August 27, 2021

2021-SMT-0111
10 CFR 50.30

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

References: (1) SHINE Medical Technologies, LLC letter to the NRC, "SHINE Medical Technologies, LLC Application for an Operating License," dated July 17, 2019 (ML19211C143)
(2) 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)

SHINE Medical Technologies, LLC Application for an Operating License
Response to Request for Additional Information

Pursuant to 10 CFR Part 50.30, SHINE Medical Technologies, LLC (SHINE) submitted an application for an operating license for a medical isotope production facility to be located in Janesville, WI (Reference 1). The NRC staff determined that additional information was required to enable the staff's continued review of the SHINE operating license application (Reference 2).

Enclosure 1 provides the SHINE Response to the NRC staff's request for additional information (RAIs), with the exception of RAI 7-9 and RAI 7-10. The SHINE Response to these remaining RAIs will by provided by September 30, 2021.

If you have any questions, please contact Mr. Jeff Bartelme, Director of Licensing, at 608/210-1735.

I declare under the penalty of perjury that the foregoing is true and correct.
Executed on August 27, 2021.

Very truly yours,

DocuSigned by:
Jim Costedio
F52DB96989224FF...

James Costedio
Vice President of Regulatory Affairs and Quality
SHINE Medical Technologies, LLC
Docket No. 50-608

Enclosures

cc: Project Manager, USNRC
SHINE General Counsel
Supervisor, Radioactive Materials Program, Wisconsin Division of Public Health

**ENCLOSURE 1**

**SHINE MEDICAL TECHNOLOGIES, LLC**

**SHINE MEDICAL TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

**SHINE MEDICAL TECHNOLOGIES, LLC**

**SHINE MEDICAL TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

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).”

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.

[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.

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).

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

[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.

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**

The SHINE Response to RAI 7-9 will by provided by September 30, 2021.

**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**

The SHINE Response to RAI 7-10 will by provided by September 30, 2021.

**RAI 7-11**

NUREG-1537, Part 2, Section 7.4, states, in part, that the protection system should be "designed to perform its safety function after a single failure and to meet requirements for seismic and environmental qualification, redundancy, diversity, and independence." NUREG-1537, Part 2, Section 7.4, also states that the protection systems should be reliable and perform their intended safety functions under all conditions. Therefore, the design of the protection systems should consider features that can improve the reliability of the system such as independence, redundancy, diversity, maintenance, testing, and quality components.

SHINE Design Criterion 15 and TRPS Criteria 16, 17, 21, 22, 37, and 41 require the safety system not be susceptible to a single failure. (Similar criteria are also identified for the ESFAS in the SHINE FSAR.) The SHINE FSAR states that to increase reliability and address single failures, the HIPS equipment for TRPS and ESFAS includes redundancy, such that no single failure can prevent a safety actuation when required. Section 7.4.3.2, "Mode Transition," of the SHINE FSAR describes how the system design addresses the single failure criterion by implementing a system architecture comprised of three divisions of signal condition and trip determination, and two divisions of voting and actuation.

Because redundant systems can be compromised by a potential vulnerability to a CCF, the use of diversity within a safety system can be one acceptable means to address the potential for a CCF. Taking this into account, the licensee identified SHINE Design Criterion 16 to require 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. The approved TR for the HIPS platform describes the diversity attributes utilized in the base HIPS platform (i.e., equipment diversity, design diversity, and functional diversity). The approved HIPS TR identifies ASAIs 11 and 62 as requiring the licensee to demonstrate how diversity would be implemented in its application when referencing the TR in a site-specific application. Section 7.4.2.1.4 of the SHINE FSAR describes how the TRPS design address SHINE Design Criterion 16 by incorporating the diversity principles outlined in the NRC approved HIPS TR. Further, Section 7.4.5.2.4 of the SHINE FSAR describes diversity attributes, such as diversity within the equipment, considered in the HIPS design for the TRPS and ESFAS. This section also references the HIPS TR for further information on diversity.

The NRC staff agrees that using three redundant divisions with appropriately configured multiple FPGA technologies can ensure accomplishment of safety functions even in the presence of random failures, and that using diverse FPGAs provides diverse means to address vulnerabilities against CCFs. However, additional information is needed to evaluate how the diversity attributes of the HIPS platform for the TRPS and ESFAS (i.e., equipment diversity, design diversity, and functional diversity) assure performance of safety functions under all postulated random and CCFs.

Update the SHINE FSAR to describe the design, configuration, and implementation considered for the HIPS equipment for the TRPS and ESFAS to address single failure and vulnerabilities to CCFs.

The NRC staff need this information for making a finding that the TRPS and ESFAS will perform the required protective actions in the presence of any single failure or malfunction, address vulnerabilities against CCFs, and meet the identified design criteria for single failure. Further, this information 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.”

The following are examples of the types of information the NRC staff needs to evaluate how the TRPS and ESFAS meet the single failure criterion and use of diversity to address vulnerabilities to CCFs. SHINE should ensure that the response to this RAI addresses 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:

- Identification and assessment of potential vulnerabilities to CCFs

- Description of how the use of three FPGA technologies is used to decrease susceptible to CCFs. The HIPS TR described the conceptual design for two diverse FPGA technologies in a 4-channel architecture to demonstrate acceptable performance in presence of potential CCFs

- Description of diversity attributes included in the HIPS equipment for the TRPS and ESFAS relied upon to protect against digital CCFs

- Design and implementation of built-in diversity within the TRPS and ESFAS, and allocation of the safety functions among the diverse divisions to mitigate the effects of postulated failures

**SHINE Response**

Single failures and vulnerabilities to common cause failures (CCFs) are addressed through the performance of a single failure analysis and a diversity and defense-in-depth (D3) assessment. A discussion of how the single failure analysis addresses single failures is provided in the SHINE Response to RAI 7-12.

The D3 assessment was performed on the target solution vessel (TSV) reactivity protection system (TRPS) and engineered safety features actuation system (ESFAS) and identified potential vulnerabilities to digital-based CCFs. The D3 assessment used the guidance provided in NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of the Reactor Protection Systems” (Reference 3).

The D3 assessment analyzed digital-based CCFs but considers these CCFs to be beyond design basis.

The D3 assessment concluded that:

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

The D3 assessment was performed by dividing the safety-related protection systems and interconnected systems into blocks that allow for an abstract view of the system and its interconnections. These blocks consist of the monitoring and indication block, manual controls block, safety blocks, sensor blocks, and process integrated control system (PICS). The safety blocks are associated with the TRPS and ESFAS.

The identification of these blocks allowed for a diversity assessment against the following diversity attributes:

- Design Diversity
- Equipment Diversity
- Functional Diversity
- Human Diversity
- Software Diversity

Two types of diversity assessments were performed: diversity attributes within a block and diversity attributes between blocks. A summary of these assessments follows.

**Diversity Attributes within a Block**

Software Diversity: A safety block is composed of at least four types of the following field programmable gate array (FPGA)-based modules and sub- modules: safety function modules (SFMs), scheduling and bypass modules (SBMs), scheduling and voting modules (SVMs), monitoring and indication communication module (CM), and equipment interface modules (EIMs). Since each type of module performs different functions, the logic implementations are expected to differ significantly.

Design Diversity: A safety block utilizes design diversity within its inter- and intra-divisional communication. Intra-divisional communication between SFMs and SBMs or SFMs and SVMs utilize a virtual point-to-point bidirectional serial communication. Inter-divisional communication from SBMs to SVMs, from SVMs to SVMs, or from CM to other systems use one-way communication. Intra-divisional communication between SVMs and EIMs uses a point-to-multipoint communication protocol that results in SVMs not having to request information from EIMs.

Each EIM implements a digital and analog method for initiating protective actions. The automatic signal actuation is generated within the digital portion (i.e., FPGA) of the EIM. The manual signal actuation originates from the physical switches in the manual controls block. In the EIM, both manual and automatic actuation signals are used by the actuation and priority logic (APL) that is implemented using discrete analog components.

Functional Diversity: SFMs are configured and programmed for different purposes. The safety functions implemented within an SFM are based on its inputs. This results in SFM implementations performing different functions.

Each EIM can control four groups of field components. Limiting the number of components that an EIM can control results in EIMs configured for functions only associated with those groups of components. For example, an EIM may be required to close valves on an irradiation unit (IU) Cell Safety Actuation while another EIM opens breakers to perform a Driver Dropout actuation. Although there are instances where EIMs implement different safety functions, there are certain EIMs that implement more than one safety function. For example, an EIM associated with the high voltage power supply (HVPS) breakers may be needed for IU Cell Safety Actuation and a Driver Dropout actuation signal.

By configuring the SFMs such that their implementations receive different inputs and perform different functions and by limiting the number of field components that an EIM can control, functional diversity is achieved within the safety blocks by having multiple methods of detecting anticipated operational occurrences and postulated accidents.

Within the monitoring and indication block there are two types of displays (i.e., displays that provide operators capability for both indication and control and displays that provide indication only). Displays providing both indication and control receive and transmit information to components within the PICS block. The different purposes and different input sources of the displays results in functional, software and design diversity within the same block.

The PICS block provides a degree of functional diversity by segmenting I/O networks by system and facility location.

## Diversity Attributes Between Blocks

### Human Diversity

The use of different instrumentation and controls (I&C) platforms creates inherent human diversity between certain blocks. Each I&C system implements different functions with different hardware architectures. Safety blocks are primarily designed for safety-related actuation based on trip or no-rip indication. PICS is primarily designed for monitoring and control of process parameters. Monitoring and indication blocks have a primary purpose of providing information to the operator and accepting operator input. Human diversity is an implicit attribute of the FPGA equipment, chip design, and software tool diversity of the Safety Block; however, it is neither explicitly defined nor verified for this block.

### Equipment Diversity

Equipment diversity is the use of different equipment to perform similar safety functions.

Initiation of protective actions can be done manually by operators using physical switches or done automatically by safety blocks associated with the TRPS and ESFAS.

Between blocks, fundamentally different FPGA technology is used to achieve equipment diversity. At the chip level, the three FPGA types operate in fundamentally different ways during operation and programming. The FPGAs require different internal subcomponents and different manufacturing methods. FPGA equipment diversity in the form of three fundamentally different FPGA technologies when coupled with the different development tools is an effective solution for the digital-based CCF vulnerabilities present in the HIPS platform.

### Design Diversity

Design diversity is the use of different approaches including both software and hardware to solve the same or similar problem.

To limit the potential and the consequences of a digital-based CCF, different FPGA chip architecture or different equipment manufacturers are used. The diverse FPGA technologies or manufacturers inherently have additional design diversity attributes based on the different development tools used for each FPGA technology. This equipment and tool diversity results from the different FPGA chip architectures and programming methods. The diversity in FPGA equipment, chip designs, and development tools arethe fundamental methods for mitigating the potential for digital-based CCFs since these diversity attributes directly mitigate CCFs associated with a specific FPGA technology.

### Software Diversity

Software diversity is a subset of design diversity and is the use of different programs designed andimplemented by different development groups with different key personnel to accomplish the same safety goals.

Due to the design diversity discussed above for the FPGA equipment, the use of different programmable technologies results in the use different design tools that would not introduce the same failure modes.

Functional Diversity

Functional diversity is introduced by having different purposes and functions between blocks.

Safety blocks are associated with the TRPS and ESFAS. These blocks will initiate protective actions if operating limits are exceeded to prevent or mitigate design basis events (DBEs).

Monitoring and indication blocks allow for an operator to monitor and control both safety and non-safety systems. The operator can maintain a plant within operating limits or initiate necessary protectiveactions.

PICS provides automatic control of systems to maintain the plant within operating limits including constraining certain operational transients.

Sensor blocks function to provide parameter information to the safety blocks.

SHINE has revised Subsection 7.4.5.2.4 of the FSAR to provide a description the D3 assessment. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

**RAI 7-12**

NUREG-1537, Part 2, Section 7.4 states, in part, that the shutdown function of the protection system should be fail-safe against malfunction and electrical power failures.

SHINE Design Criteria 16 and 17 require the protection systems be designed to fail into a safe state if conditions such as disconnection of the system, loss of power, or postulated adverse environments are experienced. Further, TRPS Criterion 16 requires the system be designed to perform its protective functions after experiencing a single random active failure in non-safety control systems or in the TRPS, and such failure should not prevent the TRPS, and credited passive redundant control components, from performing its intended functions.

Section 7.4.2.1.4 of the SHINE FSAR describes how the TRPS design would meet SHINE Design Criterion 16; and Section 7.4.2.1.5 of the SHINE FSAR describes how the TRPS would meet SHINE Design Criterion 17. However, the descriptions provided focus on independence of the safety systems, as well as the requirement for the systems to be protected from earthquakes, adverse environmental conditions, and loss of power. These descriptions do not cover what known failures can affect the systems, how they would be addressed, and the fail-safe state of variables controlled by the safety systems. Also, the provided descriptions in the SHINE FSAR do not demonstrate whether failures of other systems, especially connected non-safety systems, would not prevent the TRPS from performing its safety function.

The TRPS and ESFAS are credited for the safe operation of the SHINE facility. Therefore, the SHINE FSAR should describe the potential vulnerabilities that can affect their operation and how the systems would behave under specific identified failure modes. Typically, a failure mode and effect analysis (FMEA) are performed to identify potential failures and how the system will behave during such failures. In addition, the failure analysis would determine and describe the safe state that the system outputs would default in conditions such as communication failures,

disconnection of the system, or loss of power. Section 7.4.3.8, “Loss of External Power,” of the SHINE FSAR identifies and describes the safe-state of controlled components associated with safety actuations during a loss of power. However, information was not provided in the SHINE FSAR for other potential failure modes.

