion 17.

SHINE has revised Subsections 7.4.2.1.7 and 7.5.2.1.7 of the FSAR to enhance the description of how the TRPS and ESFAS meet SHINE Design Criterion 19.

SHINE has revised Subsections 7.4.2.1.8 and 7.5.2.1.9 of the FSAR to enhance the description of how the TRPS and ESFAS meet SHINE Design Criterion 38.

SHINE has revised Subsections 7.4.2.1.9 and 7.5.2.1.10 of the FSAR to enhance the description of how the TRPS and ESFAS meet SHINE Design Criterion 39.

TRPS Design Criteria

SHINE has revised Subsection 7.4.2.2.1 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 2 and TRPS Criterion 3.

SHINE has revised Subsection 7.4.2.2.2 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 4, TRPS Criterion 7, and TRPS Criterion 9. SHINE has also revised Subsection 7.4.5.4 of the FSAR to provide reference to the programmable logic development plan (PLDP).

SHINE previously revised Subsection 7.4.2.2.3 of the FSAR via the SHINE Response to RAI 7-17 (Reference 3) to enhance the description of how the TRPS meets TRPS Criterion 14.

SHINE has revised Subsection 7.4.2.2.4 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 16. SHINE previously revised Subsection 7.4.2.2.4 of the FSAR via the SHINE Response to RAI 7-12 and RAI 7-19 (Reference 3) to enhance the description of how the TRPS meets TRPS Criterion 17.

SHINE has revised Subsection 7.4.2.2.5 of the FSAR to revise the language of TRPS Criterion 26 and enhance the description of how the TRPS meets TRPS Criterion 19, TRPS Criterion 23, TRPS Criterion 24, and TRPS Criterion 26.

SHINE has revised Subsection 7.4.2.2.7 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 28.

SHINE has revised Subsection 7.4.2.2.8 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 29, TRPS Criterion 30, TRPS Criterion 31, and TRPS Criterion 32.

SHINE has revised Subsection 7.4.2.2.9 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 33, TRPS Criterion 37, TRPS Criterion 38, TRPS Criterion 40, and TRPS Criterion 42.

SHINE has revised the description of how the TRPS meets TRPS Criterion 45 in Subsection 7.4.2.2.10 of the FSAR, as described in Enclosure 1.

SHINE previously revised Subsection 7.4.2.2.11 of the FSAR via the SHINE response to RAI 7-16 (Reference 3) to enhance the description of how the TRPS meets TRPS Criterion 46.

SHINE has revised Subsection 7.4.2.2.12 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 47, TRPS Criterion 48, and TRPS Criterion 49.

SHINE has revised Subsection 7.4.2.2.13 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 50.

SHINE has revised Subsection 7.4.2.2.14 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 53.

SHINE has revised Subsection 7.4.2.2.15 of the FSAR to enhance the description of how the TRPS meets TRPS Criterion 55.

ESFAS Design Criteria

SHINE has revised Subsection 7.5.2.2.1 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 2 and ESFAS Criterion 3.

SHINE has revised Subsection 7.5.2.2.2 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 4, ESFAS Criterion 7, ESFAS Criterion 8, ESFAS Criterion 9, and ESFAS Criterion 13.

SHINE previously revised Subsection 7.5.2.2.3 of the FSAR via the SHINE Response to RAI 7-17 (Reference 3) to enhance the description of how the ESFAS meets ESFAS Criterion 14.

SHINE has revised Subsection 7.5.2.2.4 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 16 and ESFAS Criterion 18.

SHINE previously revised Subsection 7.5.2.2.4 of the FSAR via the SHINE Response to RAI 7-12 and RAI 7-19 (Reference 3) to enhance the description of how the ESFAS meets ESFAS Criterion 17.

SHINE revised Subsection 7.5.2.2.5 of the FSAR to revise the language of ESFAS Criterion 27 and enhance the description of how the ESFAS meets ESFAS Criterion 20, ESFAS Criterion 24, ESFAS Criterion 25, and ESFAS Criterion 27.

SHINE has revised Subsection 7.5.2.2.7 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 29.

SHINE has revised Subsection 7.5.2.2.8 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 30, ESFAS Criterion 31, and ESFAS Criterion 33.

SHINE has revised Subsection 7.5.2.2.9 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 34, ESFAS Criterion 38, ESFAS Criterion 39, and ESFAS Criterion 43.

SHINE has revised the description of how the ESFAS meets ESFAS Criterion 46 in Subsection 7.5.2.2.10 of the FSAR as described in Enclosure 1.

SHINE previously revised Subsection 7.5.2.2.11 of the FSAR via the SHINE Response to RAI 7-16 (Reference 3) to enhance the description of how the ESFAS meets ESFAS Criterion 47.

SHINE has revised Subsection 7.5.2.2.12 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 48, ESFAS Criterion 49, and ESFAS Criterion 50.

SHINE has revised Subsection 7.5.2.2.13 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 51.

SHINE has revised Subsection 7.5.2.2.14 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 54.

SHINE has revised Subsection 7.5.2.2.15 of the FSAR to enhance the description of how the ESFAS meets ESFAS Criterion 55 and ESFAS Criterion 56.

(b) SHINE has revised the description of how the TRPS meets TRPS Criterion 41 in Subsection 7.4.2.2.9 of the FSAR and the description of how ESFAS meets ESFAS Criterion 42 in Subsection 7.5.2.2.9 of the FSAR to provide an explanation of the maintenance bypass of the execute features for the TRPS and ESFAS. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

The SHINE Response to RAI 7-14 (Reference 3) provides a discussion of the options for taking safety function modules (SFMs) out of service.

(c) SHINE has revised Subsections 7.4.2.1.6 and 7.5.2.1.6 of the FSAR to enhance the description of how the TRPS and ESFAS design meet SHINE Design Criterion 18, including a discussion of the intended design of components shared to protect and control certain operations, clarification on nonsafety-related inputs to the TRPS and ESFAS, what sensors have both protective and control functions, and a description of how the TRPS and ESFAS would perform protection functions given a failure of a shared component. A markup of the FSAR incorporating these changes is provided as Attachment 1.

(d) The SHINE target solution operating limits in the TSV are listed in Table 4a2.2-2 of the FSAR and are the acceptable target solution design limits referenced by SHINE Design Criterion 14.

SHINE Design Criterion 14 requires that the TRPS is designed to "(1) initiate, automatically, the operation of appropriate systems to ensure that specified acceptable target solution design limits are not exceeded as a result of anticipated transients; and (2) sense accident conditions and to initiate the operation of safety-related systems and components." While part (2) of SHINE Design Criterion 14 applies to all analyzed excess reactivity scenarios, part (1) of SHINE Design Criterion 14 specifically applies to conditions arising from anticipated transients.

SHINE defines anticipated transients as those conditions of normal operation which are expected to occur one or more times during the life of the SHINE facility.

The SHINE Safety Analysis (SSA) methodology, as described in Chapter 13 of the FSAR, ensures that postulated accident scenarios are brought to either highly unlikely or low consequence (i.e., below the SHINE Safety Criteria) with the use of credited controls. For a limited number of postulated excess reactivity scenarios, including high neutron production at cold conditions, the target solution power density design limits are exceeded without exceeding the SHINE Safety Criteria. However, these excess reactivity scenarios are not anticipated transients because they are not expected to occur one or more times during the life of the SHINE facility. Therefore, they do not require TRPS to automatically initiate controls specifically related to the target solution design limits.

Insertion of excess reactivity due to high neutron production at cold conditions is not an anticipated transient. There are no TRPS functions necessary to protect against exceeding the design limit identified in limiting condition for operation (LCO) 3.1.6 because there are not any anticipated transients that would result in exceeding this limit. For the anticipated transient of a driver restart, the timing of the Driver Dropout function provides protection against exceeding the design limits identified in LCO 3.1.7.

The TRPS does prevent exceeding the target solution design limits for anticipate transients and senses accident conditions to initiate the operation of safety-related systems and components. The TRPS monitors several system variables. Subsection 7.4.4.1 of the FSAR addresses the specific variables that provide input to the TRPS, the instrument range for covering normal and accident conditions, the accuracy for each variable, the analytical limit, and the response time.

If at any point a monitored variable exceeds its setpoint, the TRPS automatically places the irradiation unit (IU) into a state that mitigates the hazard. The primary variables that are monitored to prevent exceeding the target solution design limits during anticipated transients are the high time-averaged neutron flux (described in Subsection 7.4.4.1.3 of the FSAR), high wide range neutron flux (described in Subsection 7.4.4.1.4 of the FSAR), low primary closed loop cooling system (PCLS) flow (described in Subsection 7.4.4.1.7 of the FSAR), high and low PCLS temperature (described in Subsections 7.4.4.1.5 and 7.4.4.1.6 of the FSAR), low TSV off-gas system (TOGS) mainstream flow (described in Subsection 7.4.4.1.11 of the FSAR), and high TOGS condenser demister outlet temperature (described in Subsection 7.4.4.1.13 of the FSAR). The safety actuations that prevent the system from exceeding target solution design limits during anticipated transients are the IU Cell Safety Actuation, IU Cell Nitrogen Purge, and Driver Dropout. These safety actuations are described in Subsection 7.4.3.1 of the FSAR.

There are no anticipated transients that require the initiation of the ESFAS to ensure that target solution design limits are not exceeded.

SHINE has revised Subsections 7.4.2.1.2 and 7.5.2.1.2 of the FSAR to enhance the description of how the TRPS and ESFAS satisfy SHINE Design Criterion 14. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

(e) The SHINE Response to RAI 7-11 (Reference 3) provides a discussion of the diversity and defense-in-depth (D3) assessment that was performed using the guidance provided in NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of the Reactor Protection Systems” (Reference 4). The purpose of the D3 assessment is to identify potential vulnerabilities to digital-based common-cause failures (CCFs) in the TRPS and ESFAS.

The implementation of the highly integrated protection system (HIPS) platform for SHINE includes functional diversity by way of monitoring different input process parameters on different SFMs for use in mitigation of transients and accidents. This is consistent with Section 2.6.4 of NUREG/CR-6303, which states that, “two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects.” In the SHINE application of functional diversity, different methods of detecting transients and accidents are applied to one SFM than another. For example, source range neutron flux, power range neutron flux, and PCLS temperature are input to one SFM while TOGS mainstream flow, TOGS dump tank flow, and low-high TSV dump tank level are input to another. Since the system parameters input to one SFM are processed with unique logic compared to the logic used to process inputs to another SFM, functional diversity is achieved consistent with NUREG/CR-6303.

SHINE did not allocate different individual process parameters to different SFMs to initiate protective action for each event because the results of the D3 analysis do not indicate the need for this to address the potential consequences of a digital-based CCF and a requirement does not exist for this allocation for a non-power production or utilization facility. Plant process parameters are considered in the SSA, as described in Section 13a2 of the FSAR. The SSA, applying a risk-based methodology similar to the guidance of NUREG-1520, “Standard Review Plan for Fuel Cycle Facilities License Applications” (Reference 5), did not require two different plant process parameters to be sensed to initiate protective actions against the same event.

A description of how the TRPS and ESFAS design addresses Application Specific Action Item (ASAI) 10 is provided in the SHINE Response to Part (b) of RAI 7-10. A description of different types of field programmable gate array (FPGA) technologies used in the TRPS and ESFAS design is addressed in the discussion of ASAI 64 in the SHINE Response Part (b) of RAI 7-10.

SHINE has revised Subsection 7.4.5.2.5 of the FSAR to enhance the description of how functional diversity is applied. SHINE previously revised Subsection 7.4.5.2.4 of the FSAR via the SHINE Response to RAI 7-11 (Reference 3) to describe how the D3 assessment was performed to identify potential vulnerabilities to CCFs.

(f) The TRPS and ESFAS do not have automatic interlocks to prevent an operator from putting all instrument channels in maintenance bypass. The technical specifications provide administrative controls to prevent placing the same SFM across more than one division in maintenance bypass. Additional detail is provided in the evaluation of the HIPS platform ASAI 7 provided in TECRPT-2018-0028, “HIPS Platform Application Specific Action Item Report for the TRPS and ESFAS,” provided as Attachment 2.

SHINE has revised Subsections 7.4.2.2.9 and 7.5.2.2.9 to revise the language of TRPS Criterion 34 and ESFAS Criterion 35, and also revised the associated descriptions of how they are satisfied to include an exception for the use of maintenance bypass and a discussion of its acceptability. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

RAI 7-10

NUREG-1537, Part 2, Section 7.4, states, in part, that “the applicant should thoroughly describe the [protection system], listing the protective functions performed by the [protection system], and the parameters monitored to detect the need for protective action.” Additionally, NUREG-1537, Part 2, Section 7.4, states, in part, that the SAR should include the design bases, acceptance criteria, and guidelines used for design of the protection system, as well as an “analysis of adequacy of the design to perform the functions necessary to ensure safety, and its conformance to the design bases, acceptance criteria, and the guidelines used.” Therefore, the design bases, acceptance criteria, and guidelines used for design of the TRPS and ESFAS should be specified, and an analysis of the adequacy of the designs to perform the functions necessary to ensure safety and conform to the design bases and acceptance criteria should be provided in the SHINE FSAR.

Sections 7.1.2 and 7.1.3 of the SHINE FSAR state that both the TRPS and ESFAS use the NRC-approved HIPS platform. The NRC’s SE for the HIPS platform excluded the HIPS platform circuit boards and their instrument chassis, application-specific architecture, the application-specific design process, and application-specific equipment qualification. As such, the NRC staff identified 65 ASAIs to be addressed by any applicant referencing the TR in a site-specific license application as a means of demonstrating compliance with the approved platform and site-specific use in accordance with the applicable requirements in 10 CFR Part 50. SHINE’s disposition of these ASAIs were provided in response to RAI 7-4 (ADAMS Accession No. ML20254A355). The NRC staff reviewed this information and found several dispositions to be acceptable. However, many other dispositions are insufficient for demonstrating how the HIPS-platform-based TRPS and ESFAS meet the stated design criteria in the SHINE FSAR.

For example, ASAI 2 requires that an applicant demonstrate that the HIPS platform used to implement the application-specific system is unchanged from the base platform addressed in HIPS TR SE. Otherwise, the applicant must clearly and completely identify any modification or addition to the base HIPS platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes. The SHINE response to RAI 7-4 stated that the Sections 7.1, “Summary Description,” and 7.4.5, “Highly Integrated Protection System Design,” of the SHINE FSAR provide evidence that the HIPS platform used to implement the TRPS and ESFAS design is unchanged from the base platform described in the HIPS platform TR. After reviewing the information in Subsections 7.1 and 7.4.5 of the SHINE FSAR, the NRC staff determined that the application of the HIPS platform used to implement the TRPS and ESFAS design is different from the base platform addressed in the TR for the HIPS platform. Fundamentally, the approved HIPS platform uses two different FPGA technologies with a two-out-of-four safety logic channel configuration. Whereas, the HIPS equipment for the TRPS and ESFAS appears to use three different FPGA technologies with a two-out-of-three safety logic channel configuration.

The NRC staff performed an audit of the HIPS equipment for the SHINE facility on May 12, 2021. This audit focused on Audit Topic 1 identified in the audit plan (ADAMS Accession No. ML21130A313). During the audit discussions, the NRC staff better understood the modified version (e.g. system requirements and configuration) of the HIPS platform for the SHINE facility. The NRC staff also identified differences between the previously approved HIPS TR platform, and the HIPS-based TRPS and ESFAS. For example, the NRC staff learned from the audit that (1) the TRPS includes the remote input sub-module (RISM) or scheduling, bypass, and voting modules (SBVM), but the HIPS platform describe in the TR does not contain these modules; (2) the TRPS and ESFAS are combined in the same equipment rack, whereas the HIPS TR depicts instrument channels and actuation divisions in separate racks of equipment; and (3) the use of a gateway communication between TRPS/ESFAS and PICS.

However, information in Section 7.4.5 of the SHINE FSAR is not consistent with the requirements and descriptions in the HIPS design documents discussed in the audit. Consequently, referencing and relying upon the NRC-approved HIPS TR without clearly describing the differences in the SHINE facility implementation of HIPS platform in the TRPS and ESFAS design is not sufficient for staff to verify the intended function of the TRPS and ESFAS, and conformance with associated SHINE, TRPS, and ESFAS design criteria.

Therefore, update and clarify the following:

(a) How the TRPS and ESFAS specifically implement the generic HIPS platform;

(b) How ASAIs 2, 4, 5, 6, 7, 9, 10, 11, 12, 18, 21, 23, 24, 25, 26, 30, 32, 33, 34, 42, 43, 45, 46, 47, 49, 50, 51, 54, 57, 62, 63, 64 and 65 identified for specific implementation of the HIPS platform are dispositioned for the SHINE facility; and

(c) The differences between the representative system architecture described in the HIPS platform TR and the architecture proposed for the TRPS and ESFAS.

The SHINE FSAR should be revised, as necessary, to describe the implementation of HIPS platform; demonstrate how the ASAIs are being dispositioned by the design of the SHINE facility; and describe the TRPS and ESFAS architecture. This information is necessary for the NRC staff to verify the acceptability of the HIPS platform for use in the TRPS and EFSAS, and to make a reasonable assurance finding of adequate protection based on demonstration of the

TRPS and ESFAS compliance to the identified design criteria. (The NRC staff recognizes that this additional information may address the information needs identified in RAI 7-9.) Specifically, the information requested in parts (a) through (c) above is necessary to support the evaluation findings in Section 7.4 of NUREG-1537, Part 2, including that "[t]he 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."

As part of the response to this RAI, the SHINE FSAR should be updated to contain additional information on the types and configuration of modules, equipment configuration, equipment communication, configuration of maintenance and operational bypass, configuration of the HIPS capabilities for self-testing and diagnostics, design attributes implemented (e.g., redundancy, diversity, etc.), HIPS design process, and HIPS equipment qualification that demonstrate the equipment meets the SHINE environmental qualification requirements.

The following are examples of the types of information the NRC staff needs to evaluate how the TRPS and ESFAS are designed and implement the HIPS TR. SHINE should ensure that the responses to parts (a) through (c) of this RAI address these examples. However, the NRC staff notes that these are representative examples and not an exhaustive list of all information SHINE may determine to be appropriate to include in its RAI response and any FSAR updates:

- Number and types of FPGAs used in the HIPS architecture for TRPS and ESFAS that demonstrate built-in diversity. The SHINE FSAR (e.g., Section 7.4.2.1.4) states that the HIPS will use three types of FPGAs. However, the TR for the HIPS platform describes using two types of FPGAs in a 4-channel architecture to provide adequate built-in diversity

- Differences and similarities of modules approved in the HIPS TR and modules used in the HIPS for the TRPS and ESFAS. For example, (1) the HIPS TR does not include RISM or SBVM modules, but the TRPS does, and (2) the HIPS TR depicts instrument channels and actuation divisions in separate racks of equipment, while the TRPS and ESFAS are combined in the same equipment rack. Also, include a description of each module configuration for the TRPS and ESFAS

- Use of functional segregation in the HIPS based TRPS and ESFAS for achieving defense-in-depth

- Data validation, transmission, bypass, and voting for the SBVM installed in the HIPS for the TRPS and ESFAS

- Design and implementation of the built-in self-test functions (e.g., in the SFM). This information is particularly important for parts of the HIPS platform that rely solely on self-testing to ensure operability (e.g., there are no surveillance requirements to determine operability in the TSs)

- Design and development processes followed for the logic in the HIPS for the TRPS and ESFAS

- Verification and validation activities performed for the logic in the HIPS for the TRPS and ESFAS

- Configuration management established for the logic in the HIPS for the TRPS and ESFAS

- Aspects of the development environment addressed in the HIPS TR that are applicable to the SHINE application

SHINE Response

(a) The generic HIPS platform is described in Section 2.0 of Topical Report TR-1015-18653, "Design of the Highly Integrated Protection System Platform," (Reference 6). The specific SHINE implementation of the HIPS platform for the TRPS and ESFAS was compared against the generic HIPS platform described in Sections 2.1 through 2.6.3 of TR-1015-18653. Differences between the generic HIPS platform and the specific SHINE implementation for the TRPS and ESFAS are documented in Section 5 of TECRPT-2018-0028. These differences documented in Section 5 of TECRPT-2018-0028 include discussions of the remote input sub-modules (RISMs), scheduling bypass and voting modules (SBVMs), and self-test functions. Additional detail on self-test functions is provided in the SHINE Response to RAI 7-15 (Reference 3).

(b) A description of how ASAIs 2, 4, 5, 6, 7, 9, 10, 11, 12, 18, 21, 23, 24, 25, 26, 30, 32, 33, 34, 42, 43, 45, 46, 47, 49, 50, 51, 54, 57, 62, 63, 64 and 65 are dispositioned for the SHINE facility is provided in Section 3 of TECRPT-2018-0028.

(c) Section 3 of TR-1015-18653 describes the representative architecture provided for reference to help describe the attributes of the HIPS platform and how it could be used in an application. For the SHINE architecture, an overview of the SHINE instrumentation and control systems, which includes the TRPS and ESFAS, is provided in Section 7.1 of the FSAR. A description of the TRPS system architecture is provided in Subsection 7.4.1 of the FSAR. A description of the ESFAS system architecture is provided in Subsection 7.5.1 of the FSAR. Detailed documentation of TRPS and ESFAS architecture is contained in system design descriptions.

The representative architecture for the approved HIPS platform described in TR-1015-18653 uses two different FPGA technologies with a four-division configuration. The SHINE application of the HIPS platform for the TRPS and ESFAS uses three different FPGA technologies with a three-division configuration. The difference in the number of divisions is an application-specific architectural difference, not a platform-specific difference. Each division uses discrete components and FPGA technology consistent with TR-1015-18653. A description of how the division configuration satisfies ASAI 9 and ASAI 64 is provided in Section 3 of TECRPT-2018-0028.

