

SAFETY EVALUATION BY THE OFFICE OF NEW REACTORS

LICENSING TOPICAL REPORT (TR)-1015-18653-P (REVISION 1)

“DESIGN OF HIGHLY INTEGRATED PROTECTION SYSTEM PLATFORM”

NUSCALE POWER, LLC

DOCKET: PROJ0769

1.0 INTRODUCTION

By letter dated December 23, 2015, NuScale Power, LLC (NuScale) submitted a request for the U.S. Nuclear Regulatory Commission (NRC) staff to review Topical Report (TR)-1015-18653, “Highly Integrated Protection System Platform,” Revision 0 (Reference (Ref.) 6.1-1). Specifically, NuScale requested staff review and approval to confirm that the Highly Integrated Protection System (HIPS) platform meets the applicable regulatory requirements associated with the fundamental instrumentation and control (I&C) design principles. The NRC accepted the TR for review by letter dated February 19, 2016 (Ref. 6.1-2).

By letter dated November 4, 2016, NuScale responded to the staff’s request for additional information (RAI)s by submitting an updated revision of the proprietary and nonproprietary versions of TR-1015-18653, “Design of Highly Integrated Protection System Platform,” Revision 1 (Ref. 6.1-3).

The TR describes key design concepts for the digital I&C (DI&C) platform cooperatively developed by Rock Creek Innovations, LLC, and NuScale. Specifically, the TR describes the design attributes of the HIPS platform standardized circuit boards and their instruments chassis. The HIPS platform is based on field programmable gate array (FPGA) technology. The TR describes the testing and diagnostics concepts applied to the HIPS platform.

The purpose of this safety evaluation (SE) is to assess the suitability of the HIPS platform for use in safety-related applications in U.S. nuclear power plants (NPPs). This review will determine if the HIPS platform meets the applicable regulatory requirements associated with the fundamental I&C design principles of independence, redundancy, predictability and repeatability, and diversity and defense in depth (D3) as provided by the guidance in Design-Specific Review Standard (DSRS) (Ref. 6.1-6), Chapter 7.0, Sections 7.1.2, 7.1.3, 7.1.4, and 7.1.5.

The scope of the review excludes the quality of the HIPS platform standardized circuit boards and their instruments chassis, the quality of the design process, and the comprehensiveness of its equipment qualification. These activities are application specific, dependent on the equipment vendor to be used to implement the HIPS platform. To support its SE, the staff

conducted a regulatory audit from July 6, 2016, to July 7, 2016, at the NuScale offices located in Rockville, MD (Ref. 6.1-4). The purpose of the audit was to (1) deepen the understanding of the HIPS platform and associated design documents, (2) review nondocketed information related to the HIPS platform, and (3) confirm whether or not fundamental I&C design principles and regulatory requirements were being met.

The staff plans to conduct an additional regulatory audit from January 30, 2017, to February 3, 2017, at the Ultra Electronics facility in Wimborne, United Kingdom (Ref. 6.1-5). The purpose of the audit is to witness the prototype HIPS platform factory acceptance testing. The staff plans to observe the hardware configuration of the prototype test specimen and the performance characteristics of the platform.

Section 2.0 of this SE identifies the applicable regulatory bases and corresponding guidance and regulatory acceptance criteria against which the staff evaluated the TR. Section 3.0 contains the I&C technical evaluation of the TR submittal and includes a description of the generic platform. Section 4.0 describes the limitations and conditions that apply to applicants referencing this SE for use of the HIPS platform in safety-related applications in NPPs. Section 5.0 provides the staff's findings and conclusions. Section 6.0 lists the references. Section 7.0 contains the list of acronyms.

2.0 REGULATORY EVALUATION

The acceptance criteria used by staff as the basis for the review of NuScale's approach are set forth in the "Design-Specific Review Standard for NuScale Small Modular Reactor Design," hereafter referred to as the Design-Specific Review Standard (DSRS) (Ref. 6.1-6). This document-sets forth a method for compliance with applicable sections of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 6.1-7), and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 6.1-8).

The suitability of a DI&C platform for use in safety systems depends on how it incorporates the fundamental I&C design principles of independence, redundancy, predictability and repeatability, and D3, as well as important platform functionality, including the capability for testing and calibration. Because this platform is intended for use in safety systems and other safety-related applications, the NRC evaluated the TR against its ability to support application-specific system provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet dated January 30, 1995 (Ref. 6.1-9), based on the guidance contained in the DSRS Chapter 7.0, as they apply for this TR, for the NuScale small modular reactor (SMR) design, which provides acceptance criteria for this standard. The NRC similarly evaluated the TR against IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," (Ref. 6.1-10) and the DSRS for the NuScale SMR design.

The determination of full compliance with the applicable regulations remains subject to a plant-specific licensing review of a full system design based on the HIPS platform. Application-specific action items (ASAs) identify criteria that applicants or licensees referencing this SE should address (see Section 4.0). In part, these criteria facilitate an applicant's or licensee's ability to establish full compliance with the design criteria and regulations identified in DSRS Chapter 7, Table 7-1, "Instrumentation and Control—Mapping of Regulatory Requirements, Guidance, and DSRS Acceptance Criteria," applicable to the applicant's or licensee's DI&C system and in effect at the time of the HIPS platform review. Regardless, the ASAs identified in Section 4.0 do not obviate an applicant's or licensee's responsibility to adequately address new or changed design criteria or regulations that apply at the time of application, in addition to those that would apply to this SE when making a voluntary change to its facility or TR.

The following regulations and Commission policy statement are applicable to the TR:

- In 10 CFR 50.55a(h), the Office of the Federal Register (OFR) approved for incorporation by reference into 10 CFR 50.55a the 1991 version of IEEE Std. 603-1991, including the correction sheet dated January 30, 1995.
- The staff requirements memorandum (SRM), dated July 21, 1993, to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, describes the NRC position on D3 in item 18.II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems."

The staff evaluated the TR using applicable portions of the following guidance:

- Regulatory Guide (RG) 1.152, "Criteria for Use of Computers In Safety Systems of Nuclear Power Plants," Revision 3, issued July 2011, describes a method acceptable to the staff for complying with the NRC's regulations as they apply to high functional reliability and design requirements for computers used in safety systems of NPPs.
- RG 1.153, "Criteria for Safety Systems of Nuclear Power Plants," Revision 1, issued Jun. 1996, describes a method acceptable to the staff for complying with NRC regulations with respect to the design, reliability, qualification, and testability of the power and I&C portions of the safety systems of NPPs before the incorporation of IEEE Std. 603-1991 by reference into the regulations.
- RG 1.75, "Criteria for Independence of Electrical Safety Systems," Revision 3, issued February 2005, describes a method acceptable to the staff for meeting the physical independence of the circuits and electrical equipment that comprise or are associated with safety systems.

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994, summarizes several D3 analyses performed after 1990 and presents an acceptable method for performing such analyses.
- DI&C-ISG Interim Staff Guidance-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," Revision 1, issued March 2009, describes methods acceptable to the staff to prevent adverse interactions among safety divisions and between safety-related equipment and equipment that is not safety related.

3.0 TECHNICAL EVALUATION

The subsections below identify and describe the HIPS platform's I&C components and evaluate these components and their development against the regulatory evaluation criteria identified in Section 2.0. Section 3.1 describes the HIPS platform, including the I&C components and architecture. Each of the remaining subsections provides a specific technical evaluation against the applicable regulatory evaluation criteria.

3.1 HIPS Platform Description

The HIPS platform is a logic-based platform that does not use software or microprocessors for operation.¹ It is composed of logic implemented using discrete components and FPGA technology. The scope of the HIPS platform does not include the cabinet and peripheral devices, such as sensors, external redundant power supplies, breakers, terminal boards, and fuse holders. The maintenance workstation (MWS) is not part of the base platform, so it is not within the scope of the TR. The MWS is only included to support the evaluation on monitoring/indication, testing, and calibration.

The scope of this SE is limited to the HIPS platform, which consists of various discrete components and modules. The HIPS platform is intended to be used as a generic DI&C platform in safety-related applications in NPPs.

Sections 3.1.1 to 3.1.4 give an overview of the HIPS platform chassis, backplane, back panel, and module types. Section 3.1.5 discusses the HIPS platform communication bus design concepts. Sections 3.1.6 to 3.1.8 provide an overview of the representative protection system (PS) architecture, the PS gateway, and the MWS. Section 3.1.9 contains the staff evaluation of the self-diagnostics, test, and calibration capabilities to detect and annunciate equipment failures and to support maintenance and surveillance tests.

¹ Unlike microprocessor-based computer systems, FPGA technology does not rely on an operating system, software drivers for peripheral devices, or an executable software program. However, the MWS contains software maintenance tools that are used to retrieve/confirm the configuration of the installed equipment. In addition, the MWS contains software maintenance tools that are used to update setpoints and tunable parameters in the nonvolatile memory when the safety function module is out of service (OOS) (i.e., the OOS switch is activated).

3.1.1 HIPS chassis

The HIPS chassis is an industry standard 48.26 centimeters (cm) (19 inches (in.)) wide cabinet-mountable card frame. The HIPS chassis is 26.67 cm (10.5 in.) tall and 40.01 cm (15.75 in.) deep. The individual HIPS modules slide in from the front, and all permanent cabling and connectors are made on the HIPS back panel. Figure 3-1 shows a populated HIPS chassis with the trip/bypass plate.



Figure 3-1 Populated HIPS chassis with the trip/bypass plate

3.1.2 HIPS Backplane

The HIPS backplane is a printed circuit board (PCB) with female connectors and copper traces. The HIPS backplane has no active components. The quantity and location of female connectors, along with traces on the HIPS backplane, are unique to each HIPS platform implementation. Three types of signals are traced on the backplane: (1) power and grounding signals, (2) communication signals, and (3) hardwired module (HWM) signals.

The HIPS backplane is mounted at the rear of the HIPS chassis to provide an interconnection between the various HIPS modules and field inputs. Signals on the backplane are only traced to modules that need that signal. Multiple chassis backplanes can be connected to create a virtual single backplane across all chassis.

The HIPS backplane is designed using the Association Connecting Electronics Industries standard IPC-6012B, "Qualification and Performance Specification for Rigid Printed Boards," (see Ref 6.1-18).

3.1.3 HIPS Back Panel

The HIPS back panel is how the HIPS backplane is mounted to the HIPS chassis. The HIPS back panel provides structural support for connectors mounted in the rear, allowing wiring into and out of the HIPS chassis.

3.1.4 HIPS Modules

The HIPS module represents a line-replaceable unit. The HIPS module consists of a base PCB, a set of rear connectors, a front panel, and electronic components. In some modules, additional submodules may be mounted to the base board (see Section 3.1.4.1). The HIPS module has a predefined set of rear connectors mounted to the base PCB for connection to the HIPS backplane. The HIPS module has a front plate with specific user interface items (e.g., light-emitting diodes (LEDs), switches). All HIPS modules provide two LED indicators that show the state of the module latches, the operational state of the module, and the presence of any faults.

The front panel has injector/ejector latches mounted for insertion and removal of the HIPS module to and from a populated HIPS chassis. All HIPS modules can be hot swapped from a powered chassis without damaging the module or the chassis. Hot swap capability supports maintenance activities without disrupting other modules within the chassis (see Section 3.1.4.1.3). In addition, self-tests are performed to ensure the HIPS module is inserted in the correct location (see Section 3.1.9).

The HIPS platform includes four different HIPS modules capable of performing dedicated functions: (1) safety function module (SFM), (2) communication module (CM), (3) equipment interface module (EIM), and (4) HWM.

3.1.4.1 Safety Function Module

The SFM is responsible for signal conditioning and actuation of safety function(s) from input signals. The SFM provides scaled value of input process to nonsafety controls and safety display for monitoring purposes. The SFM is composed of three functional areas: (1) signal conditioning/analog-to-digital conversion (input submodule), (2) SFM digital logic circuits, and (3) communications engines.

Each SFM can handle up to four input submodules, and the input type can be any combination of analog and digital (see Section 3.1.4.1.1). The input submodules used on an SFM are limited to only those required to implement its safety function.

The SFM uses an FPGA device to contain all digital logic circuits. The SFM logic functions are implemented within the FPGA portion of the SFM and consist of multiple deterministic-state machines. The output of each of the input submodules is sent to four signal paths in the FPGA. One of the signal paths is to the monitoring and indication bus (MIB) logic function. The other three signal paths (i.e., safety data bus (SDB)1, SDB2, and SDB3) are inputs to core logic functions that do the following:

- Convert the output of the input submodules into engineering units.
- Perform the safety function algorithm.
- Compare the safety function algorithm output to a setpoint and make a determination of trip or engineered safety feature (ESF) actuation.
- Generate permissives and control interlocks.

These bulleted items can be performed by a core logic function that is logically independent (i.e., each core logic function has its own gate-level implementation) from any other core logic function. This allows both for three functionally independent core logic functions and for the continuation of three redundant signal paths. The safety function algorithm is processed through three redundant paths to provide error detection and fault tolerance of the safety function.

The two other logic functions within the FPGA are (1) the MIB logic function and (2) the calibration and testing bus (CTB) logic function. The MIB logic function obtains the parameter value(s) from the input submodule. The MIB logic function also obtains trip determination information, status information, and diagnostic information from each of the three redundant core logic functions. This information is sent to the MWS through the MIB. The CTB functional logic allows the MWS to update the tunable parameters in the nonvolatile memory (NVM).

The NVM contains the source of setpoints and tunable parameters for all logic paths. The setpoint and tunable parameters can be modified when the SFM is out of service (OOS) (i.e., the OOS switch is activated). Some of the parameters in the NVM cannot be modified with the SFM installed in the chassis. At module startup, the NVM parameters are loaded into registers in each core logic function. Once loaded, each core logic function runs independently and does not access the NVM while the SFM is in service. Activating the OOS switch permits modification of the tunable parameters in NVM. The new NVM parameters can be loaded into the core logic paths by activating the load switch on the front of the SFM while the SFM is OOS.

The SFM includes built-in self-test (BIST) capabilities to detect single-point failures in each channel, the FPGA logic circuits, the NVM configuration, and the power management logic. The BIST capabilities are described throughout the SE sections below.

3.1.4.1.1 Input Submodule

The input submodule performs signal conditioning and analog-to digital conversion and contains a serial interface. These digital signals are made available to the SFM's FPGA.

In its Request for Additional Information (RAI) 3, Question 07.01 Draft DSRS-7, the staff asked the applicant to describe the different input types the input submodule can receive. In its response to RAI 3, Question 07.01 Draft DSRS-7, dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that input types can be any combination of standard analog signals, such as the resistance temperature detector (RTD), thermocouple, 4–20 milliamperes, 10–50 milliamperes, and 0–10 volts. The input submodule can accept inputs from digital sensors that are transmitted as analog signals (e.g., voltage or current signal loop or binary input signals). Lastly, the applicant stated that the HIPS platform is not designed to decode or use the digital signal superimposed on top of the conventional analog signal that is sent by a “smart” device or transmitter. Based on the applicant's response to RAI 3, Question 07.01 Draft DSRS-7, the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Section 2.5.1.1, “Input Submodule,” provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-7, is resolved and closed.

The HIPS platform can process nonsafety-related inputs to the PS (e.g., anticipatory turbine or main feedwater trip signals required by 10 CFR 50.34(f)(2)(xxiii)). The logic developed for the nonsafety-related inputs will be developed as safety related and qualified to the same level as the safety-related logic. These nonsafety-related inputs are used for indication only and will only be sent to the MIB logic function for processing. Because the signal path (i.e., MIB) is not connected to the SDB communication engines, it cannot affect the safety data on the SDBs (i.e., SDB1, SDB2, and SDB3). In addition, isolation between the nonsafety-related field input signals and the HIPS platform is maintained by galvanic isolators on the SFM. These galvanic isolation features used to isolate nonsafety-related inputs are passive safety-related features that do not rely on power to provide the required protection.

The input submodule self-testing and auto calibration features are designed to detect failures and faults related to the FPGA-related portions of an instrument channel. The input submodule has built-in testing capabilities that perform an autocalibration of the analog-to-digital conversion (ADC) process. TR Section 8.2.1.1 describes the self-testing feature of the SFM. The SFM input sub-module performs a continuous self-test by interleaving test samples in between data samples. The self-testing of these units is handled by interleaving test samples of known voltage references in between the data samples.

3.1.4.1.2 Communication Engines

The communication engine consists of five separate and logically independent communication ports (i.e., capable of transmitting data regardless of the status of the other communication

engines). Each port is dedicated to one of the RS-485 communication buses (i.e., SDB1, SDB2, SDB3, MIB, and CTB).

Each communication engine is connected to an RS-485 physical layer. This provides the capability for communication on the corresponding communication bus of the backplane. The bus topology is physically a multidrop RS-485 configuration using a master-slave protocol. The communication engines on an SFM are the slaves. However, while physically configured in a multidrop topology, the communication engine implemented in the FPGA of an SFM creates a virtual point-to-point connection. As slaves on the communication bus, SFMs do not initiate communication. Instead, they await a request for information from the master. Embedded within the request packet from the master is the unique identifier of a slave. Although the request packet is received by all communication engines on that bus, only the slave that corresponds with the unique identifier provides a response packet; hence, a virtual point-to-point communication session is established.

The MIB can be used to transmit channel input data to other plant equipment (e.g., indicators or plant computers) to allow for performance of manual or automated channel checks.

3.1.4.1.3 Bypass or Trip Operation

Each SFM that has a safety-related function has an associated trip/bypass switch connected to an HWM that isolates the signal and places the trip or bypass information on the backplane where it is routed only to the scheduling and bypass modules (SBMs) where it is used. Each SFM also has an OOS switch installed on its front plate. When an SFM is placed OOS and its associated trip/bypass switch is in bypass, all safety-related functions on that SFM are placed into maintenance bypass at the SBM. Depending on the position of the trip/bypass switch, when the OOS switch on the SFM is activated, the SBM forces the safety function in trip or bypass, respectively, and takes the channel OOS. It also provides the appropriate alarm output. The decision to put a channel in either bypass or trip is specific to the application.

In RAI 3, Question 07.01 Draft DSRS-10, Item (a), the staff asked the applicant to describe how the voting logic would be altered for all reactor trip and ESF functions for cases of single failure and maintenance bypass and for both, simultaneously. In its response to RAI 3, Question 07.01 Draft DSRS-10, Item (a), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the voting logic does not change in the HIPS platform design in response to the OOS switch. Instead, the OOS switch results in a forced trip or bypass input to the coincidence voting logic. With a trip input, an additional trip input on any of the other divisions will result in actuation (e.g., 1-out-of-3 of the remaining divisions). With a bypass input, a trip input on two of the other divisions will result in actuation (e.g., 2-out-of-3 of the remaining divisions). If an SFM has only one safety function, that function could be individually bypassed or tripped when that SFM OOS is activated. If an SFM has more than one safety function, it is not possible to trip/bypass only one of those functions when that SFM OOS is activated. Furthermore, the applicant described four ways the voting logic would respond for reactor trip and ESF functions for cases of single failure and maintenance bypass and for both, simultaneously:

- (1) Single SFM in Maintenance Bypass: If an individual SFM is placed into maintenance bypass (yellow) and the failure of all SFMs in one division (red) is assumed, enough SFMs are still available (green) for a minimum 2-out-of-4 coincidence vote, as shown in Table 3-1.

Table 3-1 Single SFM in Maintenance Bypass

Division A	Division B	Division C	Division D	Coincidence Vote
SFM #1	SFM #1	SFM #1	SFM #1	3-out-of-4
SFM #2	SFM #2	SFM #2	SFM #2	2-out-of-4
SFM #3	SFM #3	SFM #3	SFM #3	3-out-of-4
SFM #4	SFM #4	SFM #4	SFM #4	3-out-of-4

- (2) Entire Division in Maintenance Bypass: If all of the SFMs in one division are taken into maintenance bypass (yellow) and all of the SFMs in another independent division fail (red), at least two SFMs are still available (green) for a minimum 2-out-of-4 vote, as shown in Table 3-2.

Table 3-2 Entire Division in Maintenance Bypass

Division A	Division B	Division C	Division D	Coincidence Vote
SFM #1	SFM #1	SFM #1	SFM #1	2-out-of-4
SFM #2	SFM #2	SFM #2	SFM #2	2-out-of-4
SFM #3	SFM #3	SFM #3	SFM #3	2-out-of-4
SFM #4	SFM #4	SFM #4	SFM #4	2-out-of-4

- (3) SFMs in Different Divisions in Maintenance Bypass: If all of the SFMs in one division are taken into maintenance bypass (yellow) and multiple SFMs can be placed OOS across different divisions (yellow) (i.e., as long as the same SFM across more than one division is not taken to maintenance bypass), and all of the SFMs in another independent division fail (red), at least two SFMs are still available (green) for a minimum 2-out-of-4 vote, as shown in Table 3-3.

Table 3-3 SFMs in Different Divisions in Maintenance Bypass

Division A	Division B	Division C	Division D	Coincidence Vote
SFM #1	SFM #1	SFM #1	SFM #1	2-out-of-4
SFM #2	SFM #2	SFM #2	SFM #2	2-out-of-4
SFM #3	SFM #3	SFM #3	SFM #3	2-out-of-4
SFM #4	SFM #4	SFM #4	SFM #4	2-out-of-4

- (4) Same SFM in Different Divisions in Maintenance Bypass: If the same SFMs in two different divisions are taken into maintenance bypass (yellow) and the failure of all SFMs in another different division is assumed (red), the application-specific implementation would not be able to satisfy the single-failure criterion, as shown in Table 3-4 (green). As such, administrative controls (e.g., procedures, technical specifications) are needed to prevent an operator from placing the same SFM across more than one division into maintenance bypass.

Table 3-4 Same SFM in Different Divisions in Maintenance Bypass

Division A	Division B	Division C	Division D	Coincidence Vote
SFM #1	SFM #1	SFM #1	SFM #1	1-out-of-4
SFM #2	SFM #2	SFM #2	SFM #2	3-out-of-4
SFM #3	SFM #3	SFM #3	SFM #3	3-out-of-4
SFM #4	SFM #4	SFM #4	SFM #4	3-out-of-4

Based on the staff's review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-10, Item (a), the staff found the applicant's response acceptable, because at least two SFMs are available for a minimum 2-out-of-4 coincidence vote (with the exception of case #4), thereby satisfying the single-failure criterion, required by IEEE Std 603-1991, Clause 5.1. Consequently, ASAI-7 is needed to establish administrative controls (e.g., procedures, technical specifications) to prevent an operator from placing the same SFM across more than one division into maintenance bypass. The staff also reviewed the markup of TR Section 2.5.2, "Bypass or Trip Operation," provided with the response and found it acceptable. The applicant subsequently incorporated the proposed change into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-10, Item (a), is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-10, Item (b), the staff asked the applicant to provide design information on where the maintenance bypass mode will be on trip and bypass for a channel. In its response to RAI 3, Question 07.01 Draft DSRS-10, Item (b), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that each SFM that has a safety-related function has an associated trip/bypass switch that is connected to an HWM that isolates the signal and places the trip or bypass information on the backplane, where it is routed only to the SBMs where it is used. Each SFM also has an OOS switch installed on its front plate. When an SFM is placed in OOS and its associated trip/bypass switch is in bypass, all safety-related functions on that SFM are placed into maintenance bypass at the SBM. Depending on the position of the trip/bypass switch, when the OOS switch on the SFM is activated, the SBM forces the safety function in trip or bypass, respectively, and takes the channel OOS. It also provides the appropriate alarm output. The decision to put a channel in either bypass or trip is specific to the application. Based on the applicant's response to RAI 3, Question 07.01 Draft DSRS-10, Item (b), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Section 2.5.2 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-10, Item (b), is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-10, Item (c), the staff asked the applicant to describe how bypassing an SFM will maintain the availability of individual functions in each safety channel. In its response to RAI 3, Question 07.01 Draft DSRS-10, Item (c), dated August 19, 2016 (see Ref. 6.1-20), the applicant described four cases in the response to Draft DSRS-10, Item (a), on how bypassing an SFM will maintain the availability of individual functions in each safety channel. The staff determined that at least two SFMs are available for a minimum 2-out-of-4 coincidence vote (with the exception of case #4). Consequently, ASAI-7 is needed to establish administrative controls (e.g., procedures, technical specifications) to prevent an operator from placing the same SFM across more than one division into maintenance bypass. Based on the staff's review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-10, Item (c), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Section 2.5.2 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-10, Item (c), is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-10, Item (d), the staff asked the applicant to discuss how the maintenance bypass is maintained in the presence of a single failure. In its response to RAI 3, Question 07.01 Draft DSRS-10, Item (d), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that it described four cases on how the voting logic would respond for reactor trip and ESF functions for cases of single failure and maintenance bypass and for both, simultaneously. The staff determined that at least two SFMs are available for a minimum 2-out-of-4 coincidence vote (with the exception of case #4), thereby satisfying the single failure criterion. Consequently, ASAI-7 is needed to establish administrative controls (e.g., procedures, technical specifications) to prevent an operator from placing the same SFM across more than one division into maintenance bypass. Based on the staff's review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-10, Item (d), the staff found the applicant's response

acceptable. The staff also reviewed the markup of TR Section 2.5.2 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-10, Item (d), is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-10, Item (e), the staff asked the applicant to describe how the HIPS platform supports the implementation of maintenance bypass in accordance with technical specifications. In its response to RAI 3, Question 07.01 Draft DSRS-10, Item (e), dated August 19, 2016 (see Ref. 6.1-20), the applicant described the functionality of the OOS and its associated trip/bypass switch when all safety-related functions on that SFM are placed into maintenance bypass or trip condition at the SBM. Furthermore, the applicant stated that the typical plant technical specifications require plant operators to put plant PS channels in the trip condition or allow PS channels to be put in bypass. The staff agrees with the applicant's position that the HIPS platform OOS and trip/bypass switch allows a system to be configured to comply with either of these technical specifications requirements. Based on the staff's review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-10, Item (e), the staff found the applicant's response acceptable. Therefore, RAI 3, Question 07.01 Draft DSRS-10, Item (e), is resolved and closed.