The approved TR for the HIPS platform describes the self-testing features of the system to detect malfunctions in certain modules or functions. Because these features would depend on how they are configured for each application, ASAIs 12 and 57 require an applicant to 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. These ASAIs also require that the system be configured to alarm and assume a fail-safe state in the event of a failure. Further, ASAI 51 requires that an applicant or licensee 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. This should be done with sufficient detail to allow assessment of the complexity of the TRPS and evaluation of opportunities for malfunction or operability failure during facility operation. In its responses to RAI 7-4, SHINE described how these ASAIs were dispositioned. However, the SHINE FSAR does not include sufficient information for the NRC staff to evaluate how failures were identified and analyzed for the HIPS platform for the TRPS and ESFAS. Also, the SHINE FSAR does not include sufficient details on the configuration of self-test and diagnostics to conform to the maintenance and testing features described in the HIPS TR.

(a) Update the FSAR to describe the failure modes analyzed, as well as the design, configuration, and implementation of testing and maintenance features considered for the HIPS equipment for the TRPS and ESFAS.

(b) Provide information on how the TRPS and ESFAS would respond to each of the failures in the HIPS platform (i.e., assume a fail-safe state, only alarm failure, or assume a fail-safe state and alarm failure).

The NRC staff needs this information for making a finding that the TRPS and ESFAS will perform the required protective actions in the presence of any single failure or malfunction, including malfunctions from connected systems, and meet the identified design criteria. The information requested in parts (a) and (b) 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.”

The following are examples of the types of information the NRC staff needs to evaluate how the TRPS and ESFAS respond to identified failure modes. SHINE should ensure that the responses to parts (a) and (b) 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:

- A summary of failure modes identified for the modules included in the HIPS for the TRPS and ESFAS, including a description of the analyses used to confirm the adequacy of relevant design elements and safety features to perform their intended functions

- Failures detected by self-tests and diagnostics or periodic surveillance are consistent with the assumed failure detection methods of the TRPS and ESFAS single-failure analysis

**SHINE Response**

a) A failure modes and effects analysis (FMEA) was conducted for the TRPS and the ESFAS. The FMEA is a qualitative assessment which follows a systematic approach for identifying the modes of single system component failures and for evaluating their consequences. The primary purpose of the FMEA is to consider each part of the system, how it may fail, and what the effect of the failure on the system would be in the presence of a single failure.

   Specifically, the FMEA documents the following:

   - Identification of the component being analyzed
   - Identification of the functions performed by the component being analyzed
   - Identification of each failure mode for each feature or location of the component
   - Identification of all mechanisms of failure that could result in the failure mode
   - Description of the effects of the failure on the overall system
   - Description of how the failure can be detected
   - Provides any information that the analyst may feel is pertinent to the analysis of each component, particularly whether the failure is acceptable or unacceptable

   The FMEA analyzed failure modes of system components associated with the TRPS and ESFAS. A summary of failure modes analyzed for major TRPS and ESFAS components follows:

   - Analog sensors and detectors failing low or high, short circuiting, open circuiting, failing as is, or having a loose connection.
   - Discrete sensors and detectors receiving false inputs.
   - SFMs experiencing a short circuit, open circuit, or ground at signal input; an open, short, or ground at the power supply terminal; a communication engine failure; module connectors cracked or damaged; a module failed to engage fully with backplane connector; a failure to make a trip determination; or a spurious trip determination.
   - Input-sub module (ISM) or remote input submodule (RISM) incorrect scaling of analog inputs or incorrect analog/digital conversions.
   - SBMs experiencing a loss of communication engine or incorrectly communicated data to an SFM; a loss of communication engine or failure to communicate data to a scheduling, bypass, and voting module (SBVM); a failure to bypass a trip signal; a spurious bypass; an open, short, or ground at signal input; an open, short, or ground at the power supply terminal; module connectors cracked or damaged; or a module failed to engage fully with the backplane connector.
   - SBVM experiencing a loss of communication engine or incorrectly communicated data to SFM; a loss of communication engine or incorrectly communicated data to SBM; a loss of communication engine or incorrectly communicated data to an EIM; an open, short, or ground at signal input; an open, short, or ground at the power supply terminal; module connectors cracked or damaged; or a module failed to engage fully with the backplane connector.

- EIM experiencing loss of communication engine to SBVM; an open, short, or ground at signal input; an open, short, or ground at the power supply terminal; module connectors cracked or damaged; a module failed to engage fully with the backplane connector; or a failure to actuate on manual actuation command.
- Hard-wired module (HWM) experiencing a logic signal on backplane incorrectly indicates open input, a logic signal on backplane incorrectly indicates closed input, a loss of power to a bank of eight inputs, or a loss of power to more than one bank of eight inputs.
- A HWM, when an out-of-service (OOS) switch is active or a SFM is not responding, indicates Bypass when the switch is in Trip; or indicates Trip when the switch is in Bypass.

Because of the triple redundant architecture within each redundant division of equipment for the TRPS and ESFAS, failure mechanisms that affect a single function have no effect on facility operation. As documented in the FMEA, 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.

In conjunction with the FMEA, SHINE performed a single failure analysis of the TRPS and ESFAS. The assessment applied to the sense and command and execute features of the TRPS and ESFAS used for safety-related functions. The scope of the assessment included sensors, trip determination, signal conditioning, DC-DC converters and power supplies, and actuation logic. The single failure analysis determined that for functions requiring either 1-out-of-2 (1oo2) voting or 2-out-of-3 (2oo3) voting, a single failure of a channel will not prevent a protective action when required.

For TRPS and ESFAS functions with 1oo2 voting, the single failure criterion is not satisfied when the associated trip/bypass switch is taken to bypass, and an actuation will occur should the associated trip/bypass switch be taken to trip. Additional discussion on the operation of the trip/bypass switch is provided in the SHINE Response to RAI 7-14.

For TRPS and ESFAS functions with 2oo3 voting, the single failure analysis concluded that the single failure criterion would continue to be met if the associated channels trip/bypass switch is taken to trip but not if it is taken to bypass. Additional discussion on the operation of the trip/bypass switch is provided in the SHINE Response to RAI 7-14.

The failures analyzed in the FMEA for the TRPS and ESFAS concluded that failures would be detected by self-test, diagnostics, or periodic surveillances. These methods of failure detection are described in the SHINE Response to RAI 7-15.

b) For each of the failure modes associated with each component, the effect on the system and method of failure detection is documented in the FMEA. 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.

SHINE has revised Subsection 7.4.5.2.2 of the FSAR to provide additional details of the FMEA and single failure analysis performed for the TRPS and ESFAS. SHINE has also revised

Subsections 7.4.2.2.4 and 7.5.2.2.4 of the FSAR to describe how the FMEA and single failure analysis support meeting TRPS Criteria 17 and ESFAS Criteria 17. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

**RAI 7-13**

NUREG-1537, Part 2, Section 7.4, states, in part, that the SAR should describe operation of the protection system, "listing the protective functions performed by the [protection system], and the parameters monitored to detect the need for protective action." Further, NUREG-1537, Part 2, Section 7.4, states, in part, that the facility "should have operable protection capability in all operating modes and conditions, as analyzed in the SAR" and "[t]he range of operation of sensor (detector) channels should be sufficient to cover the expected range of variation of the monitored variable during normal and transient…operation."

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

Section 7.4 and 7.5 in the SHINE FSAR describe operation of TRPS and ESFAS, respectively. Tables 7.4-1, "TRPS Monitored Variables," and 7.5-1, "ESFAS Monitored Variables," in the SHINE FSAR list variables monitored, their analytical limits, safety logic, instrument range, accuracy, and instrument response for the TRPS and ESFAS, respectively.

Protection systems should provide necessary information to the operator in the control room related to safety systems process parameters and equipment status for operation, safety, and protection of the facility. SHINE Design Criterion 16 also credits manual actuation as one of the diverse means to provide defense-in-depth. The SHINE FSAR states that an operator can control multiple systems within the facility and provides defense-in-depth to analyzed accidents. For the operator to perform any actions, the operator would require data to act upon. Further, the control room includes a main control board (described in Section 7.6.1, "Description," of the SHINE FSAR) that contains manual actuation interfaces (e.g., switches and pushbuttons) and display screens showing variables important to safety to provide diverse means for operators to actuate automated safety functions.

The SHINE FSAR identifies variable monitored but it does not clearly describe the information to be displayed in the control room console and main control board for operation of the facility and manual actuation of safety functions, if necessary.

In addition, ASAI 30 requires an applicant or licensee to describe how the information displays are accessible to the operator and are visible from the location of any controls used to perform a manually controlled protective action provided by the front panel controls of a HIPS-based system. ASAI 65 requires demonstration that the HIPS platform equipment provides diversity for indication and component control signals to ensure HIPS platform monitoring and control performance in the presence of a digital CCF. In response to RAI 7-4, SHINE describes how it intends to address these ASAIs and notes that the TRPS and ESFAS is not used to display information for the operator or to affect a manually-controlled protective action. The NRC staff agrees that information is not directly displayed in the TRPS and ESFAS, but instead these systems transmit process parameters and equipment status to PICS for display in the control console and main control board. Based on the information provided, SHINE has not identified

the TRPS and ESFAS monitored variables that are transmitted to PICS and main control board for the operator to perform manual protective functions.

Update the SHINE FSAR to describe variables monitored and displayed to operate the facility and provide diversity for manual operator action, if necessary.

The NRC staff needs this information to make a finding that the TRPS and ESFAS will provide all necessary information in the control room for operators to operate IUs and perform manual safety actuation, if necessary, and meet the design criteria. The information requested in above is necessary to support the evaluation findings in Section 7.4 of NUREG-1537, Part 2, including that "[t]he protection channels and protective responses are sufficient to ensure that no safety limit, limiting safety system setting, or [protection system]-related limiting condition of operation discussed and analyzed in the SAR will be exceeded."

The following are examples of the types of information the NRC staff needs to evaluate how the TRPS and ESFAS respond to identified failure modes. SHINE should ensure that the response to 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:

- Information necessary to be displayed for the operator to manually actuate safety functions, if necessary

- A description of the PICS design demonstrating how monitored variables from the TRPS and ESFAS are sufficiently diverse such that any failure does not prevent the operator from obtaining or resolving conflicting information

**SHINE Response**

Each division of the TRPS and ESFAS transmits monitoring and indication information to the PICS. The following information from the TRPS and ESFAS will be displayed in the facility control room (FCR):

- Mode and Fault status for each Highly Integrated Protection System (HIPS) module
- Status and value of the monitored variables identified in Tables 7.4-1 and 7.5-1 of the FSAR
- Trip/Bypass switch status
- Divisional partial trip determination status
- Divisional full trip determination status
- TRPS IU cell operational mode status
- Actuation output and fault status
- Actuated component position feedback status

This monitoring and indication information provides operators with a status of variables monitored by the TRPS and ESFAS, as well as a status of the TRPS and ESFAS systems themselves, enabling operators to determine if manual actuation of a safety function is necessary.

The TRPS and ESFAS monitoring and indication information will be available to the operators in the FCR 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 FCR near where the manual control for actuating TRPS and ESFAS safety functions are located.

The TRPS and ESFAS provides redundant outputs to the PICS. The PICS receives the outputs from the TRPS and ESFAS onto a fault-tolerant server comprised of internal redundant physical servers. The use of redundant outputs from the TRPS to redundant internal physical servers on the PICS ensures that a failure would not prevent the operator from obtaining or resolving conflicting information.

By displaying TRPS and ESFAS monitoring and indication information at multiple locations in the FCR, including near manual controls for actuating TRPS and ESFAS equipment, the design ensures the operator has sufficient information to operate the facility and take manual operator action, as necessary.

SHINE has revised Subsection 7.4.5.2.4 of the FSAR to provide a description of the information available to the operators in the FCR. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

**RAI 7-14**

NUREG-1537, Part 2, Section 7.4, states that the protection system should be designed for reliable operation. In some circumstances, an applicant or licensee may bypass a function or component. Bypassing a component allows the licensee to take it out of service during operation or maintenance.

Section 7.4.2.2.9 of the SHINE FSAR identifies the TRPS criteria related to bypasses, permissives and interlocks, and removal of equipment from service. In this section, SHINE explains that the TRPS (and similarly the ESFAS) includes maintenance and operational bypasses, as well as a description of how the design meets the TRPS criteria.

SHINE Design Criterion 15 requires that the “removal from service of any [safety system] 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.” Sections 7.4.4.2, “Operational Bypass, Permissives, and Interlocks,” and 7.4.4.3 of the SHINE FSAR describe the HIPS design features to meet these identified criteria.

Section 7.4.4.2 of the SHINE FSAR describes the use of operational by passes during the operation of the IU cells. Section 7.4.4.3 of the SHINE FSAR describes how the TRPS can be placed in maintenance bypass. Further, the SHINE TSs identify the surveillance requirements needed to demonstrate operability of the system, the use of maintenance bypass, and the maximum amount of time permitted for the maintenance bypass.

In addition, the approved HIPS TR describes features for placing certain modules of the HIPS platform in bypass. Because these were conceptual descriptions of these features, the NRC staff identified ASAIs 42, 43, and 45 to require a licensee using the approved HIPS platform to describe how the HIPS equipment is used for operational and maintenance bypasses and provide the TS requirements. SHINE’s response to RAI 7-4 described how these ASAIs were addressed for the TRPS and ESFAS. However, these descriptions do not provide sufficient detail to ensure that the HIPS equipment for TRPS and ESFAS conform to the conceptual designs and features approved in the HIPS TR for using bypass (see RAI 7-10). Additionally,

the SHINE FSAR and proposed TSs contain inconsistencies on allowed bypass states and limiting conditions, respectively.