The TRPS and ESFAS have redundant gateways that provide nonsafety-related communications from the TRPS and ESFAS to the process integrated control system (PICS). A description of the gateway architecture is provided in Section 3 of TECRPT-2018-0028 in the descriptions of how ASAI 26 and ASAI 28 are dispositioned. A description of the differences between how the communications gateway is constructed for the TRPS and ESFAS and how it was constructed for the generic HIPS platform is provided in Section 5.5.2 of TECRPT-2018-0028.

A description of design and development processes performed for logic activities, verification and validation activities performed for the logic, configuration management established for the logic, and aspects of the development environment are provided in Section 3 of TECRPT-2018-0028 in the description of how ASAI 58 is dispositioned.

A description of the use of functional segregation in the TRPS and ESFAS for achieving defense-in-depth is provided in Section 3 of TECRPT-2018-0028 in the description of how ASAI 9 is dispositioned.

The architecture of the SHINE application of the HIPS platform does not locate safety-related TRPS and safety-related ESFAS equipment in the same rack. The safety-related ESFAS equipment is located in separate cabinets from the safety-related TRPS equipment. The nonsafety-related communications gateway described above is located in the ESFAS Division C cabinet.

SHINE has revised Subsection 7.4.5.1 of the FSAR to enhance the description of the implementation of the HIPS platform and discuss disposition of the ASAIs. A markup of the FSAR incorporating these changes is provided as Attachment 1.

SHINE revised the FSAR to provide additional information on equipment communication via the SHINE Response to RAI 7-13 (Reference 3). SHINE revised the FSAR to provide additional information on the configuration of maintenance and operational bypass via the SHINE Response to RAI 7-14 (Reference 3). SHINE revised the FSAR to provide additional information on the configuration of the HIPS capabilities for self-testing and diagnostics via the SHINE Response to RAI 7-15 (Reference 3). SHINE revised the FSAR to provide additional information on design attributes implemented via the SHINE Response to RAI 7-11 and RAI 7-12 (Reference 3). SHINE has revised Subsection 7.4.5.4 of the FSAR as part of the SHINE Response to RAI 7-9 to provide additional information on the HIPS design process. SHINE revised the FSAR to provide additional information on HIPS equipment qualification via the SHINE Response to RAI 7-16 (Reference 3).

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 July 1, 2021 (ML21172A195)

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, “Application for an Operating License Response to Request for Additional Information,” dated August 27, 2021 (ML21239A049)

4. U.S. Nuclear Regulatory Commission, “Method for Performing Diversity and Defense-in-Depth Analyses of the Reactor Protection Systems,” NUREG/CR-6303, December 1994

5. U.S. Nuclear Regulatory Commission, “Standard Review Plan for Fuel Cycle Facilities License Applications,” NUREG-1520, Revision 2, June 2015

6. NuScale Power, LLC letter to NRC, “NuScale Power, LLC Submittal of the Approved Version of NuScale Topical Report TR-1015-18653, ‘Design of the Highly Integrated Protection System Platform,’ Revision 2 (CAC No. RQ6005),” NuScale Power, LLC, September 13, 2017 (ML17256A892)

ENCLOSURE 3
ATTACHMENT 1

SHINE MEDICAL TECHNOLOGIES, LLC

SHINE MEDICAL TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE SUPPLEMENT NO. 8 AND RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

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

57 pages follow

(low-high and high-high), which are provided to PICS via TRPS (Subsections 7.4.4.1.8 and 7.4.4.1.9).

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

Control Functions

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

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

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

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

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

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

Interlocks and Permissives

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

The PICS additionally provides permissives and interlocks to:

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

described in the technical specifications. Each SFM can be placed in maintenance bypass or in a trip state by use of the out-of-service (OOS) switch located on the front of the SFM and an associated trip/bypass switch located below the SFM, as described in Subsection 7.4.4.3. Placing an SFM in trip or bypass causes all channels associated with that SFM to be placed in trip or bypass, respectively.

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

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

7.4.2 DESIGN CRITERIA

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

7.4.2.1 SHINE Facility Design Criteria

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

7.4.2.1.1 Instrumentation and Controls

> 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 monitored variables for performance of design basis functions are presented in Table 7.4-1 and include the instrument range for covering normal and accident conditions, the accuracy for each variable, the response time, and the analytical limit. ~~Operation of the TRPS in response to the analyzed events is presented in~~ Subsection 7.4.4.1 provides a discussion of each of these variables, including details on how they are maintained within the prescribed operating range.

7.4.2.1.2 Protection System Functions

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

The safety functions of the TRPS credited to maintain the acceptable target solution design limits (Table 4a2.2-2) during anticipated transients are IU Cell Safety Actuation (Subsection 7.4.3.1.1), IU Cell Nitrogen Purge (Subsection 7.4.3.1.2), and Driver Dropout (Subsection 7.4.3.1.4). The primary variables that are monitored to prevent exceeding the target solution design limits during anticipated transients are the high time-averaged neutron flux (Subsection 7.4.4.1.3), high wide range neutron flux (Subsection 7.4.4.1.4), high and low primary closed loop cooling system (PCLS) temperature (Subsections 7.4.4.1.5 and 7.4.4.1.6), low PCLS flow (Subsection 7.4.4.1.7), low TSV off-gas system (TOGS) mainstream flow (Subsection 7.4.4.1.11), and high TOGS condenser demister outlet temperature (Subsection 7.4.4.1.13). There are no anticipated transients that would result in target solution design limits being exceeded.

Operation of the TRPS in response to the analyzed events is presented in Subsection 7.4.4.1. This section describes the parameters monitored to sense accident conditions and automatic system response to actuation setpoints in monitored variables. Subsection 7.4.3.1 contains a description of the TRPS safety functions relied upon for specific accident scenarios and demonstrates that the TRPS is able to sense accident conditions and initiate the operation of safety-related systems and components.

7.4.2.1.3 Protection System Reliability and Testability

SHINE Design Criterion 15 – The protection systems are designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection systems are sufficient to ensure that: (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection systems are designed to permit periodic testing, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

~~High functional reliability is addressed in SHINE Design Criterion 19. The HIPS design incorporates predictability and repeatability principles to ensure an extremely high probability of accomplishing safety functions (Subsection 7.4.5.2.3).~~The HIPS platform design for the TRPS supports high functional reliability, in part, by incorporating predictability and repeatability principles to ensure an extremely high probability of accomplishing safety functions, as described in Subsection 7.4.5.2.3. High functional reliability is further addressed in SHINE Design Criterion 19 (Subsection 7.4.2.1.7).

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

~~The TRPS design utilizes functional independence.~~ Structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident (Subsection 7.4.5.2.1).

Redundancy within t~~T~~he TRPS, as described in Subsection 7.4.5.2.2, consists of three divisions of input processing and trip determination and two divisions of actuation logic arranged such that no single failure can prevent a safety actuation when required, and no single failure in a single measurement channel can generate an unnecessary safety actuation (Subsection 7.4.3.4). This was validated by the performance of a~~A~~ single failure analysis of the TRPS, ~~was~~ performed in accordance with Institute of Electrical and Electronics Engineers (IEEE) Standard 379-2000 (IEEE, 2000), as described in Subsection 7.4.5.2.2.

A channel of TRPS can be taken out of service by placing the channel in trip or using the maintenance bypass function, as described in Subsection 7.4.4.3. A channel can be taken to trip without an adverse impact on redundancy, as described in Subsection 7.4.4.3.

The maintenance bypass function allows an individual safety function module to be removed from service ~~for required testing without loss of redundancy~~ for up to two hours in accordance with the technical specifications, for the purpose of performing required technical specification surveillance testing (Subsection 7.4.4.3). 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. By allowing a single SFM module to be placed in maintenance bypass in accordance with the technical specifications, technical specifications surveillances can be performed to verify the operability of TRPS components during system operation, which supports in-service testability.

Self-test features are provided for components that do not have setpoints or tunable parameters. The discrete logic of the actuation and priority logic (APL) of the EIM does not have self-test capability but is instead functionally tested (~~S~~Subsection 7.4.4.4). Calibration, testing, and diagnostics are addressed in Section 8.0 of Topical Report TR-1015-18653, “Design of the Highly Integrated Protection System Platform” (NuScale, 2017). Self-testing capabilities provide indication of component degradation and failure, which allows action to be taken to ensure that no single failure results in the loss of the protection function.

7.4.2.1.4 Protection System Independence

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

~~The TRPS is designed as Seismic Class 1 and is protected from the effects of earthquakes, tornadoes, and floods (Subsection 7.4.3.6).~~ The TRPS 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 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.

The inputs to the TRPS that have both safety-related protection functions and nonsafety-related control functions are TOGS oxygen concentration (Subsection 7.4.4.1.10) and TOGS mainstream flow (Subsection 7.4.4.1.11). For each of these inputs, the nonsafety-related control function is based upon the median value of the inputs to the TRPS (Subsection 7.3.1.1.2). Since the median value is selected, a failure of a single input will not impact the control function.

Nonsafety-related inputs to the TRPS from the PICS are limited to those for control, discrete mode output, and monitoring and indication only variables and are further described in Subsection 7.4.3.4. A failure of these nonsafety-related inputs will not impede the TRPS from performing its safety function because the safety function is prioritized over the nonsafety-related input as described in Subsection 7.4.3.12. This limitation of inputs, and the prioritization of the safety function, ensures that interconnection of the TRPS and PICS is limited to assure that safety is not significantly impaired.

7.4.2.1.7 Protection Against Anticipated Transients

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

~~The TRPS design utilizes functional independence; structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident (Subsection 7.4.5.2.1). The TRPS includes redundancy such that no single failure can prevent a safety actuation when required (Subsection 7.4.3.4). The architecture provides two diverse methods for an actuation of the safety functions at the division level, automatic (Subsections 7.4.3.1 and 7.4.4.1) and manual (Subsection 7.4.3.7), and FPGAs in each division are of a different physical architecture to prevent CCF (Subsection 7.4.5.2.4).~~The application of the HIPS platform to the TRPS ensures an extremely high probability of accomplishing the required safety functions by applying the attributes of independence, redundancy, and predictability and repeatability. Collectively, these attributes ensure the TRPS functions in a highly consistent manner with high reliability. Independence principles contribute to ensuring an extremely high probability of accomplishing safety functions by ensuring that structures, systems, and components that comprise a division are physically separated. Independence is further described in Subsection 7.4.5.2.1. Redundancy principles contribute to ensuring an extremely high probability of accomplishing safety functions by ensuring that no single failure can prevent a safety actuation, as described in Subsections 7.4.3.4 and 7.4.5.2.2. Predictability and repeatability principles contribute to ensuring an extremely high probability of accomplishing safety functions by ensuring the TRPS produces the same outputs for a given set of input signals within well-defined response time limits. Predictability and repeatability is further described in Subsection 7.4.5.2.3.

7.4.2.1.8 Monitoring Radioactivity Releases

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

The TRPS monitors for potential radioactivity releases from the primary confinement boundary by monitoring radiological ventilation zone 1 exhaust subsystem (RVZ1e) IU cell radiation, as described in Subsection 7.4.4.1.15. ~~Specific monitored variables are addressed in Subsection 7.4.4.1.~~ Additional radioactivity release monitoring is provided by the engineered safety features actuation system (ESFAS) (Section 7.5) and by nonsafety-related radiation monitoring systems (Section 7.7). The radiation release monitoring provided by the TRPS, ESFAS, and nonsafety-related radiation monitoring systems provides monitoring for potential

effluent discharge paths and plant environs that may be released from normal operations, including anticipated transients, and from postulated accidents.

7.4.2.1.9 Hydrogen Mitigation

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

The TRPS monitors variables and provides actuations to ~~prevent and mitigate~~protect against hydrogen deflagration in the primary system boundary or TSV dump tank ~~(Subsection 7.4.4.1)~~. The low TOGS oxygen concentration signal and low TOGS mainstream flow signal protect against a deflagration in the primary system boundary (Subsections 7.4.4.1.10 and 7.4.4.1.11). The low TOGS dump tank flow signal protects against a deflagration in the TSV dump tank (Subsection 7.4.4.1.12).

7.4.2.2 TRPS System Design Criteria

7.4.2.2.1 Access Control

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

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

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

The TRPS development design uses ~~a defensive system architecture described in Subsection 7.4.5.3.2 that~~the process described in Subsection 7.4.5.3.1 to prevent~~s~~ unauthorized physical and electronic access.

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

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

7.4.2.2.2 Software Requirements Development

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

The ~~system~~programmable logic design requirements are specified in the ~~system~~programmable logic requirements specifications (~~Sy~~PLRS), which ~~is~~are generated in accordance with the vendor ~~SyRS development procedure (Subsection 7.4.5.4.2.1)~~ programmable logic development lifecycle process (Subsection 7.4.5.4.2). A ~~system~~programmable logic design ~~description~~specification (PLDS) is generated to define the ~~system~~programmable logic design details. ~~Software requirements~~Programmable logic development is addressed in Subsection 7.4.5.4.

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

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

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

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

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

~~Design basis requirements are specified in the SyRS and system design description (Subsection 7.4.5.4.2.1).~~ The programmable logic lifecycle process for the TRPS includes development of a Programmable Logic Development Plan (PLDP), V&V Plan, and Configuration Management Plan to control programmable logic development and its associated safety analysis, V&V, and configuration management activities (Subsection 7.4.5.4.2.1).

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

SHINE has delegated V&V activities related to the safety-related control system development, including V&V documentation, to the vendor. The vendor Project V&V Plan for the system

development was tailored and adapted for FPGA technology from the guidance in IEEE Standard 1012-2004 (IEEE, 2004a). The V&V activities are performed using an internal V&V team from within the design organization (Subsection 7.4.5.4.5).

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

~~The programmable logic lifecycle process addresses design interfaces, which includes addressing any impacts on the safety system, control console, or display instruments during the lifecycle process, as stated in Subsection 7.4.5.4.2.~~The programmable logic lifecycle process includes development of a Configuration Management Plan (Subsection 7.4.5.4.6) to control tracing of programmable logic development from requirements specifications to implementation and address any impacts on TRPS programmable logic functions. The configuration control process as it relates to control consoles and display instruments, which are part of the nonsafety-related PICS, is described in Subsection 7.6.2.2.2. The SHINE configuration management program will ensure consistency among the design requirements between TRPS and PICS.

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

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

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

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

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

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

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 the facility control room, protected from radiological and environmental hazards during normal operation, maintenance, testing, and postulated accidents, and cables and sensors outside the facility control room are designed for their respective environments (Subsection 7.4.3.5). 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-related inputs into the TRPS are designed and controlled so they do not prevent the TRPS from performing its safety functions. Single failure is additionally addressed in Subsection 7.4.3.4.

The modes of single system component failures and satisfaction of the single failure criterion were evaluated for the TRPS using an FMEA and single failure analysis. The FMEA determined that there are no single failures or non-detectable failures that can prevent the TRPS from performing its required safety functions. The single failure analysis determined that for functions requiring either one-out-of-two voting or two-out-of-three voting, a single failure of a channel will

not prevent a protective action when required. Additional discussion of the FMEA and single failure analysis is provided in Subsection 7.4.5.2.2.

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

The TRPS is comprised of three divisions of signal condition and trip determination, and two divisions of voting and actuation. This configuration allows for the architecture to handle a single failure of a field input, signal conditioning circuit, or trip determination and still maintain the ability to provide needed number of valid inputs to the voting circuitry. A single failure of the voting logic or the actuation logic is also acceptable within the configuration as the redundant division of voting logic and actuation logic is capable of performing the safety function. Functional independence is addressed in Subsection 7.4.5.2.1 and redundancy is addressed in Subsection 7.4.5.2.2. Single failure is additionally addressed in Subsection 7.4.3.4.

The modes of single system component failures and satisfaction of the single failure criterion were evaluated for the TRPS using an FMEA and single failure analysis. The FMEA determined that there are no single failures or non-detectable failures that can prevent the TRPS from performing its required safety functions. The single failure analysis determined that for functions requiring either one-out-of-two voting or two-out-of-three voting, a single failure of a channel will not prevent a protective action when required. Additional discussion of the FMEA and single failure analysis is provided in Subsection 7.4.5.2.2.

7.4.2.2.5 Independence

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

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

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

The APL (which is constructed of discrete components and part of the EIM) is designed to provide priority to safety-related signals over nonsafety-related signals. Division A and Division B priority logic of the TRPS prioritizes the following TRPS inputs, with the first input listed having the highest priority and each successive input in the list having a lower priority than the previous: (1) Automatic Safety Actuation, Manual Safety Actuation, and 2) PICS nonsafety control signals (Subsection 7.4.3.12). When the enable nonsafety control is not active, the nonsafety-related control signals are ignored. If the enable nonsafety control is active, and no automatic safety actuation or manual safety actuation command is present, the nonsafety control signal can control the component (Subsection 7.4.3.3).

The mode transition request input, which is a nonsafety-related input from the PICS, will not adversely affect the function of the TRPS. The mode transition request is described in Subsection 7.4.4.2.

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

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

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

The TRPS structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident (Subsection 7.4.5.2.1) and nonsafety-related TRPS inputs and outputs are routed in non-divisional cable raceways and are segregated from safety-related inputs and outputs (Subsection 7.4.3.9). Wiring for redundant divisions uses physical separation and isolation to provide independence for circuits (Subsection 7.4.5.2.1) in accordance with IEEE Standard 384-2008 (IEEE, 2008).

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

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

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

~~TRPS data communications protocol is detailed in Section 7.5.1 of Topical Report TR-1015-18653 (NuScale, 2017). The protocol is used on the safety buses as a simple master-slave communication protocol and employs a cyclic redundancy checksum feature to ensure the integrity of the communicated information between modules.~~There are no data communications as safety inputs to the TRPS. Safety-related data communications are internal to the system only. The data communications to nonsafety-systems are unidirectional. Data communications ~~is~~are discussed in Subsection 7.4.5.2.5.

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

~~The maximum response time of the TRPS components from when an input signal exceeds a predetermined setpoint to the time that the TRPS deenergizes the EIM output switching for actuated components is conservatively set to a maximum of 500 milliseconds (Subsection 7.4.5.2.3).~~ The TRPS implements deterministic data communications, as described in Subsection 7.4.5.2.5.

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

TRPS communication protocols are verified as conforming to the validated protocol specifications by the Project V&V Plan (Subsection 7.4.5.4.5).

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

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

The TRPS platform operates in a fully deterministic manner, as described in Subsection 7.4.5.2.5, which allows implementation of a simple communication protocol using a predefined message structure at fixed time intervals. This ensures that a consistency of performance will exist that prevents performance deficits from adversely affecting the TRPS architecture.

7.4.2.2.6 Prioritization of Functions

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

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

7.4.2.2.7 Fail Safe

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

Controlled components associated with safety actuations are designed to go to their safe state when deenergized (Subsection 7.4.3.8). TRPS outputs become deenergized on a loss of electrical power to the TRPS.

7.4.2.2.8 Setpoints

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

Setpoints in the TRPS are based on a documented methodology that identifies each of the assumptions and accounts for the uncertainties in each instrument channel. The setpoint methodology is further described in Subsections 7.2.1 and 7.4.3.11. Environmental allowances and measurement computational errors are accounted for in the uncertainty analysis used to establish the setpoints. The setpoint analysis parameters in the documented analyses are consistent with the safety analysis, system design basis, technical specifications, facility design, and expected maintenance practices.

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

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

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

Multiple setpoints are used for the IU ~~s~~Safety ~~a~~Actuation~~s~~ based on neutron flux, dependent on the IU operating conditions (Subsections 7.4.4.1.1, 7.4.4.1.3, and 7.4.4.1.4). Each setpoint is processed independently in the partial trip determination portions of the TRPS. Operational bypasses are applied based upon IU operating conditions in the final trip determination portion of the TRPS, ~~used~~ as described in Subsection 7.4.4.2, to ensure the more restrictive setpoint is used when required.

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

Setpoints in the TRPS are based on a documented methodology that identifies each of the assumptions and accounts for the uncertainties in each instrument channel. The setpoint methodology is further described in Subsections 7.2.1 and 7.4.3.11. Setpoint analysis parameters typically consider instrument precision, sensitivity, accuracy, loop uncertainties, and computational errors. The established setpoints and associated uncertainties ensure adequate margin to analytical limits or safety limits described in the technical specifications, which ensures that the sensitivity of each sensor channel is commensurate with the knowledge of the variable.

7.4.2.2.9 Operational Bypass, Permissives, and Interlocks

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

TRPS operating permissives are used to control the modes of operation of the IU cells. The mode transition functions are described in Subsection 7.4.3.2. Operational use of the permissives and conditions to be satisfied and operational bypasses is addressed in Subsection 7.4.4.2. The TRPS receives input for the facility master operating permissive from the ESFAS. The TRPS functions associated with the facility master operating permissive are described in Subsection 7.4.3.2. A maintenance bypass function is available and is described in Subsection 7.4.4.3. There are no permissive conditions associated with the maintenance bypass capability.

TRPS Criterion 34 – TRPS interlocks shall ensure that operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required, with the exception of the use of the maintenance bypass capability.

Operator action is required to transition the TRPS between normal operating modes as described in Subsection 7.4.3.2. Operational bypasses are initiated or removed dependent on the TRPS mode of operation as described in Subsection 7.4.4.2. Interlocks are provided by TRPS to prevent the operator from transitioning to the next operating mode unless certain conditions are met, as described in Subsection 7.4.3.2, to ensure that operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required. There are not automatic interlocks to prevent an operator from putting all instrument channels in maintenance bypass (Subsection 7.4.4.3). Administrative controls are provided by the technical specifications to prevent placing the same SFM across more than one channel in maintenance bypass.

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

TRPS implements logic associated with each mode of operation to prevent an operator from activating a bypass through changing the IU cell mode out of sequential order. Each mode of operation is achieved through manual input from the operator when permissive conditions for the next mode in the sequence have been met (Subsection 7.4.4.2).

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

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

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

By design, certain variables as input to the safety actuations are bypassed in each operating mode, as described in Subsection 7.4.4.2. The TRPS logic associated with each mode of operation prevents an operator from activating a bypass through changing the IU cell mode out

of sequential order (Subsection 7.4.4.2), which allows the TRPS to retain the capability to accomplish its required safety functions for the mode of operation. Use of the maintenance bypass ~~either preserves the single failure criterion where three channels are provided or~~ is performed in accordance with technical specification requirements (Subsection 7.4.4.3).