3.1.4.2 Communication Modules

The CMs are responsible for controlling, collecting, and transmitting information between HIPS modules or to external components. The CMs also support hardwired signal inputs using logic level backplane signals from the HWM. If used, these hardwired signals are connected directly from the HWM within the same chassis or connected chassis. The basic CMs are composed of the following circuits:

- FPGA
- scheduling and communication logic
- indication and diagnostic information (IDI)
- CM logic functions
- hardwired signals
- communication physical layers

The CMs use an FPGA device to implement the logic circuits, based on the specific functions the CMs will perform. The logic implemented in the FPGA includes the scheduling logic, any functions that the CMs are to perform, and IDI logic circuits.

There are two types of CMs: (1) the SBM, and (2) the scheduling and voting module (SVM). The three SBMs are the bus masters and are responsible for scheduling the communications on their SDB. The SBM validates and transmits the data through isolated one-way transmit-only fiber to both divisions of the reactor trip system (RTS) and ESF actuation system (ESFAS) to their respective SVMs. The three SVMs are the bus masters for the SDBs in each RTS division and in each division of ESFAS. The SVMs in both the RTS and ESFAS platforms receive the

data from the respective SBMs in the four separation groups and independently perform a 2-out-of-4 voting on the information.

The five RS-485 communication buses (i.e., SDB1, SDB2, SDB3, MIB, and CTB) use a master-slave communication protocol and are used only for intradivisional communication. There can only be one master (i.e., SBM or SVM) on a communication bus, and it must be a communication engine on a CM. Each of the four fiber-to-copper physical layers can be configured as receive only or transmit only. Interdivisional communication must be through the transmit-only or receive-only fiber-optic ports. Unlike the RS-485 buses, connections to and from the fiber-optic ports are physical point-to-point connections.

The CMs includes BIST capabilities to detect single-point failures in each channel and the FPGA logic circuits. The data message error checking also detects any failures that may occur in the CM (see Section 3.1.9).

3.1.4.3 Equipment Interface Module

The equipment interface module (EIM) is responsible for voting on triple modular redundant (TMR) signal paths and voting on architecture-level redundancy. The EIM provides the final equipment actuation output and includes priority logic circuitry for automatic and manual actuation inputs. The EIM is composed of the following circuits:

- FPGA block
 - communication logic
 - 2-out-of-3 voting
- hardwired signals logic
- actuation and priority logic (APL)
- switching output
- position feedback

The logic implemented in the FPGA includes the bus communication logic, automatic actuation 2-out-of-3 voting logic for the three SDB inputs, and the IDI logic circuits. The bus communication logic processes the safety data from the SDBs (i.e., SDB1, SDB2, and SDB3) and sends the data to the automatic actuation 2-out-of-3 voting logic. The IDI logic collects status and diagnostic information from the various circuits on the EIM, and then it is sent to the MIB communication logic for processing.

The automatic actuation 2-out-of-3 voting logic performs a 2-out-of-3 vote on the actuation signals received from the three SDBs to determine if an actuation is warranted for the primary, secondary, or both APL circuits. The APL circuits do not have to perform the same function. The safety data communication is TMR and voted on, which allows for automatic actuation signals to be generated when plant conditions necessitate such actuation, even in the presence of a single communication failure (see Section 3.6.2.1).

Similar to the CM, the EIM includes BIST capabilities to detect single-point failures in each channel and the FPGA logic circuits.

Similar to the hardwired signal circuit on a CM, hardwired signals from the back panel that originate from the HWM are distributed to the primary and secondary APL.

The APL is constructed of discrete logic components and receives commands from the automatic actuation voting logic and the hardwired signal inputs. APL may be a combination of safety and nonsafety inputs. The logic processes the highest priority command based on inputs. APL IDI is provided to the IDI on the FPGA portion of the EIM. The circuitry of the APL is designed so that, when an actuation signal is received, either through the safety data path or through the HWM manually, the APL ensures the action carries through until completion (see Section 3.6.2.2). Upon a reset of the sense and command features, the APL continues to hold the actuated components on the requested position until deliberate operator action is taken to return the component to normal.

The self-test capability of the discrete input circuit switch is evaluated by performing an open contact test and a closed contact test. The self-test capability of the output switch is evaluated by measuring the current through the contacts while the solenoid is energized and by measuring continuity through the solenoid while the solenoid is deenergized. The APL on an EIM is met through periodic surveillance testing, as required by technical specifications.

Each EIM can control two groups of field components, and each group can have up to two field devices. The EIM is equipped with four switching outputs: two primary and two secondary. The switching output is implemented as a redundant output, where a single failure in one of the driving components is automatically detected and mitigated without affecting the output operation.

The safety-related switching output of the APL is isolated from the field to allow connection to nonsafety-related components or voltage sources.

The position feedback block consists of inputs from the field component (e.g., valve fully open, valve fully closed, breaker closed/open). This equipment feedback is used to indicate the component position for the operator and to determine whether the component has completed its safety function.

The position feedback circuit is isolated from the field in the EIM to allow connection to nonsafety-related components or voltage sources. The position feedback can also be fed into the HWM to be used in other modules, as needed, for some specific applications.

3.1.4.4 Hardwired Module

The HWM converts hardwired contact inputs into logic levels for direct connection on dedicated backplane traces to particular modules as per the detail application design. The HWM is

constructed of discrete logic components only. There are no programmable devices. Examples of signal inputs to the HWM include, but are not limited to, the following:

- trip/bypass (each redundant SFM)
- manual actuation (main control room)
- enable nonsafety (main control room)
- operational overrides (main control room)
- non-Class 1E control signals
- position feedback signals

All input signals to the HWM are isolated from the field and routed on the backplane to modules that need the signals. The HWM provides isolation for the backplane and modules from the external manual switches (e.g., enable nonsafety switch) and the nonsafety-related control signals. The enable nonsafety switch allows a plant operator, when the switch is closed, to control components with an analog binary control signal that is nonsafety related. The enable nonsafety switch is classified as part of the safety system and is used to prevent spurious nonsafety-related control signals from adversely affecting safety-related components. If the enable nonsafety switch is active, and no automatic or manual actuation signals are present, the plant operator is capable of controlling the component using the non-Class 1E control signals. If the enable nonsafety switch is not active, the nonsafety-related control signal is ignored.

The HWM contains direct current (dc)-dc isolation and galvanic isolation features that are used to isolate the signal inputs described in the bulleted list above. The isolation devices used in the HWM are classified as part of the safety system and do not rely on power (i.e., passive safety-related features) to provide the required protection. Furthermore, these isolation devices will undergo qualification testing that, at a minimum, will meet the independence requirements in RG 1.75.

In addition, a trip/bypass switch for each SFM is located in the cabinet containing the HIPS chassis (see Figure 3-1). The switches are connected to the HWM that places the trip or bypass position on the backplane of the chassis for the CMs.

3.1.5 Communication Buses

The HIPS modules communicate over three SDBs (i.e., SDB1, SDB2, and SDB3), an MIB, and a CTB. The SDBs are exclusively used for the automatic actuation path, communicating Trip/No Trip information. The CTB is exclusively used for maintenance activities, such as calibrating or testing a HIPS module. The MIB is used for communicating process values to the nonsafety control system(s) and monitoring and indication information to safety displays and plant historians.

Each communication engine is connected to an RS-485 physical layer. This provides the capability for communication on the corresponding communication bus of the backplane. The five RS-485 communication buses (i.e., SDB1, SDB2, SDB3, MIB, and CTB) use a master-slave

communication protocol and are used only for intradivisional communication. There can only be one master (i.e., SBM or SVM) on a communication bus, and it must be a communication engine on a CM. Each of the four fiber-to-copper physical layers can be configured as receive only or transmit only. Interdivisional communication must be through the transmit-only or receive-only fiber-optic ports. Unlike the RS-485 buses, connections to and from the fiber-optic ports are physical point-to-point connections.

3.1.5.1 Safety Data Bus

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3.1.5.2 Monitoring and Indication Bus

The MIB is used to provide monitoring and indication information from the HIPS modules for use in non-Class 1E control systems, plant historians, and displays in the control room. The MIB can be used to transmit channel input data to other plant equipment (e.g., indicators or plant computers) to allow for manual or automated channel checks. [REDACTED]
[REDACTED]

3.1.5.3 Calibration and Test Bus

The CTB is used for the calibration, testing, and detailed diagnostic information of the HIPS modules. [REDACTED]

3.1.6 Representative Protection System Overview

The architecture described in the TR is provided for reference to describe the attributes of the HIPS platform and how it could be used in an application. This example architecture is intended to illustrate the capability of the HIPS platform to implement a prospective system architecture and does not define a proposed usage.

The example architecture of the HIPS platform (see Figure 3-2) contains the following:

- four separation groups of input sensors and detectors
- four separation groups of signal conditioning
- four separation groups of trip determination
- two divisions of RTS and reactor trip breakers
- two divisions of ESFAS voting and ESFAS equipment

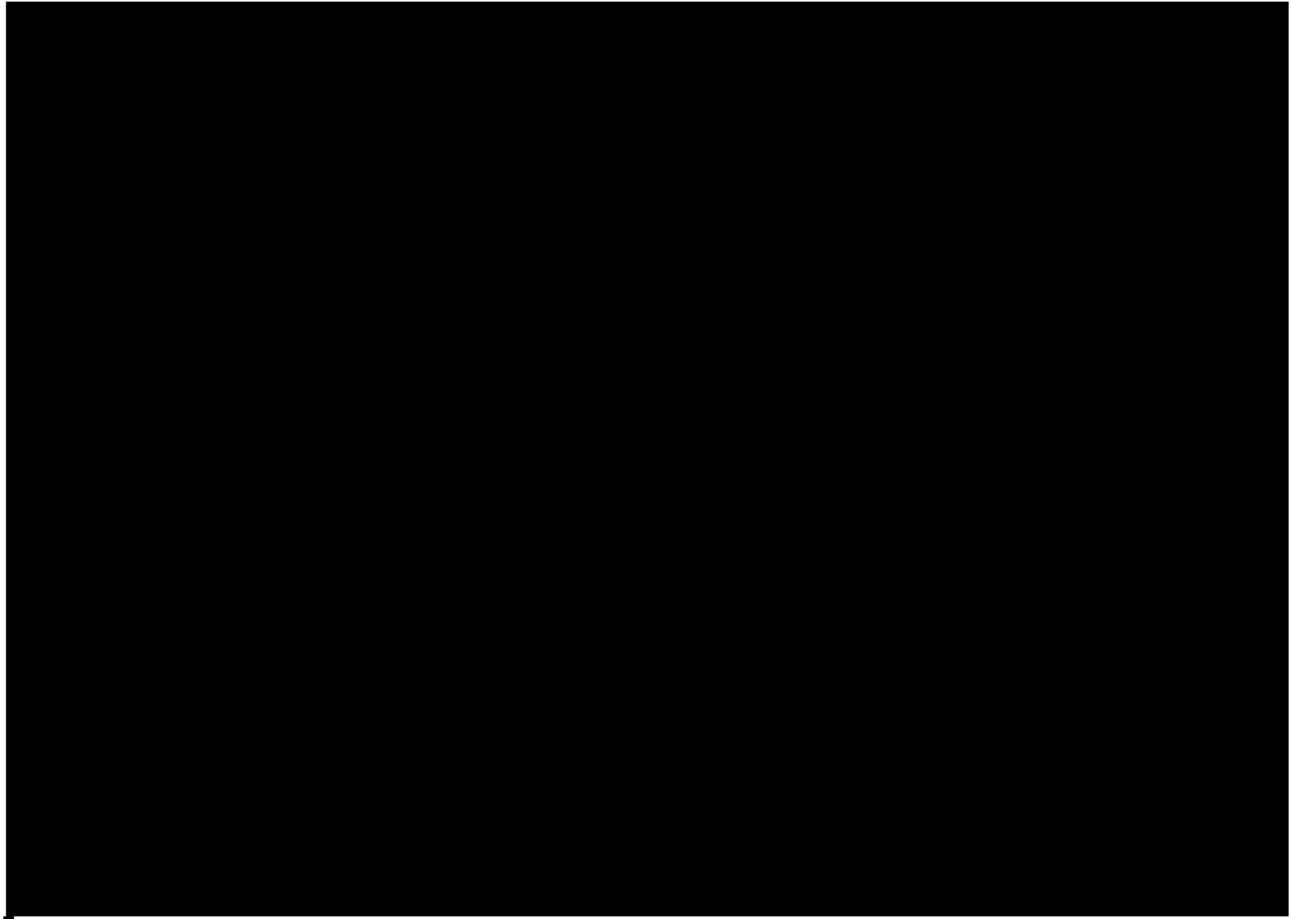
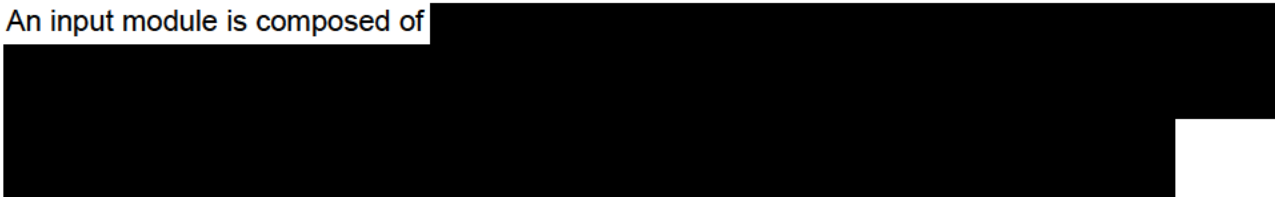


Figure 3-2 Representative of protection system architecture

Redundant sets of sensors and detectors feed each separation group and provide inputs to the signal conditioning block. Each process parameter is measured using different sensors and is processed by different algorithms, which are executed by independent logic engines.

Process sensors provide inputs to the signal conditioning block. Signal conditioning is composed of multiple input modules that are responsible for conditioning, measuring, filtering, and sampling field input signals. Each input module is dedicated to a specific input type.

An input module is composed of



The trip determination block receives process input values from the signal condition block, composed of independent safety function modules, where a specific module implements a

single set of functions. A set of safety functions may consist of group functions related to a primary variable. Each SFM contains a unique logic engine dedicated to implementing one set of safety functions, resulting in a unique processing logic for each SFM that is therefore different than that for all other SFMs.

Process input values are communicated using a deterministic path and are provided to a specific SFM. Input values are then converted to engineering units to determine what safety function or set of safety functions is implemented on that specific SFM. SFMs can make a reactor trip determination, ESFAS actuation determination, or both. The reactor trip determination is based on a predetermined set point and provides a trip or no-trip demand signal to each RTS division through an isolated transmit-only serial data path. The ESFAS actuation determination is based on a predetermined set point and provides an actuation or do-not-actuate demand signal to each ESFAS division through an isolated transmit-only serial data path.

Each of two RTS divisions receives inputs from all trip determination blocks through isolated receive-only serial data paths. The trip units are combined in the RTS voting logic so that two or more reactor trip inputs from the trip determination modules produce an automatic reactor trip output signal that actuates the reactor trip breakers associated with that division. A manual trip capability also provides a direct trip of the reactor trip breakers, as well as input to the automatic actuation, to ensure the sequence is maintained.

The ESFAS consist of two divisions of actuation logic arranged so that no single failure can prevent a safeguards actuation when required, and no single failure in a single measurement channel can generate an unnecessary safeguards actuation.

ESFAS provides both automatic and manual initiation of critical protection functions. Each of two ESFAS divisions receives inputs from all trip determination modules through isolated receive-only serial data paths. Specific actuation logic and voting occur with the ESFAS block. When the ESFAS logic and voting determine an actuation is required, the ESFAS sends the actuation demand signal to dedicated APL circuits that actuate the appropriate ESF equipment.

3.1.7 Protection System Gateway

The PS gateway is not part of the base platform so it is not within the scope of this SE. Nevertheless, the PS gateway is included to support the discussion on monitoring and indication.

The PS gateway receives data from the MIB-CMs in the four separation groups and both divisions of the RTS and ESFAS. The gateway master CM combines all of the data from the separation groups and the RTS and ESFAS, packages it into a data stream, and sends it to the safety display and indication (SDI) hub and the MWS. There are two PS gateway chassis for each PS division.

The CMs in the gateway provide more layers of isolation of the signals from the separation groups and the RTS and ESFAS and then another layer of isolation from the gateway to the SDI system and the MWS. Each communication port can only be configured as transmit or receive, and the communication outside of the gateway is over fiber-optic cables.

3.1.8 Maintenance Workstation

The MWS is not part of the base platform so it is not within the scope of this SE. Nevertheless, the MWS is included to support the discussion on monitoring/indication, testing, and calibration.

The MWS supports online monitoring using the MIB-CM through one-way isolated communication ports over point-to-point fiber-optic cables. The MWS supports offline, OOS management (e.g., troubleshooting, calibration, and surveillance testing). Each PS division has a nonsafety-related MWS for the purpose of maintenance and calibration. The Division I MWS receives data from all four separation groups and Division I RTS and ESFAS data. The one-way read-only data are connected through the PS gateway for their division and are available continuously on each division's MWS.

The MWS is used to update setpoints and tunable parameters in the SFMs when the safety function is OOS. Physical and logical controls are put in place to prevent modifications to a safety channel when it is being relied upon to perform a safety function. A temporary cable and OOS switch is 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, the HIPS platform provides an indication that can be used to drive an alarm in the main control room to inform the operator.

3.1.9 Calibration, Testing, and Diagnostics Capabilities

IEEE Std. 603-1991, Clause 5.7, "Capability for Test and Calibration," states that the safety system shall have the capability for testing and calibration while retaining the capability to accomplish its safety functions. It further states this capability shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. Appropriate justification must be provided, acceptable reliability of equipment operation must be demonstrated, and the capability shall be provided while the generating station is shut down. DSRs Section 7.2.15, "Capability for Test and Calibration," provides acceptance criteria for IEEE Std. 603-1991, Clause 5.7.

TR Section 8, "Calibration, Testing, and Diagnostics," describes the diagnostics and maintenance features provided by the HIPS platform and directly addresses IEEE Std. 603-1991, Clause 5.7. These features include the use of BIST, CRC checks, periodic surveillance testing, and other tests in each type of module, as appropriate, to verify normal operation.

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

Calibration of the SFM involves the temperature and analog input submodules. The discrete input submodule does not require calibration. In RAI 3, Question 07.01 Draft DSRS-8, the staff asked the applicant to give detailed information on the automatic calibration tests for the input submodules, to provide detection of operability and correction for drift, and to explain how those tests comply with Clause 5.7 of IEEE Std. 603-1991. In its response to RAI 3, Question-07.01 Draft DSRS-8, dated August 19, 2016 (see Ref. 6.10), the applicant described the self-test and calibration tests for the SFM input submodules. At every scan cycle, the analog input submodule

[REDACTED]

It is acknowledged that tests of components not part of the platform itself would have to be covered by manual tests. Therefore, the staff agrees that these self-test and calibration tests can provide detection of operability and correction for drift. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-8, the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Section 8.2.1.1, "Input Sub-Module," provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-8, is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-6, Item (g), the staff asked the applicant to describe the provisions for the HIPS platform that provide calibration and testing for execute features. In its response to RAI 3, Question 07.01 Draft DSRS-6, Item (g), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the HIPS platform provides self-testing and auto calibration features for the SFM (including the input sub-module (ISM)) and EIM (i.e., discrete input operation and high-drive output features) that support sense and command functions. Furthermore, the applicant stated that the HIPS platform does not provide any self-testing features for execute functions. The staff agrees with the applicant's position that these test methods and test frequencies are application-specific items. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-6, Item (g), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Sections 8.2.1, "Safety Function Module"; 8.2.3.1, "FPGA Testing"; 8.2.3.3, "Actuation and Priority Logic"; 8.2.4, "Communication Buses"; 8.2.6, "Built-In Self-Testing"; and 8.2.7, "Module Testing," provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-6, Item (g), is resolved and closed.

The HIPS platform has end-to-end self-testing that covers each module from sensor input to the output switching logic (with the exception of the APL). The individual self-tests on the different

components of the HIPS platform evaluate whether the entire platform is functioning correctly. For the APL (which contains discrete logic) periodic surveillance testing, as required in technical specifications determine if the APL is functioning correctly. In the overlap method, the modules check if each is functioning correctly, and the error checking on the communication buses verifies that the transfer of data is correct.

The surveillance testing on analog and temperature input submodule types uses the MWS as the primary test interface. Self-testing for an SFM with a discrete input submodule is sufficient for checking the performance of the submodule, since there are no calibration requirements.

[REDACTED]

In RAI 3, Question 07.01 Draft DSRS-6, Item (a), the staff asked the applicant to describe the self-testing features that are performed in the SFM and EIM. In its response to RAI 3, Question 07.01 Draft DSRS-6, Item (a), dated August 19, 2016 (see Ref. 6.1-20), the applicant described the self-testing performed by the SFM. These tests include the following:

- SFM BIST including startup and operational testing of the [REDACTED]
- SFM [REDACTED]
- SFM monitors [REDACTED]
- SFM ISM [REDACTED]
- SFM ISM [REDACTED]

In addition, the applicant described the self-testing performed by the EIM. These tests include the following:

- EIM BIST including startup and operational testing of the [REDACTED]
- EIM [REDACTED]
- EIM monitors [REDACTED]
- the [REDACTED]
- discrete input operation self-testing
- high-drive output self-testing
- 2-out-of-3 voting logic for the three SDB inputs

These self-testing features are separate and independent of the safety function logic. The staff assessed these self-testing features of the SFM and EIM modules and determined that they do not affect the ability of any module to perform its safety function. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-6, Item (a), the staff found the applicant's response acceptable. Therefore, RAI 3, Question 07.01 Draft DSRS-6, Item (a), is resolved and closed.

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

The BIST feature in the FPGA logic is separate and independent of the FPGA safety function logic; thus, the programming of the safety function FPGA logic is not made more complex by the inclusion of the diagnostic and self-test FPGA logic. In RAI 3, Question 07.01 Draft DSRS-6, Item (b), the staff asked the applicant to provide the safety classification of the BIST feature. In its response to RAI 3, Question 07.01 Draft DSRS-6, Item (b), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the BIST features are considered auxiliary features that are part of the safety systems by association (i.e., not isolated from the safety system) and are designed to the same development standards as the safety-related features. The staff found the applicant's response to RAI 3, Question 07.01 Draft DSRS-6, Item (b), acceptable because the BIST features within the FPGA are classified as part of the safety system. The staff also reviewed the markup of TR Sections 8.2, "Testing," and 8.2.6 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.06 Draft DSRS-6, Item (b), is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-13, the staff asked the applicant to describe the provisions for the HIPS platform, which provide self-diagnostics and test failure reporting during system startup. In its response to RAI 3, Question 07.01 Draft DSRS-13, dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the FPGAs on the SFM and EIM use the BIST feature provided by the FPGA. The BIST

[REDACTED]

Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-13, the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Section 8.2.6 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-13, is resolved and closed.

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

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

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

The performance of the core logic within the SFM FPGA, as well as the SDB communications buses, can be monitored by reviewing the results of the periodic injection of a partial trip determination actuation (PTDA) test signal into one core logic within the SFM FPGA in a round robin fashion. The effects of the PTDA can be observed by reviewing actuation status data information transmitted out of the HIPS platform using the MIB. The test injection can be used to confirm that the core logic and the SDBs are functioning correctly from the SFM output through the 2-out-of-3 TMR voting in the EIM. The periodic injection of the PTDA test signal has no adverse impact on the safety function of the division, since the other two core logics and SDBs not being tested remain fully functional and can process PTDA decisions made in the SFM logic.

The HIPS platform has design features that directly support methods to perform cross-checking between redundant safety-system channel sensors or between sensor channels that bear a known relationship to each other. The HIPS platform design features to use coincidence logic support implementation of application-specific diagnostic logic and confirmation of continued execution through the MWS. However, the establishment of the types of any automatic sensor cross-check as a credited surveillance test function, as well as the provisions to confirm the continued execution of the automatic tests during plant operations, is an application-specific activity.