Update the SHINE FSAR to describe the design, configuration, and implementation of the bypass function considered for the HIPS equipment for the TRPS and ESFAS. Further, describe how the HIPS design meets SHINE Design Criterion 15.

The NRC staff requires this information to determine that SHINE's use of maintenance or operational bypasses do not affect the reliability of the system and that the system can perform its safety and protection functions. The information requested 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."

The following are examples of the types of information the NRC staff needs to evaluate how the TRPS and ESFAS meet the design criteria identified for operational and maintenance bypass. SHINE should ensure that the response to this RAI addresses 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:

- Design and implementation of bypass capabilities of modules in the HIPS for the TRPS and ESFAS
- Information on how signals and voting logics are treated during trip, inoperable, and bypass states
- Use of the out-of-service switch and trip/bypass switches and differences between maintenance bypass and trip states
- Effects of using bypass at the module level and/or division in the single failure criterion
- Transmission of trip or bypass signal through the hardwired module and effect on the bypass and voting modules
- Restrictions identified in the TR of the HIPS platform for placing the same SFM across more than one division in maintenance bypass

**SHINE Response**

SHINE employs operational bypass and maintenance bypass functions for the HIPS equipment for the TRPS. SHINE employs maintenance bypass functions for the HIPS equipment for the ESFAS.

Operational Bypass

Subsection 7.4.4.2 of the FSAR describes the use of operational bypasses for the TRPS during the operation of the IU cells. Operational bypasses for the TRPS are based upon the mode of operation and are automatically implemented within the SBVMs to bypass safety actuations that

are not required for each mode. Operator action is required to request the TRPS to transition to the next mode of operation. A mode transition request occurs via separate discrete inputs from PICS to each of the Division A and B HWMs, which then converts the mode transition input to a logic level signal and makes the signal available to the associated SBVMs within the division. When associated permissives are satisfied and the manual operator action for mode transition occurs, the TRPS progresses to the next mode and the TRPS SBVMs will 1) automatically bypass the final trip determinations for safety actuations that are not required for that particular mode of operation, and 2) will automatically remove any bypasses of the final trip determinations for safety actuations that are required for that particular mode of operation. If the permissive conditions are not met for transitioning to the next mode and the operator action occurs, the TRPS will not advance to the next mode of operation.

The status of TRPS operational bypasses is first provided by the SBVMs to the associated divisional monitoring and indication communications module (MICM) on the monitoring and indication bus (MIB). This status information is then provided to PICS for indication to the operators.

Maintenance Bypass

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 SBMs, SBVMs, EIMs, and HWMs.

When a SBM is removed from its chassis, the Division A and B SBVMs which correspond with the safety data bus (SDB) of the removed SBM will assert all partial trip signals associated with that SBM to the trip state for input to the coincident voting performed in the SBVMs. The impacted SDB will be in a 1-out-of-3 (1oo3) trip state for all safety functions that require Division C input within the SBVM and the other two SDBs will be in a 0-out-of-3 (0oo3) trip state within the SBVMs. When this occurs, the Division C SFMs and Division A and B SBVMs will provide fault indication information to the PICS (see the SHINE Response to RAI 7-13) for alerting the operators that there is an issue with the SBM.

When a SBVM is removed from its chassis, the other corresponding (SBVM-1, SBVM-2, or SBVM-3) divisional SBVM (either Division A or B) will assert all partial trip signals associated with the missing SBVM to the trip state for input to the coincident voting performed in the SBVM. The impacted SDB will be in a 1oo3 trip state within the SBVM and the other two SDBs will be in a 0oo3 trip state within the SBVMs. When this occurs, the following modules will provide fault indication information to the PICS for alerting the operators that there is an issue with the SBVM:

- All SFMs in the same division as the removed SBVM
- All EIMs in the same division as the removed SBVM
- All SBMs
- The other corresponding divisional SBVM

When an EIM is removed from its chassis, nothing will occur because the redundant EIM to the one removed will continue to provide actuation capability for all actuation components associated with the EIM. When this occurs, all of the SBVMs in the same division as the removed EIM will provide fault indication information to the PICS for alerting the operators that there is an issue with the EIM.

When a HWM is removed from its chassis, all hardwired inputs to the associated division via the HWM will become inactive. For the TRPS, removal of an HWM will effectively bypass the associated TSV Fill Isolation Valve Full Closed and HVPS Breaker Full Open input signals, which are safety inputs to the TRPS. For the ESFAS, a removed HWM will not affect any safety functions because there are no safety inputs to the HWMs.

The HWM includes a FPGA, which is a departure from the NRC-approved HIPS Topical Report (TR) (Reference 4) description of a HWM; however, this is acceptable because the function of the FPGA on the HWM is only to drive the module front panel light-emitting diode (LED) indications and to provide module operational status to the MICM. The FPGA on the HWM cannot affect the function of receiving hardwired inputs and making them available on the backplane of the chassis. When a HWM is removed from its chassis, the MICM for the division will provide fault indication information to the PICS, alerting the operators that there is an issue with the HWM.

SFM input channels of the TRPS and ESFAS can be taken out-of-service (OOS) through the use of the OOS switches located on the front of each SFM and an associated separate trip/bypass switch located below each SFM. The OOS switch has two positions: Operate and OOS. When the switch is placed in the OOS position, the respective divisional SBMs or SBVMs will force the partial trip information associated with the SFM to the trip or bypass state, depending on the position of the trip/bypass switch, and take the channel OOS. Any time an SFM module is placed in an OOS condition, the SBMs or SBVMs associated with the SFM read the state of the trip or bypass switch to determine if the SFM input channels should be bypassed or treated as a trip when continuing the flow of data through the system.

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

The SFMs continually provide the status of their OOS switch to the associated divisional SBMs or SBVMs along with their partial trip information. With an SFM’s OOS switch in the OOS position and the associated trip/bypass switch in the trip position, the associated divisional SBMs or SBVMs will then assert all partial trip information associated with the SFM to the trip state for input to coincident logic voting in the SBVMs. All of the partial trip information associated with all inputs for this SFM would be in a maintenance trip condition for this case. For those safety functions that use 2oo3 coincident voting, a single failure of the same SFM in another division would not defeat the safety function because the third remaining divisional SFM is available to complete a 2oo3 vote if required. For those safety functions that only use 1oo2 coincident voting, the safety functions would be actuated when the OOS switch is placed into the OOS position with the associated trip/bypass switch in the trip position.

With an SFM's OOS switch in the OOS position and the associated trip/bypass switch in the bypass position, the associated divisional SBMs or SBVMs will then assert all partial trip information associated with the SFM to the bypassed state (not tripped) for input to coincident logic voting in the SBVMs. All of the partial trip information associated with all inputs for this SFM would be in a maintenance bypass condition for this case. For safety functions that use either 1oo2 or 2oo3 coincident voting, a single failure of the same SFM in another division would defeat the safety function. Placing a single SFM in maintenance bypass is allowed by the technical specifications for up to two hours for the purpose of performing required technical specification surveillance testing. 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.

Limiting Conditions for Operation (LCOs) 3.2.3 and 3.2.4 of the technical specifications contain a note that specifies that any single SFM may be bypassed for up to two 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 from placing the same SFM across more than one division into maintenance bypass.

With an SFM's OOS switch in the OOS position and the associated trip/bypass switch in either the trip or bypass position, the input channels associated with the SFM are inoperable. The input to the voting logic for the maintenance trip and bypass states are discussed above.

The maintenance bypass function supports the in-service testability requirement of SHINE Design Criterion 15 for the TRPS and ESFAS. By allowing a single SFM module to be placed in maintenance bypass in accordance with the technical specifications requirements, technical specifications surveillances can be performed to verify the operability of TRPS and ESFAS components during system operation. As described above, the time that the maintenance bypass feature is allowed to be used is limited to two hours. This satisfies the SHINE Design Criterion 15 requirement that the removal from service of any component or channel does not result in the loss of required minimum redundancy unless the acceptability of operation of the protection system can be otherwise demonstrated.

Self-testing capabilities, as described in the SHINE Response to RAI 7-15, 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, as required by SHINE Design Criterion 15. The results of these self-tests, along with the ability to perform in-chassis calibration and modification to configurable variable and set-points with the maintenance work station (MWS), ensure that 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, as required by SHINE Design Criterion 15. The self-tests provide indications of component degradation or failure, and the MWS provides the ability to obtain diagnostic information and perform maintenance on individual channels to identify and address component failures. The MWS is described in detail in the SHINE Response to RAI 7-18.

Through the use of the maintenance bypass function, self-testing capabilities, and the MWS, SHINE ensures that SHINE Design Criterion 15 is met for the TRPS and ESFAS, as described above.

SHINE has revised Subsections 7.4.4.2, 7.4.4.3, and 7.5.4.4 of the FSAR to describe the design, configuration, and implementation of the bypass function considered for the HIPS equipment for the TRPS and ESFAS. SHINE has also revised Subsections 7.4.2.1.3 and 7.5.2.1.3 of the FSAR to ensure consistency with the technical specifications and to provide additional description of how SHINE Design Criterion 15 is met for the TRPS and ESFAS. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

**RAI 7-15**

NUREG-1537, Part 2, Section 7.4, states, in part, that the protection system be "sufficiently distinct in function from the [control system] that its unique safety features can be readily tested, verified, and calibrated." In addition, NUREG-1537, Part 2, Section 7.4, also states, in part, that the protection system "function and time scale should be readily tested to ensure operability of at least minimum protection for all…operations." Therefore, the TRPS and ESFAS should be designed to be readily tested and calibrated to ensure operability. Additionally, the TSs, including surveillance tests and intervals, should ensure availability and operability of these actuation systems.

SHINE Design Criterion 15 requires the TRPS be designed to permit periodic testing, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred. Section 7.4.4.3 of the SHINE FSAR describes how a channel can be placed in maintenance bypass and its effect on the voting logic. Section 7.4.4.4, "Testing Capability," of the SHINE FSAR describes testing capabilities included in the TRPS.

The approved TR for the HIPS platform describes the diagnostic and maintenance features (e.g., built-in self-testing, periodic testing, etc.) available in the HIPS platform. Because the HIPS platform diagnostic and maintenance features were conceptual designs, the NRC staff identified ASAIs 13, 14, 24, 25, 32 ,49, 50, and 51 as necessary for facility-specific implementation. The ASAIs require an applicant or licensee to describe how diagnostic and maintenance features are implemented in the site-specific application. Specifically, an applicant or licensee should (1) demonstrate diagnostic and maintenance features provide necessary test coverage, and (2) demonstrate that the use of these features won't prevent the system from performing its safety and protection functions. In response to RAI 7-4, SHINE described whether these ASAIs are applicable to SHINE and their dispositions.

The NRC staff generally agrees with the SHINE's stated applicability of these ASAIs to the TRPS and ESFAS. However, the description and information in the SHINE FSAR do not include sufficient detail on the configuration of self-testing and diagnostics to evaluate conformance to the maintenance and testing features described in the HIPS TR and how the SHINE design criteria are met.

Update the SHINE FSAR to describe how diagnostic and maintenance features are implemented in the HIPS equipment for the TRPS and ESFAS. Demonstrate that the features provide necessary test coverage. Also, demonstrate that the use of these features won't prevent the systems from performing their safety and protection functions.

The NRC staff need this information to verify that testing and maintenance of the TRPS and ESFAS will ensure operability of the equipment and meet the SHINE Design Criterion 15. The information requested 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."

The following are examples of the types of information the NRC staff needs to evaluate testing and maintenance features implemented in the TRPS and ESFAS. SHINE should ensure that the response to this RAI addresses 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:

- Modification of configurable variables and setpoints
- Features and limitations to perform in-chassis calibration
- Surveillance tests using automatic sensor cross-check
- Test and calibration functions of the HIPS platform and compliance with regulatory guidance
- Validation of self-testing functions in HIPS equipment

**SHINE Response**

A description of the diagnostic and maintenance test features in the HIPS platform equipment for the TRPS and ESFAS follows.

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 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 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. The actuation priority logic is a simple circuit that has acceptable reliability to be tested when the IU 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 ESFAS 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

The TRPS and ESFAS have redundant gateways which gather the output of the MICMs for each of the three divisions, as depicted in Figure 7-15-1. The data for each of the three divisions are compared to perform a channel check, and the results are provided to the PICS.

The TRPS and ESFAS incorporate failure detection and isolation techniques. Fault detection and indication occurs at the module level, which enables plant personnel to identify the module that needs to be replaced. Self-testing will generate an alarm and report a failure to the operator and place the component (e.g., SFM; SBVM; or EIM components) in a fail-safe state.

The self-testing features of the HIPS platform are designed, developed, and validated at the same level as the functional logic. The overlapped self-test features of the HIPS platform are integral to the operation of the system and are therefore designed, developed, and validated to the same rigor as the rest of the platform.

The MWS is used to perform modification of configurable variables and setpoints, as well as in-chassis calibration, of TRPS and ESFAS equipment, as descried in the SHINE Response to RAI 7-18. A limitation is placed on the use of the MWS in that an SFM will not receive data from the MWS unless it has been placed into OOS, which is further described in the SHINE Response to RAI 7-18.