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

Operator action is required to transition the TRPS between normal operating modes as described in Subsection 7.4.3.2. Operational bypasses are initiated or removed dependent on the TRPS mode of operation as described in Subsection 7.4.4.2. Interlocks are provided by TRPS to prevent the operator from transitioning to the next operating mode unless certain conditions are met, as described in Subsection 7.4.3.2. A maintenance bypass function is available, as described in Subsection 7.4.4.3. There are no permissive conditions associated with the maintenance bypass capability.

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

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

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

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

Operator action is required to transition the TRPS between normal operating modes as described in Subsection 7.4.3.2. Operational bypasses are initiated or removed dependent on the TRPS mode of operation as described in Subsection 7.4.4.2. Interlocks are provided by the TRPS to prevent the operator from transitioning to the next operating mode unless certain conditions are met, as described in Subsection 7.4.3.2. If operating conditions change so that an active operating bypass is no longer permissible to use, the TRPS removes the appropriate operating bypasses or initiates the appropriate safety function(s).

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

~~Where three channels are provided, taking an SFM out of service preserves the single failure criterion for variables associated with that SFM. In cases where only two channels are provided, taking a channel out of service will actuate the associated safety function. For testing purposes, placing a channel in maintenance bypass will be allowed by technical specifications for up to two hours to perform required testing. Two hours is considered acceptable due to the continued~~

~~operability of the redundant channel(s) and the low likelihood that an accident would occur in those two hours (~~There are no maintenance bypass capabilities associated with execute features for the TRPS. The maintenance bypass capabilities are associated with the sense and command features only. Maintenance bypass capabilities and their acceptability for use are further discussed in ~~Subsection 7.4.4.3)~~.

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

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

7.4.2.2.10 Completion of Protective Actions

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

Figure 7.4-1 shows how the TRPS latches in a protective action and maintains the state of a protective action until operator input is initiated to reset the output of the TRPS. Completion of protective actions is described in Subsection 7.4.3.3.

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

Only deliberate operator action can be taken to reset the TRPS following a protective action. Figure 7.4-1 shows how the TRPS latches in a protective action and maintains the state of a protective action until operator input is initiated to reset the output of the TRPS. Completion of protective actions is described in Subsection 7.4.3.3.

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

A ~~safety-related~~n enable nonsafety switch (when enabled) allows a facility operator to control the output state of the TRPS with a hardwired binary control signal from the nonsafety-related controls. If the enable nonsafety switch is active, and no automatic safety actuation or manual safety actuation signals are present, the operator is capable of energizing or deenergizing any EIM outputs using the nonsafety-related hardwired control signals (Subsection 7.4.3.3). Additionally, safety-related signals are prioritized over nonsafety-related signals (Subsection 7.4.3.12).

7.4.2.2.11 Equipment Qualification

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

TRPS rack mounted equipment is installed in a mild operating environment and is designed to meet the environmental conditions described in Subsection 7.4.3.5. Rack mounted TRPS equipment is tested to appropriate standards to show that the effects of EMI/RFI and power surges are adequately addressed. This testing includes emissions testing, susceptibility testing, and surge withstand testing. Appropriate grounding of the TRPS is performed in accordance with Section 5.2.1 of IEEE Standard 1050-2004 (IEEE, 2004b).

7.4.2.2.12 Surveillance

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

The TRPS design supports testing, maintenance, and calibration, as described in Subsections 7.4.4.3 and 7.4.4.4. Surveillance t~~T~~esting performed using the maintenance bypass capability during operation is controlled in accordance with the technical specifications to ensure that ~~at least one division of~~ the TRPS is capable of performing its safety functions when required (Subsection 7.4.4.3). Self-testing features provide for monitoring as described in Subsection 7.4.4.4 to provide indication to the operator if conditions exist that could challenge operability of the equipment.

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

The TRPS design supports testing, maintenance, and calibration, as described in Subsections 7.4.4.3 and 7.4.4.4. End-to-end testing of the entire TRPS platform can be performed through overlap testing. All TRPS components have self-testing capabilities, except the discrete APL of EIM which is functionally tested. The TRPS continuously provides redundant indication of self-testing results to the PICS to indicate to operators that the TRPS is operating correctly following testing, calibration, or inspections.

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

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

7.4.2.2.13 Classification and Identification

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

Each TRPS cable and component is uniquely identified in accordance with the SHINE component numbering guidelines. By identifying the specific component associated with the

TRPS, the safety classification can be determined. The unique identification number indicates the applicable system and division (Subsection 7.4.3.10).

7.4.2.2.14 Human Factors

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

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

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

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

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

~~To support the use of manual safety actuations, t~~The TRPS associated with each IU includes redundantly isolated outputs for each safety-related instrument channel to provide monitoring and indication information to the PICS (Subsection 7.4.3.7), which includes indication of TRPS actuation device status. This supports annunciation of the channel initiating a protective action. The TRPS requires manual operator reset when conditions to resume operation are met and satisfied as described in ~~See also~~ TRPS Criterion 44 (~~regarding manual operator reset in Subsection 7.4.2.2.10~~).

7.4.2.2.15 Quality

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

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

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

The TRPS design, 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 7.4.3.13).

7.4.3 DESIGN BASIS

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

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

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

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

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

7.4.3.1 Safety Functions

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

7.4.3.1.1 IU Cell Safety Actuation

An IU Cell Safety Actuation is initiated in response to process variables indicating abnormal conditions. An IU Cell Safety Actuation shuts down the irradiation process and isolates the primary system boundary and primary confinement boundary.

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

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

- 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.

Mode 3 to Mode 4 Transition Criteria

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

Mode 3 to Secure State Transition Criteria

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

Mode 4 to Mode 0 Transition Criteria

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

Mode 4 to Mode 3 Transition Criteria

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

Secure State to Mode 3 Transition Criteria

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

7.4.3.3 Completion of Protective Actions

The TRPS is designed so that once initiated, protective actions will continue to completion. Only deliberate operator action can be taken to reset the TRPS following a protective action.

Figure 7.4-1 shows how the TRPS latches in a protective action and maintains the state of a protective action until operator input is initiated to reset the output of the TRPS to normal operating conditions.

The output of the TRPS is designed so that actuation through automatic or manual means of a safety function can only deenergize the output. If there is no signal present from the automatic safety actuation or manual safety actuation, then the output of the EIM remains in its current state. A ~~safety-related~~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 exist in the design where TRPS only actuates a Division A component and there is no corresponding Division B component, or, there is a passive check valve credited as a redundant component. These situations are considered acceptable since the safety function includes a separate, redundant, and passive component (i.e., check valve) which does not need to be monitored or manipulated by the TRPS.

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

- RVZ1r RPCS return isolation valve – Closed
- TPS target chamber supply isolation valves – Closed
- TPS deuterium supply isolation valves – Closed
- TPS target chamber exhaust isolation valves – Closed
- TPS neutron driver evacuation isolation valves – Closed
- TOGS RPCS supply isolation valves – Closed
- TOGS RPCS return isolation valve – Closed
- NDAS target/ion source cooling supply isolation valve – Closed
- NDAS target/ion source cooling return isolation valve – Closed
- NDAS vacuum pump cooling supply isolation valve – Closed
- NDAS vacuum pump cooling return isolation valve – Closed

Nitrogen Purge Components

- ~~N2PS inerting gas~~SCAS nitrogen purge isolation valves – Open
- TOGS nitrogen vent isolation valves – Open

7.4.3.9 Fire Protection

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

Physical separation is used to achieve separation of redundant sensors. Wiring for redundant divisions uses physical separation and isolation to provide independence for circuits. Separation of wiring is achieved using separate wireways and cable trays for each of Division A, Division B, and Division C. Division A and C cables are routed along the south side of the RPF to go to the facility control room and Division B cables are routed on the north side of the RPF. Where possible, conduit is routed subgrade to provide additional separation. Instrument transmitters are located in separate areas: A and C instrumentation is located primarily on the east side of the main production facility G-line wall, while Division B is along the west side of the wall.

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

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

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

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

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

7.4.4.5 Technical Specifications and Surveillance

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

7.4.5 HIGHLY INTEGRATED PROTECTION SYSTEM DESIGN

7.4.5.1 HIPS Design Summary

A HIPS platform is used to achieve the desired architecture for system control. The HIPS platform is a generic digital safety-related instrumentation and control platform devoted to the implementation of safety-related applications in nuclear facilities. The platform is a logic-based platform that does not utilize software or microprocessors for operation. It is composed of logic that is implemented using discrete components and FPGA technology. The 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.

necessary. Other information at the operator workstations or the main control board is aggregated from instruments throughout the facility and displayed to the operator. Section 7.6 provides further detail on the SHINE display systems.

7.4.5.2.5 Simplicity

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

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

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

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

Use of fundamentally different FPGA architectures provides a simple and verifiable approach to equipment and design diversity. In the D3 assessment (Subsection 7.4.5.2.5), 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.

7.4.5.4.1 Key Responsibilities

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

The vendor is responsible for developing and delivering the safety-related control systems in accordance with the processes identified in this section.

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

7.4.5.4.2 Programmable Logic Lifecycle Process

The programmable logic lifecycle process is shown in Figure 7.4-3 and provides an overview of the programmable logic development process from planning through installation. The programmable logic lifecycle process is implemented through the vendor system design control procedure. The procedure defines the minimum system design control tasks from the planning phase through the shipment phase.

Design interfaces are established during the design development process, and during the design review and approval process. Design interfaces are controlled in accordance with the Project Management Plan. The design interfaces include addressing any impacts on the safety system, control console, or display instruments during the lifecycle process.

7.4.5.4.2.1 Planning Phase

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

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

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

- Project PLDP
- Project Configuration Management Plan
- Project V&V Plan
- Project Equipment Qualification Plan
- Project Test Plan
- Project Security Plan
- Project Integration Plan

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

7.4.5.4.2.2 Requirements Phase

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

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

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

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

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

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

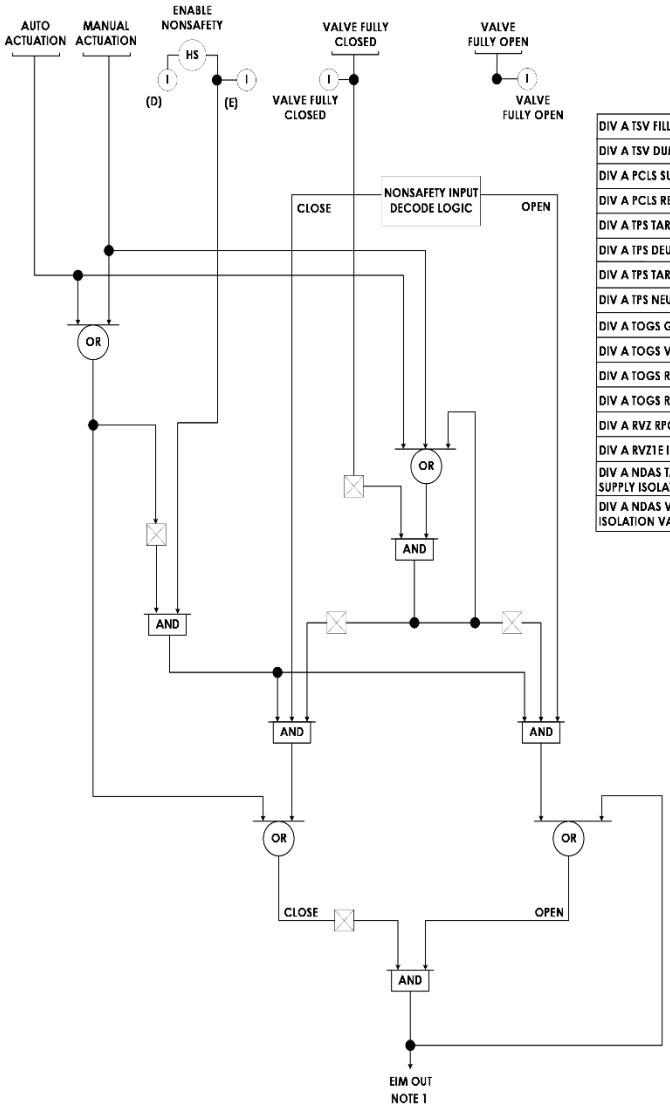
- Model elements that represent programmable logic requirements including derived requirements, or
- Model elements that do not represent programmable logic requirements.

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

7.4.5.4.2.3 Design Phase

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

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

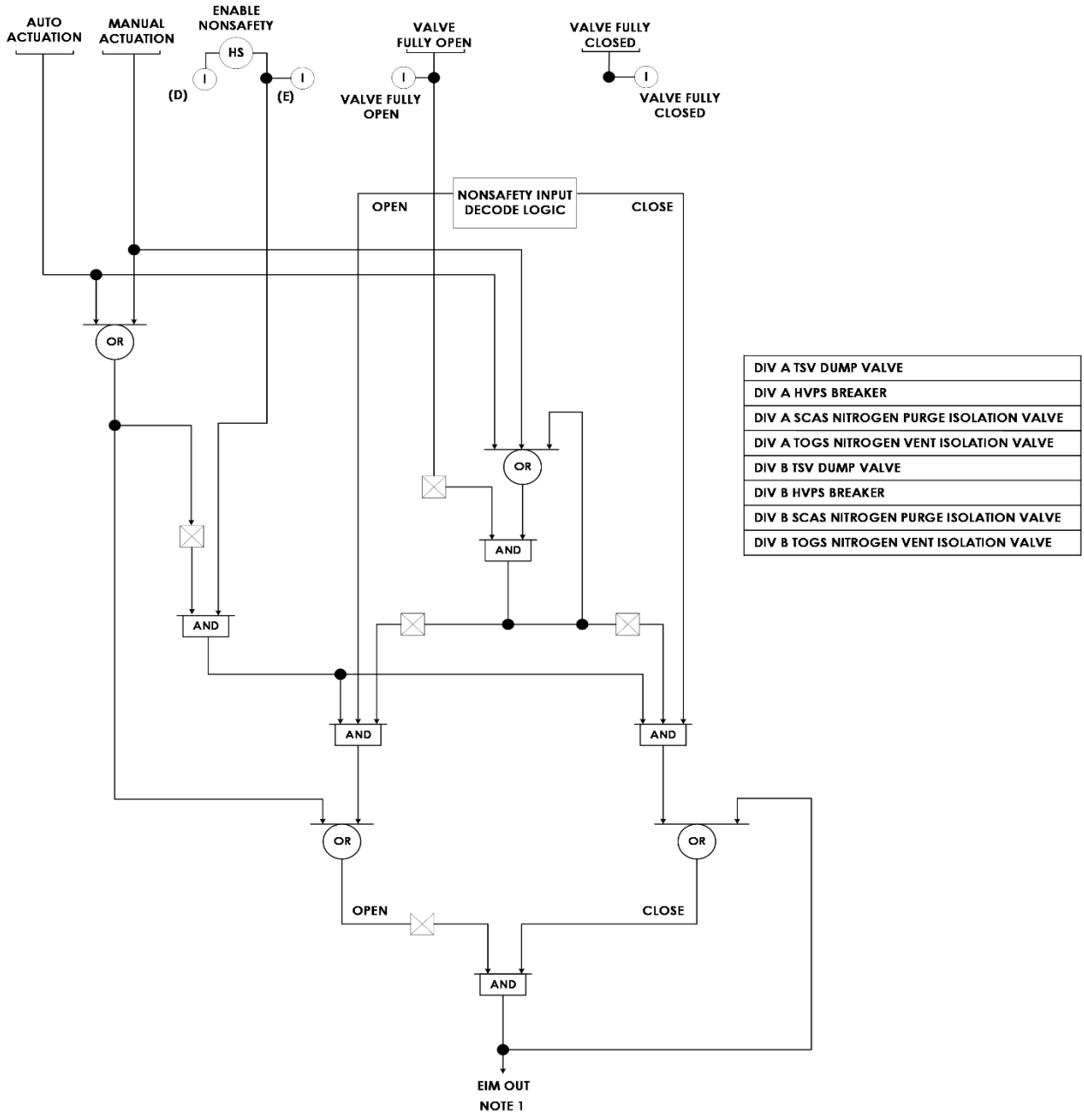


DIV A TSV FILL ISOLATION VALVE	DIV B TSV FILL ISOLATION VALVE
DIV A TSV DUMP TANK DRAIN ISOLATION VALVE	DIV B PCLS RETURN ISOLATION VALVE
DIV A PCLS SUPPLY ISOLATION VALVE	DIV B TPS TARGET CHAMBER SUPPLY ISOLATION VALVE
DIV A PCLS RETURN ISOLATION VALVE	DIV B TPS DEUTERIUM SUPPLY ISOLATION VALVE
DIV A TPS TARGET CHAMBER SUPPLY ISOLATION VALVE	DIV B TPS TARGET CHAMBER EXHAUST ISOLATION VALVE
DIV A TPS DEUTERIUM SUPPLY ISOLATION VALVE	DIV B TPS NEUTRON DRIVER EVACUATION ISOLATION VALVE
DIV A TPS TARGET CHAMBER EXHAUST ISOLATION VALVE	DIV B TOGS GAS SUPPLY LINE ISOLATION VALVE
DIV A TPS NEUTRON DRIVER EVACUATION ISOLATION VALVE	DIV B TOGS VACUUM TANK ISOLATION VALVE
DIV A TOGS GAS SUPPLY LINE ISOLATION VALVE	DIV B TOGS RPCS SUPPLY ISOLATION VALVE
DIV A TOGS VACUUM TANK ISOLATION VALVE	DIV B RVZ RPCS RETURN ISOLATION VALVE
DIV A TOGS RPCS SUPPLY ISOLATION VALVE	DIV B RVZ1E IU CELL ISOLATION VALVE
DIV A TOGS RPCS RETURN ISOLATION VALVE	DIV B VTS LOWER LIFT TANK TARGET SOLUTION VALVE (1)
DIV A RVZ RPCS SUPPLY ISOLATION VALVE	DIV B VTS LOWER LIFT TANK TARGET SOLUTION VALVE (2)
DIV A RVZ1E IU CELL ISOLATION VALVE	DIV B NDAS TARGET/ION SOURCE COOLING RETURN ISOLATION VALVE
DIV A NDAS TARGET/ION SOURCE COOLING SUPPLY ISOLATION VALVE	DIV B NDAS VACUUM PUMP COOLING RETURN ISOLATION VALVE
DIV A NDAS VACUUM PUMP COOLING SUPPLY ISOLATION VALVE	

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

Priority Logic

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

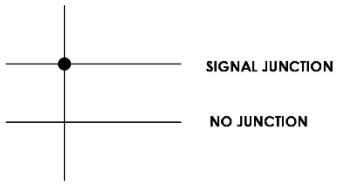


NOTE 1: OUTPUT OF EIM IS DEENERGIZE TO ACTUATE TO POSITION DEFINED FOR LOSS OF POWER

Priority Logic

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

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



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

Legend

trip or bypass causes all channels associated with that SFM to be placed in trip or bypass, respectively.

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

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

7.5.2 DESIGN CRITERIA

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

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

7.5.2.1 SHINE Facility Design Criteria

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

7.5.2.1.1 Instrumentation and Controls

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

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

each of these variables, including details on how they are maintained within the prescribed operating range.

7.5.2.1.2 Protection System Functions

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

There are no anticipated transients that require the initiation of the ESFAS to ensure specified acceptable target solution design limits (Table 4a2.2-2) are not exceeded.

Operation of the ESFAS in response to the analyzed events is presented in Subsection 7.5.4.1. This section describes the parameters monitored to sense accident conditions and automatic system response to actuation setpoints in monitored variables. Subsection 7.5.3.1 contains a description of the ESFAS safety functions relied upon for specific accident scenarios and demonstrates that the ESFAS is able to sense accident conditions and initiate the operation of safety-related systems and components.

7.5.2.1.3 Protection System Reliability and Testability

SHINE Design Criterion 15 – The protection systems are designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection systems are sufficient to ensure that: (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection systems are designed to permit periodic testing, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

~~High functional reliability is addressed in SHINE Design Criterion 19 (Subsection 7.5.2.1.7). The HIPS design incorporates predictability and repeatability principles to ensure an extremely high probability of accomplishing safety functions (Subsection 7.4.5.2.3).~~The HIPS platform design for the ESFAS supports high functional reliability, in part, by incorporating predictability and repeatability principles to ensure an extremely high probability of accomplishing safety functions, as described in Subsection 7.4.5.2.3. High functional reliability is further addressed in SHINE Design Criterion 19 (Subsection 7.5.2.1.7).~~-~~

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

~~The ESFAS design utilizes functional independence; s~~Structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident (Subsection 7.4.5.2.1).

Redundancy within t~~T~~he ESFAS, as described in Subsection 7.4.5.2.2, consists of two or three divisions of input processing and trip determination (dependent on the monitored variable) and two divisions of actuation logic arranged such that no single failure can prevent a safety actuation

when required (Subsection 7.5.3.3). This was validated by the performance of a~~A~~ single failure analysis of the ESFAS, ~~was~~ performed in accordance with IEEE Standard 379-2000 (IEEE, ~~-~~ 2000), as described in Subsection 7.4.5.2.2.

A channel of ESFAS can be taken out of service by placing the channel in trip or using the maintenance bypass function, as described in Subsection 7.5.4.4. A channel can be taken to trip without an adverse impact on redundancy, as described in Subsection 7.5.4.4.

The maintenance bypass function allows an individual safety function module to be removed from service ~~for required testing~~ in accordance with the technical specifications, for the purpose of performing required technical specification surveillance testing (Subsection 7.5.4.4). 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. By allowing a single SFM module to be placed in maintenance bypass in accordance with the technical specifications, technical specifications surveillances can be performed to verify the operability of ESFAS components during system operation, which supports in-service testability.