In RAI 3, Question 07.01 Draft DSRS-6, Item (e), the staff asked the applicant to describe the influence that self-tests and other surveillance tests have on the safety function and describe any mechanisms that support the conclusions. In its response to RAI 3, Question 07.01 Draft DSRS-6, Item (e), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that surveillance testing of a system using the HIPS platform is performed with the system inoperable, OOS, or not required, as specified in plant technical specifications. The staff agrees with the applicant in that these controls and the self-testing feature of the SFM (see Section 3.1.4.1.1) provide reasonable assurance that the surveillance tests have no adverse impact on the safe operation of the plant and ensure that the HIPS platform equipment is performing correctly before the system is declared operable and put in service. The applicant also described the use of the MWS to support surveillance testing. The MWS support online monitoring using the MIB-CM through one-way isolated communication ports over point-to-point fiber-optic cables, to make the operational status of the HIPS platform-based system, including diagnostic results, available to plant personnel. The MIB logic function also obtains trip determination information, status information, and diagnostic information from each of the three redundant core logic functions. In addition, the HIPS platform provides a communication path from the MWS to the SFMs through the CTB to allow for calibration and parameter updates to each safety function. Section 3.1.8 also discusses the temporary cable to the MWS and the OOS switch, which requires the equipment to be in an inoperable status (i.e., either in bypass or

trip). Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-6, Item (e), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Sections 4.8, "Access Control Features," and 8.2.1.1 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-6, Item (e), is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-6, Item (f), the staff asked the applicant to discuss the coverage capabilities of the self-testing features. In its response to RAI 3, Question 07.01 Draft DSRS-6, Item (f), dated August 19, 2016 (see Ref. 6.1-20), the applicant described the SFM input submodule and EIM self-testing features. In its response, the applicant also described other self-testing features of the HIPS modules to detect failures and faults related to the communication buses and FPGA-related portions of the independent divisions of a system. For the APL, the applicant stated that individual transistors and logic gates are designed to be tested for functionality by periodic surveillance tests. The individual self-tests on the different components of the HIPS platform ensure that the entire platform is functioning correctly. The applicant also stated that the MIB can be used to transmit channel input data to other plant equipment (e.g., indicators or plant computers) to allow for the performance of manual or automated channel checks. The staff agrees with the applicant's position that these self-testing features could take the place of technical specification surveillance requirements (e.g., channel functional tests) that are performed during power operation to verify setpoints and the PS actuation capability. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-6, Item (f), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Sections 8.2.1 and 8.3, "Surveillance Requirements," provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-6, Item (f), is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-6, Item (c), the staff asked the applicant to discuss the surveillance periodic testing of the actuation and priority logic. In its response to RAI 3, Question 07.01 Draft DSRS-6, Item (c), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the individual transistors and logic gates in the EIM APL are simple discrete components that are designed to be tested for functionality by periodic surveillance tests. In addition, the applicant stated that the test method and test frequency are application-specific items. The individual transistors and logic gates in the EIM APL are simple enough to be tested for functionality by periodic surveillance tests. In addition, these surveillance tests have no adverse impact on the safe operation of the plant and ensure that the HIPS platform equipment is performing correctly before the system is declared operable and put in service. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-6, Item (c), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Section 8.2.3.3 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-6, Item (c), is resolved and closed.

In RAI 3, Question 07.01 Draft DSRS-6, Item (d), the staff asked the applicant to describe which failures have been identified through analysis but cannot be detected through equipment or diagnostics and to explain how those undetectable failures are addressed. In its response to RAI 3, Question 07.01 Draft DSRS-6, Item (d), dated August 19, 2016 (see Ref. 6.1-20), the applicant described the use of BIST, CRC checks, periodic surveillance testing, and other tests in each type of module to verify normal operation. The applicant further stated that it is expected that a system using the HIPS platform will have additional surveillance tests performed for the entire circuit (i.e., from sensor to actuated component) to check channel calibration, logic actuation, and response times. These tests would demonstrate the functional performance of analog portions of the circuit not tested by the HIPS self-testing features and would be proposed by an applicant or licensee referencing this SE. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-6, Item (d), the staff found the applicant's response acceptable. In addition, conformance to IEEE Std. 603, Clause 5.7, requires ASAI-25 to provide additional diagnostics or testing functions to address any system-level failures that are identified only through periodic surveillance. The staff also reviewed the markup of TR Sections 8.2.4, 8.2.7, and 8.3 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-6, Item (d), is resolved and closed.

All HIPS modules include two 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.

The staff has reviewed the diagnostics and self-test capabilities for the HIPS platform and finds them to be suitable for a digital system used in safety-related applications in NPPs. The diagnostics capabilities are found to be adequate to provide the detection capabilities for a representative system configuration based on the HIPS platform. In addition, the staff determined that the self-testing features of the HIPS modules do not affect the ability of any module to perform its safety function. Nevertheless, successful demonstration of all applicable ASAs identified in Section 4.0, together with the successful evaluation of the other fundamental design principles, such as independence (see Section 3.2), redundancy (see Section 3.3), diversity (see Section 3.4), and predictability and repeatability (see Section 3.5), provide an adequate description of how the diagnostics and self-test capabilities could be achieved for an application referencing this SE.

3.1.10 Prototype Testing

The purpose of prototype testing is to demonstrate the operation of the HIPS platform and the testing and diagnostic capabilities of the system. To assess the claims made in the TR, the staff plans to conduct a regulatory audit to observe both the base hardware of the platform in typical system configurations and the implementation of applications demonstrating the use of the HIPS platform (Ref. 6.1-5). This information would contribute to verifying the claims made in the

TR that the HIPS platform will be acceptable for use in safety-related I&C in U.S. nuclear applications. The NRC will prepare and issue a summary audit report in accordance with NRO-REG-108 within 90 days following completion of the audit.

3.2 Review of Independence

The staff evaluated the I&C system design described in the TR to confirm that it meets the independence requirements of Clause 5.6, "Independence," of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003. Through a review of design attributes of the HIPS platform and other design details in the TR, the staff confirmed that the proposed design exhibits independence among (1) redundant portions of a safety system, (2) safety systems and the effects of design-basis events (DBEs), and (3) safety systems and other systems. For each of these areas, the staff evaluated the following:

- physical independence
- electrical independence
- communications independence
- functional independence

The staff evaluation included other fundamental design principles, such as redundancy, predictability and repeatability, and D3 to inform the review of I&C system independence.

Through a review of design information, including functional block diagrams, descriptions of operation, platform design concepts, and other design details, the staff sought to determine whether the TR provides information sufficient to demonstrate conformance with the guidance on independence in RG 1.75, RG 1.152, RG 1.53, and DI&C-ISG-04 or establishes ASAls as necessary to fully comply with the regulatory requirements for an applicant or licensee referencing this SE.

TR Section 4.0, "Independence," details how the internal platform independence features provide the capability to implement system designs that can satisfy the system independence requirements of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003, Clause 5.6.

3.2.1 Physical and Electrical Independence

Physical independence is attained by physical separation and barriers. Electrical independence is achieved by the use of separate power sources. Transmission of signals between independent channels is attained through isolation devices.

The determination of the physical independence in a plant is an application-specific activity dependent on the design and implementation of the full safety system. The example architecture presented for the HIPS platform is representative of one separation group (i.e., Separation Group-A) and Division I of the RTS and ESFAS in a safety system. Since the TR does not address a specific application, establish a definitive safety system design, or

identify any plant I&C architecture, the evaluation against this requirement is limited to considering the means provided within the platform to implement system designs that contribute to satisfying the physical independence requirement.

The electrical independence evaluation includes a review of the isolation devices used for interfaces between (1) independent divisions and (2) safety systems and other systems. The review includes an evaluation of the safety classification of the isolation devices, as well as the use of redundant power sources in the HIPS platform.

In TR Sections 4.2, "Safety Function Module," and 4.3, "Communication Modules," the applicant committed to using RG 1.75 to establish separation criteria between safety-related and nonsafety-related equipment. However, the TR did not identify which revision of RG 1.75 will be used for the HIPS platform. Therefore, the staff issued RAI 3, Question 07.01 Draft DSRS-1, asking the applicant for this information. In its response to RAI 3, Question 07.01 Draft DSRS-1, dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the HIPS platform will comply with Revision 3 of RG 1.75. The staff considers the use of RG 1.75, Revision 3, as an acceptable approach for complying with the NRC's regulatory requirements concerning the physical independence of the circuits and electrical equipment that comprise or are associated with safety systems. RG 1.75, Revision 3, endorses the use of industry standard IEEE 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," (see Ref. 6.1-21). In IEEE 384-1992, Clause 7.2.2, the standard describes the use of isolation devices for maintaining independence between safety and nonsafety I&C circuits and between redundant safety channels of I&C systems. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-1, the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Sections 4.2 and 11, "References," provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-1, is resolved and closed.

TR Section 4.1, "HIPS Platform Grounding," describes the four different isolation domains in the HIPS platform (i.e., CHASSIS, digital ground (DGND), EARTH, and FIELD). The staff assessed the types of isolation between these four domains: (1) isolation between DGND and FIELD, (2) isolation between DGND and CHASSIS or EARTH, (3) isolation between FIELD and CHASSIS or EARTH, (4) separation of CHASSIS and EARTH, and (5) isolation between FIELD and FIELD. For items (1)–(3), and (5), the HIPS platform provides galvanic isolation features in accordance with the electrical isolation requirements in RG 1.75, Revision 3, and the testing features of Section 5.2 of International Electrotechnical Commission (IEC) Std. 60950-1: 2005, "Information Technology Equipment—Safety—Part 1: General Requirements," (see Ref. 6.1-22). Item (4) does not require isolation, but separation must be maintained to ensure noise currents are not coupled onto the CHASSIS from noise filters.

The HIPS platform galvanic isolation features used to isolate nonsafety-related inputs are passive safety-related features that do not rely on power to provide the required protection. The isolation devices used in the HIPS-based system are classified as part of the safety system. In

addition, these isolation devices will undergo qualification testing that, at a minimum, will meet the independence requirements in RG 1.75, Revision 3. Since all other components of the HIPS platform are classified as safety related, the HIPS platform supports meeting the requirements of Clause 5.6.3.1, "Interconnected Equipment."

TR Section 4.5, "Hardwired Module," describes the use of an enable nonsafety switch in the HWM. However, it was not clear to the staff how electrical isolation is maintained for the HWM with the non-Class 1E signals (i.e., enable nonsafety (from the main control room) and the non-Class 1E control signals). In addition, the staff was not clear on the intended use of the enable nonsafety switch. Therefore, in RAI 3, Question 07.01 Draft DSRS-3, the staff asked the applicant to specify the safety classification of the HWM; describe the functionality, safety classification, and intended use of the enable nonsafety switch; and explain how isolation is provided and independence is maintained. In its response to RAI 3, Question 07.01 Draft DSRS-3, dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the HWM is an analog component with no digital functions that is designed as a safety-related component. In addition, the applicant stated that the enable nonsafety switch allows a plant operator to control components with an analog binary control signal that is nonsafety related. Furthermore, the applicant stated that the enable nonsafety switch is designed as a safety-related component.

The HWM performs a safety-related function to provide physical and electrical isolation (i.e., dc-dc and galvanic isolation) for the backplane and modules from the external manual switches (e.g., enable nonsafety switch) and the nonsafety-related control signals. These isolation devices conform to the guidelines of RG 1.75. The enable nonsafety switch is classified as part of the safety system and is used to prevent spurious nonsafety-related control signals from adversely affecting safety-related components.

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. 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 component. In this case, the HWM provides isolation for the nonsafety-related signal path when the enable nonsafety switch is active.

Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-3, the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Section 4.5 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-3, is resolved and closed.

TR Section 4.6.2, "Communication Independence outside the Platform," states that electrical and physical isolation of the four separation groups is achieved by the use of dedicated fiber-optic connections between the SBM and the SVM. The four communication ports on each SBM are configured as fiber-optic transmit-only ports. Two of the ports send data over fiber-optic cables to the two divisions of RTS. The other two ports send data over fiber-optic

cables to the two divisions of ESFAS. The dedicated fiber-optic connections are all point-to-point for each SDB.

The MIB-CM provides Class 1E isolation between the Class 1E equipment and nonsafety equipment via four copper-to-fiber-optic ports. The remaining copper-to-fiber-optic ports on the separation group MIB-CM are configured as receive only and receive information from the MWS through a temporary cable that is connected during maintenance activities.

The MPS gateway provides Class 1E isolation between the Class 1E equipment and SDIS hubs via copper-to-fiber-optic ports on the MPS gateway.

TR Section 4.2 states that the HIPS platform design provides for the use of redundant power sources to the HIPS chassis backplane. The redundant power source is auctioneered once it is on the board and converted to the needed voltages of the FPGA. In RAI 3, Question 07.01 Draft DSRS-2, Item (b), the staff asked the applicant to provide the classification of the isolators and state whether the power for the isolator complies with IEEE Std. 603-1991. In its response to RAI 3, Question 07.01 Draft DSRS-2, Item (b), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the HIPS platform galvanic isolation features used to isolate nonsafety-related inputs are passive safety-related features that do not rely on power to provide the required protection. In addition, the HIPS platform is designed to be powered from a safety-related power source. The power converters within the HIPS platform are designed as safety-related equipment. The use of nonsafety-related power sources would have to be addressed as an application-specific item. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-2, Item (b), the staff found the applicant's response acceptable, because it is in conformance with the acceptance criteria in DSRS Section 7.1, "Instrumentation and Controls—Fundamental Design Principles." The staff also reviewed the markup of TR Section 4.2 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Draft DSRS-2, Item (b), is resolved and closed.

Based on this evaluation, the staff determined the TR independence approach adequately describes how electrical isolation is achieved. Specifically, the staff makes the following findings:

- The HIPS platform conforms to the physical independence guidance in RG 1.75, Revision 3.
- Electrical isolation between nonsafety sensor inputs to the SFM is provided through the use of galvanic isolation.
- Electrical isolation is provided between the HIPS platform-based Class 1E equipment and nonsafety equipment through the use of an isolation device.

- The HWM provides dc-dc and galvanic isolation between the HIPS platform-based Class 1E equipment and the nonsafety equipment.
- Isolation devices are classified as part of the safety system and powered in accordance with IEEE Std. 603-1991 and the guidelines contained in RG 1.75, Revision 3.
- Communication to nonsafety-related systems is provided through transmit-only or receive-only fiber-optic ports. These ports provide electrical isolation for either transmit-only or receive-only unidirectional communication links.
- The MIB-CM provides Class 1E isolation between the Class 1E equipment and nonsafety equipment via four copper-to-fiber-optic ports. The remaining copper-to-fiber-optic ports on the separation group MIB-CM are configured as receive only and receive information from the MWS through a temporary cable that is connected during maintenance activities.
- The MPS gateway provides Class 1E isolation between the Class 1E equipment and SDIS hubs via copper-to-fiber-optic ports on the MPS gateway.
- The HIPS platform supports an installation that provides redundant electrical power sources to the HIPS chassis backplane. In addition, the HIPS platform is designed to be powered from a safety-related power source.

The successful demonstration of all applicable ASAs identified in Section 4.0 of this SE, together with the successful evaluation of the other fundamental design principles, such as redundancy (see Section 3.3), diversity (see Section 3.4), and predictability and repeatability (see Section 3.5), are adequate to describe how physical and electrical independence could be achieved for an applicant or licensee referencing this SE.

3.2.2 Communications Independence

IEEE Std. 603-1991, Clause 5.6 requires independence among (1) redundant portions of a safety system, (2) safety systems and the effects of DBEs, and (3) safety systems and other systems.

IEEE Std. 7-4.3.2-2003, endorsed by RG 1.152, Revision 2, Clause 5.6, "Independence," provides guidance on how digital systems can meet IEEE 603 requirements. This clause of IEEE Std. 7-4.3.2 states that, in addition to the requirements of IEEE Std. 603-1991, data communication between safety channels or between safety and nonsafety systems shall not inhibit the performance of the safety function. Guidance on interdivisional communications appears in DI&C-ISG-04. Section 3.8 further discusses the conformance to DI&C-ISG-04.

Communication Independence within the Platform

The HIPS platform is designed such that a safety division functions independently of other safety divisions. With the exception of the interdivisional voting, the communication within the safety function group (SFG) is independent and does not rely on communication outside the respective SFG or division to perform the safety function.

For voting purposes, the communication uses point-to-point fiber optics through the SDB connections between the SBM and SVMs. The divisions do share voting data with other divisions through the SVM. The division voters are not dependent on voting data from other divisions because the division voters will still be able to complete their safety function, even if the SVM voting data have errors or are not available. The division voters would apply a safe default for the missing inputs.

The HIPS platform provides an FPGA approach that implements communication logic circuits that nonintrusively monitor safety function logic circuits so communication activities cannot delay or otherwise adversely affect the performance of the safety functions. Additionally, the TR states that communication functions do not perform communication handshaking and do not accept any interrupts from any communication devices.

Communication Independence outside the Platform

The determination of interconnections between the HIPS platform and other nonsafety systems in a plant through common equipment or communication links is an application-specific activity. The base platform architecture identified in the TR does not specify any direct connections or bidirectional communication between the HIPS and any other system. However, the TR does identify the capability for one-way communication to nonsafety-related components across the MIB-CMs through fiber-optic cabling and an isolation PS gateway. To promote independence, the MIB-CMs can only provide status and diagnostics information to the control system, PS gateway, and safety display and indication system through one-way, transmit-only, isolated outputs. However, the PS gateway is not part of the base platform and, thus, is not within the scope of this evaluation. Consequently, fulfilling this requirement involves an ASAI (i.e., ASAI-22) for verification that the PS gateway (or any other device not part of the base HIPS platform) cannot transmit messages on the MIB-CMs and thus compromise independence between the safety system and any other systems connected to the PS gateway.

All data communications going out of or into the HIPS chassis use the one-way isolated communication ports on the CMs. The CMs are part of the safety-related HIPS platform and are qualified as safety-related modules and Class 1E to non-Class 1E isolation.

The TR classifies the MWS and PS gateway as nonsafety related. To promote independence, the PS can only provide status and diagnostics information to the nonsafety-related control system, PS gateway, and both divisions of the SDI system through one-way, transmit-only, isolated outputs. However, the control system, PS gateway, and SDI are not part of the base

platform and, thus, are not within the scope of this evaluation. Consequently, fulfilling this requirement involves an ASAI (i.e., ASAI-22) for verification that the PS gateway (or any other device not part of the base HIPS platform) cannot transmit messages on the MIB-CMs and thus compromise independence between the safety system and any other systems connected to the PS gateway.

Each division of the PS has a nonsafety-related MWS for maintenance and calibration. The MWS supports online monitoring using the MIB-CM through one-way isolated communication ports over point-to-point fiber-optic cables. The one-way isolated data from the HIPS platform to the MWS include the setpoint and tunable parameter information for each SFM. The only time communication from the MWS to the HIPS chassis is allowed is when the SFM is placed OOS by activating the OOS switch to the "OOS" position and a temporary cable is attached from the MWS to the MIB-CM for that separation group.

In RAI 3, Question 07.01 Draft DSRS-2, Item (a), the staff asked the applicant to demonstrate that any failure of nonsafety-related inputs does not have an adverse impact on the safety functions. In its response to RAI 3, Question 07.01 Draft DSRS-2, dated August 19, 2016 (see Ref. 1-10), the applicant stated that the HIPS platform is designed to process nonsafety-related information in a manner that prevents adverse impacts on the safety functions. The HIPS platform can process nonsafety-related inputs to the PS (e.g., anticipatory turbine or main feedwater trip signals required by 10 CFR 50.34(f)(2)(xxiii)). The input submodule provides galvanic isolation and prevents adverse impacts on the SFM. These input signals are then processed by the SFM, and the trip determination is transmitted on the triple redundant SDBs. The nonsafety-related monitoring information is processed by the MIB logic and transmitted over the MIB, which is functionally separate from the SDB logic and buses to prevent adverse impacts on the SDB signal paths. Interdivision communication from the MIB uses fiber-optic cables to provide galvanic isolation and prevent adverse impacts on the SFM and MIB-CM safety functions from modules or devices outside the MIB division. The HIPS platform galvanic isolation features used to isolate nonsafety-related inputs are passive safety-related features that do not rely on power to provide the required protection. The independence of the SDBs from the MIB and CTB is supported by the standards used for the design of the backplane traces and surge withstand capability testing performed as part of module equipment qualification. The staff determined that these design concepts provide reasonable assurance that any failure of nonsafety-related inputs does not have an adverse impact on the safety functions. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-2, Item (a), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Sections 4.2 and 4.3 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-2, is resolved and closed.

Based on this evaluation, the staff determined that the TR independence approach adequately describes how communication independence is achieved. Specifically, the staff makes the following findings:

- The design of the data communication system supports meeting the requirements of IEEE Std. 603-1991, Clause 5.6, as endorsed by RG 1.153.
- The design of the data communication system supports conformance to the guidance for the separation and isolation of data processing functions of interconnected computers contained in IEEE Std. 7-4.3.2-2003, Clause 5.6, as endorsed by RG 1.152.
- The design of the data communication system supports conformance to the guidance of DI&C-ISG-04.

The successful demonstration of all applicable ASAs identified in Section 4.0 of this SE, together with the successful evaluation of the other fundamental design principles, such as redundancy (see Section 3.3), diversity (see Section 3.4), and predictability and repeatability (see Section 3.5), are adequate to describe how communication independence could be achieved for an applicant or licensee referencing this SE.

3.2.3 Functional Independence

Functional independence provides additional assurance on the isolation of a safety system from other safety systems. Functional independence seeks to prevent safety function failures by ensuring that physically and electrically independent portions of safety systems (with the exception of coincidence voting) do not depend on information from other independent portions of the safety system. The concept of functional diversity (using different parameters, different technologies, different logic or algorithms, or different actuation means to provide several ways of detecting and responding to a significant event) helps accomplish functional independence but does not totally address it.

Considering functional independence in the I&C system design helps demonstrate that the successful completion of the system's safety functions is not dependent upon any behavior, including failures and the normal operation of another system, or upon any signals, data, or information derived from the other system. Functional independence could also be used as a means of achieving isolation between redundant systems.

The example architecture presented for the HIPS platform is representative of one separation group (i.e., separation Group-A) and Division I of the RTS and ESFAS in a safety system. Each bus is a differential bus with a single master and multiple slaves. The three CMs connected to SDBs are the bus masters for the three SDBs. The MIB-CM is the bus master for the MIB and the CTB.

The SFM can accept up to four sensor inputs and each SFM implements a safety function or a group of safety functions related to a primary variable, such as a high and low trip from the same pressure input. Each module contains a unique logic engine dedicated to implementing one safety function or SFG. This results in the gate-level implementation of each safety function being different from other safety functions.

The output of each of the input submodules is sent to three redundant signal paths in the FPGA. The safety function algorithm is processed through three redundant paths that are independent of each other and independent of the MIB and CTB logic functions. The trip determination result for each signal path is processed through a separate independent communication engine and connected to an independent SDB.

The trip determination block receives process input values from the signal condition block. It is composed of independent SFMs, where a specific module implements a single set of functions. A set of safety functions may consist of a group of functions related to a primary variable. Each SFM is dedicated to implementing one safety function or function group. This results in the gate-level implementation of each safety function being different from other safety functions. A removal of one SFM only affects the SFG that is implemented by that SFM and no other SFG or SFM. This design attribute supports functional independence and diversity.

Dedicating SFMs to a function or group of functions based on their input simplifies an SFM by having simpler and dedicated logic circuits. This simple approach provides inherent function segmentation, creating simpler and separate SFMs that can be more easily tested. This segmentation also helps limit module failures to a subset of safety functions. Each SFM can be assigned a unique address that can be used throughout a division of a HIPS platform implementation.

The functions within the FPGA of each module are implemented with finite-state machines to achieve deterministic behavior. The HIPS platform does not rely on a complex system/platform controller. Each module runs on its own clock domain and performs its functions autonomously. The use of a single clock domain within a module eliminates metastability concerns within a module.

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

Input values are converted to engineering units to determine what safety function or set of safety functions is implemented on that specific SFM. SFMs can make a reactor trip determination, ESFAS actuation determination, or both. A reactor trip determination is based on a predetermined set point and provides a trip or no-trip demand signal to each RTS division through an isolated transmit-only serial data path. An ESFAS actuation determination is based on a predetermined set point and provides an actuation or do-not-actuate demand signal to each ESFAS division through an isolated transmit-only serial data path.

Each of two RTS divisions receive inputs from all trip determination blocks through isolated receive-only serial data paths. The trip units are combined in the RTS voting logic so that two or more reactor trip inputs from the trip determination modules produce an automatic reactor trip

output signal that actuates the reactor trip breakers associated with that division. A manual trip capability also provides a direct trip of the reactor trip breakers, as well as input to the automatic actuation, to ensure the sequence is maintained.

The ESFAS provides both automatic and manual initiation of critical protection functions. Each of two ESFAS divisions receives inputs from all trip determination modules through isolated receive-only serial data paths. Specific actuation logic and voting occur with the ESFAS block. When the ESFAS logic and voting determine an actuation is required, the ESFAS sends the actuation demand signal to dedicated APL circuits to actuate the appropriate ESF equipment.

Based on this evaluation, the staff determined the TR independence approach adequately describes how functional independence is achieved. Specifically, the staff makes the following findings:

- The SFG components (i.e., SFM, SBM, and SDB) are functionally independent from the division components (i.e., SVM and EIM).
- The SFGs and divisions are self-reliant and have no dependency on functions outside the SFGs or divisions.

The successful demonstration of all applicable ASAs identified in Section 4.0 of this SE, together with the successful evaluation of the other fundamental design principles, such as redundancy (see Section 3.3), diversity (see Section 3.4), and predictability and repeatability (see Section 3.5), are adequate to describe how functional independence could be achieved for an applicant or licensee referencing this SE.

3.3 Review of Redundancy

Redundancy is commonly used in I&C safety systems to achieve system reliability goals and conformity with the single-failure criterion. The staff evaluated the I&C system design described in the TR to confirm that it meets the redundancy requirements of the applicable regulations through conformance to the guidance listed below. Through a review of design attributes of the HIPS platform and other design details, as shown in the TR, the staff confirmed that the proposed design exhibits redundancy in the areas of power, module, communication, equipment interface, and platform. The TR is expected to provide information that describes what level of redundancy is used in the safety system 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 PS can be otherwise demonstrated. In addition to redundancy, the application should describe the means employed in the I&C design for guarding against common-cause failures (CCFs).

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the staff determined whether the TR provides information sufficient to demonstrate conformance with the guidance on the single-

failure criterion in RG 1.53 or to establish ASAs for an applicant or licensee referencing this SE to demonstrate full compliance with regulatory requirements.

TR Section 5.0, "Redundancy," details how the internal platform redundancy designed into the HIPS platform described below, along with a specific system architecture design could be used to demonstrate that an applicant's I&C safety system design achieves reliability goals and conforms to the single-failure criterion.

Power Supply Redundancy

TR Section 5.1, "Power Supply," describes the HIPS platform redundant auctioneered dc power feeds to supply both the general logic design and the FPGA core supply power requirements. Fuses are used to protect the HIPS modules from cases of severe overcurrent and board failures.