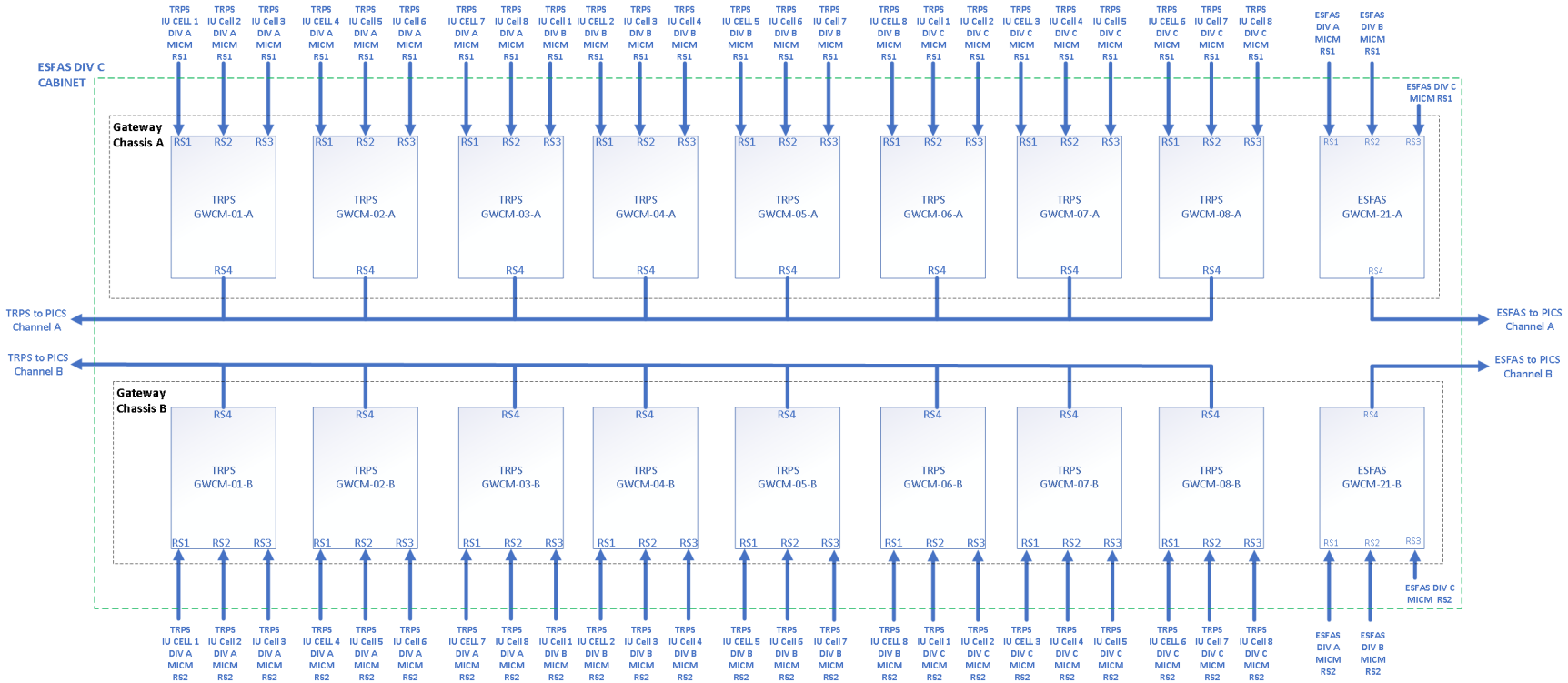
Diagnostic data for the division of the TRPS and ESFAS are provided to the MWS. Diagnostics data are communicated via the MIB, which is a physically separate communications path from the safety data path, ensuring the diagnostics functionality is independent of the safety functionality.

The description of the self-testing features and use of the MWS described above satisfies Section 5.5.2 and Section 5.5.3 of Institute of Electrical and Electronics Engineers (IEEE) Standard 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations” (Reference 5), as described in Appendix B of NuScale Power, LLC (NuScale) Topical Report TR-1015-18653, “Design of the Highly Integrated Protection System Platform Topical Report” (Reference 4).

By complying with these sections of IEEE Standard7-4.3.2-2003, as described in Appendix B of TR-1015-18653, and incorporating diagnostic and maintenance test features that test from the sensor inputs of the TRPS and ESFAS through to the actuated equipment, the necessary test coverage is provided in the SHINE application of the HIPS platform.

SHINE has revised Subsection 7.4.5.5 of the FSAR to provide additional description of the diagnostic and maintenance features associated with the HIPS platform for the TRPS and ESFAS. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

## Figure 7-15-1: TRPS and ESFAS Gateway Communications Architecture



**RAI 7-16**

NUREG-1537, Part 2, Section 7.4, states, in part, that the design of the protection systems should be adequate to perform the functions necessary to ensure safety. Therefore, the design of the SHINE facility should include provisions for the protection systems to reliably operate in the normal range of environmental conditions and postulated credible accidents, transients, and other events at the facility that could require their operation.

SHINE Design Criterion 16 requires the system be 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.

Sections 7.4.3.5, "Operating Conditions," and 7.4.3.6, "Seismic, Tornado, Flood," of the SHINE FSAR describe operating and transient conditions in the facility and seismic requirements. However, these sections do not confirm whether the TRPS and ESFAS have been tested to demonstrate that they will function in these conditions. Further, the approved HIPS TR identifies ASAI 18 for an applicant to demonstrate system qualification for installation and operation in mild environment locations. In response to RAI 7-4, SHINE references Sections 7.4.3.13, "Design Codes and Standards," and 7.5.3.12, "Design Codes and Standards," of the SHINE FSAR, which identify the codes and standards to be used in qualifying the TRPS and ESFAS equipment. While these sections describe applicable environmental qualification criteria, they do not demonstrate that the TRPS and ESFAS have been qualified to meet the environmental qualification criteria and associated SHINE design criterion.

Update the SHINE FSAR to demonstrate that the HIPS equipment for the TRPS and ESFAS has undergone environmental, seismic, radiation and emissions qualifications. Also, demonstrate that the results envelope the operating and transient conditions identified for the facility.

The NRC staff needs this information to make a finding that the TRPS and ESFAS are qualified to operate under the different conditions in the facility and meet the applicable design criteria. The information requested above is necessary to support the evaluation findings in Section 7.4 of NUREG-1537, Part 2, including that "[t]he [protective system] is designed to prevent or mitigate hazards…so that the full range of normal operations poses no undue radiological risk to the health and safety of the public, the facility staff, or the environment." The following are examples of the types of information the NRC staff needs to evaluate qualification of the TRPS and ESFAS. SHINE should ensure that the response to this RAI addresses 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:

- Confirmation of qualified life for the TRPS and ESFAS equipment
- Confirmation that the effects of electromagnetic interference/radiofrequency interference (EMI/RFI) and power surges, including computer-based digital systems, are addressed
- Confirmation that the protection systems meet the site-specific requirements for seismic and normal range and postulated credible accidents and transients of environmental conditions anticipated within the SHINE facility

**SHINE Response**

The HIPS equipment for the TRPS and the ESFAS has been qualified by the vendor. A discussion of the environmental, seismic, radiation, and emissions qualifications of the HIPS equipment for TRPS and ESFAS follows.

Environmental Qualification

Mild environmental qualification was performed for the HIPS equipment for TRPS and ESFAS using guidance provided in Sections 4.1, 5.1, 6.1, and 7 of IEEE Standard 323-2003, “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations” (Reference 6). Environmental qualification was performed considering temperature, relative humidity, radiation, and pressure. Because the HIPS equipment for TRPS and ESFAS will be located in a mild environment and will not be subject to harsh environmental conditions during normal operation or transient conditions, a qualified life determination is not required.

The HIPS equipment for TRPS and ESFAS has been designed for continuous operation up to 140 degrees Fahrenheit (°F) and limited operation up to 158 °F. A proof test was performed in an environmental chamber, which verified the normal and abnormal temperature exposure levels for the HIPS equipment. The temperature conditions under which the proof test was performed and satisfactorily completed envelop the normal and transient temperature conditions that the HIPS equipment is expected to operate in, as provided in Tables 7.2-2 and 7.2-3 of the FSAR.

The HIPS equipment for the TRPS and ESFAS is acceptable for mild environment relative humidity conditions. Non-condensing humidity does not represent a credible failure mode applicable to the HIPS equipment. During the proof test discussed above, humidity was not controlled and varied based upon the temperature at the time of testing. Acceptance criteria of the proof test were met, demonstrating that the equipment is expected to operate under required conditions for humidity.

The HIPS equipment for the TRPS and ESFAS is acceptable for the design radiation environment. As provided in Table 7.2-1 of the FSAR, the total integrated dose (TID) for areas of the facility that the HIPS equipment will be installed is calculated as 1.0E+03 rad TID. When performing the HIPS equipment qualification, the vendor reviewed industry studies that compiled radiation effects data on a wide range of materials showing that the least radiation resistance threshold for organic compounds (i.e., nonmetallic materials) is greater than 1.0E+04 rad gamma. For electronic components, studies have shown that metal oxide semiconductor devices may be susceptible at a lower level of 3.0E+03 rad gamma. Since the service conditions for the HIPS equipment for the TRPS and ESFAS is less than these bounding values, no further evaluation for radiation in the environmental qualification was required.

The HIPS equipment for the TRPS and ESFAS is acceptable for normal atmospheric pressure, which is the normal and transient pressures provided in Tables 7.2-2 and 7.2-3 of the FSAR. Normal atmospheric pressure is not considered adverse to the HIPS equipment operation; the HIPS components are not pressure sealed, and therefore, do not create any differential pressure or failure mechanism.

Seismic Qualification

The HIPS equipment for the TRPS and ESFAS was subjected to a proof test in accordance with Section 8 of IEEE Standard 344-2013, “Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Generating Stations” (Reference 7). The HIPS equipment for the TRPS and ESFAS underwent biaxial and triaxial excitation testing.

For the biaxial excitation testing, the HIPS equipment for the TRPS and ESFAS was tested in each of four orientations: front to back and vertical, in phase 0 degrees; side to side and vertical, in phase, 90 degrees; front to back and vertical, out of phase, 180 degrees; and side to side and vertical, out of phase, 270 degrees. Each set of four orientations constituted a single run. Five operating basis earthquake (OBE) tests were performed in each direction for a total of 20 OBE runs. One safe shutdown earthquake (SSE) test was performed in each direction for a total of four SSE runs.

For the triaxial excitation testing, the HIPS equipment for the TRPS and ESFAS was tested in each of three orientations with respect to the excitation, as follows:

| Direction Label | Direction Description | Specimen Orientation |
|---|---|---|
| X | Horizontal - East/West | Side to Side |
| Y | Horizontal - North/South | Front to Back |
| Z | Vertical | Vertical |

The triaxial excitation test was performed in all three directions for each test. A total of five OBE tests were performed.

The results of the proof test demonstrated that for all test runs, structural integrity of the HIPS equipment for the TRPS and ESFAS was maintained and no mechanical damage was observed. Acceptance criteria of the seismic testing were met to demonstrate qualification of the equipment for the TRPS and ESFAS.

Electromagnetic Interference (EMI)/Radio-Frequency Interference (RFI) Qualification

A summary of the EMI/RFI qualification of the HIPS equipment for the TRPS and ESFAS follows. Although the regulatory positions of Regulatory Guide 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems” (Reference 8) are specific to nuclear power plants and are not applicable to non-power production and utilization facilities, this regulatory guide, which provides an acceptable method for qualifying computer-based digital systems, informed the EMI/RFI qualification of the HIPS equipment for the TRPS and ESFAS. HIPS equipment for the TRPS and ESFAS will be grounded per Section 5.2.1 of IEEE Standard 1050-2004, “Guide for Instrumentation and Control Equipment Grounding in Generating Stations” (Reference 9).

Emissions testing for HIPS equipment for the TRPS and ESFAS was performed using the testing methods listed in Regulatory Position 3, Table 2, of Regulatory Guide 1.180.

Susceptibility Testing for HIPS equipment for the TRPS and ESFAS was performed using the testing methods listed in Regulatory Position 4, Table 6, of Regulatory Guide 1.180.

Surge withstand testing for HIPS equipment for the TRPS and ESFAS was performed using the International Electrotechnical Committee (IEC) methods listed in Regulatory Position 5, Table 21, of Regulatory Guide 1.180.

The results of this testing was satisfactory and demonstrates that the HIPS equipment for the TRPS and ESFAS and confirms that the effects of EMI/RFI and power surges are addressed.

SHINE has revised Subsections 7.4.2.2.11, 7.4.3.5, 7.4.3.6, 7.5.2.2.11, 7.5.3.4, and 7.5.3.5 of the FSAR to provide additional description of the environmental, seismic, radiation, and emissions qualification testing of the TRPS and ESFAS. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

**RAI 7-17**

NUREG-1537, Part 2, Section 7.4, states that the protection systems "should be designed for reliable operation in the normal range of environmental conditions anticipated within the facility."

The SHINE FSAR identified codes and standards to which SHINE committed to use to demonstrate meeting the SHINE design criteria, meeting NRC guidance and regulations, and developing high quality ICS.

Chapter 7 of the SHINE FSAR includes a list of codes and standards "that are applied to the design" of the TRPS and ESFAS (e.g., SHINE FSAR Section 7.4.3.13 identifies codes and standards applied to the TRPS design). However, the SHINE FSAR does not describe how these codes and standards were used or how the current design conforms to the applied standards. In RAI 7-3 (ADAMS Accession No. ML20255A026), the NRC staff requested a description of how codes and standards listed in the SHINE FSAR are used to design each of the ICS. But this information was not included in the response.