Self-test features are provided for components that do not have setpoints or tunable parameters. The discrete logic of the actuation and priority logic (APL) of the EIM does not have self-test capability but is instead functionally tested (Subsection 7.5.4.5). Calibration, testing, and diagnostics ~~is~~are addressed in Section 8.0 of Topical Report TR-1015-18653 (NuScale, 2017). Self-testing capabilities provide indication of component degradation and failure, which allows action to be taken to ensure that no single failure results in the loss of the protection function.

7.5.2.1.4 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 ESFAS control and logic functions operate inside of the facility control room where the environment is mild, not exposed to the irradiation process, and is protected from earthquakes, tornadoes, and floods (Subsections 7.5.3.4 and 7.5.3.5). The ESFAS structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident. Division independence is maintained throughout, extending from the sensor to the devices actuating the protective function (Subsection 7.4.5.2.1).

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 7.5.3.1 and 7.5.4.1) and manual (Subsection 7.5.3.6), and field programmable gate arrays (FPGAs) in each division are of a different physical architecture to prevent common cause failure (~~Subsections 7.4.5.2.4~~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.

7.5.2.1.7 Protection Against Anticipated Transients

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

~~The ESFAS design utilizes functional independence; structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident (Subsection 7.4.5.2.1). The ESFAS includes redundancy such that no single failure can prevent a safety actuation when required (Subsection 7.5.3.3). The architecture provides two diverse methods for an actuation of the~~

~~safety functions at the division level, automatic and manual, and FPGAs in each division are of a different physical architecture to prevent common cause failure (Subsections 7.4.5.2.4 and 7.5.3.6).~~The application of the HIPS platform to the ESFAS ensures an extremely high probability of accomplishing the required safety functions by applying the attributes of independence, redundancy, and predictability and repeatability. Collectively, these attributes ensure the ESFAS functions in a highly consistent manner with high reliability. Independence principles contribute to ensuring an extremely high probability of accomplishing safety functions by ensuring that structures, systems, and components that comprise a division are physically separated. Independence is further described in Subsection 7.4.5.2.1. Redundancy principles contribute to ensuring an extremely high probability of accomplishing safety functions by ensuring that no single failure can prevent a safety actuation, as described in Subsections 7.4.5.2.2 and 7.5.3.3. Predictability and repeatability principles contribute to ensuring an extremely high probability of accomplishing safety functions by ensuring the ESFAS produces the same outputs for a given set of input signals within well-defined response time limits. Predictability and repeatability is further described in Subsection 7.4.5.2.3.

7.5.2.1.8 Criticality Control in the Radioisotope Production Facility

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

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

7.5.2.1.9 Monitoring Radioactivity Releases

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

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

monitoring for potential effluent discharge paths and plant environs that may be released from normal operations, including anticipated transients, and from postulated accidents.

7.5.2.1.10 Hydrogen Mitigation

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

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

7.5.2.2 ESFAS System Design Criteria

7.5.2.2.1 Access Control

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

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

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

The ESFAS development design uses ~~a defensive system architecture described in Subsection 7.4.5.3.2 that~~the process described in Subsection 7.4.5.3.1 to prevent~~s~~ unauthorized physical and electronic access during the development phases.

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

Access control features prevent unauthorized physical and electronic access to CDAs during the operational phase and during transition from development to operations. Access control, cyber security, and the secure development operating environment are described in Subsection 7.4.5.3 ~~Subsection 7.4.4.1.3~~. ~~Subsection 7.4.4.1.3~~Subsection 7.4.5.3 ~~also~~ describes prevention of unauthorized access during the development and operational phases. Post-development installation and testing is performed and controlled by the safety-related control system vendor as described in Subsection 7.4.5.4.2.6 ~~Subsections 7.4.4.1.4 and 7.4.5.4.2.6~~.

7.5.2.2.2 Software Requirements Development

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

The ~~system~~programmable logic design requirements are specified in the ~~system~~programmable logic requirements specifications (PLRS), which ~~is~~are generated in accordance with the vendor ~~system requirements specification development procedure (Subsection 7.4.5.4.2.1)~~programmable logic development lifecycle (Subsection 7.4.5.4.2). A ~~system~~programmable logic design ~~description~~specification (PLDS) is generated to define the ~~system~~programmable logic design details. ~~Software requirements~~Programmable logic development is addressed in Subsection 7.4.5.4 ~~Subsection 7.4.4.1.4~~.

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

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

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

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

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

~~Design basis requirements are specified in the system requirements specification and system design description (Subsection 7.4.5.4.2.1).~~ The programmable logic lifecycle process for the ESFAS includes development of a Programmable Logic Development Plan (PLDP), V&V Plan, and Configuration Management Plan to control programmable logic development and its associated safety analysis, V&V, and configuration management activities (Subsection 7.4.5.4.2.1).

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

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

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

~~The programmable logic lifecycle process addresses design interfaces, which includes addressing any impacts on the safety system, control console, or display instruments during the lifecycle process, as stated in Subsection 7.4.5.4.2.~~The programmable logic lifecycle process includes development of a Configuration Management Plan (Subsection 7.4.5.4.6) to control tracing of programmable logic development from requirements specifications to implementation and address any impacts on ESFAS programmable logic functions. The configuration control process as it relates to control consoles and display instruments, which are part of the nonsafety-related PICS, is described in Subsection 7.6.2.2.2. The SHINE configuration management program will ensure consistency among the design requirements between ESFAS and PICS.

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

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

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

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

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

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

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

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

7.5.2.2.3 General Instrumentation and Control Requirements

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

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

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

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

7.5.2.2.4 Single Failure

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

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

The modes of single system component failures and satisfaction of the single failure criterion were evaluated for the ESFAS using an FMEA and single failure analysis. The FMEA determined that there are no single failures or non-detectable failures that can prevent the ESFAS from performing its required safety functions. The single failure analysis determined that for functions requiring either one-out-of-two voting or two-out-of-three voting, a single failure of a channel will not prevent a protective action when required. Additional discussion of the FMEA and single failure analysis is provided in Subsection 7.4.5.2.2.

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

The ESFAS is comprised of three divisions of signal conditioning and trip determination, and two divisions of voting and actuation. This configuration allows for the architecture to handle a single failure of a field input, signal conditioning circuit, or trip determination and still maintain the ability to provide the needed number of valid inputs to the voting circuitry. A single failure of the voting logic or the actuation logic is also acceptable within the configuration as the redundant division of voting logic and actuation logic is capable of performing the safety function. Functional independence is addressed in Subsection 7.4.5.2.1 and redundancy is addressed in Subsection 7.4.5.2.2. Single failure is additionally addressed in Subsection 7.5.3.3.

The modes of single system component failures and satisfaction of the single failure criterion were evaluated for the ESFAS using an FMEA and single failure analysis. The FMEA determined that there are no single failures or non-detectable failures that can prevent the ESFAS from performing its required safety functions. The single failure analysis determined that for functions requiring either one-out-of-two voting or two-out-of-three voting, a single failure of a channel will not prevent a protective action when required. Additional discussion of the FMEA and single failure analysis is provided in Subsection 7.4.5.2.2.

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

The ESFAS provides ~~separate~~independent, redundant communication paths to the PICS display systems from each of the three ESFAS divisions. ESFAS divisions A and B are powered from a separate division of the UPSS; ESFAS division C receives auctioneered power from both UPSS divisions A and B. This redundancy in communication paths and power sources ensures no single failure concurrent with a design basis event prevents operators from being presented necessary information (Subsection 7.5.3.3). Display of monitoring and indication information in the facility control room is described in Subsection 7.4.5.2.4. Loss of external power to the PICS is described in Subsection 7.3.3.6. An FMEA and single failure analysis, as described in Subsection 7.4.5.2.2, determined no single failure would impact the ability of the ESFAS to provide information to the PICS.

7.5.2.2.5 Independence

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

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

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

The APL, which is constructed of discrete components and part of the equipment interface module, is designed to provide priority to safety-related signals over nonsafety-related signals. Division A and division B priority logic of the ESFAS prioritizes the following ESFAS inputs, with the first input listed having the highest priority and each successive input in the list having a lower priority than the previous: (1) Automatic Safety Actuation, Manual Safety Actuation, and (2) PICS nonsafety control signals (Subsection 7.5.3.11). When the enable nonsafety control is not active, the nonsafety-related control signals are ignored. If the enable nonsafety control is active, and no automatic safety actuation or manual safety actuation command is present, the nonsafety control signal can control the component (Subsection 7.5.3.2).

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

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

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

The ESFAS structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident (Subsection 7.4.5.2.1) and nonsafety-related ESFAS inputs and outputs are routed in non-divisional cable raceways and are segregated from safety-related inputs and outputs (Subsection 7.5.3.8). Wiring for redundant divisions uses physical separation and isolation to provide independence for circuits (Subsection 7.4.5.2.1) in accordance with IEEE Standard 384-2008 (IEEE, 2008).

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

HIPS communication paths are designed with simplicity such that a single failure does not cause all safety functions of a division to be inoperable. The design uses triple redundant

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

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

~~ESFAS data communications protocol is detailed in Section 7.5.1 of Topical Report TR-1015-18653 (NuScale, 2017). The protocol is used on the safety buses as a simple master-slave communication protocol and employs a cyclic redundancy checksum feature to ensure the integrity of the communicated information between modules.~~There are no data communications as safety inputs to the ESFAS. Safety-related data communications are internal to the system only. The data communications to nonsafety-systems are unidirectional. Data communications ~~is~~are discussed in Subsection 7.4.5.2.5.

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

~~The maximum response time of the ESFAS components from when an input signal exceeds a predetermined setpoint to the time that the ESFAS deenergizes the equipment interface module output switching for actuated components is conservatively set to a maximum of 500 milliseconds (Subsection 7.4.5.2.3).~~ The ESFAS implements deterministic data communications, as described in Subsection 7.4.5.2.5.

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

ESFAS communication protocols are verified as conforming to the validated protocol specifications by the Project V&V Plan (Subsection 7.4.5.4.5).

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

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

The ESFAS platform operates in a fully deterministic manner, as described in Subsection 7.4.5.2.5, which allows implementation of a simple communication protocol using a predefined message structure at fixed time intervals. This ensures that a consistency of performance will exist that prevents performance deficits from adversely affecting the ESFAS architecture.

7.5.2.2.6 Prioritization of Functions

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

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

7.5.2.2.7 Fail-Safe

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

Controlled components associated with safety actuations are designed to go to their safe state when deenergized (~~Table 7.5-2~~Subsection 7.5.3.7). ESFAS outputs become deenergized on a loss of electrical power to the ESFAS.

7.5.2.2.8 Setpoints

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

Setpoints in the ESFAS are based on a documented methodology that identifies each of the assumptions and accounts for the uncertainties in each instrument channel. The setpoint methodology is further described in Subsections 7.2.1 and 7.5.3.10. Environmental allowances and measurement computational errors are accounted for in the uncertainty analysis used to establish the setpoints. The setpoint analysis parameters in the documented analyses are consistent with the safety analysis, system design basis, technical specifications, facility design, and expected maintenance practices.

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

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

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

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

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

Setpoints in the ESFAS are based on a documented methodology that identifies each of the assumptions and accounts for the uncertainties in each instrument channel. The setpoint methodology is further described in Subsections 7.2.1 and 7.5.3.10. Setpoint analysis parameters typically consider instrument precision, sensitivity, accuracy, loop uncertainties, and computational errors. The established setpoints and associated uncertainties ensure adequate margin to analytical limits or safety limits described in the technical specifications, which ensures that the sensitivity of each sensor channel is commensurate with the knowledge of the variable.

7.5.2.2.9 Operational Bypass, Permissives and Interlocks

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

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2). The ESFAS incorporates the Facility Master Operating Permissive key switch in the system design to select operation in the normal, unsecured mode or operationally secured (Subsection 7.5.4.3). A maintenance bypass function is available, as described in Subsection 7.5.4.4. There are no permissive conditions associated with the maintenance bypass capability.

ESFAS Criterion 35 – ESFAS interlocks shall ensure that operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required, with the exception of the use of the maintenance bypass capability.

The ESFAS has no operational bypasses included in the design, and therefore no interlocks are required to prevent operator actions from defeating an automatic safety function (Subsection 7.5.4.2). There are not automatic interlocks to prevent an operator from putting all instrument channels in maintenance bypass (Subsection 7.5.4.4). Administrative controls are provided by the technical specifications to prevent placing the same SFM across more than one channel in maintenance bypass.

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

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

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

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

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

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

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

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2). A maintenance bypass function is available, as described in Subsection 7.5.4.4. There are no permissive conditions associated with the maintenance bypass capability~~is provided and utilized for maintenance and testing purposes (Subsection 7.5.4.4)~~.

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

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

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

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

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

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

~~Where three channels are provided, taking a SFM out of service preserves the single failure criterion for variables associated with that SFM. In cases where only two channels are provided, taking a channel out of service will actuate the associated safety function. For testing purposes, placing a channel in maintenance bypass will be allowed by technical specifications for up to two hours to perform required testing. Two hours is considered acceptable due to the continued operability of the redundant channel(s) and the low likelihood that an accident would occur in those two hours (Subsection 7.5.4.4).~~There are no maintenance bypass capabilities associated with execute features for the ESFAS. The maintenance bypass capabilities are associated with the sense and command features only. Maintenance bypass capabilities and their acceptability for use are further discussed in Subsection 7.5.4.4.

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

There are no operational bypasses in the ESFAS design (Subsection 7.5.4.2). Any ESFAS channels placed in maintenance bypass for maintenance or testing, or removed from

maintenance bypass, will be displayed redundantly to the operators in the facility control room through the monitoring and indication bus to the PICS (Subsection 7.5.4.4). The PICS is described in Section 7.3 and operator displays and human factors considerations are addressed in Section 7.6.

7.5.2.2.10 Completion of Protective Actions

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

Figure 7.5-1 shows how the ESFAS latches in a protective action and maintains the state of a protective action until operator input is initiated to reset the output of the ESFAS. Completion of protective actions is described in Subsection 7.5.3.2.

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

Only deliberate operator action can be taken to reset the ESFAS following a protective action. Figure 7.5-1 shows how the ESFAS latches in a protective action and maintains the state of a protective action until operator input is initiated to reset the output of the ESFAS. Completion of protective actions is described in Subsection 7.5.3.2.

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

A ~~safety-related~~n enable nonsafety switch (when enabled) allows a facility operator to control the output state of the ESFAS with a hardwired binary control signal from the nonsafety-related controls. If the enable nonsafety switch is active, and no automatic safety actuation or manual safety actuation signals are present, the operator is capable of energizing or deenergizing any EIM outputs using the nonsafety-related hardwired control signals (Subsection 7.5.3.2). Additionally, safety-related signals are prioritized over nonsafety-related signals (Subsection 7.5.3.11).

7.5.2.2.11 Equipment Qualification

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

ESFAS rack mounted equipment is installed in a mild operating environment and is designed to meet the environmental conditions described in Subsection 7.5.3.4. Rack mounted ESFAS equipment is tested to appropriate standards to show that the effects of EMI/RFI and power surges are adequately addressed. This testing includes emissions testing, susceptibility testing, and surge withstand testing. Appropriate grounding of the ESFAS is performed in accordance with Section 5.2.1 of IEEE Standard 1050-2004 (IEEE, 2004b).

7.5.2.2.12 Surveillance

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

The ESFAS design supports testing, maintenance, and calibration to ensure operability as described in Subsections 7.5.4.4 and 7.5.4.5. Surveillance t~~T~~esting performed using the maintenance bypass capability during operation is controlled in accordance with the technical specifications to ensure that ~~at least one division of~~ the ESFAS is capable of performing its safety functions when required (Subsection 7.5.4.4). Self-testing features provide for monitoring as described in Subsection 7.5.4.5 to provide indication to the operator if conditions exist that could challenge operability of the equipment.

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

The ESFAS design supports testing, maintenance, and calibration, as described in Subsections 7.5.4.4 and 7.5.4.5. End-to-end testing of the entire ESFAS platform can be performed through overlap testing. ESFAS components have self-testing capabilities, except the discrete APL of the EIM which is functionally tested. The ESFAS continuously provides redundant indication of self-testing results to the PICS to indicate to operators that the ESFAS is operating correctly following testing, calibration, or inspections.

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

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

7.5.2.2.13 Classification and Identification

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

Each ESFAS cable and component is uniquely identified in accordance with SHINE component numbering guidelines. By identifying the specific component associated with the ESFAS, the safety classification can be determined. The unique identification number indicates the applicable system and division (Subsection 7.5.3.9).

7.5.2.2.14 Human Factors

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

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

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

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

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

~~To support the use of manual safety actuations, t~~The ESFAS includes redundantly isolated outputs for each safety-related instrument channel to provide monitoring and indication information to the PICS (Subsection 7.5.3.6), which includes indication of ESFAS actuation device status. This supports annunciation of the channel initiating a protective action. The~~See also~~ ESFAS requires manual operator reset when conditions to resume operation are met and satisfied as described in ESFAS Criterion 45 ~~regarding manual operator reset in~~ (Subsection 7.5.2.2.10).

7.5.2.2.15 Quality

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

The safety-related ESFAS is designed, fabricated, erected, and tested by SHINE's safety-related control system vendor in accordance with the vendor's Project Quality Assurance Plan (~~Subsection 7.4.4.1.4~~Subsection 7.4.5.4). SHINE is responsible for oversight of the vendor and maintaining the vendor as an approved supplier on the SHINE approved supplier list (Subsection 7.4.5.4.1).

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

The ESFAS design, 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.

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

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

7.5.3.2 Completion of Protective Actions

The ESFAS is designed so that once initiated, protective actions will continue to completion. Only deliberate operator action can be taken to reset the ESFAS following a protective action.

Figure 7.5-1 shows how the ESFAS latches in a protective action and maintains the state of a protective action until operator input is initiated to reset the output of the ESFAS to normal operating conditions.

The output of the ESFAS is designed so that actuation through automatic or manual means of a safety function can only change when a new position is requested. If there is no signal present from the automatic safety actuation or manual actuation, then the output of the EIM remains in its current state. A ~~safety-related~~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.

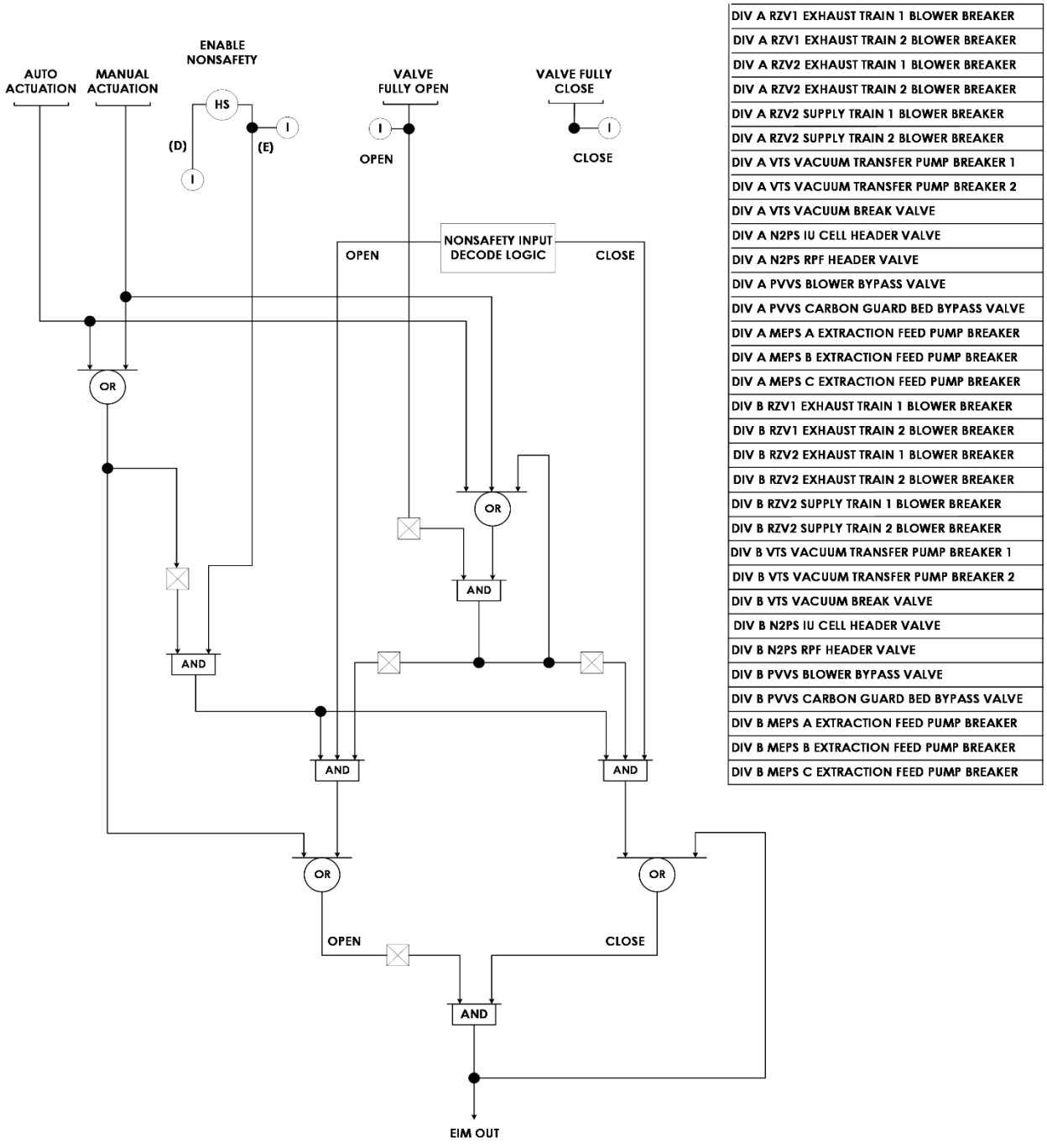
Nonsafety-related inputs into the ESFAS are designed and controlled so they do not prevent the ESFAS from performing its safety functions. The only nonsafety inputs into the ESFAS are those from the PICS for controls and monitoring/indication only variables. The nonsafety control signals from the PICS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