Safety Module Redundancy

As stated in TR Section 5.2, "Safety Function Module Internal Redundancy," the SFM is designed with three redundant signal paths and is set for a 2-out-of-3 comparison. This internal redundancy provides for easy fault detection, giving higher reliability from spurious activation without increasing the complexity of the design.

Communication Redundancy

TR Section 5.3, "Communication Redundancy," describes a communication scheme comprised of triple redundant communication paths and is further evaluated in Section 3.2.2 of this SE. These redundant paths provide fault tolerance and the ability to replace a CM on line without causing a trip or actuation. From the output of the input submodule to the EIM voting, the three redundant safety data signal paths remain independent and redundant.

Equipment Interface Redundancy

To address equipment interface redundancy, TR Section 5.4, "Equipment Interface Module Redundancy," provides for redundant EIMs, which are further evaluated in Section 3.1.4.3 of this SE. These parallel EIMs allow for more thorough testing and equipment removal, thus providing a higher reliability for the field components from spurious activation.

Platform Redundancy

An applicant incorporating the TR into a representative architecture, as described in the TR, would be able to demonstrate redundancy in multiple areas of the architecture. The redundancy within the HIPS platform architecture would include (1) four separation groups of sensors and detectors, (2) four separation groups of trip determination, and (3) two divisions of RTS and ESFAS circuitry. The architecture could use the HIPS platform design of four separation groups

as one of the mechanisms employed to satisfy single-failure criteria and improve system availability.

The HIPS platform could then be used for 2-out-of-4 voting, so that a single failure of an input process signal will not prevent a reactor trip or ESF equipment actuation from occurring when required. In addition, a single failure of an input process signal will not cause spurious actuation or inadvertent reactor trips or ESF equipment actuations when they are not required.

Section 3.6.2.1 of this SE provides the staff evaluation for IEEE Std. 603-1991, Clause 5.1, "Single Failure Criterion." Section 4.0 of this SE establishes ASAs that are necessary to demonstrate full compliance as it applies to redundancy.

The staff also considered the following IEEE Std. 603-1991 requirements in the review of redundancy:

- Clause 5.7 provides requirements for test and calibration of safety system equipment. Section 3.6.2.7 contains the staff evaluation for IEEE Std. 603-1991, Clause 5.7, and establishes ASAs that are necessary to demonstrate full compliance as it applies to redundancy.
- Clause 6.3, "Interaction with Other Systems," provides requirements for interactions between sense and command features and other systems. Section 3.6.3.3 contains the staff evaluation for IEEE Std. 603-1991, Clause 6.3, and establishes ASAs that are necessary to demonstrate full compliance as it applies to redundancy.
- Clause 6.5, "Capability for Testing and Calibration," provides requirements for testing and calibration of sense and command feature sensors during reactor operation. Section 3.6.3.5 contains the staff evaluation for IEEE Std. 603-1991, Clause 6.5, and establishes ASAs that are necessary to demonstrate full compliance as it applies to redundancy.
- Clause 6.7, "Maintenance Bypass," provides maintenance bypass requirements for sense and command features. Section 3.6.3.7 contains the staff evaluation for IEEE Std. 603-1991, Clause 6.7, and establishes ASAs that are necessary to demonstrate full compliance as it applies to redundancy.
- Clause 7.5, "Maintenance Bypass," provides maintenance bypass requirements for execute features. Section 3.6.4.5 contains the staff evaluation for IEEE Std. 603-1991, Clause 7.5, and establishes ASAs that are necessary to demonstrate full compliance as it applies to redundancy.

Based on this evaluation, the staff has determined that the redundancy approach, including the successful demonstration of all applicable ASAs provided in Section 4.0 of this SE, together with the successful evaluation of the other fundamental design principles, such as

independence (see Section 3.2), diversity (see Section 3.4), and predictability and repeatability (see Section 3.5), are adequate to describe how independence could be achieved for an application referencing this SE.

3.4 Review of Diversity

The objective of this review is to verify that (1) the HIPS platform has a level of diversity such that there are two or more redundant components that will be able to perform the safety functions, and (2) the different components will have different attributes so as to reduce the likelihood of CCF. The staff focused its review of diversity in HIPS platform design on whether the safety functions can be achieved in the event of a postulated CCF in the DI&C system based on the HIPS platform. Conformance with these objectives is sufficient to demonstrate that the applicable regulatory requirements have been met:

- The regulations in 10 CFR 50.55a(h) require compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in 10 CFR 50.55a(h)(2) and (3). This standard includes Clause 5.1. This clause states, in part, that the safety system must perform all safety functions required for a DBE in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.
- The SRM to SECY-93-087 describes the NRC position on D3 in item 18.II.Q.
- IEEE Std. 7-4.3.2 provides guidance on performing an engineering evaluation of software CCFs for digital-based systems, including the use of manual action and nonsafety-related systems or components, or both, to provide means to accomplish the function that would otherwise be defeated by the CCF.
- NUREG/CR-6303 summarizes several D3 analyses performed after 1990 and presents an acceptable method for performing such analyses.

TR Section 6.0, "Diversity," discusses the diversity attributes required within the HIPS platform design to eliminate the consideration of software CCFs, which include equipment, design, and functional diversity.

The HIPS platform uses two diverse FPGA technologies to achieve equipment diversity. The diverse FPGA technologies result in an associated level of chip design diversity, since FPGA vendors use different development tools to provide the final configured FPGAs. These tools have inherent diversity related to the differences in FPGA chip architectures and programming methods.

The HIPS platform also provides functional diversity with the use of different protection logic on an SFM for each safety function or SFG. A separate SFM is provided for each different type or group of input sensor(s) (e.g., pressure, temperature, level, flow, or neutron flux). As a result, the programmable logic design for an SFM is completely unique when compared to the protection logic for any other SFM. In addition, the safety function or SFG is implemented on separate SFM hardware boards within the same division (or separation group).

Human diversity is not specifically credited in the HIPS platform for mitigating the potential for digital CCFs. However, human diversity is an implicit attribute of the FPGA equipment, chip design, and software tool diversity.

The example in the TR of a four-division PS is based on using one FPGA technology in two divisions and the other FPGA technology in two divisions shown as red and yellow in Figure 3.3 below. The applicant makes an argument that, in this arrangement, a CCF associated with one FPGA technology would not defeat the safety function, since two divisions would be unaffected because of the FPGA diversity and would accomplish the safety function. Figure 3-3 depicts the FPGA equipment diversity allocation in a representative architecture configured such that the CCF of a single FPGA technology does not defeat the safety functions assumed in the plant safety analyses. This figure illustrates the allocation of the two FPGA technologies (shown as red and yellow) across an architecture that includes four divisions of trip determination and two divisions each for RTS and ESFAS actuation. Two divisions of trip determination and one division each for RTS and ESFAS actuation remain available to perform the system safety functions if a digital CCF disables one FPGA technology.

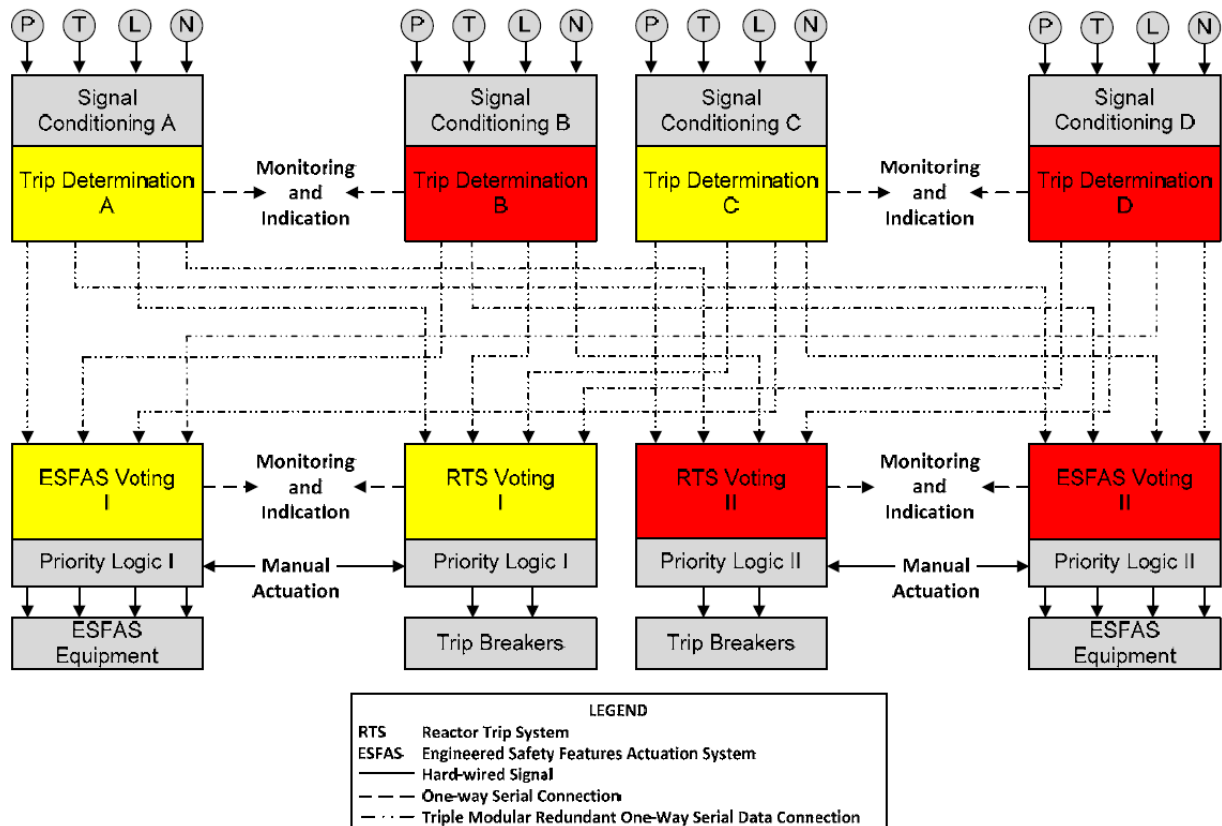


Figure 3-3 FPGA equipment diversity allocation in a representative architecture

TR Section 6.4, “HIPS Diversity Summary,” illustrates the effects of digital CCF for a system using the HIPS diversity strategy for two cases (see Table 3-5 of this SE). The green check shows areas of the architecture unaffected by a digital CCF. The red X shows areas of the architecture affected by the digital CCF example. Case 1 shows the impact of a digital CCF on a representative architecture using the HIPS platform equipment when equipment (i.e., FPGA technology diversity) and module functional diversity are credited for mitigation. In this example, the digital CCF affects the FPGA technology used in the division A and C SFMs. Case 2 shows the impact of a digital CCF on a representative architecture using the HIPS platform equipment when only equipment diversity is credited for mitigation. In this example, the digital CCF affects the FPGA technology used in all of the division A and C modules.

Table 3-5 Effects of Digital CCF for HIPS Diversity Strategy

Event	Module	A	C	B	D
Transient or accident (no CCF)	SFM	✓	✓	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or accident with CCF (Case 1 – equipment (FPGA) and module functional diversity)	SFM	✗	✗	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or accident with CCF (Case 2 - equipment (FPGA) diversity)	SFM	✗	✗	✓	✓
	CM	✗	✗	✓	✓
	EIM	✗	✗	✓	✓

Credit for functional diversity of the SFM, CM, and EIM can limit the effects of a CCF related to a particular FPGA technology; however, equipment diversity (i.e., FPGA technology diversity) is sufficient to ensure the system safety function is performed in the presence of a postulated software CCF that is limited to a single FPGA technology.

D3 provides reasonable assurance that a safety task will be accomplished when necessary to mitigate plant anticipated operational occurrences and postulated accidents while also providing a defense against CCFs. D3 is the principle of providing multiple barriers to any credible failure that would prevent a function from achieving its objective. Diversity, in the context of DI&C, is the principle of using different technologies, equipment manufacturers, logic processing equipment, signals, logic and algorithms, development teams and personnel, and functions to provide a diverse means of accomplishing a safety function. As an element of D3, diversity decreases the probability that a particular function will fail to achieve its objective.

Software-based or software-logic-based digital system development errors are a credible source of CCF. Common software includes software, firmware, and logic developed from software-based development systems. Generally, digital systems cannot be proven to be error free; thus, they are considered susceptible to CCF, because identical copies of the software-based logic and architecture are present in redundant divisions of safety-related systems. Since CCF is not classified as a single failure (as defined in RG 1.53), design-basis evaluations need not assume that a postulated CCF is a single failure. Consequently, analyses can employ realistic assumptions to evaluate the effect of CCF coincident with DBEs.

For designs that use digital safety systems, the staff has established a four-point position on D3 for new reactor designs and for digital system modifications to operating plants. The SRM to SECY-93-087, and particularly item 18.II.Q, forms the foundation of this position.

In reviewing the diversity attributes within the HIPS platform, the staff focused on the areas noted below.

Diverse System Characteristics

If a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, should be capable of performing either the same function or a different function that will accomplish the same protection action. If the D3 assessment identifies a CCF that could prevent an automated safety system from performing a function credited in the safety analysis, the application should describe a diverse means for accomplishing the credited safety function or a different function that provides the same protection.

The HIPS platform design has built-in equipment diversity to address the potential digital CCF concerns. The FPGA portion of an SFM, CM, and EIM is the only portion of the HIPS platform that may be vulnerable to software CCF. The HIPS platform requires the use of at least two different FPGA architectures, one being an OTP or flash-based FPGA and the other being a SRAM-based FPGA. The low-level architectural aspects of these two types of architecture are different and inherently create differences in how the FPGA is configured and how it operates once it has been configured. The two architectures have the following inherent differences:

- (1) The OTP or flash-based architecture is configured to a certain logic structure by using an OTP or a flash cell, respectively, to either allow connection or not between fixed logic elements within the FPGA. Once this configuration is established, it remains fixed when the FPGA is powered or when it is not powered.
- (2) The SRAM architecture relies on the use of an external “configuration” memory to provide the configuration information to the FPGA. Each time the SRAM-based FPGA is powered up, it reconfigures itself with the “lookup” table obtained from the external memory or configuration chip.

Table 3-6 summarizes the inherent differences between these two types of FPGA technologies.

Table 3-6 Inherent Differences between FPGA Architecture Choices

Differences	Difference Type	FPGA Architecture #1		FPGA Architecture #2
		OTP	Flash FPGA	SRAM FPGA
Architecture	Inherent	Versatiles	Versatiles	Lookup Table
Logic Storage Cell	Inherent	OTP Switch	Flash-based Switch	SRAM Cell
Power-Off Characteristics	Inherent	Configuration is Retained When Power is Off	Configuration is Retained When Power is Off	Configuration is Lost When Power is Off
Configuration Chip	Inherent	Not Needed	Not Needed	Needed for Startup

The diverse FPGA technologies described above inherently have additional design diversity attributes based on the different development tools used for each FPGA technology. This tool diversity results from the different FPGA chip architectures and programming methods. Various differences in diverse FPGA architecture require different set of design and system development activities for fabricating HIPS platform and therefore would yield, human diversity attributes as well. Intentional differences are required in the software tools used for the development of the FPGAs: design synthesis, design analysis, physical design, design simulation, and physical programming. Additionally, the design simulation tools used by the independent verification and validation (iV&V) teams must be different than those used by the design teams; however, the same tool can be used by iV&V teams for both FPGA technologies. These design diversity attributes are consistent with NUREG/CR-6303, which defines design diversity as the use of different approaches, including both software and hardware, to solve the same or similar problems. Table 3-7 summarizes the intentional differences in the use of software.

Table 3-7 Intentional Differences between FPGA Architecture Choices

Differences	Difference Type	FPGA Architecture #1		FPGA Architecture #2
		OTP	Flash FPGA	SRAM FPGA
Design Synthesis Tool(s)	Intentional	Suite A	Suite A	Suite B
Design Analysis Tool(s)	Intentional			
Physical Design Tool(s)	Intentional			
Design Simulation Tool(s)	Intentional			
Physical Programming Tool(s)	Intentional			

iv&V Design Simulation Tool(s)	Intentional	Different than Suite A and Suite B
--------------------------------	-------------	------------------------------------

The HIPS platform design supports functional diversity by requiring segregation of safety functions by their inputs. For example, each of two SFMs within a division of the HIPS platform monitors a different parameter (i.e., SFM #1—reactor power; SFM #2—pressurizer pressure). The logic implemented within an SFM is unique to its input(s). A failure of an SFM would be limited to the safety functions of that SFM and would not prevent other SFMs from performing their safety functions. The safety functions performed by the SFM, CM, and EIMs are functionally diverse.

The APL portions within an EIM support the implementation of different actuation means and different response time scales. The APL is implemented using discrete components and is not vulnerable to a software CCF. It can receive multiple signals and, based on their priority, actuate a function (e.g., ESFAS function, trip function). The first input is generated automatically from the digital portion of the HIPS platform. Having the capability for hardwired signals into each EIM supports the capability for additional and diverse actuation means (e.g., manual signal from the main control room, nonsafety manual signals, and nonsafety automatic signals) that inherently supports different time scales. As an example, a division of APL circuits may receive inputs automatically from the digital portion of a HIPS platform, inputs from safety-related manual controls in the main control room, and input signals from a nonsafety control system.

The staff based its evaluation of diversity design features of the HIPS platform on TR Revision 1, which incorporated the proposed changes provided as part of the following RAI responses in NuScale letter LO-0716-50303, dated August 19, 2016 (Ref. 6.1-20). The staff issued these RAIs for TR Revision 0.

In NRC RAI No. 3, Question 07.01 Draft DSRS-4, the staff asked the applicant to describe (1) how the two different types of FPGA technologies provide a defense against digital CCFs in the HIPS platform, and (2) how this diversity approach does not require a separate actuation system to mitigate digital CCFs. In response to the RAI, NuScale stated that the HIPS platform uses two diverse FPGA technologies to achieve equipment diversity. At the chip level, the two FPGA technologies operate in different ways during operation and programming. The diverse FPGA technologies inherently have additional design diversity attributes based on the different development tools used for each FPGA technology. This tool diversity results from the different FPGA chip architectures and programming methods. The diversity in FPGA equipment, chip designs, and development tools are the fundamental method for mitigating the potential for digital CCFs in the HIPS platform, since these diversity attributes directly mitigate CCFs associated with a specific FPGA technology. The HIPS platform diversity strategy can be implemented in system I&C architectures that ensure that system-level safety functions are not defeated by a CCF in one or the other type of FPGAs, and this strategy can eliminate the need for additional coping or consequence analyses, since a system can be configured such that the CCF of a single FPGA technology does not defeat the safety functions assumed in the plant

safety analyses. The staff found the applicant's response to this RAI and the proposed changes to TR Sections 6.1.1, "Field Programmable Gate Array"; 6.2, "Design Diversity"; and 6.4 "HIPS Diversity Summary," acceptable. The applicant has incorporated all of these proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, NRC RAI No. 3, Question 07.01 Draft DSRS-4, is resolved and closed.

In NRC RAI No. 3, Question 07.01 Draft DSRS-5, the staff asked the applicant to explain (1) why the HIPS platform will not require an additional independent design or verification and validation (V&V) team, and (2) why it is acceptable to use the same iV&V design simulation tool for both FPGA technologies. In its response to the RAI question, the applicant cited recent Massachusetts Institute of Technology research sponsored by the NRC for its decision to not use separate design or iV&V teams for developing HIPS platforms using different FPGA technologies. This research concludes that independently developed software is very likely to contain CCF modes and states the following:

Knight and Leveson showed, back in the mid-1980's, that making multiple versions of the software using different teams does not solve the problem either Knight and Leveson, 1986. Others replicated the Knight and Leveson experiments to try to demonstrate they were wrong, but simply replicated the results Knight and Leveson, 1990. People make mistakes on the hard cases in the input space; they do not make mistakes in a random fashion. Therefore, independently developed software is very likely to contain CCF failure modes.

In fact, almost all serious accidents caused by software have involved errors in the requirements, not in the implementation of those requirements in software code (computer instructions) Leveson, 1995. In most accidents, the software requirements have had missing cases or incorrect assumptions about the behavior of the system in which the software is operating. Often there is a misunderstanding by the engineers of the requirements for safe behavior, such as an omission of what to do in particular circumstances that are not anticipated or considered. The software may be "correct" in the sense that it successfully implements its requirements, but the requirements may be unsafe in terms of the specified behavior in the surrounding system, the requirements may be incomplete, or the software may exhibit unintended (and unsafe) behavior beyond what is specified in the requirements. Redundancy or even multiple versions of the implementations of the requirements does not help in these cases.

The RAI response also cited the National Research Council, which the staff asked to conduct a study on applying DI&C technology to commercial NPP operations. The study has a number of conclusions and recommendations that are relevant to the application of diversity in the HIPS platform design. With respect to common-mode software failure potential, the report concluded the following:

Conclusion 3. The USNRC guidelines on assessing whether adequate diversity exists need to be reconsidered. With regard to these guidelines: (a) The committee agrees that providing digital systems (components) that perform different functions is a potentially effective means of achieving diversity. Analysis of software functional diversity showing that independence is maintained at the system level and no new failure modes have been introduced by the use of digital technology is no different from that for upgrades or designs that include analog instrumentation. (b) The committee considers that the use of different hardware or real-time operating systems is potentially effective in achieving diversity provided functional diversity has been demonstrated. With regard to real-time operating systems, this applies only to operating systems developed by different companies or shown to be functionally diverse. (c) The committee does not agree that use of different programming languages, different design approaches meeting the same functional requirements, different design teams, or different vendors' equipment used to perform the same function is likely to be effective in achieving diversity. That is, none of these methods is a proof of independence of failures. Conversely, neither is the presence of these proof of dependence of failures.

Conclusion 4. There appears to be no generally applicable, effective way to evaluate diversity between two pieces of software performing the same function. Superficial or surface (syntactic) differences do not imply failure independence, nor does the use of different algorithms to achieve the same functions. Therefore, funding research to try to evaluate design diversity does not appear to be a reasonable use of USNRC research funds.

In response to RAI part (2), on why it is acceptable to use the same iV&V design simulation tool for both FPGA technologies, the applicant stated that the purpose of the iV&V effort is to check the development of the FPGAs by the design team. The required independence is the attribute that is most effective in identifying any errors that might be introduced by a flaw in FPGA design development. The purpose of the required diversity in the iV&V design simulation tool is to check the development of the FPGAs with a tool that is different from the development tool. This diversity compensates for any errors that might be introduced by a flaw in either of the development tools. The use of a single iV&V tool allows for a common comparison of the FPGA configurations developed with diverse tools. The common comparison base supports a better evaluation of test results to determine the likely source of error (e.g., introduced by the development tool or introduced by a logic design error). The use of different iV&V tools would require the consideration of errors introduced by one of the iV&V tools as a potential source of error.

The staff found the applicant's response to this RAI and the proposed changes to TR Sections 6.2, 6.4, and 11 acceptable. The applicant has incorporated all of these proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI No. 3, Question 07.01 Draft DSRS-5, is resolved and closed.

An applicant or licensee referencing this SE must provide the basis for the allocation of safety functions among the two diverse divisions to mitigate the effects of a postulated CCF concurrent with Chapter 15 events in the final safety analysis report. This is ASAI-9.

An applicant or licensee referencing this SE must verify that all diversity attributes of the HIPS platform (i.e., equipment, design, and functional diversity) conform to the diversity design details provided in the TR. This is ASAI-10.

An applicant or licensee referencing this SE must verify that the diverse FPGA technologies have unique identification. This is ASAI-11.

Based on the above discussion, the staff finds the built-in diversity attributes of the HIPS platform support conformance with 10 CFR 50.55a(h), specifically IEEE Std. 603-1991, Clause 5.1; the NRC policy in the SRM to SECY-93-087, Item 18.II.Q; and guidance in NUREG/CR-6303 and IEEE Std. 7-4.3.2, provided that a licensing application referring to this SE addresses the ASAI-11 identified in Section 4.0 of this SE.

3.5 Review of Repeatability and Predictability

The review evaluated the methods described in the application to demonstrate that the HIPS platform performance is predictable and repeatable. Predictable and repeatable system behavior refers to the case in which input signals and system characteristics result in output signals through known relationships among the system states and responses to those states. Such a system will produce the same outputs for a given set of input signals (and the sequence of inputs) within well-defined response time limits to allow timely completion of credited actions. I&C safety systems should be designed to operate in such a predictable and repeatable manner, which is also called “deterministic” behavior.

This review evaluated the predictability and repeatability of the HIPS platform performance and outputs, including its data communications systems for a given set of input signals. The objective of this review was to (1) confirm that the HIPS platform design and communication protocols provide features to ensure that the system (or logic) produces the correct response to inputs within the time credited to produce a response, and (2) confirm that hazards that could challenge predicted behavior have been adequately identified and accounted for in the design.

This evaluation also confirmed that the HIPS platform design supports compliance with 10 CFR 50.55a(h) that incorporates by reference IEEE Std. 603-1991, which provides requirements related to safety system performance and the timing of the safety system response. Clause 4, “Safety System Design,” of IEEE Std. 603-1991 requires the applicant to establish the design basis for each safety system, including documentation of the following:

- A. the variables that are to be monitored to manually or automatically control each protective action; the analytical limit associated with each variable, the ranges (normal,

abnormal, and accident conditions); and the rates of change of these variables (Clause 4.4)

B. the critical points in time after the onset of a DBE (Clause 4.10)

In addition, Clause 5.5, "System Integrity," of IEEE Std. 603-1991 requires that safety systems be designed to accomplish their safety-related functions under the range of conditions enumerated in the design basis. After initiation by either automatic or manual means, the sequence of protective actions (from receipt of a signal from the sense and command features to the actuated equipment that performs the safety function) shall go to completion in conformance with IEEE Std. 603-1991, Clause 5.2, "Completion of Protective Action."