The NRC staff recognizes that NUREG-1537 identifies the guidelines of Institute of Electrical and Electronics Engineers Std. 7-4.3.2-1993, "IEEE Standard Criteria for digital Computers in Safety Systems of Nuclear Power Generating Stations," and Regulatory Guide 1.152, Revision 1, "Criteria for Digital Computers In Safety Systems of Nuclear Power Plants," American National Standards Institute/American Nuclear Society (ANSI/ANS)-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry," ANSI/ANS-15.15-1978, "Criteria for the Reactor Safety Systems of Research Reactors," and draft ANSI/ANS-15.20, "Criteria for the Control and Safety Systems for Research Reactors," but does not identify additional specific codes and standards for the system to conform. Nevertheless, NUREG-1537 states that a reliable system is built using accepted engineering and industrial practices.

Update the SHINE FSAR to describe how codes and standards listed in the SHINE FSAR are used to design each of the ICS.

The NRC staff need this information to verify that engineering and industrial practices were used to design reliable protection systems that will perform the intended safety functions when required and meet the applicable design criteria. The information requested 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."

The following are examples of the types of information the NRC staff needs to evaluate how codes and standards used to design, build, and test the TRPS and ESFAS. SHINE should ensure that the response to this RAI addresses 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:

- Codes and standards used for the design and development of the logic for the TRPS and ESFAS, including traceability of the codes and standards to system design and testing documents

- Codes and standards used for the environmental, seismic, radiation, and EMI/RFI qualification of the HIPS for the TRPS and ESFAS, including traceability to system design and testing documents

**SHINE Response**

The following codes and standards are used for the design of the TRPS and ESFAS:

IEEE Standard 379-2000, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 10)

IEEE Standard 379-2000 is used as the guidance for a FMEA and single failure analysis used in the design and development in the logic for the TRPS and the ESFAS. Subsections 7.4.2.1.3 and 7.5.2.1.3 of the FSAR describe how SHINE applies IEEE Standard 379-2000 in demonstrating that the design of TRPS and ESFAS satisfy SHINE Design Criterion 15.

Traceability of IEEE Standard 379-2000 to system design is provided in the TRPS and ESFAS system design description documents. These documents state that IEEE Standard 379-2000 provides the guidance for the FMEA and single failure analysis and provide traceability matrices that show how the FMEA and single failure analysis are used to demonstrate satisfaction of the relevant design criteria in the design of the system. The FMEA and single failure analysis are documented in the SHINE design basis.

IEEE Standard 384-2008, "Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 11)

Section 5.1.1.2, Table 1 of Section 5.1.3.3., and Table 2 of Section 5.1.4 of IEEE Standard 384-2008 are used for guidance for physical separation and electrical isolation to maintain the independence of TRPS and ESFAS circuits. Section 5.1.1.2, Table 1 of Section 5.1.3.3, and Table 2 of Section 5.1.4 of IEEE Standard 384-2008 are used to provide guidance for spatial separation between cable and raceway groups. Section 6.1.2.1, Section 6.1.2.2, and Section 6.1.2.3 of IEEE Standard 384-2008 are used to provide guidance for electrical isolation between nonsafety-related and safety-related circuits, as described in Subsection 8a2.1.5 of the FSAR. Subsection 7.4.2.2.5 of the FSAR describes how SHINE apples IEEE Standard 384-2008 in demonstrating that the design of TRPS satisfies TRPS Criteria 20 and 21. Subsection 7.5.2.2.5 of the FSAR describes how SHINE apples IEEE Standard 384-2008 in demonstrating that the design of ESFAS satisfies ESFAS Criteria 21 and 22. Subsections 7.4.3.9 and 7.5.3.8 of the FSAR describe how SHINE applies IEEE Standard 384-2008 in meeting fire protection considerations for the TRPS and ESFAS, respectively.

Traceability of IEEE Standard 384-2008 to system design is provided in the TRPS and ESFAS system design description documents. These documents state that portions of IEEE Standard 384-2008 provide the required guidance for physical separation and electrical isolation of TRPS and ESFAS circuits and provide traceability matrices that show how the physical separation and electrical isolation are used to demonstrate satisfaction of relevant design criteria in the design of the system.

IEEE Standard 1012-2004, "Standard for Software Verification and Validation" (Reference 12)

IEEE Standard 1012-2004 is used in the development of the vendor project verification and validation (V&V) plan. V&V activities and tasks are tailored and adapted from the guidance in IEEE Standard 1012-2004. This standard is used to provide guidance on the programmable logic products and processes employed throughout the programmable logic lifecycle. The project V&V plan assigns software criticality levels consistent with Section 4 of IEEE 1012-2004 and assigns requirements for V&V tasks based upon these assigned levels. Subsections 7.4.2.2.2 and 7.5.2.2.2 of the FSAR describe how SHINE applies IEEE Standard 1012-2004 in demonstrating that the design of TRPS and ESFAS satisfy TRPS Criterion 8 and ESFAS Criterion 8, respectively. Subsection 7.4.5.4.5 of the FSAR provides additional detail on the application of IEEE Standard 1012-2004 in V&V activities.

The vendor project V&V plan specifically requires use of the guidance of IEEE Standard 1012-2004, as described above, and this plan is contained in the SHINE design basis. TRPS and ESFAS system design description documents reference the project V&V plan in traceability matrices that demonstrate satisfaction of relevant design criteria in the design of the system. By tracing to the project V&V plan, which directs compliance with specific guidance contained in IEEE Standard 1012-2004, the system design descriptions provide traceability of IEEE Standard 1012-2004 to system design.

IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 5)

The SHINE application of the HIPS platform conforms to IEEE Standard 7-4.3.2-2003 for the TRPS and ESFAS, as described in Appendix B of NuScale Topical Report TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report" (Reference 4). 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 7-4.3.2-2003.

Traceability of IEEE Standard 7-4.3.2-2003 to system design is provided through the application-specific action item (ASAI) assessment that provides traceability from the SHINE application of the HIPS platform to the NRC-approved TR-1015-18653.

SHINE has revised Subsection 7.4.5.1 of the FSAR to describe conformance of the HIPS platform to IEEE Standard 7-4.3.2-2003. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

Section 8 of IEEE Standard 344-2013, "Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Generating Stations" (Reference 7)

Section 8 of IEEE Standard 344-2013 is used to provide testing methodology for seismic qualification. A detailed description of the testing methodology used and testing documentation requirements is provided in the SHINE Response to RAI 7-16. Subsection 7.4.2.2.3 of the FSAR

describes how SHINE applies Section 8 of IEEE Standard 344-2013 in demonstrating that the design of TRPS satisfies TRPS Criterion 14. Subsection 7.5.2.2.3 of the FSAR describes how SHINE applies Section 8 of IEEE Standard 344-2013 in demonstrating that the design of ESFAS satisfies ESFAS Criterion 14. Subsections 7.4.3.6 and 7.5.3.5 of the FSAR describe how SHINE applies Section 8 of IEEE Standard 344-2013 in meeting seismic considerations for TRPS and ESFAS equipment, respectively.

Traceability of Section 8 of IEEE Standard 344-2013 to system design is provided in the TRPS and ESFAS system design description documents. These documents specify the use of Section 8 of IEEE Standard 344-2013 in the equipment qualification of the TRPS and ESFAS and reference the standard in the traceability matrices that demonstrate satisfaction of relevant design criteria in the design of the system. The HIPS platform equipment qualification plan for the TRPS and ESFAS and the HIPS platform environmental and seismic qualification test report for the TRPS and ESFAS document use of IEEE Standard 344-2013, as described above.

Section 5.2.1 of IEEE Standard 1050-2004, “Guide for Instrumentation and Control Equipment Grounding in Generating Stations” (Reference 9)

Section 5.2.1 of IEEE Standard 1050-2004 is used to provide guidance for the grounding of the TRPS and ESFAS as part of addressing the effects of EMI/RFI. A detailed description of how grounding helps address the effects of EMI/RFI is provided in the SHINE Response to RAI 7-16. Subsections 7.4.2.2.11 and 7.5.2.2.11 of the FSAR describe how SHINE applies Section 5.2.1 of IEEE Standard 1050-2004 in demonstrating that the design of TRPS and ESFAS satisfy TRPS Criterion 46 and ESFAS Criterion 47, respectively.

Traceability of Section 5.2.1 of IEEE Standard 1050-2004 to system design is provided in the TRPS and ESFAS system design description documents. These documents specify the use of Section 5.2.1 of IEEE Standard 1050-2004 in the equipment qualification of the TRPS and ESFAS and reference the standard in the traceability matrices that demonstrate satisfaction of relevant design criteria in the design of the system. During EMI/RFI testing, the HIPS equipment for the TRPS and ESFAS was grounded to simulate the installed configuration, which complies with Section 5.2.1 of IEEE Standard 1050-2004.

Sections 4.1, 5.1, 6.1, and 7 of IEEE Standard 323-2003, “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations” (Reference 6)

Sections 4.1, 5.1, 6.1, and 7 of IEEE Standard 323-2003 are used to provide guidance for the qualification of the TRPS and ESFAS for a mild operating environment and not subject to harsh environmental conditions during normal operation or transient conditions. A detailed description of the environmental qualification of the TRPS and ESFAS is provided in the SHINE Response to RAI 7-16.

Traceability of IEEE Standard 323-2003 to system design is provided through the HIPS platform equipment qualification plan for the TRPS and ESFAS and the HIPS platform environmental and seismic qualification test report for the TRPS and ESFAS. These documents specify the use of IEEE 323-2003 for the environmental qualification of HIPS equipment as described above.

SHINE has revised Subsections 7.4.2.2.3 and 7.5.2.2.3 of the FSAR to provide a description of how SHINE applies IEEE Standard 323-2003 in demonstrating that the design of TRPS and

ESFAS satisfy TRPS Criterion 14 and ESFAS Criterion 14, respectively. A mark-up of the FSAR incorporating these changes is provided as Attachment 1.

**RAI 7-18**

NUREG-1537, Part 2, Section 7.4, states, in part, that "[t]he sensitivity of each sensor channel should be commensurate with the precision and accuracy to which knowledge of the variable measured is required for the protective function." This information is necessary to ensure that adequate margins exist between analytical limits and instrument setpoints so that protective actions are initiated before SLs are exceeded.

Sections 7.4.2.1.3, "Protection System Reliability and Testability," 7.4.4, "Operation and Performance," and 7.4.5.3.3, "Access Control," of the SHINE FSAR note that there are setpoints and tunable parameters that may require periodic modification. To do this, the operator would use the maintenance workstation (MWS) in the HIPS equipment when the safety function is out of service. To prevent inadvertent changes, the HIPS equipment includes physical and logical features to allow changes to these values. The setpoints and tunable parameters are stored in the nonvolatile memory (NVM) in the MWS.

The approved TR for the HIPS equipment states that the MWS was not part of the base platform, and thus was not evaluated by the NRC staff. Nevertheless, the HIPS TR briefly describes how setpoint and tunable parameters can be modified. The TR also mentions that the logic associated with setpoints and tunable parameters is part of the safety function module in the HIPS platform.

Because the MWS was not described in detail and evaluated in the HIPS TR, the NRC staff needs information on how the MWS would be used to change setpoints and tunable parameters.

Update the SHINE FSAR to describe modifications to setpoints and tunable parameters, including operation and configuration of the NVM, separation of the safety logic and calibration functions, modifications of NVM during operation, and controls to prevent inadvertent changes to setpoint and tunable parameters.

This information is necessary to support the evaluation findings in Section 7.4 of NUREG-1537, Part 2, including that "[t]he protection channels and protective responses are sufficient to ensure that no safety limit, limiting safety system setting, or [protection system]-related limiting condition of operation discussed and analyzed in the SAR will be exceeded."

**SHINE Response**

Modification of setpoints and tunable parameters is accomplished via the MWS as described below.

Setpoint Modification with the MWS

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. TRPS and ESFAS setpoints and real time process parameters are stored and processed in their raw value within the SFMs.

The MWS allows a technician password protected access to select the system (i.e., TRPS or ESFAS), the specific IU cell (for TRPS), the division (i.e., A, B, or C), the specific SFM, and the trip setpoint which is to be modified. Then a MWS enable hardwired switch is required to be activated to allow for physical connection of the MWS to the calibration and test bus (CTB). The technician must then use the MWS to calculate the setpoint in raw value by entering the setpoint's percentage of the process input range, then select Calculate Setpoint from the MWS. The MWS will then calculate the setpoint raw value based on the input range and Analog-to-Digital Converter (ADC) resolution. The ability to update a setpoint is disabled unless a setpoint calculation has been performed, which supports preventing an inadvertent modification of the setpoint. When a setpoint calculation has been performed, then the option to update a setpoint is enabled to allow the technician to select it and update the data stored in the module's non-volatile memory (NVM).

The SFM's safety function logic is implemented within the FPGA using the same logic design in three different locations on the FPGA (using three independent FPGA resources). Each logic design communicates its trip data on one of the triplicated SDBs. This requires each logic design on the FPGA to use a different setpoint memory location to eliminate common cause failures and increase the safety logic fault tolerance. When the technician asserts the Update Setpoint function, the calculated setpoint raw value is then stored in three locations on the SFM module's NVM. Each of the three NVM locations will be loaded to one of the triplicated logic designs on the FPGA during startup or a manual NVM data load command from the module's front panel switch. The SFM's safety function logic is independent (i.e., different logic resources on the FPGA) from both the logic used to store information to the NVM and the logic used to load information from the NVM to the safety function logic.