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

Priority Logic

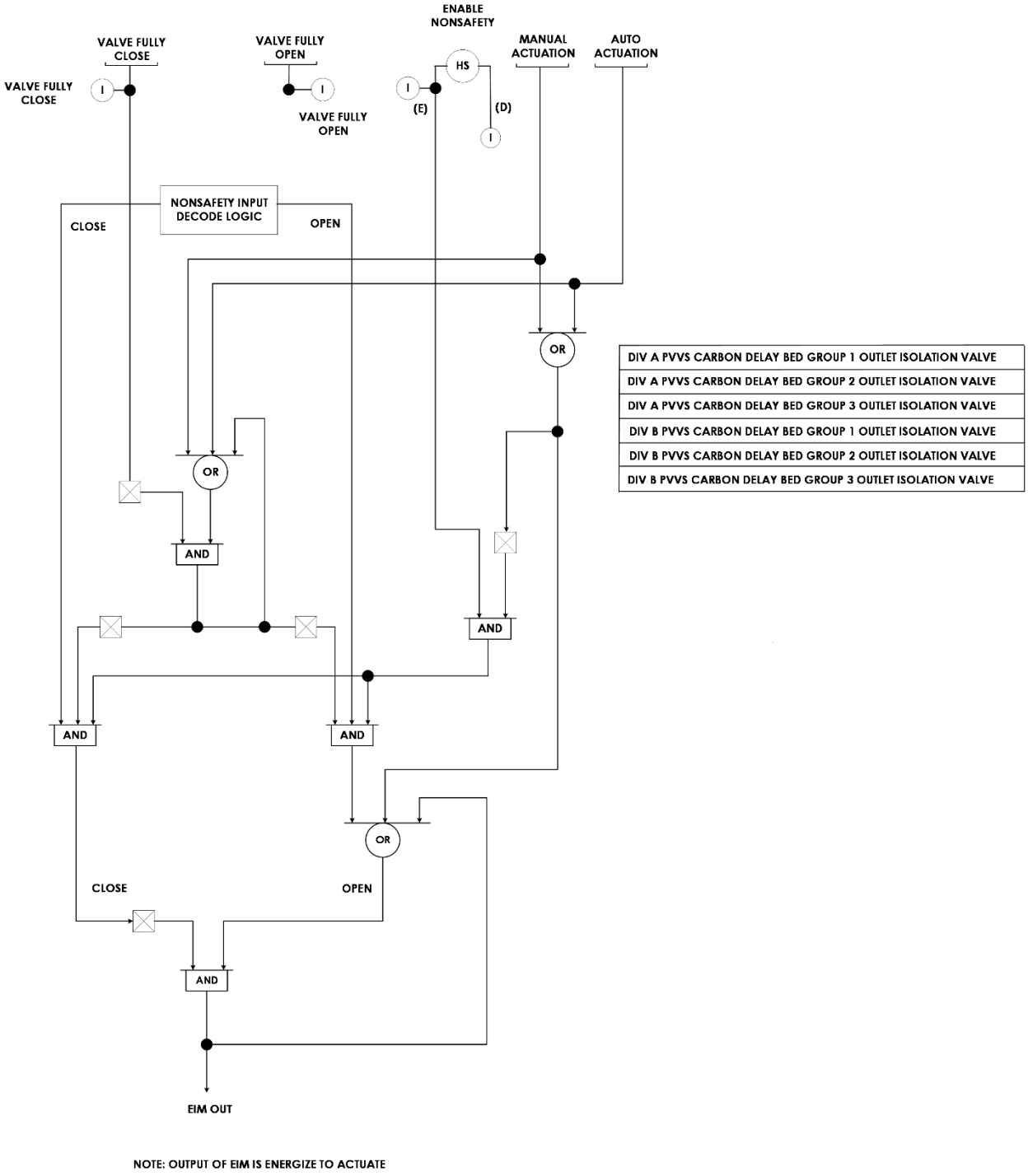
Figure 7.5-1 – ESFAS Logic Diagrams
(Sheet 23 of 27)



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

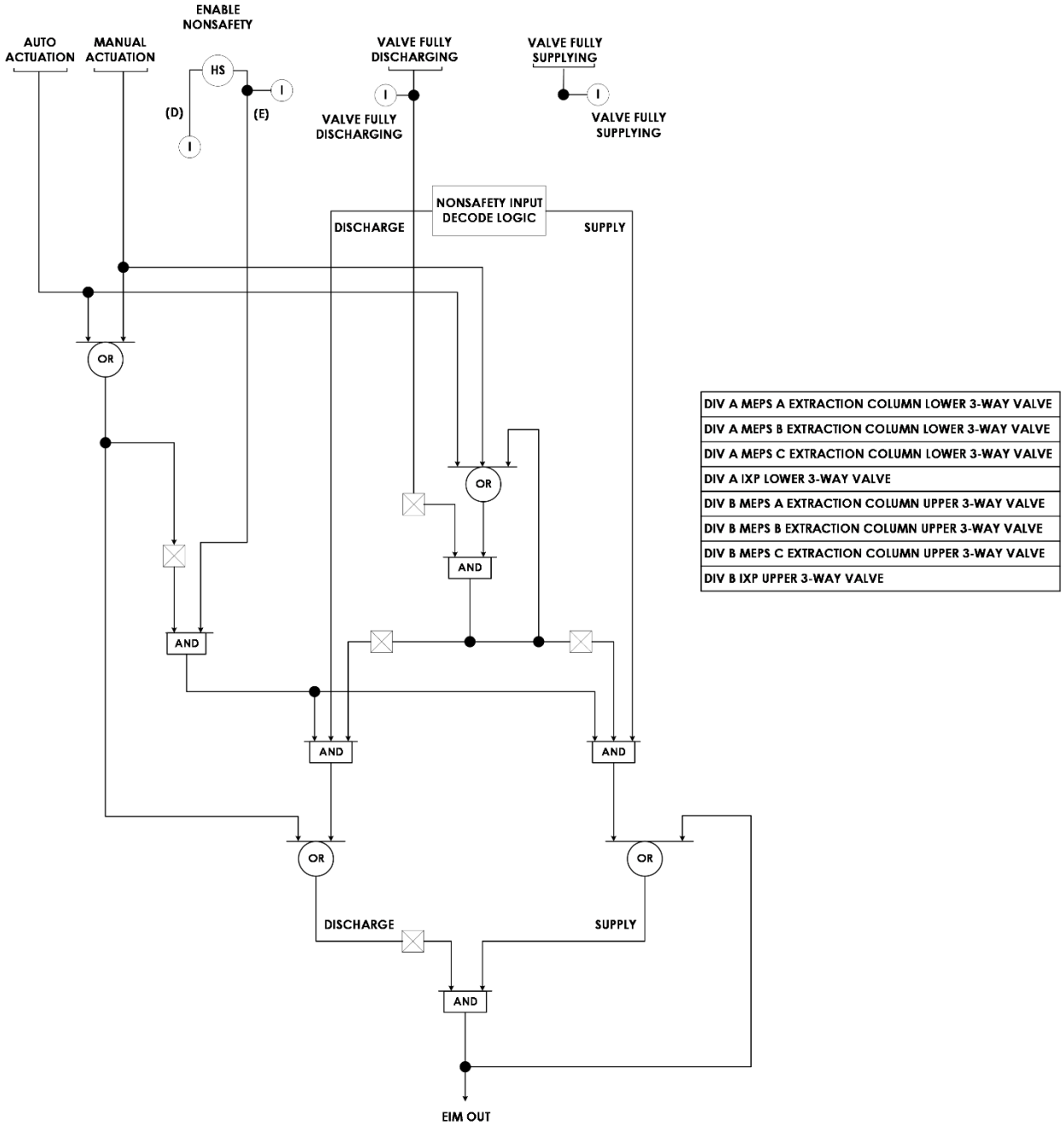
Priority Logic

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



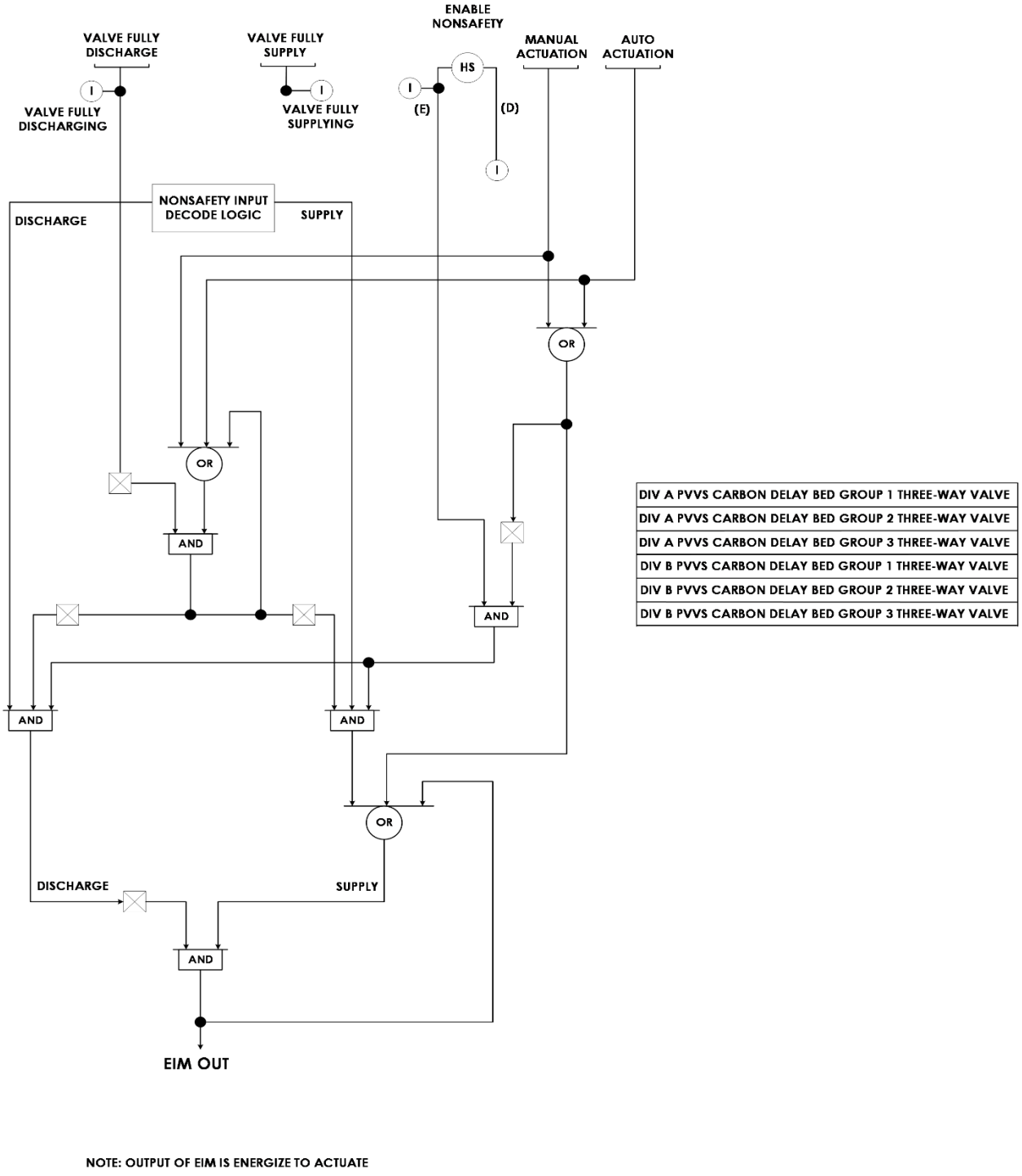
Priority Logic

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



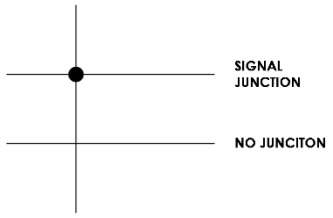
Priority Logic

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



Priority Logic

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

A – ALARM PROVIDED TO PROCESS INTEGRATED CONTROL SYSTEM	RM – RADIATION MONITOR	
I – INDICATION PROVIDED TO PROCESS INTEGRATED CONTROL SYSTEM	LS – LEVEL SWITCH	
OR – LOGICAL "OR" GATE	ZI – POSITION INDICATION	
AND – LOGICAL "AND" GATE	CT – CONDUCTIVITY TRANSMITTER	
LOGICAL "NOT" OR INVERTER GATE	PT – PRESSURE TRANSMITTER	ACRONYMS
XOR – LOGICAL "XOR" GATE	TT – TRITIUM TRANSMITTER	DIV – DIVISION
		EIM – EQUIPMENT INTERFACE MODULE
2/3 – TWO-OUT-OF-THREE VOTING GATE	TE – TEMPERATURE ELEMENT	FNHS – FACILITY NITROGEN HANDLING SYSTEM
		IU – IRRADIATION UNIT
1/2 – ONE-OUT-OF-TWO VOTING GATE	CO – CARBON MONOXIDE TRANSMITTER	IXP – IODINE AND XENON PURIFICATION SYSTEM
		MEPS – MOLYBDENUM EXTRACTION AND PURIFICATION SYSTEM
BISTABLE – INCREASING SETPOINT	FT – FLOW TRANSMITTER	N2PS – NITROGEN PURGE SYSTEM
		PICS – PROCESS INTEGRATED CONTROL SYSTEM
BISTABLE – DECREASING SETPOINT	DI – DISCRETE INPUT	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"	SSS – STORAGE AND SEPARATION SYSTEM
		TPS – TRITIUM PURIFICATION SYSTEM
	(D) – ENABLE NONSAFETY "DISABLED"	TSPS – TARGET SOLUTION PREPARATION SYSTEM
		VTS – VACUUM TRANSFER SYSTEM

Legend

Radiation monitoring information is conveyed from the radiation monitoring instruments described in Section 7.7 to the PICS and displayed in the facility control room. Radiation monitoring information is available on demand at the operator workstations.

Display values on each PICS display screen are automatically updated as more current data becomes available. Each PICS display screen presented on the operator workstation has a title or header and unique identification to distinguish each display page.

The maintenance workstation provides diagnostic information received from the ESFAS and TRPS on system status to be used as a test interface.

Limited function local displays, including radiation monitoring information, are also provided in the irradiation facility (IF) and radioisotope production facility (RPF) at select locations (Subsection 7.6.1.6).

7.6.4.2 Alarms

Alarms are integrated into the PICS display systems. The operator workstations provide detailed visual alarms to the operator to represent unfavorable status of the facility systems. Indications at the operator workstation are provided as visual feedback as well as visual features to indicate that systems are operating properly. Indication of alarms present is also provided for each IU and for the facility process systems at the main control board. Alarms are provided to inform the operator of off-normal operating system status, interlocks, engineered safety feature initiations, confinement status, and radiation fields and concentration. Alarms for facility systems are further described in Subsection 7.3.2.

7.6.4.3 Controls

Manual controls are provided on both of the PICS operator workstations, via input to the PICS, and on the main control board.

Manual controls for the safety-related TRPS and ESAFS protective functions are located at the main control board. Nonsafety manual push buttons that provide a diverse actuation to the automatically generated safety actuations are located directly below the static display screens for the associated IU or for the facility process section. A ~~safety-related~~n enable nonsafety switch is located in each main control board section next to the manual push buttons to allow the operator to control actuation components or to reset the safety-related control systems using the PICS following the actuation of a protective function. The enable nonsafety switch is a t~~hree~~wo-position ~~return-to-center~~ switch with states for Enable~~,~~ and Disable~~, and the return-to-center operating as-is state~~. To provide the operators the ability to place the facility into the Facility Secure state, a single manual key switch is located at the facility process section of the main control board below the static display screens. The switch has two positions of operation, Secured and Operating.

Manual actuation inputs from the main control board are connected downstream of the safety-related control system programmable logic functions as described in Subsection 7.4.5.2.4.

Controls for normal operation are provided at the operator workstations. Multiple equipment control displays are set up at each operator workstation for operators to select the PICS (or NDAS) display screen that coincides with the task that the operator is currently performing. Interface with the equipment control displays is through a keyboard and mouse provided for each

ENCLOSURE 3
ATTACHMENT 2

SHINE MEDICAL TECHNOLOGIES, LLC

SHINE MEDICAL TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE SUPPLEMENT NO. 8 AND RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

TECHNICAL REPORT NUMBER TECRPT-2018-0028, REVISION 1 HIPS PLATFORM APPLICATION SPECIFIC ACTION ITEM REPORT FOR THE TRPS AND ESFAS

51 pages follow

Table of Contents

List of Tables

1 Objective

The target solution vessel (TSV) reactivity protection system (TRPS) and the engineered safety features actuation system (ESFAS) are safety-related instrumentation and control (I&C) systems for the SHINE Medical Isotope Production Facility (the SHINE facility). The design of the TRPS and ESFAS is based upon the Highly Integrated Protection System (HIPS) platform that has a Topical Report (Reference 1) approved by the Nuclear Regulatory Commission (NRC) (Reference 2). The NRC's final safety evaluation report (SE) for the HIPS platform includes a list of application-specific action items (ASAIs) which identify criteria that applicants or licensees referencing the HIPS platform SE should address. The objective of this report is to provide a reference document for how these ASAIs are addressed in the design of the TRPS and ESFAS for the SHINE facility.

2 Methods

The method applied in this report was to evaluate each ASAI identified in the SE for the HIPS platform topical report (Reference 1) for applicability to SHINE's licensing application. The applicability was documented, and if the ASAI was determined to be not applicable, justification for why it is not considered applicable is provided. If the ASAI was determined to be applicable, a reference is given for the appropriate sections of the SHINE facility FSAR or for the appropriate design basis document which provides the material that addresses the ASAI. The results of this method are provided in Table 3-1.

It should be noted that some of the standards which were applied to the HIPS topical report (IEEE Std 603, IEEE Std 7-4.3.2, SECY-93-087, and DI&C-ISG-04) are not directly applicable to the SHINE application. Because the SHINE application is for a research and test reactor, NUREG-1537 outlines the criteria by which the SHINE design will be reviewed against.

3 Analysis Results

Table 3-1 HIPS Platform Application Specific Action Item Evaluation for the TRPS and ESFAS

ASAI No.	SER Referenced Section(s)	ASAI Description	Applicability and Description of How the TRPS and ESFAS Design Addresses the ASAI	Applicable SHINE design criteria for TRPS and ESFAS as stated in Sections 7.4.2 and 7.5.2 of SHINE's Final Safety Analysis Report
1	2.0	An applicant or licensee referencing this SE must establish full compliance with the design criteria and regulations identified in NuScale DSRS Chapter 7, Table 7.1, or the appropriate plant design criteria that are relevant to the specific application(s) of the HIPS platform as a safety-related I&C system in an NPP as defined in 10 CFR 50.55a(h).	Partially applicable. The SHINE facility licensing application is not anticipated to be reviewed against the guidance of the NuScale DSRS or the design criteria defined in 10 CFR 50.55a(h). However, Chapter 7 of SHINE's Final Safety Analysis Report (FSAR) documents the design criteria and regulations identified in NUREG-1537 relevant to the HIPS platform based TRPS and ESFAS designs and also provides evidence of full compliance with those design criteria and regulations.	Not applicable
2	2.0 3.0	An applicant or licensee referencing this SE must demonstrate that the HIPS platform used to implement the application-specific or plant-specific system is unchanged from the base platform addressed in this	Applicable. Changes to the base HIPS platform equipment as described in the HIPS platform topical report for the TRPS and ESFAS designs are identified and discussed in Section 5 of this report. A description of how the HIPS platform TRPS and ESFAS	Not applicable

		SE. Otherwise, the applicant or licensee must clearly and completely identify any modification or addition to the base HIPS platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes.	design implementation supports meeting the design criteria identified in NUREG-1537 is provided in Subsections 7.4.2 and 7.5.2. Descriptions of the architectural implementation of the HIPS platform is provided in the TRPS and ESFAS System Design Description (SDD) documents (Reference 6 and 7).	
3	3.6	Although the staff determined that the HIPS platform supports satisfying various sections and clauses of IEEE Std. 603-1991, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std. 603-1991. Because this SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences, an applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 603-1991 clause to its application-specific HIPS platform-based safety system or component. Furthermore, the applicant or licensee must demonstrate that the	Not applicable. Although the design of the TRPS and ESFAS will satisfy many sections and clauses of IEEE Std. 603-1991 because they are based upon the base HIPS platform design, the SHINE facility design basis is not required to conform with IEEE Std. 603. The SHINE facility design is required to conform to the guidance of NUREG-1537.	Not applicable

		plant-specific and application-specific use of the HIPS platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.		
4	3.7	Although the staff determined that the HIPS platform supports satisfying various sections and clauses of IEEE Std. 7-4.3.2-2003, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std. 7-4.3.2-2003. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. The applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 7-4.3.2-2003 clause to its application-specific HIPS platform-based safety system or component. Furthermore, the applicant or licensee must demonstrate that the	Applicable. Section 6 of this report provides a traceability matrix to support demonstration of conformance of the TRPS and ESFAS designs with IEEE Std. 7-4.3.2-2003.	Not applicable

		plant-specific and application-specific use of the HIPS platform satisfies the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.		
5	3.8	Although the staff determined that the HIPS platform includes features to support satisfying various sections and clauses of DI&C-ISG-04, an applicant or licensee referencing this SE must evaluate the HIPS platform-based system for full conformance against this guidance. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences.	Applicable. Section 7 of this report provides a traceability matrix to support demonstration of conformance of the TRPS and ESFAS designs with DI&C-ISG-04.	Not applicable
6	3.9	Although the staff determined that the HIPS platform includes features to support satisfying various sections of the SRM to SECY-93-087, an applicant or licensee referencing this SE must evaluate the HIPS platform-based	Applicable. Section 8 of this report provides a traceability matrix to support demonstration of conformance of the TRPS and ESFAS designs with SECY-93-087.	Not applicable

		system for full compliance against this requirement. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences.		
7	3.1.4.3	An applicant or licensee referencing this SE must provide administrative controls (e.g., procedures, technical specifications) to prevent an operator from placing the same SFM across more than one division into maintenance bypass concurrent with a single failure of a different division.	Applicable. Sections 3.2.1 and 3.2.2 of the technical specifications of the SHINE facility operating license application documents the required facility technical specifications applicable to placing a TRPS or ESFAS safety function module (SFM) into maintenance bypass. SHINE technical specification Limiting Conditions for Operation (LCO) 3.2.3 and 3.2.4 contain a note that specifies that any single SFM may be bypassed for up to 2 hours while the variable(s) associated with the SFM is in the condition of applicability for the purpose of performing a Channel Test or Channel Calibration. By only allowing a single SFM to by bypassed at one time, SHINE ensures that the same SFM across multiple divisions (which would be more than one SFM) will not be placed into maintenance bypass. By specifying this in the technical specifications, SHINE ensures that administrative controls are in place consistent with the NRC-approved HIPS TR to prevent an operator	TRPS Criterion 33 and 37 ESFAS Criterion 34 and 38

			from placing the same SFM across more than one division into maintenance bypass.	
8	3.2	An applicant or licensee referencing this SE should verify having appropriate physical independence between nonsafety-related and safety-related equipment to satisfy the Class 1E to non-Class 1E separation requirements, consistent with the guidelines of RG 1.75, Revision 3.	Partially applicable. Subsections 7.4.2.2.5 and 7.5.2.2.5 (Independence) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment implements physical, electrical, communications, and functional independence between nonsafety-related and safety-related equipment.	TRPS Criterion 20 and 21 ESFAS Criterion 21 and 22
9	3.4	An applicant or licensee referencing this SE must provide the basis for the allocation of safety functions between the two diverse divisions to mitigate the effects of a postulated CCF concurrent with Chapter 15 events of its final safety analysis report.	Applicable. The TRPS and ESFAS are both implemented with 3 redundant divisions. Each of the three divisions requires a different type of FPGA to address a potential CCF of one type of FPGA. The three types of FPGAs implemented on the divisional modules is as follows: • Division A: Microsemi IGLOO2 (FLASH based FPGA) • Division B: Intel MAX10 (Hybrid Flash and SRAM based FPGA) • Division C: Altera Artix-7 (SRAM based FPGA) An assessment of the design and implementation of diversity within the TRPS and ESFAS and the allocation of the safety functions among the diverse divisions to mitigate the effects of SHINE FSAR Chapter 13 events is provided in the Diversity and Defense-in-Depth Assessment of the TRPS and ESFAS (Reference 5).	Not applicable