As stated in TR Section 7.0, "Repeatability and Predictability," the fundamental design objective of the HIPS platform is to take advantage of the benefits of analog architectures installed within the existing commercial NPPs. The HIPS platform supports the independent trip determination channels in the same manner as in the analog architecture. The HIPS platform uses a virtual point-to-point connection of the trip decision to the voter level of the architecture. It also uses the point-to-multipoint arrangement achieved within the master-relay-to-slave-relay connection.

Figure 3-4 shows a typical plant signal data flow path in the HIPS platform:

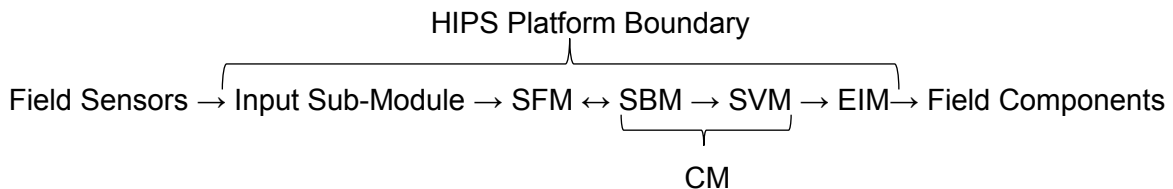


Figure 3-4 Typical plant signal data flow path in HIPS platform

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

The input submodule contains a tunable process filter that is application specific. This process filter is normally the dominate contributor to the overall time response of the system and needs to be evaluated in the application-specific submittal. Continuous self-test and calibration checks are performed on the analog input submodule ADCs. These tests verify the calibration of the analog portion and that the input submodule is working. The continuous calibration check verifies that the ADC is within the desired accuracy and that it has not drifted out of calibration. This supports the predictable and repeatable platform design fundamental.

A single clock base is used for all logic on the SFM as well as to derive the SDB bit frequency and sampling bits on the bus. The clock oscillator accuracy is chosen to avoid issues related to sampling the bus, given the bus architecture.

The safety function is processed through three redundant CMs to provide error detection and fault tolerance of the safety function. Each of the five buses that provide communications within the HIPS chassis has a bus master CM controlling the communications. There are three SBMs that are the bus masters for the three SDBs in each separation group, three SVMs that are the bus masters for the SDBs in each RTS division, and three SVMs in each division of the ESFAS. There is one MIB-CM in each separation group that is the bus master for the MIB and CTB, and there is one MIB-CM in each division of the RTS and the ESFAS that is the bus master for the MIB. The four communication ports on each CM that provide communications outside of the HIPS chassis can be configured as either transmit only or receive only. This provides a hardware solution for one-way communication. Each communication channel is independent and isolated for either transmit or receive. The communication ports are connected with fiber-optic cable providing electrical isolation between modules.

A single clock base is used for all logic on the EIMs as well as to derive the SDB bit frequency and sampling bits on the bus. The FPGA functions on the EIM consist of deterministic-state machines. The EIM uses discrete logic for the APL, high-drive switching outputs, hard-wired signals, and equipment feedback circuitry. This architecture performs manual actuations downstream of any software or programmable logic. The EIM is a slave module to all three SVMs and the MIB-CM. The EIM uses the FPGA device to implement the logic circuits for the automatic actuation signal voting, the handling of the IDI, and the bus communication logic. The EIM is equipped with four high-drive switching outputs. The high-drive output is implemented as a redundant output, where a single failure in one of the driving components is automatically detected and mitigated without affecting the output operation.

In RAI 3, Question 07.01 Draft DSRS-2, Item (c), the staff asked the applicant to describe how the output module of the HIPS platform provides selectable preferred states for all postulated conditions. In its response to RAI 3, Question 07.01 Draft DSRS-2, Item (c), dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Based on the staff's review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-2, Item (c), the staff found the applicant's response acceptable. The staff also reviewed the proposed changes to TR Sections 7.6, "HIPS Module Modes," and 8.2.7 provided with the RAI response and found them acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-2, Item (c), is resolved and closed.

[REDACTED]

These design attributes support the predictability and repeatability of the HIPS platform.

HIPS Platform Work Cycle

The HIPS platform work cycle described in TR Section 7.7, "HIPS Platform Work Cycle," demonstrates that the HIPS platform design requires each task to be performed in well-defined and deterministic steps in every cycle.

Figure 3-5 shows the timing of transferring the SFG PTDA from the SFM to the EIM. The timing diagram is focused on the digital portion. The diagram does include the analog input delay on the left and the analog output delay on the right side. These analog delays are dependent on the application and are simply added to the overall timing calculation. The diagram also shows the logic delays of the modules that are included in the transaction times. These logic delays are very small with regard to the communications timing; as such, they are added as an element in the worst case timing calculation.

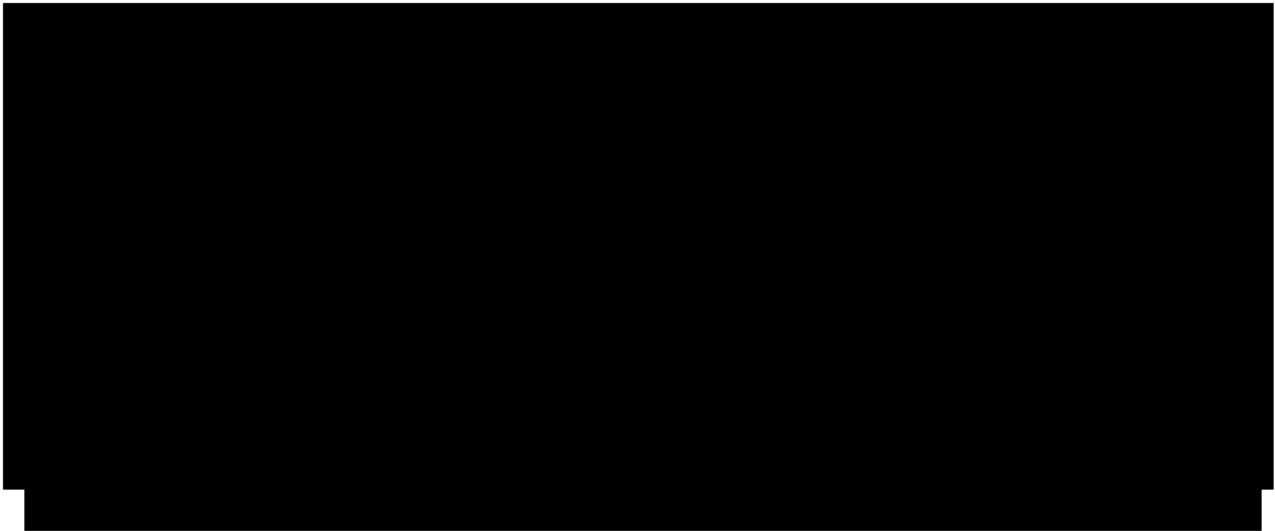


Figure 3-5 Timing diagram for a representative architecture

Each applicant or licensee is expected to provide plant-specific and application-specific safety function response time design bases as response time performance requirements to be met by a HIPS platform-based system. The actual response time of a HIPS platform-based system is determined by its overall configuration. Therefore, each applicant or licensee must determine that HIPS platform response time characteristics are suitable for its plant-specific application. The following information and staff evaluation address the HIPS platform response time characteristics and use of these characteristics in support of future plant-specific suitability determinations, because the HIPS platform is a set of components to which response time budgets are allocated.

HIPS Platform Response Time

The HIPS platform response time performance characteristics are described in general terms within the TR (Ref. 6.1-3). To meet a typical response time performance requirement, 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. Therefore, the applicant's or licensee's plant-specific and application-specific safety function response time design bases should address these response time components separately from the response time performance requirements specified for the applicant's or licensee's HIPS platform-based system.

Based on this evaluation, the staff has determined that the predictability and repeatability approach of the HIPS platform, including the successful demonstration of all applicable ASAs in Section 4.0 of this SE, together with the successful evaluation of the other fundamental design principles, such as independence (see Section 3.2), redundancy (see Section 3.3), and diversity (see Section 3.4), adequately address the fundamental design principle of predictability and repeatability (at the platform level) for an application referencing this SE.

3.6 Review of IEEE Std. 603 Requirements

The scope of IEEE Std. 603-1991 includes all I&C safety systems. Except for the requirements for independence between control systems and safety systems, IEEE Std. 603-1991 does not apply directly to nonsafety systems, such as the control systems and diverse I&C systems. Although intended only for safety systems, the criteria for IEEE Std. 603-1991 can apply to any I&C system. Therefore, for nonsafety I&C systems that have a high degree of importance to safety, the concepts of IEEE Std. 603-1991 are an appropriate starting point for the review of these systems.

IEEE Std. 603-1991 contains five clauses (Clause 4, 5, 6, 7, and 8), described in the five major subsections below, that must be considered in the evaluation of the platform. Each of these major subsections contains subordinate subsections that address the individually identifiable requirements of these clauses. Consideration is given to the degree to which each requirement can be evaluated in whole or in part within the scope of a platform review. While a number of the requirements cannot be assessed or cannot be assessed fully on the basis of the platform, each of the main requirements of IEEE Std. 603-1991 is presented. This evaluation is a means for subsequent application-specific and plant-specific submittals to account for those elements of review that are contained in this document.

TR Appendix A summarizes the regulatory compliance of the HIPS platform with IEEE Std. 603-1991. However, it was not clear to the staff how the HIPS design specifications conform to RG 1.153 and the referenced standard, IEEE Std. 603-1991. Therefore, in RAI 3, Question 07.01 Draft DSRS-15, the staff asked the applicant to explain the basis for its claims; specifically, conformance to RG 1.153, and compliance with associated clauses in IEEE Std. 603-1991. In its response to RAI 3, Question 07.01 Draft DSRS-1, dated August 19, 2016 (see Ref. 6.1-20), the applicant revised Appendix A to add the application-specific information and make other conforming changes based on the RAI responses. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-15 (see Sections 3.6.1 to 3.6.5), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Appendix A provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-15, is resolved and closed.

Although the staff determined that the HIPS platform supports satisfying various sections and clauses of IEEE Std. 603-1991, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std. 603-1991. Because this SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences, an applicant or licensee is expected to identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 603-1991 clause to its application-specific HIPS platform-based safety system or component. Furthermore, the applicant or licensee must demonstrate that the plant-specific and application-specific use of the

HIPS platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

3.6.1 Clause 4 Safety System Design

Clause 4 of IEEE Std. 603-1991 states that a specific basis shall be established and documented for the design of each safety system of the nuclear power generating station. The individual clauses under Clause 4 require identification and documentation of specific design-basis information. The subclauses of this requirement can be characterized as follows:

Clause 4.1	identification of the DBEs
Clause 4.2	safety functions and corresponding protective actions
Clause 4.3	permissive conditions for each operating bypass capability
Clause 4.4	identification of variables monitored
Clause 4.5	minimum criteria for manual initiation and control of protective actions
Clause 4.6	identification of the minimum number and location of sensors
Clause 4.7	range of transient and steady-state conditions
Clause 4.8	identification of conditions that may degrade performance
Clause 4.9	the methods to be used to determine reliability
Clause 4.10	the critical points in time after the onset of a DBE
Clause 4.11	the equipment protective provisions
Clause 4.12	any other special design basis

The determination and documentation of the design basis for a safety system are application-specific activities dependent on the plant design. Since the TR does not address a specific application of the platform, the design basis for a safety system is not available for review, and no evaluation of the HIPS platform against these regulatory requirements could be performed. Therefore, the staff did not evaluate of the HIPS platform against the regulatory requirements of Clause 4 of IEEE Std. 603-1991.

3.6.2 Clause 5 Safety System Criteria

Clause 5 of IEEE Std. 603-1991 contains fifteen clauses that apply to all safety system functions and features. Through these clauses, Clause 5 of IEEE Std. 603-1991 requires that safety systems maintain plant parameters, with precision and reliability, within acceptable limits established for each DBE. The power and I&C portions of each safety system must comprise more than one SFG (or division), and any single SFG must be able to accomplish the safety function. The establishment of SFGs to accomplish a given safety function is a plant-specific and application-specific activity and the TR scope does not include specific applications. Therefore, the following evaluations against the requirements of Clause 5 of IEEE Std. 603-1991 are limited to capabilities and characteristics of the HIPS platform that are relevant to meet each requirement.

3.6.2.1 Clause 5.1 Single-Failure Criterion

Clause 5.1 of IEEE Std. 603-1991 requires that safety systems be able to perform all safety functions required for a DBE in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable, but nondetectable, failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions. DSRS Section 7.1.3, "Redundancy," provides acceptance criteria for the single-failure criterion. In addition, DSRS Section 7.1.5, "Diversity and Defense-in-Depth," contains acceptance criteria for the single-failure criterion.

The determination that no single failure within the safety system can prevent required protective actions at the system level is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those features and capabilities that support adherence to the single-failure criterion by a system design based on the platform. Since the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architecture, the evaluation against this requirement is limited to design features provided by the HIPS platform to address failures.

The architecture of the HIPS platform established for safety applications employs four redundant and independent SFGs and two redundant and independent divisions of RTS and ESFAS. Redundancy within the HIPS platform enables it to inherently withstand most single failures on a single data path without disabling the capability to perform its function. Other design features of the HIPS platform that support the capability to withstand the effects of single failures relate to independence. These features include the provision of isolation concepts used to support monitoring and indication features (see Sections 3.1.9 and 3.2). The remaining identifiable single failures are addressed at the platform level through detection and indication by automatic diagnostics and self-tests or periodic surveillance.

The use of redundancy at the platform level supplements the conventional use of redundancy at the system level to satisfy the single-failure criterion (see Section 3.2). In addition, the use of redundancy generally enables the HIPS platform to mitigate the effects of postulated single failures without loss of a safety function. However, platform-level redundancy cannot substitute for system-level mitigation of the effects of a single failure on a safety function nor can it resolve potential CCF vulnerabilities. Consequently, provisions for a system-level failure mode and effect analysis (FMEA) must be established as an ASAI and evaluated as part of an application-specific review. This is ASAI-12.

The HIPS platform provides diagnostics and self-test capabilities to detect and enable indication of module component failures during startup and operation. Section 3.1.9 discusses the staff evaluation of these capabilities. These platform-level capabilities contribute to meeting Clause 5.1 of IEEE Std. 603-1991 by providing the means to detect most postulated component failures. Periodic surveillance is needed to detect some postulated failures. Consequently, provisions for surveillance testing must be established as an ASAI and evaluated as part of an application-specific review. This is ASAI-13.

The HIPS platform provides design concepts that address the fundamental design principles of independence and D3. Sections 3.2 and 3.4 discuss the staff evaluation of these capabilities. These platform-level capabilities contribute to meeting Clause 5.1 of IEEE Std. 603-1991 by providing the means to withstand the effects of single failures. However, a single-failure analysis is needed to identify actions to be taken when errors and failures are indicated and managed after they are detected. Consequently, provisions for a single-failure analysis must be established as an ASAI and evaluated as part of an application-specific review. This is ASAI-14.

Based on the review items discussed above, the HIPS platform design features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.1 of IEEE Std. 603-1991. However, ASAI-12 to ASAI-14 are necessary to establish full compliance with this regulatory requirement.

3.6.2.2 Clause 5.2 Completion of Protective Action

Clause 5.2 of IEEE Std. 603-1991 states that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion, and deliberate operator action shall be required to return the safety systems to normal. DSRS Section 7.2.3, "Reliability, Integrity, and Completion of Protective Action," provides acceptance criteria for this requirement.

The determination that protective actions of the execute features of a safety system continue to completion after initiation and require a deliberate operator action thereafter to restore to normal are plant-specific and application-specific activities that require an assessment of a full system design. A platform-level assessment can only address those features and capabilities that support adherence to the completion of protective actions by a system design based on the platform. Since the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architecture, the evaluation against this requirement is limited to design features provided by the HIPS platform to enable system-level protective actions to proceed to completion.

Once protective actions are initiated with the HIPS system, the RTS and ESF actuations proceed to completion. The circuitry of the APL is designed so that, when an actuation signal is received, either through the safety data path or through the HWM manually, the APL ensures the action through until completion. Upon a reset of the sense and command features, the APL continues to hold the actuated components on the requested position until deliberate operator action is taken to return the component to normal. The design approach to be implemented is consistent with plant-specific functional logic to enable system-level protective actions to proceed to completion.

To support meeting the requirements of IEEE Std. 603-1991, the HIPS RTS and ESFAS are designed so that any single failure in these systems will not prevent proper protective action at

the system level. No single failure will defeat more than one of the four redundant and independent SFGs and two redundant and independent divisions of RTS and ESFAS. These redundant SFGs and divisions are electrically isolated and physically separated. Qualified isolation devices will undergo qualification testing that, at a minimum, will meet the independence requirements as described in RG 1.75, Revision 3. These provisions are for protection against single failures and for independence. Sections 3.2, 3.3, and 3.6.2.1 discuss the staff evaluation of these capabilities.

The HIPS platform is designed to produce the same outputs for a given set of input signals within well-defined response time limits to allow timely completion of credited actions. Section 3.5 contains the staff evaluation of these capabilities. These platform-level capabilities contribute to meeting Clause 5.2 of IEEE Std. 603-1991 by providing the means to enable system-level protective actions to proceed to completion.

Based on the review items discussed above, the HIPS platform design features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.2 of IEEE Std. 603-1991. However, ASAI-15 is necessary to establish full compliance with this regulatory requirement.

3.6.2.3 Clause 5.3 Quality

Clause 5.3, "Quality," of IEEE Std. 603-1991 states that the components and modules within the safety system must be of a quality consistent with minimum maintenance requirements and low failure rates, and safety-system equipment must be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance (QA) program. DSRS Section 7.2.1, "Quality," provides acceptance criteria for this requirement. These acceptance criteria state that the QA provisions of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 apply to a safety system.

The TR does not address a QA program, because this is an application-specific activity dependent on the equipment vendor to be used to implement the HIPS system. Since the TR does not address a specific application of the platform, the QA program is not available for review, and no evaluation of the HIPS platform against this regulatory requirement could be performed. Therefore, this SE does not address the evaluation against the requirement of Clause 5.3 of IEEE Std. 603-1991. ASAI-16 is necessary to establish full compliance with this regulatory requirement.

3.6.2.4 Clause 5.4 Equipment Qualification

Clause 5.4, "Equipment Qualification," of IEEE Std. 603-1991 states that safety system equipment must be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting the performance requirements as specified in the design basis. DSRS Section 7.2.2, "Equipment

Qualification,” provides acceptance criteria for this requirement. These acceptance criteria state that the equipment qualification (EQ) is limited to a confirmation that I&C equipment (including isolation devices) subject to qualification requirements has been selected and identified in the application.

The TR does not address an EQ program, because this is an application-specific activity dependent on the equipment vendor to be used to implement the HIPS system. Since the TR does not address a specific application of the platform, the EQ program is not available for review, and no evaluation of the HIPS platform against this regulatory requirement could be performed. Therefore, this SE does not address the evaluation against the requirements of Clause 5.4 of IEEE Std. 603-1991. ASAI-17 is necessary to establish full compliance with this regulatory requirement.

3.6.2.5 Clause 5.5 System Integrity

Clause 5.5 of IEEE Std. 603-1991 states that each safety system design must remain capable of accomplishing its safety functions under the full range of applicable conditions enumerated in the design basis. DSRS Section 7.2.3 contains acceptance criteria for this requirement.

The TR states that application-specific system-level requirements are necessary to define a safe state and the conditions required to enter a fail-safe state. The TR also requires an applicant or licensee referencing this SE to identify system-level failure modes, methods of detection, and system responses and document these characteristics in an application-specific FMEA. Therefore, the determination of system integrity is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those characteristics that can support fulfillment by a system design based on the HIPS platform. Since the TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to considering the integrity demonstrated by the platform and its features to ensure that a safe state can be achieved in the presence of failures. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, an application-specific evaluation is necessary to establish full compliance with Clause 5.5 of IEEE Std. 603-1991. This is ASAI-18.

The HIPS platform demonstrates calculated response time characteristics and supports the definition and demonstration of maximum and minimum response time performance to meet safety system performance and determinism requirements. Section 3.5 discusses the staff evaluation of the response time and deterministic performance. The staff's evaluation concluded that the HIPS platform's response time and determinism support meet the criteria of this clause at the platform level and are suitable to support safety applications. The actual response times for particular safety functions are application-specific, and acceptable performance depends on the overall system design, architecture, and required plant safety functions. Therefore, ASAI-19 is identified to confirm suitability of the response time characteristics of the HIPS platform for a particular safety function implementation and to demonstrate acceptable relevant response times. Consequently, evaluation for full

conformance against this portion of the acceptance criteria remains for an application-specific review.

The HIPS platform describes the capabilities of equipment fail-safe behavior in response to detectable failures. Section 3.5 discusses the staff evaluation of these capabilities. These platform-level capabilities contribute to meeting Clause 5.5 of IEEE Std. 603-1991 by providing the means to ensure that a safe state can be achieved in the presence of failure.

The redundancy provided by the HIPS platform provides fail-safe behavior in response to detectable failures, and alarms the condition through status information that is displayed locally (i.e., HIPS module LEDs) and can be transmitted for display. The staff determined that the redundancy features of the HIPS platform provide fault tolerance and allow a safe state to be maintained through continued operation (see Section 3.3). The diagnostics and self-test capabilities of the HIPS platform, discussed in Section 3.1.9, provide an acceptable means for placing the system in a safe state and alarming the failure condition for those failures detected by diagnostics. In many instances, the safe state can consist of a HIPS module entering the fail-safe state mode [REDACTED]. However, the specific response to particular failures depends on an application-specific system design and is, therefore, subject to a plant-specific review.

The provision of surveillance testing and operator monitoring of failures that are not automatically detected by diagnostics or a self-test depends on an application-specific system design, which can include application-level diagnostics and status indications to operators. An application-specific FMEA is needed to identify specific surveillance provisions to detect system failures for which automatic detection through diagnostics and self-tests are not provided. ASAI-12 establishes full compliance with this regulatory requirement.

Based on the review items discussed above, the HIPS platform features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.5 of IEEE Std. 603-1991. ASAI-12, ASAI-18, and ASAI-19 are necessary to establish full compliance with this regulatory requirement.

3.6.2.6 Clause 5.6 Independence

Clause 5.6 of IEEE Std. 603-1991 requires, in part, independence among (1) redundant portions of a safety system, (2) safety systems and the effects of DBEs, and (3) safety systems and other systems. DSRS Section 7.1.2, "Independence," provides acceptance criteria for this requirement.

These acceptance criteria state that four aspects of independence ((1) physical independence, (2) electrical independence, (3) communications independence, and (4) functional independence) should be addressed for each of the previously listed cases. The NRC provides guidance for the evaluation of physical and electrical independence in RG 1.75, Revision 3, which endorses IEEE Std. 384-1992, "Standard Criteria for Independence of Class 1E

Equipment and Circuits.” The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the use of separate power sources. Transmission of signals between independent channels should be through isolation devices. Functional independence should prevent safety function failures by ensuring that physically and electrically independent portions of safety systems (with the exception of coincidence voting) do not depend on information from other independent portions of the safety system.

Establishing independence for a safety system is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those capabilities that can support adherence to the independence requirement by a system design based on the platform. Since the TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to considering the means provided within the platform to promote independence.

The HIPS platform describes the internal platform independence features that provide the capability to implement systems designs that can satisfy the system independence requirements of IEEE Std. 603-1991. Section 3.2 discusses the staff evaluation of these capabilities. These platform-level capabilities contribute to meeting Clause 5.5 of IEEE Std. 603-1991 by providing the features that can support the electrical and communication provisions of this clause at the platform level. ASAs are necessary to establish full compliance with Clause 5.6. Sections 3.6.2.6.1 to 3.6.2.6.4 discuss these ASAs.

The evaluations below against the requirements of Clause 5.6 of IEEE Std. 603-1991 are limited to the capabilities and characteristics of the HIPS platform that are relevant to meeting each requirement.

3.6.2.6.1 Clause 5.6.1 Between Redundant Portions of a Safety System

Clause 5.6.1, “Between Redundant Portions of a Safety System,” of IEEE Std. 603-1991 states that the safety systems are to be designed so that there is sufficient independence between redundant portions of a safety system for the redundant portions to be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any DBE requiring that safety function. DSRs Section 7.1.2 does not provide any additional acceptance criteria beyond those in Clause 5.6.1.

The determination of independence between redundant portions of a safety system is an application-specific activity that requires an assessment of a full system design. Since the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architecture, the evaluation against this requirement is limited to considering the

means provided within the platform to implement system designs that contribute to satisfying this requirement. A platform-level assessment can only address those features and capabilities that support adherence to independence between redundant portions of a safety system by a system design based on the platform. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full compliance with Clause 5.6.1 of IEEE Std. 603-1991.

Although the HIPS platform supports the use of unique components within different redundant portions of a safety system, application-specific activities should assess the full system design to ensure different redundant portions of a safety system do not rely on a common component. Compliance with ASAI-20 provides reasonable assurance that the safety system will retain the capability to accomplish the safety function caused by the loss or failure of any common component.

Although the HIPS platform supports the use of separate power sources, application-specific activities should assess the full system design to ensure the redundant power sources separately supply the redundant power conversion features within the HIPS platform. Compliance with ASAI-21 provides reasonable assurance that the safety system will retain the capability to provide redundant power sources.