The SFM will not receive data from the MWS unless it has been placed into OOS. The technician must place the module into the OOS mode by selecting OOS from the module's front panel manual switch before updating a setpoint.

For the setpoint to be stored successfully, the MWS issues three separate write commands to the NVM, each write command storing the same setpoint raw value into one of the three NVM memory locations. The three NVM memory locations are determined by the MWS based on the specific trip setpoint to be modified. Each of the write commands is issued from the MWS and the data is sent to the module's NVM as follows:

1) The MWS calculates a Cyclic Redundancy Check (CRC) and sends the data to the divisional MICM that corresponds to the module to be updated.
2) The MICM receives and verifies the data integrity, then calculates a CRC then sends it to the intended module.
3) The SFM logic receives and verifies the data integrity, then calculates a CRC for the data and sends it to its NVM.
4) The NVM receives and stores the CRC/data in the intended location.
5) The SFM logic will then read back the data from the same NVM location that it just performed the data write to and verify the data's integrity. This will indicate that the data was stored successfully in the intended NVM location.
6) If the data read back integrity check fails, the module will issue an NVM error, and the error will be displayed by the MWS.
7) The written data and the data read back from the module are both displayed on the MWS along with the NVM location that was used during the write and read operations to allow the technician to verify an accurate setpoint modification.

To confirm that an inadvertent modification of the setpoint did not occur, a setpoint raw value can be read from the three NVM locations using the MWS by selecting the specific SFM, then selecting Read Setpoint function. The data read from the three NVM locations will then be displayed on the MWS.

The MWS will read the module's status information and display it to the technician after each write or read operation.

The above steps update the data stored on the module's NVM, but do not update the logic on the module's FPGA. To update the logic on the FPGA, the technician must press the manual Load NVM button from the module's front panel.

To summarize the above description, the technician must perform the following steps to successfully perform a setpoint update:

1) Place the module in OOS mode by selecting OOS with the module's front panel manual switch.
2) Access the MWS interface using the correct password.
3) Enable the physical connection between the MWS and the CTB.
4) Select the appropriate setpoint from a menu in the MWS.
5) Enter the setpoint percentage.
6) Select Calculate Setpoint button.
7) Select Update Setpoint button.
8) Confirm that the displayed write and read data values and NVM locations are correct.
9) Confirm that the NVM LED is on for the intended module. This confirms that the correct module has received the data.
10) Press the NVM Load button on the module's front panel.
11) Place the module into normal operation by selecting Operate with the module's front panel manual switch.

The updated setpoint would then be operational on the triplicated FPGA logic.

Input Calibration with the MWS

Like modifying a setpoint, SFM input calibration (tunable parameters) is accomplished via the MWS with the same physical and logical controls in place to prevent modifications to a safety channel when it is being relied upon to perform a safety function.

Input calibration can be performed automatically or manually. For both methods, the MWS allows a technician password protected access to select the system (i.e., TRPS or ESFAS), the specific IU Cell (for TRPS), the division (i.e., A, B, or C), the specific SFM, and the input gain which is to be modified. Then a MWS enable hardwired switch is required to be activated to allow for physical connection of the MWS to the CTB.

The input gain manual calibration operation interface is used to update a process input gain value. The technician is required to provide an input stimulus from a calibrated device to the process input channel on the ISM, then from this MWS display, a technician selects the desired process input, enters a desired gain value, and then selects the Update Gain button of the interface. The technician may use the nominal gain value as a starting gain value or start from a

recorded last gain value. The technician will repeat this process until the process input reading is within an acceptable tolerance from the calibrated device stimulus input.

Because the ADC reads the gain value from volatile registers on the ADC, the system will store the gain values on an NVM installed on the ISM. If the calibration is performed while the SFM is installed in the chassis and powered up, the system immediately stores the gain register values to the NVM on the ISM, updates the ADC registers, and then resets the ADC so the ADC will start the next input conversions using the new gain values. This sequence of actions allows the MWS to immediately display the updated process input value for the technician to compare it to the input stimulus when the technician enters a new gain value. Ensuring the updated process input value is within an acceptable tolerance of the input stimulus supports preventing an inadvertent change to the input gain. The technician can repeat this calibration process while the SFM is powered-up in the chassis.

The ISM's safety function logic is independent (i.e., different logic resources on the FPGA) from the logic used to store information to the NVM and the logic used to configure the volatile ADC registers.

At system power up, the ISM logic will read the gain values from the NVM and will update the ADC volatile gain registers for all input channels before starting the ADC input conversion processes. The gain values are stored in the NVM on the ISM and updated to the ADC at power-up.

The automatic calibration interface of the MWS utilizes a manual input stimulus from a calibrated input device and automatically adjusts the input gain until the process input reading is within 0.001 percent of the stimulus input provided by the user. The technician does not need to enter a gain value. The system will determine the gain value required to reduce the error between the stimulus input and process input to less than 0.001 percent.

Like the setpoint modification operation, the technician must place the SFM in OOS to perform manual or automatic calibration operation.

SHINE has revised Subsection 7.4.5.3.3 of the FSAR to provide additional detail on how the MWS is used to change setpoints and tunable parameters. A markup of the FSAR incorporating these changes is provided as Attachment 1.

**RAI 7-19**

NUREG-1537 states that the protection systems should be fail-safe against malfunction and electrical power failure, should be as close to passive as can be reasonably achieved, should go to completion once initiated, and should go to completion within the time scale derived from applicable analyses in the SAR. The approved TR for the HIPS platform describes the power requirements for a licensee using the HIPS platform. Because this information would depend on the specific instrumentation and control configuration, the NRC staff identified ASAI 46 to require that an applicant referencing the HIPS TR describe power sources to the HIPS platform equipment and how they meet applicable regulatory requirements.

SHINE's response to RAI 7-4 stated that description of the TRPS and ESFAS power source is provided in Subsection 8a2.2 of the SHINE FSAR. SHINE FSAR, Section 7.4.3.4 describes how the HIPS design meets the single failure criterion, including sources of electrical power supply for each division. The information provided is insufficient to evaluate how the safety system

would be powered and how the system would be powered in case of a loss of power.

During the audit performed in May 2021, SHINE staff briefly described how off-site power is supplied to the facility and distributed to the TRPS and ESFAS. SHINE also described how this approach addresses ASAI 46. This type of information should be provided in the SHINE FSAR.

Update the SHINE FSAR to describe the power supplies and power requirements for the TRPS and ESFAS, and how the safety systems meet the design criteria.

This information 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."

The following are examples of the types of information the NRC staff needs to evaluate the power supply for the TRPS and ESFAS. SHINE should ensure that the response to this RAI addresses 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:

- Sources of power supply to each division of the TRPS and ESFAS during normal and emergency operation
- Sources of power for redundant power supplies within each division of the TRPS and ESFAS
- Safety classification of power supplies for the TRPS and ESFAS

**SHINE Response**

During both normal and emergency operation, the TRPS and ESFAS are powered from the uninterruptible electrical power supply system (UPSS), which contains two independent divisions, Division A and Division B. The UPSS provides safety-related 125-volt direct current (VDC) and 208Y/120-volt alternating current (VAC) power to system loads, including TRPS and ESFAS, as described in Subsection 8a2.2.3 of the FSAR.

During normal operation, each UPSS division receives power from the normal electrical power supply system (NPSS) through a battery charger, as described in Subsection 8a2.2.3. The NPSS receives off-site power service from the local utility. The NPSS is described in Section 8a2.1 of the FSAR.

During emergency operation, a standby generator system (SGS) provides a temporary source of nonsafety-related alternate power to the UPSS as described in Subsections 8a2.2.4, 8a2.2.5, and 8a2.2.6 of the FSAR. Isolation between the safety-related UPSS and nonsafety-related loads and power sources, which include the NPSS and SGS, is also described in Subsection 8a2.2.3. A description of how the UPSS provides power to safety-related loads upon a loss of off-site power is provided in Subsection 8a2.2.7 of the FSAR.

Division A of both the TRPS and ESFAS is powered from Division A of the UPSS. Division B of both the TRPS and ESFAS is powered from Division B of the UPSS. Division C of both the

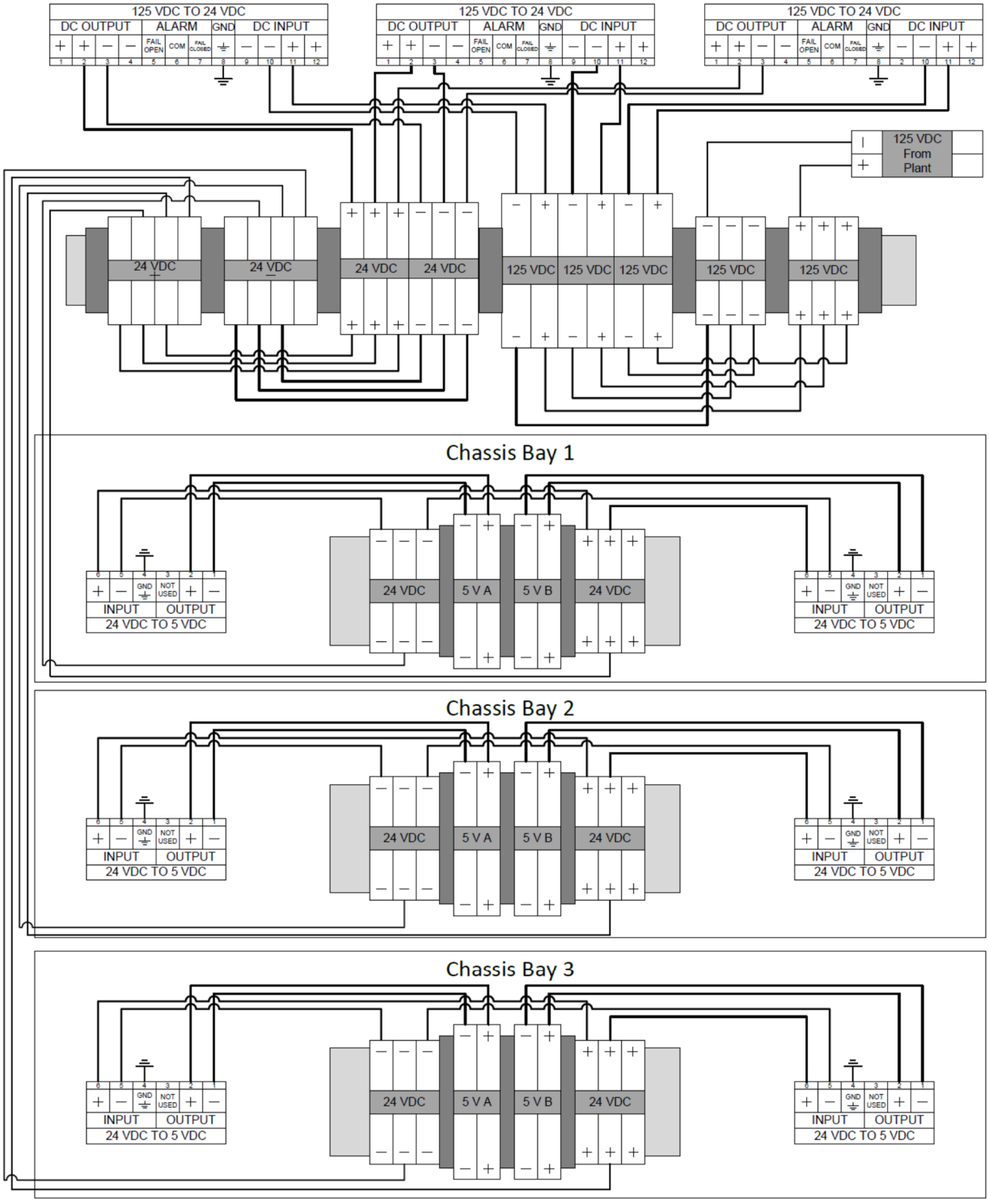
TRPS and ESFAS receives auctioneered power from Division A and Division B of the UPSS. Both the TRPS and ESFAS require 125 VDC power, which is provided by the UPSS as described above. Each TRPS and ESFAS cabinet is provided a single 125 VDC power supply from the facility as described above, which is used to power three redundant, safety-related 125 VDC to 24 VDC converters located at the top of the cabinet. The 24-volt (V) supply is then distributed to each of three chassis mounting bays as needed, where it is then used to power two redundant, safety-related 24 VDC to 5 VDC converters located beneath each chassis bay. These provide independent, safety-related +5V A and +5V B power channels to each chassis. Figure 7-19-1 provides a block diagram of the power distribution in each TRPS and ESFAS cabinet.

ASAI 21 identified in the Safety Evaluation (SE) for the HIPS platform (Reference 4) states that, “an applicant or licensee referencing this SE must provide redundant power sources to separately supply the redundant power conversion features within the HIPS platform. (i.e. the two redundant power sources are connected to a single division in a multi-division system). These power sources are provided to improve reliability and maintainability of the HIPS modules.” The redundant power sources to separately supply the redundant power conversion features were described in the preceding paragraph.

ASAI 46 identified in the SE for the HIPS platform (Reference 4) states that, “An applicant or licensee referencing this SE must describe power sources to the HIPS platform equipment and how they meet applicable regulatory requirements (i.e. the two redundant power sources are connected to a single division in a multi-division system). These power sources are provided to improve the reliability and maintainability of the HIPS modules.” SHINE Design Criterion 27 provides requirements to ensure that the UPSS is capable of permitting functioning of safety-related SSCs. The description of power sources required by ASAI 46 is provided above. Detail on how the UPSS satisfies SHINE Design Criterion 27 and applicable regulatory requirements, as required by ASAI 46, is contained in Subsection 8a2.2 of the FSAR, the SHINE Response to RAI 8-1 (Reference 13), and the SHINE Response to RAI 8-10 (Reference 14).