10	3.4	An applicant or licensee referencing this SE must verify that all diversity attributes of a HIPS platform (i.e., equipment diversity, design diversity, and functional diversity) conform to the diversity design details provided in the TR.	Applicable. An assessment of the design and implementation of diversity within the TRPS and ESFAS and the allocation of the safety functions among the diverse divisions to mitigate the effects of SHINE FSAR Chapter 13 events is provided in the Diversity and Defense-in-Depth Assessment of the TRPS and ESFAS (Reference 5).	Not applicable
11	3.4	An applicant or licensee referencing this SE must verify that the diverse FPGA technologies have unique identification.	Applicable. Subsections 7.4.3.10 and 7.5.3.9 (Classification and Identification) of the SHINE facility FSAR respectively describe how the HIPS-based TRPS and ESFAS equipment designs address unique identification.	Not applicable
12	3.6.2.1 3.6.2.5 3.6.2.6.3.1 3.6.2.6.3.3 3.8.1.18	An applicant or licensee referencing this SE should perform a system-level FMEA to demonstrate that the application-specific use of the HIPS platform identifies each potential failure mode and determines the effects of each failure. The FMEA should demonstrate that single failures, including those with the potential to cause a nonsafety system action (i.e., a control function) resulting in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions, as applicable.	Applicable. The TRPS and ESFAS Failure Modes and Effects Analysis (Reference 4) evaluates potential single failures and determines the effects of each failure for the TRPS and ESFAS. As documented in the FMEA (Reference 4), failure modes that can prevent the systems from performing their intended functions are detected by design, built-in system diagnostics, or by periodic testing. The results of the FMEA determined that there are no single failures or non-detectable failures that can prevent the TRPS or ESFAS from performing their required safety functions.	TRPS Criterion 16 and 17 ESFAS Criterion 16, 17 and 18

13	3.6.2.1	An applicant or licensee referencing this SE should demonstrate that the application-specific diagnostic, self-test, and manually initiated test and calibration features will not adversely affect channel independence, system integrity, or the system's ability to meet the single-failure criterion.	Applicable. Subsections 7.4.5.2.1 (Independence) and 7.4.5.2.2 (Redundancy) of the SHINE facility FSAR describe how the principles of redundancy and independence are incorporated into the design of the TRPS and ESFAS. The TRPS and ESFAS Failure Modes and Effects Analysis (Reference 4) evaluates potential single failures and determines the effects of each failure for the TRPS and ESFAS.	TRPS Criterion 47 ESFAS Criterion 48
14	3.6.2.1	An applicant or licensee referencing this SE must review the actions to be taken when failures and errors are detected during tests and self-tests and ensure that these actions are consistent with system requirements. In addition, the applicant or licensee should describe how errors and failures are indicated and managed after they are detected. Finally, the applicant or licensee should confirm that this information is provided in the single-failure analysis for the plant-specific application.	Partially applicable. Subsections 7.4.4.4 and 7.5.4.5 (Testing Capability) and Subsection 7.4.5.5 (System Performance Analysis) of the SHINE facility FSAR describes the self-testing and diagnostic features of the TRPS and ESFAS design. The alarm function for the SHINE facility is located in the nonsafety-related process integrated control system (PICS), which is outside the scope of the systems using the HIPS platform. Section 7.6.4.1 discusses how errors and failures are indicated via the PICS after they are detected. The TRPS and ESFAS Failure Modes and Effects Analysis (Reference 4) evaluates potential single failures and determines the effects of, and methods of detection, for each failure for the TRPS and ESFAS.	Not applicable
15	3.6.2.2 3.6.4.3	An applicant or licensee referencing this SE must demonstrate that the application-specific logic satisfies	Applicable. Subsections 7.4.3.3 and 7.5.3.2 (Completion of Protective Actions) respectively discuss how the TRPS and	TRPS Criterion 43, 44, and 45

		the completion of protective action requirements.	ESFAS ensure completion of protective actions.	ESFAS Criterion 44, 45, and 46
16	3.6.2.3 3.7.1.3	An applicant or licensee referencing this SE must confirm that the HIPS platform manufacturer is currently on the Nuclear Procurement Issues Committee list or confirm that the HIPS manufacturing quality processes conform to the applicant's or licensee's program that is compliant with 10 CFR Part 50, Appendix B (i.e., vendor is included in the applicant's Approved Vendor List). The applicant or licensee will need to demonstrate that the HIPS software and associated development life cycle conform to applicable regulatory requirements.	Partially applicable. The overall quality assurance program applied to the design of the safety-related I&C systems is described in SHINE's Quality Assurance Program Description (QAPD), 2000-09-01 (Reference 3). SHINE's QAPD is based upon ANSI/ANS-15.8-1995, which provides an acceptable method of complying with the requirements of 10 CFR 50.34 for a production or utilization facility. Subsections 7.4.2.2.15, 7.5.2.2.15 (Quality), 7.4.3.13 and 7.5.3.12 (Design Codes and Standards) of the SHINE facility FSAR respectively identify the required codes and standards to be used in the design development of the TRPS and ESFAS. Subsection 7.4.5.4 (Software Requirements Development) describes the requirements for the TRPS and ESFAS software development life cycle.	TRPS Criterion 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13 ESFAS Criterion 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13
17	3.6.2.4 3.6.2.6.2 3.7.1.4 3.8.1.17	An applicant or licensee referencing this SE must confirm that the HIPS platform equipment is qualified to the applicable regulatory requirements.	Applicable. The overall quality assurance program applied to the design of the safety-related I&C systems is described in SHINE's QAPD, 2000-09-01 (Reference 3). SHINE's QAPD is based upon ANSI/ANS 15.8-1995, which provides an acceptable method of complying with the requirements of 10 CFR 50.34 for a production or utilization facility. Subsections 7.4.3.13 and 7.5.3.12 (Design Codes and Standards) of the SHINE facility	TRPS Criterion 54 and 55 ESFAS Criterion 55 and 56

			FSAR respectively identify the required codes and standards to be used in qualifying the TRPS and ESFAS equipment.	
18	3.6.2.5 3.7.1.5.1 3.8.1.20	An applicant or licensee referencing this SE must identify the safe states for protective functions and the conditions that require the system to enter a fail-safe state. The applicant or licensee must also demonstrate system qualification for installation and operation in mild environment locations.	Applicable. The safe states for TRPS and ESFAS actuated components are provided in Subsection 7.4.3.8 and Table 7.5-2 of the SHINE facility FSAR, respectively. The conditions that require the TRPS and ESFAS to enter a fail-safe state are provided in Sections 7.4.3.1 and 7.5.3.1, respectively. A TRPS and ESFAS Failure Modes and Effects Analysis (Reference 4) was conducted for the TRPS and ESFAS, which evaluated each component of the systems, how it may fail, and what the effect of the failure on the systems would be in the presence of a single failure. Effects on the systems include assuming a fail-safe state, only alarm the failure, or assuming a fail-safe state and alarm the failure. Which of these effects occur depends on the mode of failure for each component and is documented in the FMEA. Subsections 7.4.3.13 and 7.5.3.12 (Design Codes and Standards) of the SHINE facility FSAR respectively identify the required codes, standards, and the conditions to be used in qualifying the TRPS and ESFAS equipment. HIPS platform environmental and seismic qualification testing results are documented in Reference 8. HIPS platform electromagnetic and radio frequency	TRPS Criterion 28 and 46 ESFAS Criterion 29 and 47

			interference qualification testing results are documented in Reference 9.	
19	3.6.2.5 3.7.1.5.1 3.8.1.19 3.8.1.20	An applicant or licensee referencing this SE must confirm that system real-time performance is adequate to ensure completion of protective actions within critical time frames required by the plant safety analyses.	Applicable. Assumed maximum response time and response time analysis for the TRPS and ESFAS is discussed in Subsection 7.4.5.2.3 (Predictability and Repeatability) of the SHINE facility FSAR.	SHINE Criterion 13 TRPS Criterion 14 and 24 ESFAS Criterion 14 and 25
20	3.6.2.6.1 3.8.1.2 3.8.1.16	An applicant or licensee referencing this SE must demonstrate that the full system design, any use of a shared component, the equipment's installation, and the power distribution architecture provide the required independence.	Applicable. Subsection 7.4.5.2.1 (Independence) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment implements physical, electrical, communications, and functional independence.	TRPS Criterion 18, 20, 21, 22, and 23 ESFAS Criterion 19, 21,22, 23, and 24
21	3.6.2.6.1 3.8.1.2 3.8.1.16	An applicant or licensee referencing this SE must provide redundant power sources to separately supply the redundant power conversion features within the HIPS platform.	Applicable. Division A of both the TRPS and ESFAS is powered from Division A of the uninterruptible power supply system (UPSS). Division B of both the TRPS and ESFAS is powered from Division B of the UPSS. Division C of both the TRPS and ESFAS receives auctioneered power from Division A and Division B of the UPSS. Both the TRPS and ESFAS require 125 VDC power, which the UPSS provides as described above. Each TRPS and ESFAS cabinet is provided a single 125 VDC power supply, which is used to power three (3) redundant 125 VDC to 24 VDC converters located at the top of the cabinet. The 24V supply is then	TRPS Criterion 17 ESFAS Criterion 17

			distributed to each of three (3) chassis mounting bays as needed, where it is then used to power two (2) redundant 24 VDC to 5 VDC converters located beneath each chassis bay. These provide independent +5V A and +5V B power channels to each chassis.	
22	3.2.2 3.6.2.6.3.1 3.8.1.1 3.8.1.2 3.8.1.3 3.8.1.8 3.8.1.16	An applicant or licensee referencing this SE must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety to nonsafety-related systems.	Applicable. Subsection 7.4.5.2.1 (Independence) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment implements physical, electrical, communications, and functional independence.	TRPS Criterion 20, 21 and 22 ESFAS Criterion 21, 22 and 23
23	3.6.2.6.3.2 3.6.2.6.4 3.8.1.1 3.8.1.2 3.8.1.16	An applicant or licensee referencing this SE must perform isolation testing on the HIPS platform equipment to demonstrate the capability to satisfy the Class 1E to non-Class 1E isolation requirements, consistent with the guidelines of RG 1.75, Revision 3.	Partially applicable. Subsection 7.4.5.2.1 (Independence) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment implements physical, electrical, communications, and functional independence. The results of isolation testing of HIPS platform equipment consistent with the guidelines of RG 1.75, Revision 3 is provided in the HIPS Platform EMI/RFI and Isolation Testing Report (Reference 7).	TRPS Criterion 19, 20, 21, and 22 ESFAS Criterion 20, 21, 22, and 23

24	3.6.2.7 3.6.3.5	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for testing and calibration of safety-related features.	Applicable. The TRPS and ESFAS are designed with the capability for calibration and surveillance testing, including channel checks, calibration verification, and time response measurements to verify that I&C safety systems perform required safety functions. The TRPS and ESFAS allow systems, structures, and components (SSCs) to be tested while retaining the capability to accomplish required safety functions. The TRPS and ESFAS use modules from the HIPS platform which are designed to eliminate non-detectable failures through a combination of built-in self-testing and periodic surveillance testing. Testing from the sensor inputs of the TRPS and ESFAS through to the actuated equipment is accomplished through a series of overlapping sequential tests, most of which may be performed during normal plant operations. Performance of periodic surveillance testing does not involve disconnecting wires or installation of jumpers for at-power testing. The self-test features maintain division independence by being performed within the division. The part of TRPS and ESFAS that cannot be tested during normal operations is the actuation priority logic circuit on the equipment interface module (EIM). This includes the manual control room switches and the nonsafety-related interface that	TRPS Criterion 47 and 48 ESFAS Criterion 48 and 49

			provide inputs to the actuation priority logic. The actuation priority logic consists of discrete components and directly causes actuation of field components. The actuation priority logic is a simple circuit that has acceptable reliability to be tested when the irradiation unit is in Mode 0. While the TRPS and ESFAS is in normal operation, self-tests run without affecting the performance of the safety function, including its response time. TRPS and ESAFS data communications are designed with error detection to enhance data integrity. The protocol features ensure communications are robust and reliable with the ability to detect transmission faults. Similar data integrity features are used to transfer diagnostics data. The TRPS and ESFAS provides a means for checking the operational availability of the sense and command feature input sensors relied upon for a safety function during normal plant operation. This capability is provided by one of the following methods: • Perturbing the monitored variable • Cross-checking between channels that have a known relationship (channel check) • Introducing and varying a substitute input to the sensor Fault detection and indication occurs at the module level, which enables plant personnel	

			to identify the module that needs to be replaced. Built-in self-testing will generate an alarm and report a failure to the operator and place the component (e.g., safety function module (SFM), scheduling, bypass, and voting modules (SBVMs), or EIM components) in a fail-safe state. The maintenance work station (MWS) is used to perform modification of configurable variables and setpoints and in-chassis calibration of TRPS and ESFAS equipment. Prior to using the MWS, the affected SFM must be taken out of service. Physical and logical controls are put in place to prevent modifications to a safety channel when it is being relied upon to perform a safety function.	
25	3.6.2.7 3.6.3.5	An applicant or licensee referencing this SE must provide additional diagnostics or testing functions (i.e., self-tests or periodic surveillance tests) to address any system-level failures that are identified as detectable only through periodic surveillance.	Applicable. Testing capabilities for the TRPS and the ESFAS is described in Subsections 7.4.4.4 and 7.5.4.5 (Testing Capability) of the SHINE facility FSAR, respectively. The part of the TRPS and ESFAS that cannot be tested during normal operations is the actuation priority logic circuit on the equipment interface module (EIM). This includes the manual control room switches and the nonsafety-related interface that provide inputs to the actuation priority logic. The actuation priority logic consists of discrete components and directly causes actuation of field components.	TRPS Criterion 48 and 49 ESFAS Criterion 49 and 50

26	3.6.2.7 3.6.3.5	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for any automatic sensor cross-check as a credited surveillance test function and the provisions to confirm the continued execution of the automatic tests during plant operations.	Partially applicable. Required Channel Checks are discussed in the SHINE facility technical specifications. The TRPS and ESFAS have redundant gateways which gather the output of the monitoring and indication communications modules (MICMs) for each of the three divisions. The data for each of the three divisions are compared and the results are provided to the process integrated control system (PICS). The results of the comparison can be used to support performing a channel check.	TRPS Criterion 47 ESFAS Criterion 48
27	3.6.2.8.1	An applicant or licensee referencing this SE must describe any manual controls and associated displays used to support manually controlled safety actions necessary to accomplish a safety function for which no automatic control is provided.	Not applicable. The SHINE facility design basis does not include manually controlled safety actions for which no automatic control is provided.	Not applicable
28	3.6.2.8.2	An applicant or licensee referencing this SE must describe how the HIPS platform safety system status information is used in displays to provide unambiguous, accurate, complete, and timely status of safety system protective actions.	Applicable. TRPS and ESFAS monitoring and indication information is transmitted redundantly from each system's divisional monitoring and indication communications module (MICM) via one-way isolated RS-485 connections to respective redundant nonsafety gateway communications modules (GWCMs), which are located in two redundant gateway chassis. The GWCMs for the TRPS are functionally and logically	SHINE Criterion 6

			independent from the GWCMs for the ESFAS and vice versa. They are physically located within two chassis, and the two chassis are located in the ESFAS Division C cabinet. All GWCMs within Gateway Chassis A will utilize the same field programmable gate array (FPGA) type that is utilized in Division A of the TRPS and ESFAS. All GWCMs within Gateway Chassis B will utilize the same FPGA type that is utilized in Division B of the TRPS and ESFAS. This ensures that a software common cause failure for one of these two FPGA types will not disable the function of providing TRPS and ESFAS monitoring and indication information to PICS. A description of how safety system status is used in displays is provided in Section 7.6 (Control Console and Display Instruments) of the SHINE facility FSAR.	
29	3.6.2.8.3	An applicant or licensee referencing this SE must describe how the HIPS platform bypass status information is used to automatically actuate the bypass indication for bypassed or inoperable conditions, when required, and provide the capability to manually activate the bypass indication from within the control room.	Applicable. Subsections 7.4.4.3 and 7.5.4.4 (Maintenance Bypass) of the FSAR also provides a description of the use of manual switches for placing HIPS modules in bypass. A description of how the safety system status is provided to the PICS for indication to the operators is given above in the response to ASAI 28.	TRPS Criterion 42 ESFAS Criterion 43

30	3.6.2.8.4	An applicant or licensee referencing this SE must describe how the information displays are accessible to the operator and are visible from the location of any controls used to effect a manually controlled protective action provided by the front panel controls of a HIPS-based system.	Partially applicable. TRPS and ESFAS equipment is not used to display information for the operator. The TRPS and ESFAS monitoring and indication information will be available to the operators in the facility control room at the PICS operator workstations. A subset of the TRPS and ESFAS monitoring and indication information will be displayed at the main control board in the facility control room near where the manual control for actuating TRPS and ESFAS safety functions are located. SHINE FSAR Subsection 7.4.5.2.4 describes the TRPS and ESFAS information available to the operators in the facility control room.	SHINE Criterion 6
31	3.6.2.9	An applicant or licensee referencing this SE must provide additional control of access features to address the system-level aspects for a safety system using the HIPS platform.	Applicable. Subsection 7.4.5.3 (Access Control and Cyber Security) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment design addresses the control of access.	TRPS Criterion 1, 2, and 3 ESFAS Criterion 1, 2, and 3
32	3.6.2.10 3.8.1.13	An applicant or licensee referencing this SE must provide additional diagnostics or testing functions (self-tests or periodic surveillance tests) to address any system-level failures that are identified as detectable only through periodic surveillance. The applicant or licensee must also ensure that	Applicable. The self-testing and required surveillance testing for the TRPS and the ESFAS are described in Subsections 7.4.4.4 and 7.5.4.5 (Testing Capability) of the SHINE facility FSAR. The TRPS and ESFAS Failure Modes and Effects Analysis (Reference 4) identified no nondetectable TRPS or ESFAS failures.	TRPS Criterion 48 and 49 ESFAS Criterion 49 and 50

		failures detected by these additional diagnostics or testing functions are consistent with the assumed failure detection methods of the application-specific single-failure analysis.		
33	3.6.2.11	An applicant or licensee referencing this SE must establish the identification and coding requirements for cabinets and cabling for a safety system.	Applicable. Subsections 7.4.3.10 and 7.5.3.9 (Classification and Identification) of the SHINE facility FSAR respectively describes how the TRPS and ESFAS equipment is uniquely identified in accordance with SHINE component numbering guidelines. The equipment identification includes, but is not limited to, system designation (code), equipment train, and division.	TRPS Criterion 50 ESFAS Criterion 51
34	3.6.2.12	An applicant or licensee referencing this SE must demonstrate that the application-specific system design implemented with the HIPS platform meets the applicable regulatory requirements for auxiliary features.	Applicable. A supporting feature for the TRPS and ESFAS which is not a part of the systems is the electrical power provided by the uninterruptible power supply system (UPSS). Section 8a2.2 of the SHINE facility FSAR describes the design basis of the UPSS. Other auxiliary features of the TRPS and ESFAS that are a part of the systems by association (i.e., not isolated from the TRPS or ESFAS) but are not required for the TRPS and ESFAS to perform their safety functions include the following: 1) Continuous online self-testing and diagnostics	Not applicable