The redundant configuration of a multichannel safety system and the independence provided between those redundant channels are solely dependent on the safety system design. The HIPS platform can be configured into an architecture that has four separation groups that are physically and electrically independent of each other. The example architecture presented for the HIPS platform is representative of one separation group and Division I of the RTS and ESFAS in a safety system. Each bus is a differential bus with a single master and multiple slaves. The three CMs connected to SDBs are the bus masters for the three SDBs. The MIB-CM is the bus master for the MIB and the CTB.

The HIPS platform provides electrical, digital communication, and functional design features to support independence between redundant channels on the safety system design, which are discussed and evaluated in Section 3.2 of this SE. The staff determined that the redundant portions of a safety system have sufficient independence such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function.

Based on the review items discussed above, the HIPS platform features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.6.1 of IEEE Std. 603-1991. ASAI-20 and ASAI-21 are necessary to establish full compliance with this regulatory requirement.

3.6.2.6.2 Clause 5.6.2 Between Safety Systems and Effects of Design-Basis Events

Clause 5.6.2 of IEEE Std. 603-1991 states that the safety systems required to mitigate the consequences of a specific DBE must be independent of, and physically separated from, the effects of the DBE to the degree necessary to retain the capability to meet the requirements of this standard. Clause 5.6.2 further states that an EQ, in accordance with Clause 5.4, is one method that can be used to meet this requirement. DSRS Section 7.1.2 does not provide any additional acceptance criteria beyond those in Clause 5.6.2.

Determining the effects of DBEs and establishing the physical separation of the safety system from the effects of those events are application-specific activities. In addition, the EQ program is an application-specific activity dependent on the equipment vendor to be used to implement the HIPS system. However, the HIPS platform provides electrical isolation and digital communication independence features to support the independence between the HIPS platform and the effects of DBEs, which are discussed and evaluated in Section 3.2. The staff determined that there is sufficient independence between the HIPS platform and the effects of DBEs and that applications based on the HIPS platform are capable of mitigating the consequences of DBEs.

Based on the review items discussed above, the HIPS platform features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.6.2 of IEEE Std. 603-1991. ASAI-17 is necessary to establish full compliance with this regulatory requirement.

3.6.2.6.3 Clause 5.6.3 Between Safety Systems and Other Systems

Clause 5.6.3, "Between Safety Systems and Other Systems," of IEEE Std. 603-1991 states that the safety systems are to be designed such that credible failures in and consequential actions by other systems will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, the effects of a single random failure, and detailed criteria. DSRS Section 7.1.2 does not provide any additional acceptance criteria beyond those in Clause 5.6.3.

The four subsections below document the evaluation of interconnected equipment, equipment in proximity, the effects of a single random failure, and detailed criteria separately.

3.6.2.6.3.1 Clause 5.6.3.1 Interconnected Equipment

Clause 5.6.3.1 of IEEE Std. 603-1991 states that equipment that is used for both safety and nonsafety functions, as well as the isolation devices used to affect a safety system boundary, are to be classified as part of the safety systems. This clause further states that no credible failure on the nonsafety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any DBE requiring

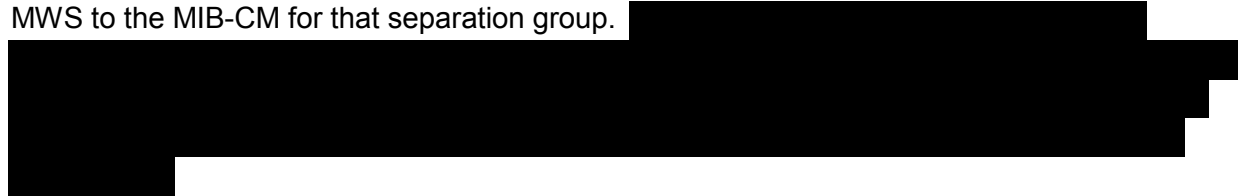
that safety function and that a failure in an isolation device will be evaluated in the same manner as a failure of other equipment in a safety system.

The determination of interconnections between a safety system and other nonsafety systems in a plant through common equipment or communication links is an application-specific activity. However, the TR does identify the capability for one-way communication to nonsafety-related components across the MIB-CMs through fiber-optic cabling and an isolation PS gateway. In addition, the TR identifies the capability for one-way communication to nonsafety-related components across the HWM and an isolation enable nonsafety switch.

The HIPS platform provides electrical, digital communication, and functional design features to support independence between a safety system and other nonsafety systems, which are discussed and evaluated in Section 3.2. All data communications going out of or into the HIPS chassis are done through the one-way isolated communication ports on the CMs. The CMs are part of the safety-related HIPS platform and are qualified as safety-related modules and Class 1E to non-Class 1E isolation.

The TR classifies the MWS and PS gateway as nonsafety related. The staff determined that none of these devices is used for the accomplishment of any safety functions (see Sections 3.1 and 3.5). To promote independence, the PS can only provide status and diagnostics information to the nonsafety-related control system, PS gateway, and both divisions of the SDI system through one-way, transmit-only, isolated outputs. However, the control system, PS gateway, and SDI are not part of the base platform and, thus, are not within the scope of this evaluation. Consequently, fulfilling this requirement involves an ASAI for verification that the PS gateway (or any other device not part of the base HIPS platform) cannot transmit messages on the MIB-CMs and thus compromise independence between the safety system and any other systems connected to the PS gateway.

Each division of the PS has a nonsafety-related MWS for the purpose of maintenance and calibration. The MWS supports online monitoring using the MIB-CM through one-way isolated communication ports over point-to-point fiber-optic cables. The one-way isolated data from the HIPS platform to the MWS include the setpoint and tunable parameter information for each SFM. The only time communication from the MWS to the HIPS chassis is allowed is when the SFM is placed OOS by activating the OOS switch and a temporary cable is attached from the MWS to the MIB-CM for that separation group.



The HWM performs a safety-related function to provide electrical isolation for the backplane and modules from the external manual switches (e.g., enable nonsafety switch) and the nonsafety-related control signals. When the enable nonsafety switch is closed, a plant operator can control components with an analog binary control signal that is nonsafety related. The enable

nonsafety switch is classified as part of the safety system and is used to prevent spurious nonsafety-related control signals from adversely affecting safety-related components.

The HIPS platform galvanic isolation features used to isolate nonsafety-related inputs are passive safety-related features that do not rely on power to provide the required protection. The isolation devices used in the HIPS-based system are classified as part of the safety system. In addition, these isolation devices will undergo qualification testing that, at a minimum, will meet the independence requirements described in RG 1.75, Revision 3. Since all other components of the HIPS platform are classified as safety related, the HIPS platform supports meeting the requirements of Clause 5.6.3.1.

Based on the review items discussed above, the HIPS platform features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.6.3.1 of IEEE Std. 603-1991. ASAI-12 and ASAI-22 are necessary to establish full compliance with this regulatory requirement.

3.6.2.6.3.2 Clause 5.6.3.2 Equipment Proximity

Clause 5.6.3.2, "Equipment in Proximity," of IEEE Std. 603-1991 states (1) that equipment in other systems that is in physical proximity to safety system equipment but that is neither an associated circuit nor another Class 1E circuit will be physically separated from the safety system equipment to the degree necessary to retain the safety system's capability to accomplish its safety functions in the event of the failure of nonsafety equipment and (2) that physical separation may be achieved by physical barriers or acceptable separation distance. This clause states that the separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std. 384-1992. Clause 5.6.3.2 further states that the physical barriers used to establish a safety system boundary shall meet the requirements of IEEE Std. 603-1991, Clauses 5.3, 5.4, and 5.5 for the applicable conditions specified in Sections 4.7 and 4.8 of the design basis.

The determination of the physical proximity of safety system equipment in relation to other equipment in a plant is an application-specific activity. In addition, the TR does not address a specific application or specify plant locations for implementation. However, the HIPS platform provides electrical isolation and digital communication independence features to support independence between the HIPS platform and nonsafety systems, which are discussed and evaluated in Section 3.2. The staff determined that there is sufficient independence between the HIPS platform and the nonsafety systems. The HIPS platform is capable of retaining the capability to accomplish its safety functions in the event of the failure of nonsafety equipment that is in physical proximity to the HIPS equipment. Based on the review items discussed above, the HIPS platform features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.6.3.2 of IEEE Std. 603-1991. ASAI-23 is necessary to establish full compliance with this regulatory requirement.

3.6.2.6.3.3 Clause 5.6.3.3 Effects of a Single Random Failure

Clause 5.6.3.3, "Effects of a Single Random Failure," of IEEE Std. 603-1991 states that, where a single random failure in a nonsafety system can (1) result in a DBE, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure.

The determination of potential failure propagation paths through interconnections between a safety system and other nonsafety systems in a plant is generally an application-specific activity. However, the HIPS platform provides electrical isolation and digital communication independence features to support independence between the HIPS platform and the effects of a single random failure, which are discussed and evaluated in Section 3.2. The staff determined that there is sufficient independence between the HIPS platform and the nonsafety systems. The HIPS platform is capable of providing a safety function even when degraded by any separate single failure. Based on the review items discussed above, the HIPS platform features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.6.3.3 of IEEE Std. 603-1991. Provisions for a system-level FMEA must be established as ASAI-12 and evaluated as part of an application-specific review to establish full compliance with this regulatory requirement.

3.6.2.6.4 Clause 5.6.4 Detailed Criteria

Clause 5.6.4, "Detailed Criteria," of IEEE Std. 603-1991 states that IEEE Std. 384-1992 provides detailed criteria for the independence of Class 1E equipment and circuits. In addition, it states that IEEE Std. 7-4.3.2-1993 contains guidance on the application of this criteria for the separation and isolation of the data processing functions of interconnected computers. The NRC gives guidance on applying the safety system criteria to computer-based safety systems in RG 1.152, Revision 3, which endorses IEEE Std. 7-4.3.2-2003 (an updated version of the 1993 edition). IEEE Std. 7-4.3.2-2003 gives computer-specific criteria (incorporating hardware, software, firmware, and interfaces) to supplement the criteria in IEEE Std. 603-1998. Although IEEE Std. 7-4.3.2-2003 references IEEE Std. 603-1998, IEEE Std. 603-1991 and the correction sheet dated January 30, 1995, remain the requirement for safety systems in accordance with 10 CFR 50.55a(h).

The determination of separation and isolation of the data processing functions of Class 1E equipment and circuits in a plant is generally an application-specific activity. However, the HIPS platform provides electrical isolation and digital communication independence features to support independence between the HIPS platform and Class 1E equipment and circuits, which are discussed and evaluated in Section 3.2. Based on the review items discussed above, the HIPS platform features and characteristics support a staff determination that the HIPS platform is suitable to satisfy Clause 5.6.4 of IEEE Std. 603-1991. ASAI-23 is necessary to establish full compliance with this regulatory requirement.

3.6.2.7 Clause 5.7 Capability for Test and Calibration

Clause 5.7 of IEEE Std. 603-1991 states that the safety system shall have the capability for testing and calibration while retaining the capability to accomplish its safety function, that this capability shall be provided during power operation, and that it shall duplicate, as closely as practicable, the performance of the safety function. DSRS Section 7.2.15 provides acceptance criteria for this requirement.

The TR does not address a specific application or establish a definitive safety system design. The determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements (e.g., accuracy, response time) that apply. The establishment of the types of surveillance necessary for the safety system to ensure detection of identifiable single failures only revealed through testing is also an application-specific activity. These are ASAI-24 and ASAI-25. For these reasons, this SE is limited to considering the means provided within the platform to enable testing and calibration for a redundant portion of a safety system (i.e., a channel).

Section 3.1.9 of this SE discusses the HIPS platform's ability to support meeting IEEE Std. 603-1991, Clause 5.7. The TR describes the acceptable use of BIST, CRC checks, periodic surveillance testing, and other tests in each type of module, as appropriate, to verify normal operation. The HIPS platform has design features that directly support methods to perform cross-checking between redundant safety system channel sensors or between sensor channels that bear a known relationship to each other. The HIPS platform design features to implement coincidence logic support the implementation of application-specific diagnostic logic and confirmation of continued execution through the MWS. However, the establishment of both the types of any automatic sensor cross-check as a credited surveillance test function and the provisions to confirm the continued execution of the automatic tests during plant operations is an application-specific activity. This is ASAI-26.

These diagnostic and test features, including calibration self-testing for the input submodules, are acceptable for meeting this regulatory requirement at the platform level. Therefore, while the evaluation confirms the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.7 of IEEE Std. 603-1991. ASAI-24 to ASAI-26 are necessary to establish full compliance with this regulatory requirement.

3.6.2.8 Clause 5.8 Information Displays

Clause 5.8, "Information Displays," of IEEE Std. 603-1991 has four subclauses associated with safety systems: 5.8.1, "Displays for Manually Controlled Actions"; 5.8.2, "System Status Indication"; 5.8.3, "Indication of Bypasses"; and 5.8.4, "Location." DSRS Sections 7.2.4, "Operating and Maintenance Bypass," and 7.2.13, "Displays and Monitoring," provide acceptance criteria for this requirement.

The design of information displays and operator workstations is an application-specific activity. Since the TR does not address a specific application nor include display devices (other than HIPS module LEDs) within the scope of the HIPS platform, the evaluation against the regulatory requirements below addresses the capabilities and characteristics of the HIPS platform that are relevant for adherence to each requirement.

3.6.2.8.1 Clause 5.8.1 Displays for Manually Controlled Action

Clause 5.8.1, “Displays for Manually Controlled Action,” of IEEE Std. 603-1991 requires unambiguous display instrumentation to be part of safety systems and to minimize the possibility of operator confusion wherever manually controlled actions are required for a safety system to accomplish its safety function and no automatic control is provided. DSRS Section 7.2.13 provides no further review guidance for Clause 5.8.1.

The TR states that display instrumentation provided for manually controlled safety actions is an application-specific system-level requirement, and the HIPS platform does not include display instrumentation for manually controlled actions. The TR then goes on to discuss the HIPS platform module capabilities to receive manual demand signals, perform the required safety actions, and drive analog or digital displays associated with the manually controlled action.

Section 3.1 addresses the staff’s evaluation of the design features provided by HIPS platform modules standardized.

Although the HIPS platform does not include display instrumentation or directly display information beyond discrete front panel status indicators, the staff determined that the HIPS platform supports meeting IEEE Std. 603-1991, Clause 5.8.1. This determination is based on the use described for the HIPS platform and the design features provided by its HIPS modules. Nevertheless, ASAI-27 is necessary when the HIPS platform supports the use of display instrumentation that supports manually controlled safety actions necessary to accomplish a safety function for which no automatic control is provided. Compliance with this ASAI will provide reasonable assurance that the supporting HIPS components and display instrumentation will be functional during plant conditions under which manual actions may be necessary.

3.6.2.8.2 Clause 5.8.2 System Status Indication

Clause 5.8.2, “System Status Indication,” of IEEE Std. 603-1991 requires unambiguous display instrumentation, which need not be part of the safety system, to minimize the possibility of operator confusion and to provide accurate, complete, and timely information pertinent to a safety system’s status, including indication and identification of protective actions. DSRS Section 7.2.4 provides no further review guidance for Clause 5.8.2.

The TR states that display instrumentation for safety systems’ status is an application-specific system-level requirement, and the HIPS platform does not include remote display

instrumentation for safety systems' status. The TR then goes on to discuss the HIPS platform modules capabilities to perform the protective actions and provide status both locally through discrete front panel indicators and remotely to display instrumentation.

Section 3.1 addresses the staff's evaluation of the design features provided by HIPS platform modules standardized.

Although the HIPS platform does not include display instrumentation or directly display information beyond discrete front panel status indicators, the staff determined that the HIPS platform supports meeting IEEE Std. 603-1991, Clause 5.8.2. This determination is based on the use described for the HIPS platform and the design features provided by its HIPS modules. Nevertheless, ASAI-28 is necessary when the HIPS platform supports the use of display instrumentation to provide indication and identification of protective actions as part of a safety system's status. Compliance with this ASAI will provide reasonable assurance that the supporting HIPS components and the display instrumentation provide unambiguous, accurate, complete, and timely status of safety system protective actions.

3.6.2.8.3 Clause 5.8.3 Indication of Bypasses

Clause 5.8.3, "Indication of Bypasses," of IEEE Std. 603-1991 requires that display instrumentation in the control room, which need not be part of the safety system, continue to indicate whether the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperable (excluding an operating bypass) for each affected SFG. Indicated bypasses are required to be automatically actuated if the bypass or inoperable condition will occur more frequently than once a year and when the affected system is required to be operable. The control room shall provide the capability to manually activate the bypass indication. DSRS Sections 7.2.4 and 7.2.13 provide no further review guidance for Clause 5.8.2.

The TR discusses the HIPS platform standardized circuit board capabilities to provide an indication of bypass for plant and application-specific protective actions and an indication of bypass both locally through discrete front panel indicators and remotely to display in the main control room. The HIPS platform supports the automatic actuation of the bypass or inoperable condition of an SFG when the MWS is actively communicating to it. Additionally, capabilities achieved through application-specific configurations allow for individual protective actions to be manually placed into bypass, which can then activate the bypass indication. TR Section 2.5.2 describes the HIPS platform's maintenance features, which address the behavior of bypass and inoperable status indications.

The staff reviewed the features and intended operation in support of safety system bypass and inoperable status indications for conformance with the guidance of DSRS Section 7.2.13 (see Section 3.1.4.1.3).

Although the HIPS platform does not include display instrumentation or directly display information beyond discrete front panel status indicators, the staff determined that the HIPS platform supports meeting IEEE Std. 603-1991, Clause 5.8.3. This determination is based on the use described for the HIPS platform and the design features provided by its standardized circuit boards. Nevertheless, ASAI-29 is necessary when the HIPS platform supports the use of display instrumentation to indicate bypassed or inoperable protective actions. Compliance with this ASAI will give reasonable assurance that the supporting HIPS components and the display instrumentation automatically actuate the bypass indication for bypassed or inoperable conditions, when required, and provide the capability to manually activate the bypass indication from within the control room.

3.6.2.8.4 Clause 5.8.4 Location

Clause 5.8.4, "Location," requires that information displays be located such that they are accessible to the operator and, if the information display is provided for manually controlled protective actions, that it be visible from the controls used to effect the actions.

The TR states that the location of displays is an application-specific system-level requirement, and the HIPS platform does not include remote display instrumentation. The TR also discusses the HIPS platform standardized circuit board capabilities to locally monitor protective action states using discrete front panel indicators and to initiate manually controlled protective actions through front panel toggle switches.

Section 3.1 addresses the staff's evaluation of the design features provided by the HIPS platform standardized circuit boards.

Although the HIPS platform does not include the location of displays, the staff determined that the HIPS platform supports meeting IEEE Std. 603-1991, Clause 5.8.4. This determination is based on the use described for the HIPS platform and the design features provided by its standardized circuit boards. ASAI-30 is necessary when the HIPS platform supports the use of display instrumentation to indicate bypassed or inoperable protective actions. Compliance with this ASAI will give reasonable assurance that the supporting HIPS components and the display instrumentation are accessible to the operator and are visible from the location of any controls used to effect a manually controlled protective action provided by the front panel controls of a HIPS-based system.

3.6.2.9 Clause 5.9 Control of Access

Clause 5.9, "Control of Access," of IEEE Std. 603-1991 requires the capability to administratively control access to safety system equipment through supporting provisions within the safety systems and/or the generating station design. DSRS Section 7.2.9, "Control of Access, Identification, and Repair," provides acceptance criteria for this requirement.

Establishing the particular approach for control of access to safety system equipment is an application-specific activity that depends on the system design. Physical access mechanisms depend on the specific implementation. The extent and nature of authorized human-system interactions depend on the allocation of function, operations and maintenance procedures, and human-machine interface capabilities addressed in a safety system design. In addition, the communication interconnections that may be provided between the safety system and other safety-related or nonsafety systems or equipment are generally dependent on the application. Since the HIPS TR does not address a specific application, the evaluation against this requirement is limited to considering the means provided within the platform to control access to the safety system equipment.

The HIPS is a modular, rack-mounted platform that is housed in cabinets. However, the cabinets themselves are not identified as part of the base platform and thus are not within the scope of this review. Consequently, the mechanisms for physical access control cannot be evaluated in this review.

The TR describes provisions intended for any HIPS-based safety system. The HIPS platform contains design features that provide the means to control physical access to PS equipment, including access to test points and the means for changing setpoints through the MWS. The MWS supports offline, OOS management (e.g. troubleshooting, calibration, and surveillance testing). The MWS is not part of the base platform, so it is not within the scope of this review. Nevertheless, it is noted that the example platform architecture described in the TR does not provide for a direct or network connection of the MWS to the HIPS platform for online maintenance. Any such connection that may be established in a specific application would require additional review.

The only time communication from the MWS to the HIPS chassis is allowed is when the SFM is placed OOS by activating the OOS switch and a temporary cable is attached from the MWS to the MIB-CM for that separation group. Any communication outside of a separation group HIPS chassis while the HIPS platform is in service is through the three SBMs and the MIB-CM through one-way isolated communication ports over point-to-point fiber-optic cables. The SFM is the only module that can be modified while installed in the chassis, which is limited to tunable parameters and setpoints in the NVM that require periodic modification. The TR does not adequately describe how many SFMs can be modified at a time. Therefore, in RAI 3, Question 07.01 Draft DSRS-11, the staff asked the applicant to provide this information. In the response to RAI 3, Question 07.01 Draft DSRS-11, the applicant stated the following:

It is expected that the MWS would be connected to one division at a time during plant operation, which can access all of the SFMs in the division. During periods when the plant is shutdown, MWSs could be connected to multiple divisions simultaneously when the I&C system is not required to be operable by plant technical specifications. Technical specification requirements for the system using the HIPS platform equipment will define specific limitations on the use of maintenance bypasses.

To change the functional logic, the SFM must be removed from the chassis and installed in a special device to allow modification of the logic of the FPGA. The OOS switch on the front of the SFM allows removing the SFM from service and physically disconnects the CTB from the SFM with the OOS switch in the operate position. The OOS switch in the OOS position connects the CTB to the SFM and allows the changing of setpoints and tunable parameters that are stored in the NVM. These design features support administrative controls of the access to a HIPS-based safety system through the OOS switch and alarms that are automatically generated when the equipment is accessed.

Based on the staff's review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-11, the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Section 2.5.1 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-11, is resolved and closed.

RG 1.152, Revision 3, describes a method that the NRC considers acceptable to comply with the regulatory criteria to promote high functional reliability, ensure design quality, and establish secure development and operational environments for the use of digital computers in safety-related systems at NPPs. The guidance for secure development and operational environments states that potential vulnerabilities should be addressed in each phase of the digital safety system life cycle. The overall guidance provides the basis for physical and logical access controls to be established throughout the digital system development process to address the susceptibility of a digital safety system to inadvertent access and modification. In RAI 3, Question 07.01 Draft DSRS-9, the staff asked the applicant to describe in the TR how the HIPS platform conforms to regulatory positions 2.1 through 2.5 of RG 1.152. In its response to RAI 3, Question 07.01 Draft DSRS-9, dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that establishing the particular secure development and operational environment provisions for a system using the HIPS platform design is an application-specific activity that depends on the system design and the manufacturer that builds the HIPS platform equipment.

The applicant described the HIPS platform design concepts that ensure a secure operating environment. The HIPS platform contains design features that provide the means to control physical access to PS equipment, including access to test points, and the means for changing setpoints and tunable parameters in the SFMs through the MWS. The typical plant installation would include integral key locks on cabinet door handles to limit access to cabinet internals and logic to initiate an alarm for an unlocked cabinet or any activated or active digital data communication access by a MWS. The MWS supports offline, OOS management (e.g., troubleshooting, calibration, and surveillance testing). Physical and logical controls are put in place to prevent modifications to a safety channel when it is being relied upon to perform a safety function. A temporary cable and an OOS switch are required to be activated before any changes can be made to an SFM. Lastly, the HIPS platform design does not have the capability for remote access to the safety system.

Based on the staff's review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-9, the staff found the applicant's response acceptable because the HIPS platform features to provide control of access are sufficient at the platform-level. The staff also reviewed the markup of TR Section 4.8 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-9, is resolved and closed.

The TR does not address a specific application or establish a definitive safety system design. Additionally, the location of safety-related equipment within the generating station is a plant-specific implementation issue. However, the staff determined the HIPS platform supports meeting Clause 5.9 of IEEE Std. 603-1991. This determination is based on the use described for the HIPS platform and the design features provided by its standardized circuit boards and their instruments chassis. ASAI-31 is necessary to provide additional access features to address the system-level aspects for a safety system using the HIPS platform.

3.6.2.10 Clause 5.10 Repair

Clause 5.10, "Repair," of IEEE Std. 603-1991 requires that safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. DSRS Section 7.2.9 provides acceptance criteria for this requirement.

The TR describes the continuously performed HIPS platform and application diagnostics, which are designed to facilitate timely recognition and identification of malfunctioning equipment. However, the TR does not address a specific application or its application diagnostics. Therefore, the scope of the TR is limited to the troubleshooting and replacement of the standardized circuit boards at the module level only. The TR also describes HIPS module features to remove and reinstall HIPS modules into the chassis without requiring the removal of power, which directly supports timely repair.

The timely identification and location of malfunctioning HIPS modules is facilitated by platform and application-specific features. The majority of HIPS hardware is rack mounted and is replaced rather than repaired, which greatly facilitates timely repair. The HIPS platform has a front plate with specific user interface items (e.g., LEDs, switches) that provides a visual indication of the modules.

Section 3.1 discusses the staff's review of the design features provided by HIPS platform standardized circuit boards and their instrument chassis. Section 3.1.9 addresses the staff's evaluation of the HIPS platform self-diagnostics, test, and calibration capabilities.

These repair capabilities are acceptable for meeting this regulatory requirement at the platform level. This determination is based on the use described for the HIPS platform and the design features provided by its standardized circuit boards. ASAI-32 is necessary to establish full conformance with Clause 5.10 of IEEE Std. 603-1991.