SHINE has revised Subsections 7.4.3.4 and 7.5.3.3 of the FSAR to provide a more complete description of the power supplies to each division of TRPS and ESFAS, respectively. A mark-up of the FSAR incorporating these changes is provided as Attachment 1. SHINE has also revised the bases related to LCO 3.2.1, LCO 3.2.2, and LCO 3.6.1 of the technical specifications to clarify the utilization voltages within TRPS and ESFAS cabinets. A mark-up of the technical specifications incorporating these changes is provided as Attachment 2.

**Figure 7-19-1: Power Distribution in TRPS and ESFAS Cabinets**



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

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

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

6. Institute of Electrical and Electronics Engineers, “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” IEEE Standard 323-2003, New York, NY

7. Institute of Electrical and Electronics Engineers, “Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Generating Stations,” IEEE Standard 344-2013, New York, NY

8. U.S. Nuclear Regulatory Commission, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Regulatory Guide 1.180, Revision 2, December 2019

9. Institute of Electrical and Electronics Engineers, “Guide for Instrumentation and Control Equipment Grounding in Generating Stations,” IEEE Standard 1050-2004, New York, NY

10. Institute of Electrical and Electronics Engineers, “Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” IEEE Standard 379-2000, New York, NY

11. Institute of Electrical and Electronics Engineers, “Standard Criteria for Independence of Class 1E Equipment and Circuits,” IEEE Standard 384-2008, New York, NY

12. Institute of Electrical and Electronics Engineers,” Standard for Software Verification and Validation,” IEEE Standard 1012-2004, New York, NY

13. SHINE Medical Technologies, LLC letter to NRC, “SHINE Medical Technologies, LLC Operating License Application Response to Request for Additional Information,” dated January 29, 2021 (ML21029A101)

14. SHINE Medical Technologies, LLC letter to NRC, “Application for an Operating License Response to Request for Additional Information,” dated July 2, 2021

**ENCLOSURE 1**
**ATTACHMENT 1**

**SHINE MEDICAL TECHNOLOGIES, LLC**

**SHINE MEDICAL TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE**
**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

**FINAL SAFETY ANALYSIS REPORT CHANGES**
**(MARK-UP)**

27 pages follow

7.4.2.1.2 Protection System Functions

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

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

7.4.2.1.3 Protection System Reliability and Testability

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

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

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

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

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

The maintenance bypass function allows an individual safety function module to be removed from service ~~for required testing without loss of redundancy~~ 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 (SSubsection 7.4.4.4). Calibration, testing, and diagnostics are addressed in Section 8.0 of Topical Report TR-1015-18653, "Design of the Highly Integrated Protection System Platform" (NuScale, 2017). 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 structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident. Division independence is maintained throughout, extending from the sensor to the devices actuating the protective function (Subsection 7.4.5.2.1). The architecture provides two diverse methods for an actuation of the safety functions at the division level, automatic (Subsections 7.4.3.1 and 7.4.4.1) and manual (Subsection 7.4.3.7), and field programmable gate arrays (FPGAs) in each division are of a different physical architecture to prevent common cause failure (CCF) (Subsection 7.4.5.2.4).

7.4.2.1.5 Protection System Failure Modes

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

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

7.4.2.1.6 Separation of Protection and Control Systems

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

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

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.

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

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

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 Subsection 7.4.4.3 and 7.4.4.4. Testing performed during operation is controlled in accordance with the technical specifications to ensure that at least one division of the TRPS is capable of performing its safety functions when required.

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

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

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

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

7.4.2.2.13 Classification and Identification

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

in the loss of the protective function, and no single failure in a single measurement channel can generate an unnecessary safety actuation.

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

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

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

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

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

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

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

### 7.4.3.5 Operating Conditions

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

During normal operation, the TRPS equipment will operate in the applicable normal radiation environments identified in Table 7.2-1 for up to 20 years, replaced at a frequency sufficient such that the radiation qualification of the affected components is not exceeded. The radiation qualification of the affected components is based upon the total integrated dose (TID) identified in Table 7.2-1 being less than the threshold values identified in industry studies.

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

### 7.4.3.6 Seismic, Tornado, Flood

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

### 7.4.3.7 Human Factors

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

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

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

## 7.4.4 OPERATION AND PERFORMANCE

Subsection 7.4.4 discusses the operation of the TRPS.

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

### 7.4.4.1 Monitored Variables and Response

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

#### 7.4.4.1.1 High Source Range Neutron Flux

The high source range neutron flux signal protects against an insertion of excess reactivity during the filling process (Subsection 13a2.1.2, Scenarios 5, 6, and 11). The signal is generated by TRPS when a source range neutron flux input exceeds the high level setpoint. The TRPS bypasses safety actuations based on the high source range neutron flux signal when filling activities cannot be in progress (i.e., Modes 2, 3, and 4), because the fill isolation valves are closed. The signal is transmitted as an analog input to the TRPS from the neutron flux detection system (NFDS) through three independent and redundant channels, one for each division of TRPS. When two-out-of-three or more high source range neutron flux signals are active, an IU Cell Safety Actuation is initiated.

#### 7.4.4.1.2 Low Power Range Neutron Flux

The low power range neutron flux signal protects against loss of the neutron beam followed by a restart of the neutron beam outside of analyzed conditions (Subsection 13a2.1.2, Scenario 4). The signal is generated by TRPS when a power range neutron flux input exceeds the low level setpoint. The low power range neutron flux is only used during the irradiation process (Mode 2) and is bypassed in the other modes of operation. Safety actuations based on the low power range neutron flux are bypassed until the power range neutron flux has reached the power range driver dropout permissive. Once power range neutron flux levels have risen above the high setpoint, then the bypass on the low power range neutron flux is removed. The power range neutron flux is measured as an analog input to the TRPS from the NFDS through three independent and redundant channels, one for each division of TRPS. When two-out-of-three or more low power range neutron flux signals are active, a timer is started that must run to completion for a Driver Dropout to be initiated. If, while the timer is running, less than two-out-of-three low power range neutron flux actuation signals are active, the timer is reset and the TRPS continues operating under normal conditions.

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

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

7.4.4.2 Operational Bypass, Permissives, and Interlocks

Permissive conditions, bypasses, and interlocks are created in each mode of operation specific to that mode to allow the operator to progress the TRPS to the next mode of operation. The TRPS implements logic associated with each mode of operation to prevent an operator from activating a bypass through changing the IU cell mode out of sequential order.

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

If the permissive conditions are not met for transitioning to the next mode and the operator action occurs, the TRPS will not advance to the next mode of operation. Below are the required conditions that must be satisfied before a transition to the following mode in the sequence can be initiated.

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

In each mode of operation, the TRPS bypasses different actuation channels when the actuation channel is not needed for initiation of an IU Cell Safety Actuation, an IU Cell Nitrogen Purge, an

- Low-high TSV dump tank level signal
- TSV fill isolation valve fully closed

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

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

- High source range neutron flux
- Low power range neutron flux
- High PCLS temperature
- Low PCLS temperature
- Low PCLS flow
- Low-high TSV dump tank level signal
- TSV fill isolation valve fully closed

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

### 7.4.4.3 Maintenance Bypass

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

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

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

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

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

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

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

#### 7.4.4.4 Testing Capability

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

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

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

Testing of input devices consists of channel checks, channel tests, and channel calibrations. Channel checks are performed while the channel is in service. Channel tests and channel

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

#### 7.4.4.5 Technical Specifications and Surveillance

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

### 7.4.5 HIGHLY INTEGRATED PROTECTION SYSTEM DESIGN

#### 7.4.5.1 HIPS Design Summary

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

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

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

#### 7.4.5.2 HIPS Design Attributes

##### 7.4.5.2.1 Independence

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

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

The TRPS and ESFAS structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident. Division independence is maintained throughout both systems, extending from the sensor to the devices actuating the protective function. Physical separation is used to achieve separation of redundant sensors. Wiring for redundant divisions uses physical separation and isolation to provide independence for circuits. Separation of wiring is achieved using separate wireways and cable trays for each of Division A, Division B, and Division C.

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

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

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

7.4.5.2.2 Redundancy

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

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

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

Coincidence voting on functions with three divisions of trip determination is implemented so that a single failure of an input process signal will not prevent a trip or actuation from occurring when required. In addition, a single failure of an input process signal with three divisions of trip determination will not cause spurious actuation or inadvertent trips or actuations when they are not required.

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

An FMEA was conducted, analyzing failure modes of system components associated with the TRPS and ESFAS. The FMEA is a qualitative assessment which follows a systematic approach for identifying the modes of single system component failures and for evaluating their consequences.

Because of the triple redundant architecture within each redundant division of equipment for the TRPS and ESFAS, failure mechanisms that affect a single function have no effect on facility operation. As documented in the FMEA, 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.

In conjunction with the FMEA, a single failure analysis of the TRPS and ESFAS was conducted. The assessment applied to the sense and command and execute features of the TRPS and ESFAS used for safety-related functions. The scope of the assessment included sensors, trip determination, signal conditioning, DC-DC converters and power supplies, and actuation logic. 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.

7.4.5.2.3 Predictability and Repeatability

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

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

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

To meet a response time performance requirement of 500 milliseconds, a HIPS platform-based system must acquire the input signal that represents the start of a response time performance requirement, perform logic processing associated with the response time performance requirement, and generate an output signal that represents the end of a response time performance requirement. These HIPS platform response time components exclude: (1) the earlier plant process delays through the sensor input to the platform, and (2) the latter delays through a final actuating device to affect the plant process (Figure 7.4-2). The required response times credited in the safety analysis for systems using the HIPS design (TRPS, ESFAS) cover the process delays through the sensor input to the platform and the delays through the final actuating device.

7.4.5.2.4 Diversity

The APL portions within an EIM support the implementation of different actuation methods. Having the capability for hardwired signals into each EIM supports the capability for additional and diverse actuation means from automated actuation. As an example, a division of APL circuits may receive inputs automatically from the programmable logic portion of the TRPS, inputs from manual controls in the facility control room, and input signals from a nonsafety control system. Both the manual controls and nonsafety control system inputs come individually into the APL and are downstream of the programmable logic portion of the TRPS architecture as shown in Figure 7.1-2.

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

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

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

In order to ensure performance in the presence of a digital CCF, the different divisions of the system (TRPS, ESFAS) use different FPGA architectures (static random access memory, flash, or one-time programmable). A diversity and defense-in-depth (D3) assessment of the TRPS and ESFAS was performed using the guidance of NUREG/CR-6303 (USNRC, 1994) to identify potential vulnerabilities to digital CCFs. The D3 assessment concluded:

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

Display of information is available to the operator(s) at various locations in the facility control room. Information from the safety-related control systems is processed through the system (TRPS or ESFAS) and is transmitted to PICS for display on the static display screens of the main control board or at the operator workstation. This monitoring and indication information provided to PICS from TRPS and ESFAS includes the status and values of the monitored variables identified in Table 7.4-1 and Table 7.5-1 as well as the status of the TRPS and ESFAS systems themselves. Display of this monitoring and indication information in the facility control room provides the information operators require to determine if manual actuation of a safety system is 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

platform features support the establishment and use of a secure operational environment and protective measures to maintain it.

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

#### 7.4.5.3.2 Cyber Security Design Features

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

The defensive system architecture has the following characteristics:

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

#### 7.4.5.3.3 Access Control

Additional access control features include:

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

Each division has a nonsafety-related MWS for the purpose of online monitoring and offline maintenance and calibration. The HIPS platform MWS supports online monitoring through one-way isolated communication ports. The MWS is used to update setpoints and tunable parameters in the HIPS chassis when the safety function is out of service. The MWS allows a technician password protected access to select the system (i.e., TRPS or ESFAS), the specific IU cell (for TRPS), the division (i.e., A, B, or C), the specific SFM, and the trip setpoint or input gain which is to be modified. 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. Controls are also put in place to prevent inadvertent changes to a setpoint or tunable parameter. A temporary cable and OOS switch are required to be activated before any changes can be made to an SFM. When the safety function is removed from service, either in bypass or trip, an indication is provided by the HIPS platform that can be used to drive an alarm in the facility

control room to inform the operator. Setpoint and calibration data are stored on the nonvolatile memory (NVM). Adjustments to parameters are performed in accordance with technical specifications, including any that establish the minimum number of redundant safety channels that must remain operable for the applicable operating mode and conditions.

#### 7.4.5.4 Software Requirements Development

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

The systems are implemented on a logic-based platform that does not utilize traditional software or microprocessors for operation. It is composed of logic implemented using discrete components and FPGA technology. The platform design was developed to support meeting the guidelines and the requirements of NRC Regulatory Guides and IEEE standards applicable to safety-related applications.

The HIPS platform has been reviewed and approved by the NRC for use in safety-related applications for commercial nuclear power plants (NuScale, 2017).

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

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

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

##### 7.4.5.4.1 Key Responsibilities

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

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

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

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

#### 7.4.5.5 HIPS Performance Analysis

HIPS system performance is addressed in Subsection 7.4.4.

Diagnostic and maintenance features provided by the HIPS platform features include the use of BIST, cyclic redundancy checks (CRC), periodic surveillance testing, and other tests in each type of module, as appropriate, to verify normal operation. Attributes of the system incorporate the diagnostic and maintenance principles outlined in Section 8.0 of Topical Report TR-1015-18653 (NuScale, 2017).