			2) Communication from safety-related portions of the TRPS and ESFAS to non-safety related systems 3) Capability for control of safety-related components by using non-safety related PICS via the APL within the EIM 4) Isolation devices and circuitry	
35	3.6.2.13	An applicant or licensee referencing this SE must demonstrate that the application-specific system design implemented with the HIPS platform meets the applicable regulatory requirements for shared systems.	Applicable. Subsection 7.1.2 and Figure 7.1-1 of the SHINE facility FSAR describes the use of a separate TRPS for each IU Cell.	SHINE Criterion 5
36	3.6.2.14	An applicant or licensee referencing this SE must confirm that the HIPS platform equipment meets any specified human factors requirements.	Applicable. Subsections 7.4.3.7 and 7.5.3.6 (Human Factors) of the SHINE facility FSAR describe how human factors are incorporated into the design of the TRPS and ESFAS.	TRPS Criterion 51 ESFAS Criterion 52
37	3.6.2.15 3.7.1.15	An applicant or licensee referencing this SE must confirm that the HIPS platform equipment meets any specified quantitative or qualitative reliability goals.	Applicable. Reliability characteristics of the TRPS and ESFAS designs are described in Subsections 7.4.2.1.3 and 7.5.2.1.3 (Protection System Repeatability and Testability) of the SHINE facility FSAR.	TRPS Criterion 23 and 24 ESFAS Criterion 24 and 25
38	3.6.3.1 3.6.4.1	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide automatic safety system	Applicable. The design criteria for the TRPS and ESFAS are provided in Subsections 7.4.2 and 7.5.2 (Design Criteria) respectively. The design basis for the sense and command features of the TRPS and ESFAS	SHINE Criterion 14

		sense and command features for required safety functions.	is provided in Subsections 7.4.4 and 7.5.4 (Operation and Performance) respectively for the TRPS and ESFAS of the SHINE facility FSAR.	
39	3.6.3.2 3.6.4.2	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide manual safety system sense and command features for required safety functions.	Applicable. The design basis for the manual sense and command features for the TRPS and ESFAS is provided in Subsections 7.4.3.7 and 7.5.3.6 (Human Factors) respectively for the TRPS and ESFAS of the SHINE facility FSAR.	TRPS Criterion 15 and 52 ESFAS Criterion 15 and 53
40	3.6.3.3	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for sense and command features to provide protection against the resulting condition of a nonsafety system action that has been caused by a single credible event, including its direct and indirect consequences.	Applicable. The design basis for the sense and command features for the TRPS and ESFAS is provided in Subsections 7.4.3.12 and 7.5.3.11 (Prioritization of Functions) respectively for the TRPS and ESFAS of the SHINE facility FSAR.	TRPS Criterion 27 ESFAS Criterion 28
41	3.6.3.4	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to acquire and condition field sensor measurements of the required variables.	Applicable. The design basis for acquiring and conditioning inputs in the TRPS and ESFAS is provided in Subsection 7.4.5 (Highly Integrated Protection System Design) of the SHINE facility FSAR.	SHINE Criterion 13
42	3.6.3.6 3.6.4.4	An applicant or licensee referencing this SE must describe how the HIPS	Applicable. Subsection 7.4.4.2 of the SHINE facility FSAR describes the use of operational bypasses for the TRPS during	TRPS Criterion 33, 34, 35, 36, 37, 38, 39, 40, and 42

		platform equipment is used for operating bypasses.	the operation of the irradiation unit (IU) cells. Automatic operational bypasses are only associated with the TRPS. As stated in FSAR Subsection 7.5.4.2, automatic operational bypasses are not used in the ESFAS.	ESFAS Criterion 34, 35, 36, 37, 38, 39, 40, 41, and 43
43	3.6.3.7	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for maintenance bypasses and provide the technical specification requirements.	Applicable. Subsection 7.4.5 (Highly Integrated Protection System Design) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment is used for maintenance bypasses. For the SHINE application, maintenance bypasses are associated with the sense and command features only for the TRPS and ESFAS. There are no maintenance bypass capabilities associated with execute features in the SHINE application of the HIPS platform. Channels associated with an SFM of the TRPS and ESFAS can be taken out of service by direct component replacement or the manipulation of manual switches. Components that are designed to be replaced directly are the scheduling and bypass modules (SBMs), SBVMs, equipment interface modules (EIMs), and HWMs. Subsections 7.4.4.3 and 7.5.4.4 of the SHINE FSAR describe how the sense and command features can be placed into maintenance bypass for the TRPS and ESFAS, respectively.	TRPS Criterion 41 ESFAS Criterion 42

			Subsections 3.2.1, 3.2.2, 3.2.5 and 3.2.6 of the technical specifications of the SHINE facility operating license application document the required facility technical specifications applicable to placing a TRPS or ESFAS SFM into maintenance bypass.	
44	3.6.3.8	An applicant or licensee referencing this SE must describe the setpoints, setpoint methodologies, or HIPS platform module accuracies used for a safety system implemented with the HIPS platform equipment.	Applicable. Subsections 7.4.3.11 and 7.5.3.10 (Setpoints) of the SHINE facility FSAR discusses the setpoints for the TRPS and ESFAS, respectively. Tables 7.4-1 and 7.5-1 respectively provide the accuracies required for the TRPS and ESFAS monitored variables.	TRPS Criterion 29, 30 and 32 ESFAS Criterion 30, 31 and 33
45	3.6.4.5	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for maintenance bypasses.	Applicable. Subsection 7.4.5 (Highly Integrated Protection System Design) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment is used for maintenance bypasses. For the SHINE application, maintenance bypasses are associated with the sense and command features only for the TRPS and ESFAS. There are no maintenance bypass capabilities associated with execute features in the SHINE application of the HIPS platform. Subsections 7.4.4.3 and 7.5.4.4 of the SHINE FSAR describe design for maintenance bypass in the TRPS and ESFAS, respectively.	TRPS Criterion 37 and 41 ESFAS Criterion 38 and 42

46	3.6.5	An applicant or licensee referencing this SE must describe power sources to the HIPS platform equipment and how they meet applicable regulatory requirements.	Applicable. The design bases description for the TRPS and ESFAS power source is provided in Section 8a2.2 of the SHINE facility FSAR. Division A of both the TRPS and ESFAS is powered from Division A of the uninterruptible power supply system (UPSS). Division B of both the TRPS and ESFAS is powered from Division B of the UPSS. Division C of both the TRPS and ESFAS receives auctioneered power from Division A and Division B of the UPSS. Both the TRPS and ESFAS require 125 VDC power, which the UPSS provides as described above. Each TRPS and ESFAS cabinet is provided a single 125 VDC power supply, which is used to power three (3) redundant 125 VDC to 24 VDC converters located at the top of the cabinet. The 24V supply is then distributed to each of three (3) chassis mounting bays as needed, where it is then used to power two (2) redundant 24 VDC to 5 VDC converters located beneath each chassis bay. These provide independent +5V A and +5V B power channels to each chassis.	SHINE Criterion 27.
47	3.7.1.5.2	An applicant or licensee referencing this SE must confirm that the manufacturer followed the same design, development, and iV&V processes for test and calibration	Applicable. The required quality and standards of TRPS and ESFAS programmable logic development processes are described in Subsection 7.4.5.4 (Software Requirements Development) of the SHINE facility FSAR. The calibration features	TRPS Criterion 4, 5, 6, 7, 8, 9, 10, 11, and 12 ESFAS Criterion 4, 5, 6, 7, 8, 9, 10, 11, and 12

		functions as for all other HIPS platform functions.	of the TRPS and ESFAS are designed, developed, and validated at the same level as the safety related functional logic. The calibration features of the TRPS and ESFAS are implemented independently from the safety functions of the system but are implemented on the same FPGA as the safety functions and are therefore designed, developed, and validated to the same rigor as the safety functions of the systems.	
48	3.7.1.5.2	An applicant or licensee referencing this SE that relies on a separate computer for the sole verification of test and calibration data should ensure adequate iV&V, configuration management, and quality assurance for the test and calibration functions of the separate computer.	Not applicable. A separate computer is not relied upon for the sole verification of test and calibration data for the TRPS and ESFAS.	Not applicable
49	3.7.1.5.3	An applicant or licensee referencing this SE must confirm that the manufacturer followed the same design, development, and iV&V processes for self-diagnostics functions as for all other HIPS platform functions.	Applicable. The required quality and standards of TRPS and ESFAS programmable logic development processes is described in Subsection 7.4.5.4 (Software Requirements Development) of the SHINE facility FSAR. The self-testing features of the TRPS and ESFAS are designed, developed, and validated at the same level as the safety related functional logic. The overlapped self-test features of the TRPS and ESFAS are integral to the operation of the system and are therefore designed, developed, and	TRPS Criterion 4, 5, 6, 7, 8, 9, 10, 11, and 12 ESFAS Criterion 4, 5, 6, 7, 8, 9, 10, 11, and 12

			validated to the same rigor as the safety functions of the systems.	
50	3.7.1.5.3	An applicant or licensee referencing this SE must verify that the manufacturer included the self-diagnostic functions within its type testing of the HIPS platform standardized circuit boards during EQ.	Applicable. Subsections 7.4.3.13 and 7.5.3.12 (Design Codes and Standards) of the SHINE facility FSAR respectively identify the required codes and standards to be used in qualifying the TRPS and ESFAS equipment, respectively. All HIPS self-diagnostic functions were included within the type testing of the HIPS platform circuit boards during EQ. Evidence of this is provided in the completed testing procedures which are included as part of the HIPS platform EQ testing results reports (References 6 and 7).	TRPS Criterion 4, 5, 6, 7, 8, 9, 10, 11, 12, and 47 ESFAS Criterion 4, 5, 6, 7, 8, 9, 10, 11, 12, and 48
51	3.7.1.5.3	An applicant or licensee referencing this SE must demonstrate that the combination of HIPS platform self-tests and system surveillance testing provide the necessary test coverage to ensure that there are no undetectable failures that could adversely affect a required safety function.	Applicable. As described in Subsections 7.4.4.4 and 7.5.4.5 (Testing Capability) of the SHINE facility FSAR, 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 and ESFAS components, except the discrete APL of the EIM, have self-testing capabilities that ensure the information passed on to the following step in the safety data path is correct. The TRPS and ESFAS Failure Modes and Effects Analysis (Reference 4) evaluated potential single failures and determined that	TRPS Criterion 47 ESFAS Criterion 48

			there are no undetectable failures that could adversely affect the required TRPS and ESFAS safety functions.	
52	3.7.1.6	An applicant or licensee referencing this SE must demonstrate that the full system design, any use of a shared component, the equipment's installation, and the communication bus architecture provide the required independence.	Applicable. Subsection 7.4.5.2.1 (Independence) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment implements physical, electrical, communications, and functional independence.	TRPS Criterion 18, 19, 20, 21, 22, 23, 24, 25, and 26 ESFAS Criterion 19, 20, 21, 22, 23, 24, 25, 26 and 27
53	3.7.1.6	An applicant or licensee referencing this SE must verify that the safety network provides communications independence and security requirements for communication from safety- to nonsafety-related systems.	Applicable. Subsection 7.4.5.2.1 (Independence) of the SHINE facility FSAR describes how the HIPS based TRPS and ESFAS equipment implements physical, electrical, communications, and functional independence.	TRPS Criterion 20 and 22 ESFAS Criterion 21 and 23
54	3.7.1.11	An applicant or licensee referencing this SE must establish the identification and coding requirements for cabinets and components for a safety system and the methods to verify that the correct firmware or software is installed in the correct hardware component.	Applicable. Subsections 7.4.5.4.6.3, 7.4.3.10, and 7.5.3.9 of the FSAR describe how the HIPS-based TRPS and ESFAS equipment design addresses equipment identification. The programmable logic lifecycle process includes automatically generating a unique FPGA logic design image number which is used as an FPGA logic design identification number. The FPGA logic design image number can be displayed on the MWS and is included on all logic design documentation and within the hardware description language (HDL) code for the image so the	TRPS Criterion 50 ESFAS Criterion 51

			user can verify the installed FPGA design against the logic design documentation. The FPGA logic design identity image number is included in the following logic development workflow outputs: • Programmable Logic Design Specifications • Programmable Logic Test Specifications • Programmable Logic Test Results • Requirements Traceability Matrix • The FPGA logic top level HDL code file The FPGA logic design image number is used as a system logic design configuration verification tool that verifies the correctness of the current system logic design within a chassis.	
55	3.8.1.1	An applicant or licensee referencing this SE must demonstrate that a full system design does not, with the exception of division voting logic, depend on any information or resource originating or residing outside its own safety division to accomplish its safety function.	Applicable. Subsection 7.4.5.2.1 (Highly Integrated Protection System Design) of the SHINE facility FSAR describes how the HIPS equipment implements divisional voting logic. Other than divisional voting logic, the TRPS and ESFAS do not depend on any information or resource originating or residing outside of each safety division to accomplish their safety functions.	TRPS Criterion 18, 20, and 21 ESFAS Criterion 19, 21, and 22
56	3.8.1.5	An applicant or licensee referencing this SE must confirm that system real-time performance is adequate, assuming the longest possible completion time to ensure the	Applicable. A response time analysis for the TRPS and ESFAS is discussed in Subsection 7.4.5.2.3 (Predictability and Repeatability) of the SHINE facility FSAR.	TRPS Criterion 23 and 24 ESFAS Criterion 24 and 25

		completion of protective actions within the critical time frames required by the plant safety analyses.		
57	3.8.1.12	An applicant or licensee referencing this SE must configure the slave modules (e.g., SFMs and EIMs) to alarm and assume a fail-safe state.	Applicable. A TRPS and ESFAS Failure Modes and Effects Analysis (Reference 4) was conducted for the TRPS and ESFAS, which evaluated each component of the systems, how it may fail, and what the effect of the failure on the systems would be in the presence of a single failure. Effects on the systems include assuming a fail-safe state, only alarm the failure, or assuming a fail-safe state and alarm the failure. Which of these effects occur depends on the mode of failure for each component and is documented in the FMEA.	TRPS Criterion 48 ESFAS Criterion 49
58	3.8.1.18	An applicant or licensee referencing this SE should verify having appropriate physical, logical, and programmatic controls during the system development phases to ensure that unwanted, unneeded, and undocumented functionality is not introduced into digital safety systems.	Applicable. Subsection 7.4.5.3.1 (Secure Development Operating Environment) and 7.4.5.4 (Software Requirements Development) of the SHINE facility FSAR describes the Secure Development Environment requirements for TRPS and ESFAS system development. As discussed in Subsection 7.4.5.4, the plans and procedures for the design/development, V&V activities, configuration management, and their associated documentation for completion of performance are to be provided by the TRPS and ESFAS vendor.	TRPS Criterion 2, 5, and 6 ESFAS Criterion 2, 5, and 6

59	3.8.1.19 3.8.1.20	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide a deterministic communication structure for required safety functions.	Applicable. TRPS and ESFAS integrity characteristics which support a deterministic communication structure are discussed in Subsection 7.4.5.2.3 (Predictability and Repeatability) of the SHINE facility FSAR.	TRPS Criterion 24 ESFAS Criterion 25
60	3.8.3.1.2	An applicant or licensee referencing this SE must demonstrate that the full system design supports cross-divisional and nonsafety communication with the appropriate independence and isolation.	Applicable. How communications independence is implemented within the TRPS and the ESFAS is discussed in Subsection 7.4.5.2.1 (Independence) of the SHINE facility FSAR.	TRPS Criterion 21 and 22 ESFAS Criterion 22 and 23
61	3.8.3.1.3	An applicant or licensee referencing this SE must demonstrate that the application-specific use of an enable nonsafety switch and its configuration details will not adversely affect the channel independence nor the operation of safety-related equipment when the safety-related equipment is performing its safety function. In addition, the applicant or licensee must demonstrate that the application-specific use of an enable nonsafety switch should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.	Applicable. The use of an enable nonsafety switch and associated priority logic within the TRPS and ESFAS is described in Subsection 7.4.5 (Highly Integrated Protection System Design) of the SHINE facility FSAR. Specific logic diagrams for how the enable nonsafety switch is implemented in TRPS and ESFAS logic is provided in Figures 7.4-1 and 7.5-1, respectively. Use of the enable nonsafety switch is also discussed in Subsections 7.4.3 and 7.5.3 of the SHINE facility FSAR.	Not applicable

62	3.9.1 3.9.2	An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide FPGA diversity between redundant portions of the systems to eliminate HIPS platform digital CCF vulnerabilities.	Partially applicable. Implementation of diversity within the TRPS and the ESFAS is discussed in Subsection 7.2.2.4 (Diversity) and Subsection 7.2.2.5 (Simplicity) of the SHINE facility FSAR. An assessment of the design and implementation of diversity within the TRPS and ESFAS and the allocation of the safety functions among the diverse divisions to mitigate the effects of SHINE FSAR Chapter 13 events is provided in the Diversity and Defense-in-Depth Assessment of the TRPS and ESFAS (Reference 5).	TRPS Criterion 16 ESFAS Criterion 16
63	3.9.2 3.9.3	An applicant or licensee referencing this SE must address any other digital CCF vulnerabilities in the application-specific D3 analysis.	Applicable. Implementation of diversity within the TRPS and the ESFAS is discussed in Subsection 7.2.2.4 (Diversity) and Subsection 7.2.2.5 (Simplicity) of the SHINE facility FSAR. An assessment of the design and implementation of diversity within the TRPS and ESFAS and the allocation of the safety functions among the diverse divisions to mitigate the effects of SHINE FSAR Chapter 13 events is provided in the Diversity and Defense-in-Depth Assessment of the TRPS and ESFAS (Reference 5).	TRPS Criterion 16 ESFAS Criterion 16
64	3.9.3	An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide FPGA diversity between redundant portions of the system architecture (e.g., in each of two redundancies in a four-fold	Partially applicable. Implementation of diversity within the TRPS and the ESFAS is discussed in Subsection 7.2.2.4 (Diversity) and Subsection 7.2.2.5 (Simplicity) of the SHINE facility FSAR. The TRPS and ESFAS are both implemented with 3 redundant divisions. Each of the three divisions requires a different type of FPGA to	TRPS Criterion 16 ESFAS Criterion 16

		redundant system or in one redundancy in a two-fold redundant system) to ensure HIPS platform safety performance in the presence of a digital CCF.	address a potential CCF of one type of FPGA. The three types of FPGAs implemented on the divisional modules is as follows: • Division A: Microsemi IGLOO2 (FLASH based FPGA) • Division B: Intel MAX10 (Hybrid Flash and SRAM based FPGA) • Division C: Altera Artix-7 (SRAM based FPGA) An assessment of the design and implementation of diversity within the TRPS and ESFAS and the allocation of the safety functions among the diverse divisions to mitigate the effects of SHINE FSAR Chapter 13 events is provided in the Diversity and Defense-in-Depth Assessment of the TRPS and ESFAS (Reference 5).	
65	3.9.4	An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide diversity for indication and component control signals to ensure HIPS platform monitoring and control performance in the presence of a digital CCF.	Partially applicable. Implementation of diversity within the TRPS and the ESFAS is discussed in Subsection 7.2.2.4 (Diversity) and Subsection 7.2.2.5 (Simplicity) of the SHINE facility FSAR. An assessment of the design and implementation of diversity within the TRPS and ESFAS and the allocation of the safety functions among the diverse divisions to mitigate the effects of SHINE FSAR Chapter 13 events is provided in the Diversity and Defense-in-Depth Assessment of the TRPS and ESFAS (Reference 5).	TRPS Criterion 16 ESFAS Criterion 16

4 Conclusions

Each application specific action item identified in the final safety evaluation report for the HIPS platform topical report (Reference 1) was evaluated for applicability to SHINE's medical isotope production facility licensing application. The resulting applicability determination was documented in Table 3-1, and if the ASAI was determined to be not applicable, justification for why it was not considered applicable was provided. If the ASAI was determined to be applicable, a reference was provided for either the appropriate sections of the SHINE facility FSAR or the appropriate design basis document which provides evidence that the applicable action items have been adequately addressed for the design of the TRPS and ESFAS.

5 HIPS Platform Modifications

This section identifies modifications and additions to the fundamental HIPS platform equipment design and functionality described in the HIPS platform topical report (Reference 1) which are to be implemented as part of the TRPS and ESFAS designs. This section does not describe the differences between the representative architecture presented in the topical report and the application specific equipment architectures for the TRPS and ESFAS.

5.1 Hardwired Module Input Routing

Section 2.5.2 of the HIPS platform topical report states that Trip/ Bypass inputs to the Hardwired Modules are "routed only to the scheduling and bypass modules (SBMs) where it is used." There are two differences for this statement in the TRPS and ESFAS designs. This first is that the inputs to the Hardwired Modules are used at the SBMs (Division C), the SBVMs (Divisions A and B), the MICMs (for monitoring and indication information), and also at the EIMs for manual actuation of protective functions and manual nonsafety functions. The second difference is that the inputs to the Hardwired Modules are made available to all modules in the same chassis. The modules listed above utilize the signals that are made available on the backplane from the Hardwired Modules.

Additionally, discussion of the use of the trip/bypass switches with the SBMs in the topical report applies the same to the use of the trip/bypass switches with the SBVMs in Divisions A and B of the TRPS and ESFAS designs.

5.2 Use of Fiber Optic Communications

Sections 2.5.3, 4.3, and 4.6.2 of the HIPS platform topical report describes the use of fiber optic ports for inter-divisional transmit-only or receive-only fiber optic ports. The TRPS and ESFAS designs do not use fiber optic ports for inter-divisional communications. The inter-divisional communications in the TRPS and ESFAS are implemented with transmit-only or receive-only copper RS-485 connections.

5.3 Communications Module (CM) Bi-Directional Communications

Section 2.5.3 of the HIPS platform topical report discusses transmit-only or receive-only communications for a CM. The TRPS and ESFAS designs utilize CMs (see discussion of the gateway communications modules in Section 5.5.2 below) in Divisions A and B to communicate bi-directionally with the PICS via the MODBUS protocol. This is justified because the function of these CMs is non-safety related and the information which is provided to the PICS from these CMs is received from each division of the TRPS or ESFAS via transmit-only isolated connections.