3.6.2.11 Clause 5.11 Identification

Clause 5.11, "Identification," of IEEE Std. 603-1991 requires safety system equipment to be distinctly identified for each redundant portion of the safety system, and this identification must be distinguishable from any other identifying markings placed on the equipment in a manner that does not require frequent use of reference material to identify the equipment and its divisional assignment. DSRS Section 7.2.9 provides acceptance criteria for this requirement.

The coding of cabinets and cabling for a safety system is an application-specific activity. In addition, the particular means for identifying safety equipment according to redundant portions of a safety system (i.e., channels or divisions) is an application-specific activity. However, component identification of the HIPS platform can contribute to the fulfillment of this requirement. The HIPS platform includes faceplate identification of the module type. The HIPS platform also provides physical labels on the PCB of each module to uniquely identify the hardware module and installed firmware.

Although the TR cannot fully address IEEE Std. 603-1991, Clause 5.11, the staff determined the HIPS platform supports meeting IEEE Std. 603-1991, Clause 5.11. This determination is based on the use described for the HIPS platform, the identification features provided by its standardized circuit boards, and the ability for the HIPS platform to accommodate plant-specific labeling requirements. ASAI-33 is necessary to ensure IEEE Std. 603-1991, Clause 5.11, is met.

3.6.2.12 Clause 5.12 Auxiliary Features

Clause 5.12, "Auxiliary Features," of IEEE Std. 603-1991 requires auxiliary supporting features, which are systems or components that provide services (such as cooling, lubrication, and energy supply) needed for the safety systems to accomplish their safety functions, to meet all requirements of the standard. Clause 5.12 of IEEE Std. 603-1991 also requires other auxiliary features that are not required for safety functions but are part of a safety system by association to be designed to meet the criteria necessary to ensure these components, equipment, and systems do not degrade the safety systems below an acceptable level. DSRS Section 7.2.8, "Auxiliary Features," provides acceptance criteria for this requirement.

The TR does not address a specific application or establish a definitive safety system design for the HIPS platform to provide an auxiliary supporting feature or some other auxiliary feature that is part of the safety system by association. Because the TR does not address a specific application or establish a definitive safety system design but its components, equipment, and resultant HIPS-based systems are intended to meet all requirements of IEEE Std. 603-1991, Clause 5.12, a unique requirement may arise for future evaluations of the HIPS platform. Regardless, the determination of whether an application of the HIPS platform is an auxiliary supporting feature or some other auxiliary feature that is part of the safety system by association is a plant-specific activity.

Although the TR cannot fully address IEEE Std. 603-1991, Clause 5.12, the staff determined the HIPS platform supports meeting IEEE Std. 603-1991, Clause 5.12. This determination is based on the use described for the HIPS platform and the evaluation of the platform against all requirements of IEEE Std. 603-1991. ASAI-34 is necessary to ensure Clause 5.12 of IEEE Std. 603-1991 is met, based on the application of a HIPS platform component as an auxiliary supporting feature or some other auxiliary feature that is part of the safety system by association.

3.6.2.13 Clause 5.13 Multi-Unit Stations

Clause 5.13, "Multi-Unit Stations," of IEEE Std. 603-1991 permits the sharing of structures, systems, and components between units at multiunit generating stations, provided that the ability to simultaneously perform safety functions in all units is not impaired. Clause 5.13 of IEEE Std. 603-1991 also contains guidance on the sharing of electrical power between units and the application of the single-failure criterion to shared systems. DSRS Section 7.2.11, "Multi-Unit Stations," provides acceptance criteria for this requirement.

The determination of the multiunit station requirements for a safety system is an application-specific activity. Since the TR does not address a specific application nor include shared systems within its scope, no evaluation against this regulatory requirement could be performed. Therefore, this SE does not address the evaluation against the requirement of Clause 5.13 of IEEE Std. 603-1991. ASAI-35 is necessary to establish full compliance with this regulatory requirement.

3.6.2.14 Clause 5.14 Human Factors Considerations

Clause 5.14, "Human Factors Considerations," of IEEE Std. 603-1991 requires human factors considerations at the initial stages and throughout the design process to ensure that any functions allocated in whole or in part to human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals. DSRS Section 7.2.14, "Human Factors Considerations," contains acceptance criteria for this requirement and states that the safety system human factors design should be consistent with the applicant's/licensee's commitments documented in Chapter 18 of the application.

The determination of human factors considerations is an application-specific activity. Since the TR does not address a specific application nor include human factor requirements within its scope, no evaluation against this regulatory requirement could be performed. Therefore, this SE does not discuss the evaluation against the requirement in Clause 5.14 of IEEE Std. 603-1991. ASAI-36 is necessary to establish full compliance with this regulatory requirement.

3.6.2.15 Clause 5.15 Reliability

Clause 5.15, "Reliability," of IEEE Std. 603-1991 requires the appropriate analysis of system designs to confirm that any established reliability goals, either quantitative or qualitative, have been met. DSRS Section 7.2.3 contains acceptance criteria for this requirement.

The determination of the reliability of a safety system is an application-specific activity that requires an assessment of a full system design. Since the TR does not address a specific application nor include a reliability analysis within its scope, no evaluation against this regulatory requirement could be performed. Therefore, this SE does not discuss the evaluation against the requirement in Clause 5.15 of IEEE Std. 603-1991. ASAI-37 is necessary to establish full compliance with this regulatory requirement.

3.6.3 Clause 6 Sense and Command Features

Clause 6, "Sense and Command Features," of IEEE Std. 603-1991 contains eight clauses that only apply to the sense and command features of safety systems. In addition to the preceding evaluation of the HIPS platform against the requirements in Clause 5 of IEEE Std. 603-1991, the staff evaluated the HIPS platform against the requirements of Clause 6. Sense and command features are the electrical and mechanical components and interconnections involved in generating those signals associated directly or indirectly with the safety functions. The scope of the sense and command features extends from the measured process variables to the execute features input terminals, thereby including the actuation device for the actuated equipment. The evaluations below against the requirements of Clause 6 of IEEE Std. 603-1991 are limited to the capabilities and characteristics of the HIPS platform relevant to meeting each requirement.

3.6.3.1 Clause 6.1 Automatic Control

Clause 6.1, "Automatic Control," of IEEE Std. 603-1991 requires that, for each DBE, all protective actions automatically initiate without operator action, except as justified in Clause 4.5 of IEEE Std. 603-1991. DSRS Section 7.2.12, "Automatic and Manual Control," contains acceptance criteria for this requirement.

The TR does not address a specific application or establish a definitive safety system, which is necessary to define the extent that setpoints, margins, errors, and response times are factored into a plant's safety analysis or associated with IEEE Std. 603-1991, Clause 4.5. In accordance with DSRS Section 7.2.12, the applicant's or licensee's analyses should confirm that the I&C safety system has been designed to demonstrate that performance specifications are met.

Section 3.1 discusses the staff's evaluation of the design features provided by HIPS platform standardized circuit boards and their instrument chassis. Section 3.5 addresses the staff's review of the HIPS platform's response time characteristics. Section 3.1.9 discusses the staff's review of self-diagnostics and test and calibration capabilities provided by the HIPS platform.

Section 3.4 addresses the staff's review of the approaches to build diversity into a HIPS-based system.

Although the TR cannot fully address Clause 6.1 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 6.1 of IEEE Std. 603-1991. This determination is based on the platform design features, deterministic behavior, built-in diversity, and adequate closure of the associated plant-specific action items. Nevertheless, an ASAI item is necessary when the HIPS platform provides safety system sense and command features that include automatic control. Compliance with ASAI-38 will give reasonable assurance that Clause 6.1 is met, and this action should include applicant or licensee analyses to confirm that the safety system has been qualified to demonstrate that specified performance requirements have been met.

3.6.3.2 Clause 6.2 Manual Control

Clause 6.2, "Manual Control," of IEEE Std. 603-1991 contains three subclauses related to the availability of manual controls in the control room. Clause 6.2.1 requires that the control room provide a means to manually initiate protective actions at the division level of automatically initiated protective actions, such that the number of discrete operator manipulations and operated equipment is minimized while the independence between redundant portions of a safety system per IEEE Std. 603-1991, Clause 5.6.1, is preserved. Clause 6.2.2 requires that the control room provide a means to manually initiate the protective actions that were not selected for automatic control, along with the associated information displays. Clause 6.2.3 requires that the control room provide a means to perform manual actions necessary to maintain safe conditions after the protective actions are completed, along with the associated information displays in sufficient quantities and locations to support surveillance and action by the number of available qualified operators. DSRs Section 7.2.12, "Automatic and Manual Control," provides acceptance criteria for this requirement.

The TR does not address a specific application, establish a definitive safety system, or locate manual controls and displays within a plant-specific control room. The TR scope also excludes information displays. However, the HIPS platform design features support the implementation of manual controls and connectivity to information displays.

The RTS and ESFAS provide manual trip capability. Manual switches in the main control room allow the operator to manually initiate a reactor trip if prescribed by procedure, along with operational bypass switches and an enable nonsafety switch. In addition, manual switches in the main control room consist of manual actuation switches for each automatic ESF function, along with operational bypass switches, reset switch, and an enable nonsafety switch. These manual switches are connected to the HWM in the RTS and ESFAS chassis, which isolates and connects these signals to the backplane, making them available to the SVMs and EIMs.

Section 3.1 discusses the staff's review of the design features provided by HIPS platform standardized circuit boards and their instrument chassis. Section 3.1.9 addresses the staff's

review of self-diagnostics and test and calibration capabilities provided by the HIPS platform. Section 3.4 discusses the staff's review of the approaches to build diversity into a HIPS-based system. Section 3.5 addresses the staff's review of the HIPS platform's response time characteristics.

Although the TR cannot fully address Clause 6.2 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 6.2 of IEEE Std. 603-1991. This determination is based on the deterministic behavior, built-in diversity feature, and platform design features. Nevertheless, an ASAI item is necessary when the HIPS platform provides safety system sense and command features that include automatic control. Compliance with ASAI-39 will give reasonable assurance that Clause 6.2 is met, and this action should include applicant or licensee analyses to confirm that the safety system has been qualified to demonstrate that specified performance requirements have been met.

3.6.3.3 Clause 6.3 Interaction with Other Systems

Clause 6.3 of IEEE Std. 603-1991 contains two subclauses related to the D3 of protective actions. Clause 6.3.1 of IEEE Std. 603-1991 contains a requirement to mitigate the consequences of a credible event (and its direct and indirect consequences) that is an initiator of a nonsafety system action resulting in a condition requiring protective action while concurrently preventing the protective actions from being performed by the channels designated as providing the principal protection against the resulting condition. The clause specifies two alternatives to fulfill the requirement. The first alternative is for channels not subject to failure from the same single credible event to be provided to limit the consequences of this event to a value specified by the design basis, using either one or a combination of both of the following options: (1) provide alternate channels that sense a set of different variables from the principal channels, or (2) provide alternate channels that use equipment different from that of the principal channel to sense the same variable. The second alternative is to provide equipment not subject to failure from the same single credible event to detect the event and limit the consequences to a value specified by the design basis, where this equipment is not considered a part of the safety system. Clause 6.3.2 of IEEE Std. 603-1991 requires three provisions that will allow Clause 6.3.1 to continue to be met during the maintenance bypass of a channel. These provisions are (1) reducing the required coincidence, (2) defeating the nonsafety system signals taken from the redundant channels, or (3) initiating a protective action from the bypassed channel. DSRS Section 7.2.10, "Interaction between Sense and Command Features and Other Systems," provides acceptance criteria for this requirement.

The TR states that the HIPS platform has the capability to be configured in a manner that meets IEEE Std. 603-1991, Clause 6.3. However, the TR does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events, along with their direct and indirect consequences. As such, the TR also states that conformance to IEEE Std. 603-1991, Clause 6.3, will be addressed during a plant-specific or application-specific implementation.

Within the first alternative provided in Clause 6.3.1, the specified differences between the alternate channels and the principal channels correspond to diversity attributes discussed in Section 3.4 of this SE. The second alternative would provide an automatic diverse backup system, as discussed in DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues," (see Ref. 6.1-23). Section 3.4 addresses the staff's evaluation of the approaches to build diversity into a HIPS-based system. Section 3.1 discusses the staff's evaluation of the design features provided by HIPS platform standardized circuit boards and their instrument chassis.

Although the TR cannot fully address IEEE Std. 603-1991, Clause 6.3, the staff determined that the HIPS platform supports meeting IEEE Std. 603-1991, Clause 6.3, by implementing either principal channels, alternate channels, or a diverse backup system. This determination is based on the built-in diversity options, platform design features to implement coincidence logic, and maintenance features to either bypass or trip channels. Nevertheless, an ASAI is necessary when the HIPS platform provides sense and command features for the principal protection against the resulting condition of a nonsafety system action that has been caused by a single credible event, including its direct and indirect consequences. Compliance with ASAI-40 will provide reasonable assurance that Clause 6.3 is met and also address DI&C-ISG-02.

3.6.3.4 Clause 6.4 Derivation of System Inputs

Clause 6.4, "Derivation of System Inputs," of IEEE Std. 603-1991 requires, to the extent practical, that sense and command feature inputs be derived from signals that are direct measures of the desired variables, as specified in the design basis. DSRs Section 7.2.6, "Derivation of System Inputs," contains acceptance criteria for this requirement.

The TR states the applicability of this clause will be evaluated on a plant-specific basis, because it applies as a system-level and application-specific requirement. As described in the TR, the manufacturer has indicated the HIPS platform directly supports a plant's existing methods for direct measurement of the desired variables, as specified in the plant's design basis, so no changes to plant transmitters or sensors will be required.

Although the TR cannot fully address Clause 6.4 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 6.4 of IEEE Std. 603-1991. This determination is based on the platform design features to acquire and condition field sensor measurements of the required variables. ASAI-41 is necessary when the HIPS platform equipment is used to acquire and condition field sensor measurements of the required variables.

3.6.3.5 Clause 6.5 Capability for Testing and Calibration

Clause 6.5 of IEEE Std. 603-1991 contains two subclauses related to ensuring the availability of sense and command feature input sensors. Clause 6.5.1 requires the means to check, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. Clause 6.5.2 requires the means

to ensure operational availability of each sense and command feature input sensor required during the post-accident period. DSRS Section 7.2.15 provides acceptance criteria for this requirement.

As described in the TR, the HIPS platform directly supports a plant's existing methods to perform cross-checking between redundant safety system channel sensors or between sensor channels that bear a known relationship to each other. Section 3.1 addresses the staff's review of the design features provided by HIPS platform standardized circuit boards. Section 3.1.9 discusses the NRC staff's evaluation of the calibration, testing, and diagnostics from the inputs at the SFM to the output of the EIM.

Although the TR cannot fully address Clause 6.5 of IEEE Std. 603-1991, the NRC staff determined that the HIPS platform supports meeting Clause 6.5 of IEEE Std. 603-1991. This determination is based on the following factors:

- Platform design features support implementation of application-specific diagnostic logic and confirmation of continued execution using the MWS.
- The classification of the hardware and FPGA logic performing diagnostic functions, as part of the tested system, are equivalent to the classification of safety function hardware and FPGA logic.
- The proposed instrumentation architecture supports meeting channel independence, system integrity, the single-failure criterion, and use of the MWS during test and calibration activities.

ASAI-24, ASAI-25, and ASAI-26 are necessary to establish full compliance with this regulatory requirement.

3.6.3.6 Clause 6.6 Operating Bypasses

Clause 6.6, "Operating Bypasses," of IEEE Std. 603-1991 requires a safety system either to (1) automatically prevent the activation of an operating bypass whenever the applicable permissive conditions are not met, or (2) when the permissive conditions are not met, initiate the appropriate safety function(s) to be bypassed. This clause further requires the safety system to take one of three actions whenever the conditions change so the permissive conditions are no longer met after an operating bypass had been established: (1) remove the appropriate operating bypass(es), (2) restore plant conditions so the permissive conditions once again exist, or (3) initiate the appropriate safety function(s). DSRS Section 7.2.4 contains acceptance criteria for this requirement.

As described in the TR, the manufacturer has indicated that the HIPS platform directly supports implementation of operating bypasses within the application-specific logic of the HIPS platform. Operational bypasses are connected through an HWM for the RTS and an HWM for the

ESFAS. These signals are isolated and placed on the backplane for each chassis and made available to the SVMs, MIB-CM, and EIMs. Each module processes these signals from the manual switches, as defined by the safety function algorithm. Finally, the manufacturer has indicated that the application-specific logic for the operating bypass will meet IEEE Std. 603-1991, Clause 6.6.

Section 3.1 addresses the staff's evaluation of the design features provided by HIPS platform standardized circuit boards. Section 3.1.9 discusses the staff's review of self-diagnostics and test and calibration capabilities provided by the HIPS platform. Section 3.5 contains the staff's review of HIPS platform response time characteristics.

Although the TR cannot fully address Clause 6.6 of IEEE Std. 603-1991, the NRC staff determined that the HIPS platform supports meeting Clause 6.6 of IEEE Std. 603-1991. This determination is based on the platform design features to implement application-specific logic. ASAI-42 is necessary to establish full compliance with this regulatory requirement.

3.6.3.7 Clause 6.7 Maintenance Bypass

Clause 6.7 of IEEE Std. 603-1991 requires a safety system to retain its ability to accomplish its safety function while sense and command features equipment is in maintenance bypass, and during the maintenance bypass, to continue to meet both the single-failure criterion of Clause 5.1 and the D3 of the protective actions of Clause 6.3. An exception to continuing to meet Clauses 5.1 and 6.3 is provided for one-out-of-two portions of the sense and command features when one portion is rendered inoperable, provided that acceptable reliability of equipment operation has been demonstrated to show that the removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on the availability of overall sense and command features. DSRS Section 7.2.4 contains acceptance criteria for this requirement.

As described in the TR, the manufacturer has indicated that the HIPS platform directly supports implementation of maintenance bypasses within the application-specific logic of the HIPS platform. In addition, the TR states that the HIPS platform directly supports implementation of maintenance bypasses in accordance with plant technical specifications.

Section 3.1 addresses the staff's evaluation of the design features provided by HIPS platform standardized circuit boards. Section 3.1.4.1.3 discusses the staff's evaluation of the maintenance bypass capabilities. Section 3.1.9 contains the staff's evaluation of the self-diagnostics and test and calibration capabilities.

Although the TR cannot fully address Clause 6.7 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 6.7 of IEEE Std. 603-1991. This determination is based on the platform design features to implement multiple redundant safety channels/divisions while maintaining independence between them and the ability to perform a maintenance bypass on an individual safety channel/division. Evaluation of this clause requires

the review of plant and application-specific technical specification content. The staff also agrees with the applicant that evaluation of this clause is application specific. As such, no broader staff determination is appropriate for the HIPS platform to address Clause 6.7 of IEEE Std. 603-1991. ASAI-43 is necessary to establish full compliance with this regulatory requirement.

3.6.3.8 Clause 6.8 Setpoints

Clause 6.8, "Setpoints," of IEEE Std. 603-1991 contains two subclauses related to the determination of sense and command feature setpoints. Clause 6.8.1 requires the allowance for uncertainties between a plant's process analytical limit, which is documented in its design basis per Clause 4.4, and a safety system device's setpoint to be determined using a documented methodology. Clause 6.8.2 requires the design to provide a positive means of ensuring that the more restrictive setpoint is used when it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions. Clause 6.8.2 additionally requires that devices to prevent improper use of less restrictive setpoints be part of the sense and command features of the safety system. DSRS Section 7.2.7, "Setpoints," contains acceptance criteria for this requirement.

Determination of the setpoints used for a safety system is an application-specific activity that requires an assessment of a full system design. Since the TR does not address a specific application nor include setpoints, setpoint methodologies, or HIPS platform module accuracies within its scope, no evaluation against this regulatory requirement could be performed. Therefore, this SE does not address the evaluation against the requirement of Clause 6.8 of IEEE Std. 603-1991. ASAI-44 is necessary to establish full compliance with this regulatory requirement.

3.6.4 Clause 7 Execute Features

Clause 7, "Execute Features," of IEEE Std. 603-1991 contains five subclauses that only apply to execute features of safety systems. In addition to the preceding evaluation of the HIPS platform against the requirements in Clause 5 of IEEE Std. 603-1991, the staff evaluated the HIPS platform against the requirements of Clause 7. Execute features are the electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling. The following evaluations against the requirements of IEEE Std. 603-1991, Clause 7, are limited.

3.6.4.1 Clause 7.1 Automatic Control

Clause 7.1, "Automatic Control," of IEEE Std. 603-1991 requires the capability to receive and act upon automatic control signals from sense and command features consistent with Clause 4.4 of the design basis. DSRS Section 7.2.12, "Automatic and Manual Control," provides acceptance criteria for this requirement.

Although the TR cannot fully address Clause 7.1 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 7.1 of IEEE Std. 603-1991. This determination is based on the staff evaluation identified in Section 3.6.3.1 of this SE, which is sufficient, based on the following three points: (1) the provisions of IEEE Std. 603-1991, Clause 7.1, which is applicable to the execute features, do not materially differ from those identified as general requirements or applicable to the sense and command features of IEEE Std. 603-1991, Clause 6.1, (2) the associated design features and capabilities of the HIPS platform do not change, based on their use to fulfill the role of either sense and command features or execute features, and (3) conformance to IEEE Std. 603-1991, Clause 7.1, requires ASAI-38 to establish full compliance with this regulatory requirement.

3.6.4.2 Clause 7.2 Manual Control

Clause 7.2, "Manual Control," of IEEE Std. 603-1991 requires that any inclusion of manual control within an actuated component in the execute features shall not defeat the requirements of Clauses 5.1 and 6.2. Clause 7.2 also requires the capability to receive and act upon manual control signals from sense and command features consistent with the design basis. DSRS Section 7.2.12 contains acceptance criteria for this requirement.

Although the TR cannot fully address Clause 7.2 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 7.2 of IEEE Std. 603-1991. This determination is based on the staff evaluation identified in Section 3.6.3.2 of this SE, which is sufficient based on the following three points: (1) the provisions of IEEE Std. 603-1991, Clause 7.2, which is applicable to the execute features, do not materially differ from those identified as general requirements or applicable to the sense and command features of IEEE Std. 603-1991, Clause 6.2, (2) the associated design features and capabilities of the HIPS platform do not change based on their use to fulfill the role of either sense and command features or execute features, and (3) conformance to IEEE Std. 603-1991, Clause 7.2, requires ASAI-39 to establish full compliance with this regulatory requirement.

3.6.4.3 Clause 7.3 Completion of a Protective Action

Clause 7.3, "Completion of a Protective Action," of IEEE Std. 603-1991 requires the design of execute features to ensure that a protective action, once initiated, follows through to completion. However, this does not preclude the use of equipment protective devices identified in Clause 4.11 or provisions for deliberate operator interventions. Also this clause requires a separate, deliberate operator action to return execute features to normal and precludes the reset of the sense and command features to automatically return execute features to normal. DSRS Section 7.2.3 provides acceptance criteria for this requirement.

Although the TR cannot fully address Clause 7.3 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 7.3 of IEEE Std. 603-1991. This determination is based on the staff evaluation identified in Section 3.6.2.2 of this SE, which is sufficient based

on the following three points: (1) the provisions of IEEE Std. 603-1991, Clause 7.3, which is applicable to the execute features, do not materially differ from those identified as general requirements or applicable to the sense and command features of IEEE Std. 603-1991, Clause 5.2, (2) the associated design features and capabilities of the HIPS platform do not change based on their use to fulfill the role of either sense and command features or execute features, and (3) conformance to IEEE Std. 603-1991, Clause 7.3, requires ASAI-15 to establish full compliance with this regulatory requirement.

3.6.4.4 Clause 7.4 Operating Bypass

Clause 7.4, "Operating Bypass," of IEEE Std. 603-1991 requires any operating bypass of execute features to comply with requirements identical to the provisions for the sense and command features. DSRS Section 7.2.4 contains the acceptance criteria for this requirement.

Although the TR cannot fully address Clause 7.4 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 7.4 of IEEE Std. 603-1991. This determination is based on the staff evaluation identified in Section 3.6.3.6 of this SE, which is sufficient based on the following three points: (1) the provisions of IEEE Std. 603-1991, Clause 7.4, which is applicable to the execute features, do not materially differ from those identified as general requirements or applicable to the sense and command features of IEEE Std. 603-1991, Clause 6.6, (2) the associated design features and capabilities of the HIPS platform do not change based on their use to fulfill the role of either sense and command features or execute features, and (3) conformance to IEEE Std. 603-1991, Clause 7.4, requires ASAI-42 to establish full compliance with this regulatory requirement.

3.6.4.5 Clause 7.5 Maintenance Bypass

Clause 7.5 of IEEE Std. 603-1991 requires any maintenance bypass of execute features to comply with requirements similar to the provisions for the sense and command features. DSRS Section 7.2.4 contains the acceptance criteria for this requirement.

Although the TR cannot fully address Clause 7.5 of IEEE Std. 603-1991, the staff determined that the HIPS platform supports meeting Clause 7.4 of IEEE Std. 603-1991. This determination is based on the staff evaluation identified in Section 3.6.3.7 of this SE, which is sufficient based on the following three points: (1) the provisions of IEEE Std. 603-1991, Clause 7.5, which is applicable to the execute features, do not materially differ from those identified as general requirements or applicable to the sense and command features of IEEE Std. 603-1991, Clause 6.7, (2) the associated design features and capabilities of the HIPS platform do not change based on their use to fulfill the role of either sense and command features or execute features, and (3) conformance to IEEE Std. 603-1991, Clause 7.5, requires ASAI-45 to establish full compliance with this regulatory requirement.