The self-testing features of the HIPS platform are designed, developed, and validated at the same level as the functional logic. The overlapped self-test features of the HIPS platform are integral to the operation of the system and are therefore designed, developed, and validated to the same rigor as the rest of the platform.

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 TRPS and ESFAS incorporate failure detection and isolation techniques. Fault detection and indication occurs at the module level, which enables plant personnel to identify the module that needs to be replaced. Self-testing will generate an alarm and report a failure to the operator and place the component (e.g., SFM, SBVM, or EIM components) in a fail-safe state.

The MWS is used to perform modification of configurable variables and setpoints and in-chassis calibration of TRPS and ESFAS equipment as described in Subsection 7.4.5.3.3.

## 7.4.6 CONCLUSION

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

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

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

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.

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

7.5.2.1.3 Protection System Reliability and Testability

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

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

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

The maintenance bypass function allows an individual safety function module to be removed from service ~~for required testing~~ 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 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). The architecture provides two diverse methods for an actuation of the safety functions at the division level, automatic and manual, and field programmable gate arrays (FPGAs) in each division are of a different physical architecture to prevent common cause failure (Subsections 7.4.5.2.4 and 7.5.3.6).

7.5.2.1.5 Protection System Failure Modes

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

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

7.5.2.1.6 Separation of Protection and Control Systems

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

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

7.5.2.2.3 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.

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

#### 7.5.2.2.5 Independence

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

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

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

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

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

The ESFAS structures, systems, and components that comprise a division are physically separated to retain the capability of performing the required safety functions during a design basis accident (Subsection 7.4.5.2.1) and nonsafety-related ESFAS inputs and outputs are

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

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

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

### 7.5.3.4 Operating Conditions

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

During normal operation, the ESFAS equipment will operate in the applicable normal radiation environments identified in Table 7.2-1 for up to 20 years, replaced at a frequency sufficient such that the radiation qualification of the affected components is not exceeded. The radiation qualification of the affected components is based upon the total integrated dose (TID) identified in Table 7.2-1 being less than the threshold values identified in industry studies.

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

### 7.5.3.5 Seismic, Tornado, Flood

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

### 7.5.3.6 Human Factors

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

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

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

#### 7.5.3.12 Design Codes and Standards

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

1) Section 8 of IEEE Standard 344-2013, IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations (IEEE, 2013); invoked as guidance to meet ESFAS Criterion 14.
2) IEEE Standard 379-2000, IEEE Standard Application of Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (IEEE, 2000); invoked as guidance to meet SHINE Design Criterion 15.
3) IEEE Standard 384-2008, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (IEEE, 2008); invoked as guidance for separation of safety-related and nonsafety-related cables and raceways to meet ESFAS Design Criteria 21 and 22, and as described in Subsection 8a2.1.3 and Subsection 8a2.1.5.
4) Section 5.2.1 of IEEE Standard 1050-2004, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations (IEEE, 2004b); invoked as guidance to meet ESFAS Design Criterion 47 and to support electromagnetic compatibility qualification for digital I&C equipment.
5) The guidance of ANSI/ANS 15.8-1995, Quality Assurance Program Requirements for Research Reactors (R2013) (ANSI/ANS, 1995), as endorsed by Regulatory Guide 2.5, Quality Assurance Program Requirements for Research and Test Reactors (USNRC, 2010), is applied as part of the SHINE Quality Assurance Program for complying with the programmatic requirements of 10 CFR 50.34(b)(6)(ii).
6) IEEE Standard 1012-2004, IEEE Standard for Software Verification and Validation (IEEE 2004a); invoked as guidance to meet ESFAS Design Criterion 8.
7) IEEE Standard 323-2003, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations (IEEE, 2003b), invoked as guidance to meet ESFAS Criterion 14.

### 7.5.4 OPERATION AND PERFORMANCE

Subsection 7.5.4 discusses the operation of the ESFAS.

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

#### 7.5.4.1 Monitored Variables and Response

Table 7.5-1 identifies specific variables that provide input into the ESFAS and includes the instrument range for covering normal and accident conditions, the accuracy for each variable, the

An SFM may also be placed in trip by use of the OOS and trip/bypass switches, as described in Sections 2.5.1 and 2.5.2 of Topical Report TR-1015-18653 (NuScale, 2017). ~~Placing an SFM in trip preserves the single failure criterion for variables associated with that SFM where three channels are provided. In cases where only two channels are provided, placing a channel in trip serves to actuate the associated safety function. Inoperable channels are required to be placed in trip, or other actions are required to be taken to mitigate the condition, in accordance with the technical specifications.~~With the OOS switch in the OOS position, the trip/bypass switch is used to activate maintenance trips and maintenance bypasses. The trip/bypass switch signal is input first to a hardwired module (HWM), which then converts the trip/bypass discrete input to a logic level signal and makes the signal available to the associated SBMs or SBVMs within the same division as the trip/bypass switch. When the OOS switch is in the Operate position and the SFM is functioning normally, the SBMs or SBVMs associated with the SFM will ignore the associated trip/bypass switch input.

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

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

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

#### 7.5.4.5 Testing Capability

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

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

## 7.9 REFERENCES

**ANSI, 1999.** Sampling and Monitoring Releases of Airborne Radioactive Substances from the Stacks and Ducts of Nuclear Facilities, ANSI N13.1-1999, American National Standards Institute, 1999.

**ANSI/ANS, 1995.** Quality Assurance Program Requirements for Research Reactors, ANSI/ANS 15.8-1995 (R2013), American National Standards Institute/American Nuclear Society, 1995.

**IEEE, 2000.** IEEE Standard Application of Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE 379-2000, Institute of Electrical and Electronics Engineers, 2000.

**IEEE, 2003a.** IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE 7-4.3.2-2003, Institute of Electrical and Electronics Engineers, 2003.

**IEEE, 2003b.** IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE 323-2003, Institute of Electrical and Electronics Engineers, 2003.

**IEEE, 2004a.** IEEE Standard for Software Verification and Validation, IEEE 1012-2004, Institute of Electrical and Electronics Engineers, 2004.

**IEEE, 2004b.** IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations, IEEE 1050-2004, Institute of Electrical and Electronics Engineers, 2004.

**IEEE, 2008.** IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits, IEEE 384-2008, Institute of Electrical and Electronics Engineers, 2008.

**IEEE, 2013.** IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations, IEEE 344-2013, Institute of Electrical and Electronics Engineers, 2013.

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

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

**USNRC, 2010.** Quality Assurance Program Requirements for Research and Test Reactors, Regulatory Guide 2.5, Revision 1, U.S. Nuclear Regulatory Commission, June 2010.

**USNRC, 2017.** Safety Evaluation by the Office of New Reactors, Licensing Topical Report (TR) 1015-18653-P (Revision 2), “Design of the Highly Integrated Protection System Platform,” NuScale Power, LLC, U.S. Nuclear Regulatory Commission, May 2017.

**ENCLOSURE 1**
**ATTACHMENT 2**

**SHINE MEDICAL TECHNOLOGIES, LLC**

**SHINE MEDICAL TECHNOLOGIES, LLC APPLICATION FOR AN OPERATING LICENSE**
**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

**TECHNICAL SPECIFICATIONS CHANGES**
**(MARK-UP)**

3 pages follow

Basis 3.2.1 LCO

Each TRPS subsystem, one associated with each IU, is required to perform safety functions specified by the SHINE safety analysis, as described in FSAR Subsection 7.4.3.1.

LCO 3.2.1 addresses only the logic, voting, and actuation portions of the TRPS. The scope of this LCO begins at the inputs to the scheduling, bypass and voting modules (SBVMs) or scheduling and bypass modules (SBMs) and extends through the equipment interface modules (EIMs), ending at the output to the actuated components. The safety function modules (SFMs) and the input channels are addressed in LCO 3.2.3. The actuated components themselves are addressed in LCO 3.4.1 (for primary Confinement and primary system boundary components), and LCO 3.6.2 (for safety-related breakers).

LCO 3.2.1 additionally addresses the two redundant 5V power supplies per TRPS subsystem, per Division. The ~~48~~24V power supplies for each Division of TRPS cabinets are addressed in LCO 3.6.1.

The TRPS bypass logic is implemented in all three Divisions. 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 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.

If one SBVM or SBM in a single Division is inoperable, the module is required to be restored to Operable within 30 days. This completion time allows for replacement of failed components, while limiting the amount of time the IUs are allowed to operate with reduced TRPS reliability. The 30 day duration is acceptable because the output of a failed SBVM is received as a trip signal by the associated EIMs, and the output of a failed SBM is received as a trip signal by the Division A and B SBVMs, preserving the single failure criterion for the remaining Operable modules.

If one 5V power supply in a single Division is inoperable, the power supply is required to be restored to Operable within 72 hours. This completion time allows for adequate time for replacement of failed components, while limiting the amount of time the IUs are allowed to operate with reduced TRPS reliability. The 72 hour duration is acceptable due to the low likelihood of an additional power supply failure on the affected Division while a power supply is inoperable, and the ability of the redundant TRPS Division(s) to sense adverse conditions and actuate equipment in response to an event.

SR

The TRPS platform has end-to-end self-testing that covers each module from sensor input to the output switching logic (except for the discrete circuitry of the actuation and priority logic). The individual self-tests on the different components of the highly integrated protection system (HIPS) platform evaluate whether the entire platform is functioning correctly, as described in FSAR Subsection 7.4.4.4. HIPS modules include light emitting diodes (LEDs) that are used to determine the state of the module latches, the operational state of the module, and the presence of any faults. The HIPS platform self-testing features and the associated front panel LEDs allow for the timely identification of certain malfunctions within the HIPS equipment. Only manual actuation and priority logic functions are not covered by the self-testing features and therefore require periodic surveillance. The actuation priority logic test verifies the functionality of the discrete priority logic circuits of the TRPS safety-related control system. The test includes testing of the manual actuation functions of TRPS. Built-in redundancy and notification of failures within the TRPS supports the surveillance frequency.

Basis 3.2.2 LCO

The ESFAS is required to perform safety functions specified by the SHINE safety analysis, as described in FSAR Subsection 7.5.3.1.

LCO 3.2.2 addresses only the logic, voting, and actuation portions of the ESFAS. The scope of this LCO begins at the inputs to the SBVMs or SBMs and extends through the EIMs, ending at the output to the actuated components. The SFMs and the input channels are addressed in LCO 3.2.4. The actuated components themselves are addressed in LCO 3.4.3 (for tritium Confinement boundary components), LCO 3.4.4 (for supercell Confinement dampers), LCO 3.6.2 (for safety-related breakers), LCO 3.8.9 (for RCA isolation dampers), and LCO 3.8.10 (for facility-specific safety-related valves and dampers).

LCO 3.2.2 also addresses the two redundant 5V power supplies per ESFAS Division. The ~~48~~24V power supplies for each Division of ESFAS cabinets are addressed in LCO 3.6.1.

The ESFAS bypass logic is implemented in all three Divisions. 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 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

Basis 3.6.1 LCO

The safety-related uninterruptible electrical power supply system (UPSS) for the facility consists of two redundant Divisions of 125-volt direct current (VDC) batteries, inverters, bypass transformers, distribution panels, and other breakers and distribution equipment necessary to feed safety-related alternating current (AC) and direct current (DC) loads, as described in FSAR Section 8a2.2. The ~~48~~24V power supplies for the TRPS and ESFAS cabinets are also within the scope of this LCO for the UPSS distribution system. The UPSS provides an emergency back-up power supply for safety-related equipment and monitoring which protects against a total or partial loss of normal facility power.

The UPSS minimum Operable Divisions ensures there is adequate backup battery power for postulated accident scenarios, as described in FSAR Subsection 8a2.2.3.

A battery is considered Operable when battery specific gravity is in the range of ≥ 1.210 and ≤ 1.300 at 77°F and battery voltage is at or greater than the minimum battery voltage provided in Table B-3.6.1.

A battery charger is considered Operable when it is energized to the voltage provided in Table B-3.6.1 and is connected to its associated DC distribution panel.

An inverter is considered Operable when it is energized to the voltage provided in Table B-3.6.1 at a frequency of 60 Hz +/- 1 Hz.

A DC distribution panel is the switchgear to which the battery, battery charger and inverter connect. A DC distribution panel is considered Operable when it is energized from either the battery or battery charger.

An AC distribution panel is the switchgear which the inverter supplies. An AC distribution panel is considered Operable when it is energized by the inverter.

Additionally, for a UPSS Division to be Operable, the inverter must be supplied by the DC distribution panel and must be supplying power to the AC distribution panel and the battery and battery charger must be connected to the DC distribution panel. This configuration ensures availability of required power on a loss of off-site power.

A single overall electrical power system serves the main production facility, including both the irradiation facility and the radioisotope production facility, as well as the site and support buildings, as described in FSAR Section 8a2.1. The normal electrical power supply system receives off-site power from the local utility.

The standby generator system (SGS) consists of a 480Y/277 VAC, 60 Hertz natural gas-driven generator, as described in FSAR Subsection 8a2.2.6. Although not required by the accident analysis, the SGS is designed to automatically start and begin step loading within one minute of and complete power transfers within five minutes of the loss of off-site power (LOOP). The SGS is sized to carry the full load of both Divisions of the UPSS. The SGS supplies power to the UPSS buses, re-charges the UPSS batteries, supplies additional loads used for life-safety or facility monitoring, and allows operational flexibility while responding to the LOOP.