5.4 Implementation of EIM Switching Outputs

Section 2.5.4.4 of the HIPS Platform topical report states that each EIM "can control two groups of field components and each group can have up to two field devices." The HIPS platform has been modified

for the TRPS and ESFAS designs such that each EIM can control up to eight field devices. Also, the redundancy of dual high side and dual low side contacts for each output switch is not implemented in the TRPS and ESFAS EIM designs. This is acceptable because the actuation loads for the SHINE application are small solenoids which does not justify using the dual high side and dual low side arrangement and allows for a higher density of outputs per EIM.

5.5 Specific Implementation of Communications Modules

5.5.1 Scheduling, Bypass, and Voting Modules

Throughout the HIPS platform topical report, the use of Scheduling and Bypass Modules (SBM) and Scheduling and Voting Modules (SVM) is discussed as part of a “representative architecture” which is provided in the topical report to help describe the design principles implemented within the HIPS platform. Both modules are example types of the HIPS Platform Communications Module. The TRPS and ESFAS designs utilize a type of Communications Module that is referred to as a Scheduling, Bypass, and Voting Module (SBVM) in Divisions A and B. The SBVM combines all functions, capabilities, and design principles described in the topical report for a SBM and a SVM into a single module. This was implemented to minimize the total number of HIPS hardware modules necessary for the required TRPS and ESFAS functionality. As such, the use of a SBVM in the TRPS and ESFAS designs does not represent a modification or addition to the HIPS Platform as described in the topical report, however it is identified in this section to explain the apparent use of a different module from that described in the topical report.

Since the SVM functionality on each SBVM will load each of the specific TRPS or ESFAS application’s voting registers with the partial trip determination actuation (PTDA) information received by its SBM functionality, Figure 7-8 of the topical report is modified as shown in Figure 5-1 below to add a note that the “Wait for Sync” is not necessary for the SBVMs. In Figure 5-1, because the TRPS and ESFAS implement 1oo2, 2oo2, or 2oo3 voting, which is different from the 2oo4 voting discussed in the HIPS platform topical report for the representative architecture, the 2oo4’s have also been removed from the HIPS platform topical report. This figure has also been modified to show the three TRPS/ESFAS divisions as opposed to the four divisions of the representative architecture in the HIPS platform topical report.

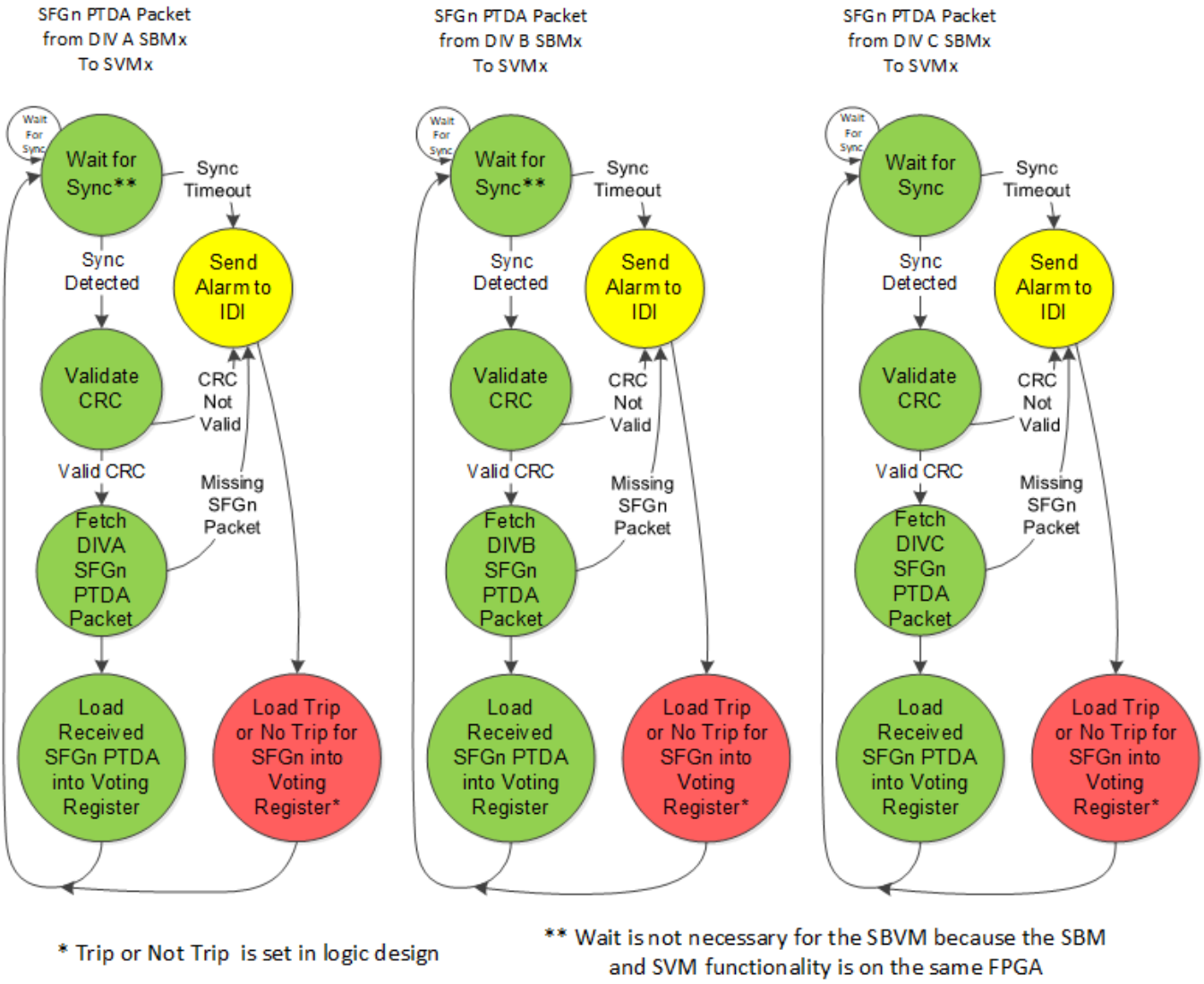


Figure 5-1: SBVM MOD_OK – Loading Voting

5.5.2 Gateway Communications Modules

The gateway communications module (GWCM) is a HIPS platform communications module not described in the HIPS platform topical report which performs only nonsafety related monitoring and indication functions. TRPS and ESFAS monitoring and indication information is transmitted redundantly from each system's divisional monitoring and indication communications module (MICM) via one-way isolated RS-485 connections to respective redundant nonsafety GWCMs, which are located in two redundant gateway chassis. The GWCMs for the TRPS are functionally and logically independent from the GWCMs for the ESFAS and vice versa. As described in Section 2.5.3 of HIPS platform topical report, the GWCMs, which are HIPS platform communications modules, have four communications ports, each of which can be configured as receive-only or transmit-only. Three of the four communications ports of each GWCM are configured as receive-only ports for their respective status and diagnostics information input. The fourth communications port of each GWCM is configured for two-way communications with the respective PICS channel using the MODBUS communications protocol. Two-way communication is a departure from the HIPS platform topical

report description of a communications module. This is acceptable because the communication from the GWCM is a nonsafety function, and the upstream communication from each MICM to a GWCM is isolated and one-way only.

5.6 SBVM Safety Data Bus Frame

As discussed above in Section 5.5, the TRPS and ESFAS utilize an SBVM which performs the functions described in the HIPS platform topical report for both the SBM and the SVM. Sections 7.6.3 through 7.7.1 of the topical report describe the operations and safety data bus frames for the SBM and SVM. The TRPS and ESFAS will incorporate a change to how the SBVM votes on the PTDA and communicates actuation data to the EIMs. Instead of sending separate trip determination actuation (TDA) information for each safety function group (SFG) to the EIMs, all safety function groups are voted on at the same time and the TDA for all SFGs are then transferred to the EIMs at once. For this change, Figure 7-12 of the topical report is modified to show a single transaction below in Figure 5-2 for the TRPS and ESFAS implementation.

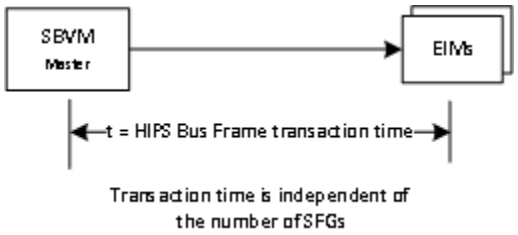


Figure 5-2: SBVM HIPS Bus Frame Transaction Time

Figure 7-14 of the topical report is modified simply to show the SBM and SVM functionality being performed by the SBVM module (dashed box) as shown below in Figure 5-3.

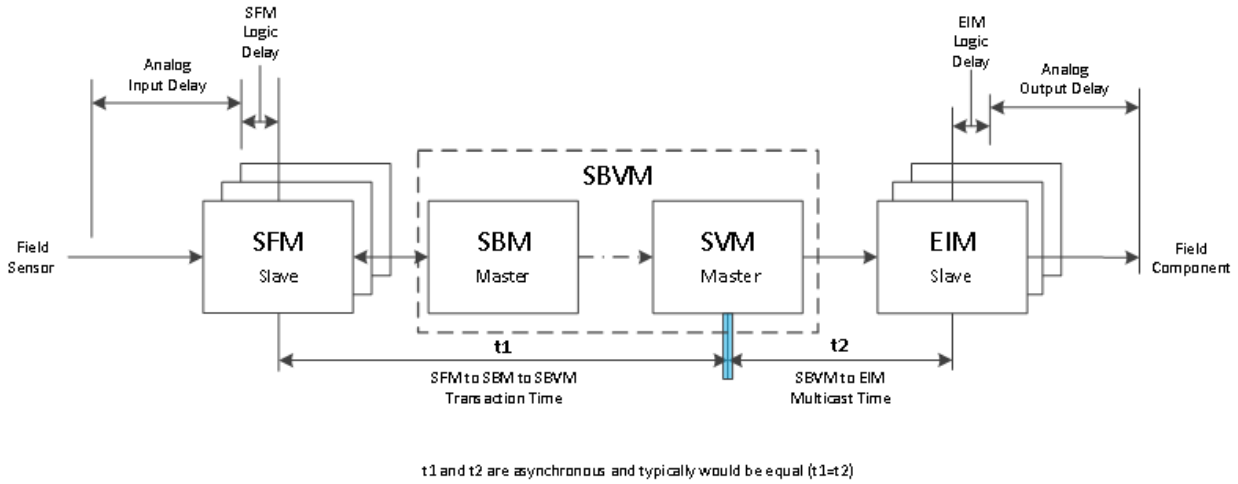


Figure 5-3: Timing diagram for the TRPS and ESFAS

5.7 Self-Testing

5.7.1 Analog to Digital Converter

Sections 7.1.1 and 8.2.1 of the HIPS platform topical report describe the self-testing features for the analog to digital converter (ADC) for an analog input submodule (ISM). The auto-calibration function described included the use of external passive components, whereas the TRPS and ESFAS designs will incorporate the critical passive components onto the ADC chip. This results in very precise values

that are factory calibrated and are significantly less prone to drift over time and temperature, therefore the auto-calibration function is not implemented for the TRPS and ESFAS designs.

5.7.2 EIM Input and Output Testing

The self-testing described in Sections 8.2.3.2 and 8.2.3.4 of the HIPS platform topical report for discrete input circuitry (open/closed contact tests) and high drive output testing is not being implemented for the TRPS and ESFAS designs. These tests were not implemented as they would require interaction between the FPGA logic and the analog APL circuitry, and it was desired to keep the interface between the FPGA and APL as simple as possible.

5.7.3 HWM Input Channel Test

The self-test identified in Section 8.2.7 of the HIPS platform topical report for HWM input signals is not being implemented for the TRPS and ESFAS designs. This test is also not implemented because it would require interaction of the FPGA with the hardwired input circuitry (used for manual protection system actuation) and it was desired to not allow any interface of the FPGA with this capability.

5.8 HIPS Module LEDs

Section 8.2.7 of the HIPS platform topical report identifies that LED tests will be performed to identify if an incorrect LED status is being displayed. This test will not be performed on a continuous basis for the TRPS and ESFAS designs for the following reasons:

- Module front panel indication is not a safety function
- Correct LED operation will be tested as part of factory and installation testing

Section 8.4 of the HIPS platform topical report describes the two LEDs on the front of each HIPS module which are used to indicate the state of the module latches, the operational state of the module, and the presence of any faults for the module. The TRPS and ESFAS designs will include the following changes to the function of the LEDs from that presented in the topical report:

- The ACTIVE LED will turn Red on a vital fault or when the module has one latch open
- The FAULT LED will never flash and not turn Red
- The FAULT LED will turn Yellow for any fault (non-vital or vital)

5.9 Remote Input Submodule (RISM)

The RISM is a new module which is not discussed in the HIPS platform topical report. The RISM is directly associated with a single SFM that allows for remotely locating one ISM from its associated SFM. The ISM used on a RISM is the same as described in the HIPS platform topical report for an ISM with the modification described above in Section 5.7. The ISM can be configured for a specific input type and calibrated as described in the HIPS platform topical report for the SFM.

Once an input channel is in digital format on the ISM, the input information is provided by the RISM via an isolated, one-way RS-485 connection to its associated SFM within the division for triplication and trip determination. There is an additional RS-485 connection between the RISM and its associated SFM which independently supports modification of tunable parameters necessary on the RISM.

6 IEEE Std. 7-4.3.2-2003 Traceability Matrix

This section provides a summary of conformance of the TRPS and ESFAS with IEEE Std. 7-4.3.2-2003.

Table 6-1: TRPS and ESFAS IEEE Std. 7-4.3.2-2003 Traceability Matrix

IEEE Std. Section Number	Section	TRPS/ESFAS Conformance
5.1	Single Failure Criteria	N/A
5.2	Completion of Protective Action	N/A
5.3	Quality	N/A
5.4	Equipment Qualification	N/A
5.5	System Integrity	
5.5.1	Design for Computer Integrity	See responses to ASAIs 18 and 19 in Table 3-1 above.
5.5.2	Design for Test and Calibration	See responses to ASAIs 47 and 48 in Table 3-1 above.
5.5.3	Fault Detection and Self-diagnostics	See responses to ASAIs 49, 50, and 51 in Table 3-1 above.
5.6	Independence	See responses to ASAIs 52 and 53 in Table 3-1 above.
5.7	Capability for Test and Calibration	N/A
5.8	Information Displays	N/A
5.9	Control of Access	N/A
5.10	Repair	N/A
5.11	Identification	N/A
5.12	Auxiliary Features	N/A
5.13	Multi-Unit Stations	N/A
5.14	Human Factors Consideration	N/A
5.15	Reliability	N/A
6	Sense and Command Features	N/A
7	Execute Features	N/A
8	Power Source Requirements	N/A

7 Digital I&C Interim Staff Guidance 04 Traceability Matrix

This section provides a summary of conformance of the TRPS and ESFAS with DI&C-ISG-04.

Table 7-1: TRPS and ESFAS DI&C-ISG-04 Traceability Matrix

ISG-04 Section Number	Requirement	TRPS/ESFAS Conformance
1	**Interdivisional Communications**	
SP 1	A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE Std. 603. It is recognized that division voting logic must receive inputs from multiple safety divisions.	See responses to ASAIs 8, 22, 23, and 55 in Table 3-1 above.
SP 2	The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division) and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.	See responses to ASAIs 8, 20, 21, 22, and 23 in Table 3-1 above.
SP 3	A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, on-line monitoring). Such a function	See responses to ASAI 22 in Table 3-1 above.

	executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.	
SP 4	The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function	N/A

	processor is unable to gain access to the shared memory.	
SP 5	The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.	See responses to ASAI 56 in Table 3-1 above.
SP 6	The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	N/A
SP 7	Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.	N/A
SP 8	Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.	See responses to ASAI 22 in Table 3-1 above.
SP 9	Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.	N/A
SP 10	Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hard-wired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g.,	N/A

	engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hard-wired logic. "Hard-wired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.	
SP 11	Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.	N/A
SP 12	Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:	N/A
	• Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.	N/A
	• Messages may be repeated at an incorrect point in time.	N/A

	• Messages may be sent in the incorrect sequence. • Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message. • Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.	
	• Messages may be inserted into the communication medium from unexpected or unknown sources.	N/A
	• Messages may be sent to the wrong destination, which could treat the message as a valid message.	N/A
	• Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.	N/A
	• Messages may contain data that is outside the expected range.	N/A
	• Messages may appear valid, but data may be placed in incorrect locations within the message.	N/A
	• Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).	N/A
	• Message headers or addresses may be corrupted.	N/A
SP 13	Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.	See responses to ASAI 32 in Table 3-1 above.
SP 14	Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.	N/A

SP 15	Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.	N/A
SP 16	Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE Std. 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.)	See responses to ASAIs 8, 20, 21, 22, and 23 in Table 3-1 above.
SP 17	Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.	See responses to ASAI 17 in Table 3-1 above.
SP 18	Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	See responses to ASAIs 12 and 58 in Table 3-1 above.
SP 19	If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.	See responses to ASAIs 19 and 59 in Table 3-1 above.
SP 20	The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.	See responses to ASAIs 18, 19, and 59 in Table 3-1 above.
2	**Command Prioritization**	
SP 1	A priority module is a safety related device or software function. A priority module must meet all of the 10 C.F.R. Part 50, Appendix A and B	N/A

	requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.	
SP 2	Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.	N/A
SP 3	Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a common-cause failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated “safe state.”), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as a containment isolation valve in an auxiliary feedwater line, there is no universal “safe state:” the valve must be open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.	N/A
SP 4	A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.	N/A
SP 5	Communication isolation for each priority module should be as described in the guidance for interdivisional communications.	N/A
SP 6	Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in RG 1.152, which endorses IEEE Std. 7- 4.3.2-2003 (with comments). This includes software applicable to	N/A

	any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices, programmable gate arrays, or other such devices. Section 5.3.2 of IEEE Std. 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.	
SP 7	Any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.	N/A
SP 8	To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all	N/A

	conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the "all possible combinations" testing.	
SP 9	Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and including failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute common-cause failure if it were to result in the disabling of the module safety function.	N/A
SP 10	The priority module must ensure that the completion of a protective action as required by IEEE Std. 603 is not interrupted by commands, conditions, or failures outside the module's own safety division.	N/A
3	**Multidivisional Control and Display Systems**	
3.1	**Independence and Isolation**	
SP 1	Nonsafety stations receiving information from one or more safety divisions:	N/A
SP 2	Safety-related stations receiving information from other divisions (safety or nonsafety):	See responses to ASAI 60 in Table 3-1 above.
SP 3	Nonsafety stations controlling the operation of safety-related equipment:	See responses to ASAI 61 in Table 3-1 above.
SP 4	Safety-related stations controlling the operation of equipment in other safety-related divisions:	N/A
SP 5	Malfunctions and Spurious Actuations	N/A
3.2	Various human factors engineering requirements.	N/A
3.3	D3 considerations may influence the number and disposition of operator workstations and possibly of backup controls and indications that may or may not be safety-related. The guidance provided herein is not dependent upon such details. D3 considerations may also impose qualification or other measures or guidelines upon equipment addressed in this ISG. The guidance presented herein does not include such considerations. Consideration of other aspects of D3 is outside the scope of this guidance. Additional guidance concerning D3 considerations is provided separately.	N/A

8 SRM for SECY-93-087 Traceability Matrix

This section provides a summary of conformance of the TRPS and ESFAS with SECY-93-087.

Table 8-1: TRPS and ESFAS SECY-93-087 Traceability Matrix

SRM Section Number	Requirement	TRPS/ESFAS Conformance
1	The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed. The staff considers software design errors to be credible common-mode failures that must specifically be included in the evaluation. An acceptable method of performing analyses is described in NUREG-0493, "A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979. Other methods proposed by an applicant will be reviewed individually.	See responses to ASAIs 9 and 62 in Table 3-1 above.
2	In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR). The vendor or applicant shall demonstrate adequate diversity within the design for each of these events. For events postulated in the plant SAR, an acceptable plant response should not result in a non-coolable geometry of the core, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment.	See responses to ASAIs 9, 10, 62, and 63 in Table 3-1 above.
3	If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. Diverse digital or nondigital systems are considered acceptable means. Manual actions from the control room are acceptable if adequate time and information are available to the operators. The amount and types of diversity may vary among designs and will be evaluated individually.	See responses to ASAIs 9, 10, 63, and 64 in Table 3-1 above.
4	A set of safety-grade displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and	See responses to ASAIs 10 and 65 in Table 3-1 above.

	diverse from the safety computer system identified in items I and 3 above. The specific set of equipment shall be evaluated individually, but shall be sufficient to monitor the plant states and actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition. In addition, the specific equipment should be intended to control the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.	

9 References

1. NuScale Power, LLC, TR-1015-18653-NP-A, “Design of the Highly Integrated Protection System Platform,” Revision 2, September 2017, NRC ADAMS Accession No. ML17256A892
2. U.S. Nuclear Regulatory Commission Letter, “Final Safety Evaluation for NuScale Power, LLC Licensing Topical Report: 1015-18653, “Design of the Highly Integrated Protection System Platform,” Revision 2,” dated June 6, 2017, ADAMS Accession No. ML17116A094.
3. SHINE Medical Technologies, 2000-09-01, “Quality Assurance Program Description (QAPD).”
4. Rock Creek Innovations, SMT-016-1000-64012, “Failure Modes and Effects Analysis,” Revision 3, August 24, 2021
5. SHINE Medical Technologies, TECRPT-2019-0041, “Diversity and Defense-in-Depth Assessment of TRPS and ESFAS,” Revision 3, September 6, 2021
6. SHINE Medical Technologies, TECRPT-2019-0048, “TRPS System Design Description,” Revision 4, August 19, 2021
7. SHINE Medical Technologies, TECRPT-2020-0002, “Engineered Safety Features Actuation System Design Description,” Revision 4, August 20, 2021
8. Rock Creek Innovations, RCI-942-1000-61000, “Environmental and Seismic Qualification Report for HIPS Platform EQTS,” Revision 2, June 2, 2021
9. Rock Creek Innovations, RCI-942-1000-61001, “EMC and Isolation Qualification Report for HIPS Platform EQTS,” Revision 0, September 2, 2021