3.6.5 Clause 8 Power Source

Clause 8, "Power Source," of IEEE Std. 603-1991 contains three clauses related to power sources for safety systems. Clause 8 of IEEE Std. 603-1991 states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems, and that specific criteria unique to the Class 1E power systems can be found in IEEE Std. 308-1980, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations," (see Ref. 6.1-24). This clause also states that, for power systems with a degree of redundancy, the safety functions and acceptable reliability must be retained while power sources are in maintenance bypass. DSRS Chapter 7, Table 7.1, "Instrumentation and Control—Mapping of Regulatory Requirements, Guidance and DSRS Acceptance Criteria," does not provide acceptance criteria for IEEE Std. 603-1991, Clause 8.

The determination of the power sources to be provided to a safety system is an application-specific activity. Since the TR does not address a specific application of the platform, the evaluation against this regulatory requirement is limited to the capabilities and characteristics of the HIPS platform that are relevant for adherence to Clause 8 and its subclauses.

Clauses 8.1, "Electrical Power Sources," and 8.2, "Non-electrical Power Sources," address requirements for electrical power sources and nonelectrical power sources, respectively. The HIPS platform only uses electrical power, and the platform scope does not include the dc power source(s), which is application specific. Thus, no evaluation of the HIPS platform against these regulatory requirements could be performed.

Clause 8.3, "Maintenance Bypass," addresses the capability of the safety system to accommodate maintenance bypass of redundant power sources. The HIPS platform is designed to accept a redundant pair of dc power feeds to its internal circuits. The redundant power, driven by separate power sources, is supplied to the platform modules through separate power traces along the HIPS chassis backplane. Thus, the platform provides suitable capability to enable the safety system to function while one redundant dc power source is failed or in bypass.

The determination of the power sources used for a safety system is an application-specific activity that requires an assessment of a full system design. Since the TR does not address specific application power sources within its scope, no evaluation against this regulatory requirement could be performed. Therefore, this SE does not address the evaluation against the requirement of Clause 7.4 of IEEE Std. 603-1991. ASAI-46 is necessary to establish full compliance with this regulatory requirement.

3.7 Review of IEEE Std. 7-4.3.2 Requirements

Equipment based on HIPS platform components is intended for use in safety systems and other safety-related applications. Therefore, the staff evaluated the TR on its ability to support the application-specific system provisions of IEEE Std. 7-4.3.2-2003. RG 1.152 states that conformance with the requirements of IEEE Std. 7-4.3.2-2003 is a method that the staff has deemed acceptable for meeting the Commission's regulations with respect to high functional reliability and design requirements for computers used in safety systems of NPPs.

With the consideration that the TR scope does not propose to meet all clauses of IEEE Std. 7-4.3.2-2003 through its components—similar to the clauses IEEE Std. 603-1991—the staff's evaluation of each clause has a limited scope that does not provide an SE of the HIPS platform against the full clause. With the additional consideration that not all provisions of the microprocessor-based software standard are directly applicable to an FPGA-based platform, the subsections below necessarily tailor the applicability of each of the IEEE Std. 7-4.3.2-2003 clauses.

Appendix B to the TR summarizes the regulatory compliance of the HIPS platform with IEEE Std. 7-4.3.2-2003. However, it was not clear to the staff how the HIPS design specifications conform to the RG 1.152 and the endorsed IEEE Std. 7-4.3.2-2003. Therefore, in RAI 3, Question 07.01 Draft DSRS-16, the staff asked the applicant to explain the basis for its claims; specifically, conformance to RG 1.152, and compliance with the associated clauses in IEEE Std. 7-4.3.2-2003. In its response to RAI 3, Question 07.01 Draft DSRS-16, dated August 19, 2016 (see Ref. 6.1-20), the applicant revised Appendix B to add the application-specific information and make other conforming changes based on the RAI responses. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-16 (see Sections 3.7.1 to 3.7.4), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Appendix B provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-16, is resolved and closed.

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

3.7.1 Clause 5 Safety System Criteria

Clause 5, "Safety System Criteria," of IEEE Std. 7-4.3.2-2003 contains 15 clauses that apply to all safety system functions and features. Some of the clauses in Clause 5 of IEEE Std. 603-1991 are supplemented by IEEE Std. 7-4.3.2-2003 to address technology-specific issues related to the use of digital computers in safety systems. The evaluations below against IEEE Std. 7-4.3.2-2003, Clause 5, are limited to capabilities and characteristics of the HIPS platform relevant to meet each requirement.

3.7.1.1 Clause 5.1 Single-Failure Criteria

Clause 5.1, "Single-Failure Criteria," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.1 of IEEE Std. 603-1991 are necessary.

The TR states that Clause 5.1 of IEEE 7-4.3.2-2003 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.1 of IEEE Std. 7-4.3.2-2003.

3.7.1.2 Clause 5.2 Competition of a Protective Action

Clause 5.2, "Competition of a Protective Action," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.2 of IEEE Std. 603-1991 are necessary.

The TR states that Clause 5.2 of IEEE Std. 7-4.3.2-2003 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.2 of IEEE Std. 7-4.3.2-2003.

3.7.1.3 Clause 5.3 Quality

Clause 5.3 of IEEE Std. 7-4.3.2-2003 states that hardware quality is addressed in IEEE Std. 603-1991 and software quality is addressed in IEEE/Electronics Industry Association Standard 12207.0-1996, "Standard for Information Technology—Software Life Cycle Processes," (see Ref. 6.1-25) and supporting standards. Clause 5.3 further requires that the digital computer development process include the development activities for both computer hardware and software, the integration of the hardware and software, and the integration of the computer with the safety system.

Clause 5.3 includes six subclauses to identify activities beyond the requirements of IEEE Std. 603-1991 necessary to meet the quality criteria for a digital computer-based system, including its software. Each subclause under Clause 5.3 addresses one of these six activities:

- Clause 5.3.1 software development
- Clause 5.3.2 software tools
- Clause 5.3.3 verification and validation (V&V)
- Clause 5.3.4 independent V&V requirements
- Clause 5.3.5 software configuration management
- Clause 5.3.6 software project risk management

The determination and documentation of the software QA plan for a safety system is an application-specific activity dependent on the equipment vendor to be used to implement the HIPS system. Since the TR does not address a specific application of the platform, the software QA plan for a safety system is not available for review, and no evaluation of the HIPS platform against these regulatory requirements could be performed. Therefore, the staff did not evaluate the HIPS platform against the regulatory requirements of Clause 5.3. ASAI-16 is necessary to establish full compliance with this regulatory requirement.

3.7.1.4 Clause 5.4 Equipment Qualification

Clause 5.4, "Equipment Qualification," of IEEE Std. 7-4.3.2-2003 contains two subclauses necessary to qualify digital computers for use in safety systems. These subclauses identify activities beyond the requirements of IEEE Std. 603-1991 necessary to meet quality criteria for a digital computer-based system, including its software.

Clause 5.4.1, "Computer System Testing," of IEEE Std. 7-4.3.2-2003 requires computer system qualification testing to be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. Clause 5.4.1 also requires all portions of the computer necessary to accomplish safety functions, or those portions where the operation or failure could impair safety functions, to be exercised during testing. This testing is required to demonstrate that performance requirements related to safety functions have been met.

Clause 5.4.2, "Qualification of Existing Commercial Computers," of IEEE Std. 7-4.3.2-2003 requires the qualification process for existing commercial computers to be accomplished by evaluating the hardware and software design using the criteria of this standard. Clause 5.4.2 also requires the acceptance to be based on evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions where the acceptance and its basis shall be documented and maintained with the qualification documentation. Clause 5.4.2 and its several subclauses then describe the commercial grade dedication process and specify requirements for that process.

For each of these clauses, the TR states that the associated requirements apply on an application-specific basis. The EQ program is an application-specific activity dependent on the equipment vendor to be used to implement the HIPS system. Since the TR does not address a specific application of the platform, the EQ program is not available for review and no evaluation of the HIPS platform against this regulatory requirement could be performed. As such, the staff

agrees that no review of the HIPS platform against Clause 5.4 of IEEE Std. 7-4.3.2-2003 is necessary. ASAI-17 is necessary to establish full compliance with this regulatory requirement.

3.7.1.5 Clause 5.5 System Integrity

Clause 5.5, "System Integrity," of IEEE Std. 7-4.3.2-2003 contains three subclauses necessary to achieve system integrity in digital equipment for use in safety systems. These subclauses are in addition to the system integrity criteria provided in IEEE Std. 603-1991.

3.7.1.5.1 Clause 5.5.1 Design for Computer Integrity

Clause 5.5.1, "Design for Computer Integrity," of IEEE Std. 7-4.3.2-2003 requires the computer to be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. Clause 5.5.1 further requires the ability to place the safety system in its preferred failure mode in the presence of a computer failure. Lastly, Clause 5.5.1 requires the retention of the safety system's ability to perform its safety functions when a computer system restart operation occurs.

The manufacturer designed the HIPS platform to handle anticipated external and internal conditions, and the HIPS platform contains design features and capabilities to ensure a safety system maintains full integrity when subjected to these conditions. The manufacturer described the operating modes and states and the classification of failures for the HIPS platform. The manufacturer also described digital communication design that contains provisions to address conditions with the potential to defeat a safety function. The staff reviewed these descriptions along with supporting requirement and specification documents.

Unlike microprocessor-based computer systems, to which Clause 5.5.1 of IEEE Std. 7-4.3.2-2003 typically applies, the HIPS platform does not contain general use computer hardware. The HIPS platform restart operation occurs much faster than a microprocessor-based computing system because the HIPS platform FPGA logic does not load an operating system, software drivers for peripheral devices, or an executable software program. Additionally, the HIPS platform FPGA logic self-diagnostics that run on restart complete much faster than a typical microprocessor-based computer's startup diagnostics.

Although the HIPS platform scope does not provide a specific safety system with a preferred failure mode, the staff determined that the HIPS platform includes design features to establish a preferred failure mode through plant-specific configuration data and in response to established internal and external conditions. The HIPS platform contains provisions to enter a fail-safe state defined by the plant-specific configuration and to force a channel's output to a defined state using the OOS switch. During the audit conducted from July 6, 2016, through July 7, 2016 (see Ref. 6.1-4), the NRC reviewed these descriptions, along with supporting requirement and specification documents. The HIPS platform also supports plant-specific safety system configurations that provide redundancy, so no single failure has the potential to defeat the safety function. The HIPS platform scope excludes use of a multidivisional workstation and contains

provisions to ensure that no nonsafety equipment can provide data to a safety channel unless the channel indicates it is in an inoperable state (e.g., indicating failure, in bypass, undergoing calibration). Additionally, plant-specific programming of the HIPS platform allows the further establishment of conditions for entry into a fail-safe state that is conservative with respect to a system's safety function.

The HIPS platform provides redundant signal paths in the SFM FPGA, triple modular redundant communication paths, redundant EIM outputs, and redundant power supplies.

Section 3.3 describes the staff's evaluation of the redundant features of the HIPS. The use of redundancy provides fault-tolerant capabilities which, coupled with diagnostics and self-testing, as discussed in Section 3.1.9 of this SE, can facilitate a high level of computer integrity.

In RAI 3, Question 07.01 Draft DSRS-12, the staff asked the applicant to describe the functionality of the NVM and how the integrity of memory is maintained during all postulated conditions for the different types of FPGAs. In its response to RAI 3, Question 07.01 Draft DSRS-12, dated August 19, 2016 (see Ref. 6.1-20), the applicant described the BIST that is used in an SRAM-based FPGA for checking the functionality of the NVM and the FPGAs included on each module.

The OTP or flash-based FPGA is a fixed configuration and does not function like the SRAM FPGA; therefore, this type of testing is not applicable for the OTP or flash-based FPGA. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-12, the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Sections 4.2 and 8.2.6 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-12, is resolved and closed.

Based on its determinations and confirmations in this section, the staff concludes that the HIPS platform system supports the construction of a safety system to meet the criteria of IEEE Std. 7-4.3.2-2003, Clause 5.5.1, because the HIPS platform contains design features and capabilities to ensure a safety system can maintain its full integrity when subjected to conditions that have significant potential for defeating the safety functions. ASAI-18 and ASAI-19 are necessary to establish full compliance with this regulatory requirement.

3.7.1.5.2 Clause 5.5.2 Design for Test and Calibration

With the exclusion of an appropriate bypass of one redundant channel being in place, Clause 5.5.2, "Design for Test and Calibration," of IEEE Std. 7-4.3.2-2003 prohibits test and calibration functions from creating any adverse effect on the ability of the computer to perform its safety function. Clause 5.5.2 also requires verification that test and calibration functions do not affect computer functions that were not included in a calibration change. When sole

verification of test and calibration data is provided on a separate computer, Clause 5.5.2 requires V&V, configuration management, and QA for test and calibration functions of the separate computer. Likewise, Clause 5.5.2 requires V&V, configuration management, and QA when the test and calibration function is built into the safety system computer. In other words, the only case where V&V, configuration management, and QA for test and calibration functions would not be required would be when these functions reside on a separate computer and do not provide the sole verification of test and calibration data for the safety system computer.

The determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements that apply. Establishment of the types of surveillance necessary for the safety system to ensure that the identifiable single failures only announced through testing are detected is an application-specific activity. Since the TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to considering the means within the platform to enable testing and calibration of an implemented system.

The HIPS platform scope does not include a separate computer to verify test and calibration data. Additionally, the HIPS platform scope does not establish whether a licensee might solely rely on a separate computer to verify test and calibration data for a future HIPS-based safety system. Therefore, this SE excludes these aspects of Clause 5.5.2 of IEEE Std. 7-4.3.2-2003.

The HIPS platform incorporates test and calibration features to provide a means to bypass channels during surveillance testing, setpoint changes, and calibration. Furthermore, the HIPS platform allows the MWS to access configuration data, which include setpoint and calibration data, when a channel is bypassed. The manufacturer designed these test and calibration functions so the functions do not impede the safety functions of a system. Section 3.1.9 addresses the staff's evaluation of the self-diagnostics and test and calibration capabilities.

Unlike microprocessor-based computer systems, to which Clause 5.5.2 of IEEE Std. 7-4.3.2-2003 typically applies, the HIPS platform does not contain executable software that uses shared processing resources (e.g., processor, processing registers, cache memory). Instead, an SFM performs individual functions supported through distinct FPGA logic, and each individual function does not share its FPGA logic resources with other functions. Within the HIPS platform, test and calibration function logic neither uses the safety data buses nor competes with safety function logic for FPGA logic resources.

The staff determined that the HIPS platform testing and calibration will not impede the safety function of a HIPS-based safety system, because the self-diagnostic functions do not compete with safety functions for the safety signal path or FPGA programming resources, and the platform provides features to limit test and calibration functions to bypassed or inoperable channels. The staff confirmed that the manufacturer included specifications for test and calibration functions (see Ref. 6.1-4). Based on these NRC staff determinations, the HIPS platform is suitable to satisfy IEEE Std. 7-4.3.2-2003, Clause 5.5.2. ASAI-47 and ASAI-48 are necessary to establish full compliance with this regulatory requirement.

3.7.1.5.3 Clause 5.5.3 Fault Detection and Self-Diagnostics

Clause 5.5.3, "Fault Detection and Self-Diagnostics," of IEEE Std. 7-4.3.2-2003 provides reliability requirements for a safety system to determine the need and scope of self-diagnostics. Clause 5.5.3 does not require self-diagnostics for systems in which failures can be detected by alternative means in a timely manner. When self-diagnostics are built into the safety system, then Clause 5.5.3 requires these functions to be subject to the same V&V processes as the safety system functions. If reliability requirements warrant self-diagnostics, then Clause 5.5.3 requires computer programs to incorporate functions to detect and report computer system faults and failures in a timely manner. Clause 5.5.3 also prohibits self-diagnostic functions from adversely affecting the ability of the computer system to perform its safety function, or from causing spurious actuations of the safety function. Lastly, whenever self-diagnostics are applied, Clause 5.5.3 requires that the system design address (1) self-diagnostics performed during system startup, (2) self-diagnostics performed periodically while the computer system is operating, and (3) failure reporting of the self-diagnostic results.

The HIPS platform incorporates self-diagnostic features to provide a means to detect and alert any failure within the HIPS platform. For each standardized circuit board, these self-diagnostic features are discussed in the specifications for that board. These specifications include startup tests, periodic tests, and reporting of test results. The manufacturer designed these self-diagnostics to not impede the safety functions of a system. Section 3.1.9 addresses the staff's evaluation of the self-diagnostics and test and calibration capabilities.

Unlike microprocessor-based computer systems, to which Clause 5.5.3 of IEEE Std. 7-4.3.2-2003 typically applies, the HIPS platform does not contain executable software that uses shared processing resources (e.g., processor, processing registers, cache memory). Instead, a HIPS platform SFM performs individual functions supported through distinct FPGA logic, and each individual function does not share its FPGA logic resources with other functions. Within the HIPS platform, self-diagnostic function logic does not compete with safety function logic for FPGA logic resources.

The HIPS platform incorporates self-diagnostic functions at powerup and periodically, along with failure result reporting capabilities. However, an applicant or licensee referencing this SE must confirm that the manufacturer followed the same design, development, and iV&V processes for self-diagnostics functions as for all other HIPS platform functions. This will ensure that the manufacturer's processes incorporate requirements and specifications and iV&V processes for self-diagnostic functions. This is ASAI-49.

The EQ program is an application-specific activity dependent on the equipment vendor to be used to implement the HIPS system. However, an applicant or licensee referencing this SE must verify that the manufacturer included the self-diagnostic functions within its type testing of the HIPS platform standardized circuit boards during EQ. The EQ will demonstrate the

continued operability of the HIPS platform's safety functions and safety signal path while the self-diagnostics are operable. This is ASAI-50.

The HIPS platform includes self-test coverage of all critical platform functions. However, an applicant or licensee referencing this SE must demonstrate that the combination of HIPS platform self-tests and system surveillance testing provide the necessary test coverage to ensure that there are no undetectable failures that could adversely affect a required safety function. This is ASAI-51.

The staff determined that the HIPS platform self-diagnostics will not impede the safety function of the system, because the self-diagnostic functions do not compete with safety functions for FPGA programming resources. The staff confirmed that the applicant included provisions for the self-diagnostic functions at powerup and periodically, along with failure result reporting capabilities. Based on these NRC staff determinations, the HIPS platform is suitable to satisfy IEEE Std. 7-4.3.2-2003, Clause 5.5.3. ASAI-49 to ASAI-51 are necessary to establish full compliance with this regulatory requirement.

3.7.1.6 Clause 5.6 Independence

Clause 5.6 of IEEE Std. 7-4.3.2-2003 prohibits data communication between safety channels or between safety and nonsafety systems from inhibiting the performance of the safety function. Clause 5.6 also recognizes that software directly associated with the performance of a safety function and other nonsafety software may reside on the same computer or use common resources. To ensure nonsafety software does not adversely affect safety software, Clause 5.6 identifies two approaches to address the issues: (1) inclusion of barrier requirements to provide adequate confidence that the nonsafety functions cannot interfere with performance of the safety functions of the software or firmware, where the barriers shall be designed in accordance with the requirements of the standard while the nonsafety software is not required to meet these requirements, and (2) if barriers between the safety software and nonsafety software are not implemented, then the nonsafety software functions are required to be developed in accordance with the requirements of this standard. DSRS Section 7.1.2 provides acceptance criteria for this requirement.

DI&C-ISG-04, Revision 1, describes methods acceptable to the staff to prevent adverse interactions among safety divisions and between safety-related equipment and equipment that is not safety related. This guidance directly addresses most of IEEE Std. 7-4.3.2-2003, Clause 5.6.

The establishment of communications among redundant portions of a safety system or between the safety system and other nonsafety systems in a plant is an application-specific activity. Since the TR does not address a specific application or provide a definitive safety system design, the evaluation of the HIPS platform against the communications independence aspect of this regulatory requirement is limited to features and capabilities of its communication independence concepts.

Unlike microprocessor-based computer systems, to which Clause 5.6 of IEEE Std. 7-4.3.2-2003 typically applies, the HIPS platform does not contain executable software that uses shared processing resources (e.g., processor, processing registers, cache memory). Instead, a HIPS platform SFM performs individual functions supported through distinct FPGA logic, and each individual function does not share its FPGA logic resources with other functions.

Section 3.1.9 addresses the staff's evaluation of the self-diagnostics and test and calibration capabilities. Section 3.2.1 discusses the HIPS electrical isolation requirements between safety and nonsafety equipment. Section 3.2.2 contains the staff's evaluation of the communication independence features provided by HIPS platform standardized circuit boards. Section 3.5 addresses the NRC staff's evaluation of the deterministic performance characteristics of the HIPS platform.

Sections 3.6.2.6 and 3.8 of this SE address compliance with Clause 5.6 of IEEE Std. 603-1991 and DI&C-ISG-04. Both evaluations include ASAs, because the prohibition against data communication between safety channels or between safety and nonsafety systems from inhibiting the performance of the safety function must be addressed based on each ASA of the HIPS platform.

The staff determined the HIPS platform supports meeting Clause 5.6 of IEEE Std. 7-4.3.2-2003, based on the evaluations and fulfillment of the ASAs provided within Sections 3.6.2.6 and 3.8. ASA-52 and ASA-53 are necessary to establish full compliance with this regulatory requirement.

3.7.1.7 Clause 5.7 Capability for Test and Calibration

Clause 5.7, "Capability for Test and Calibration," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.7 of IEEE Std. 603-1991 are necessary.

The TR states that Clause 5.7 of IEEE 7-4.3.2-2003 is not applicable to the generic HIPS platform. The staff agrees that the evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.7 of IEEE Std. 7-4.3.2-2003.

3.7.1.8 Clause 5.8 Information Displays

Clause 5.8, "Information Displays," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.8 of IEEE Std. 603-1991 are necessary.

The TR states that Clause 5.8 of IEEE 7-4.3.2-2003 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.8 of IEEE Std. 7-4.3.2-2003.

3.7.1.9 Clause 5.9 Control of Access

Clause 5.9, "Control of Access," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.9 of IEEE Std. 603 are necessary.

The TR states that Clause 5.9 of IEEE 7-4.3.2 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.9 of IEEE Std. 7-4.3.2-2003.

3.7.1.10 Clause 5.10 Repair

Clause 5.10, "Repair," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.10 of IEEE Std. 603 are necessary.

The TR states that Clause 5.10 of IEEE 7-4.3.2-2003 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.10 of IEEE Std. 7-4.3.2-2003.

3.7.1.11 Clause 5.11 Identification

Clause 5.11, "Identification," of IEEE Std. 7-4.3.2-2003 provides three identification requirements specific to software systems to ensure that the required computer system hardware and software are installed in the appropriate system configuration. These identification requirements are (1) firmware and software identification to ensure the correct software is installed in the correct hardware component, (2) means to retrieve the identification from the firmware using software maintenance tools, and (3) IEEE Std. 603-1991-compliant physical identification of the digital computer system hardware. DSRS Section 7.2.9 provides acceptance criteria for this requirement.

The determination of the coding of cabinets and cabling for a safety system is an application-specific activity. The particular means for identifying safety equipment according to redundant portions of a safety system (i.e., channels or divisions) is also an application-specific activity. Component identification for the HIPS platform can contribute to fulfillment of this requirement. In addition to faceplate identification of the module type, the HIPS platform provides physical labels on the PCB of each module to uniquely identify the hardware module and installed firmware.

Unlike microprocessor-based computer systems, to which Clause 5.11 of IEEE Std. 7-4.3.2-2003 typically applies, the HIPS platform does not contain separate and distinct executable software that must be loaded onto a system or updated at a licensed facility. The HIPS platform restricts FPGA and application-specific NVM configuration programming to the HIPS platform manufacturer. Each FPGA and NVM device permanently resides on its

standardized circuit board. Once the manufacturer programs a standardized circuit board's FPGA and its NVM per application specifications, the programmed devices are treated as hardware devices and subject to the identification control activities for the standardized circuit board upon which they permanently reside. The HIPS platform contains design features that ensure that each standardized circuit board has been correctly installed in its designated chassis and backplane location to form an application-specific system. These attributes address the first portion of IEEE Std. 7-4.3.2-2003, Clause 5.11.

In RAI 3, Question 07.01 Draft DSRS-14, staff asked the applicant to describe how software maintenance tools are used to retrieve and confirm the configuration of the installed equipment. In its response to RAI 3, Question 07.01 Draft DSRS-14, dated August 19, 2016 (see Ref. 6.1-20), the applicant stated that the HIPS platform contains features that include FPGA and NVM version identifiers, which may be viewed using maintenance equipment to confirm the configuration of the installed equipment. Furthermore, this information is stored in a section of the NVM device that is configured by the manufacturer and nonmodifiable by the end user. System and board information provides details about the configuration of a HIPS platform system and this information includes board FPGA programming, board build information, and the board's configuration. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-14, the staff found the applicant's response acceptable because these features address the second portion of Clause 5.11 of IEEE Std. 7-4.3.2-2003. The staff also reviewed the markup of TR Section 8.2.7 provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-14, is resolved and closed.

Section 3.6.2.11 of this SE addresses compliance with the IEEE Std. 603 general physical identification requirements for hardware, which includes digital hardware. Therefore, no further staff evaluation is required to address the third portion of IEEE Std. 7-4.3.2-2003, Clause 5.11.

The staff evaluated the HIPS platform design features against each portion of Clause 5.11 of IEEE Std. 7-4.3.2-2003 and the acceptance criteria described in DSRS Section 7.2.9. Based on this evaluation, the staff determined that the HIPS platform design features support meeting the second portion of Clause 5.11 of IEEE Std. 7-4.3.2-2003. ASAI-54 is necessary to establish full compliance with this regulatory requirement.

3.7.1.12 Clause 5.12 Auxiliary Features

Clause 5.12, "Auxiliary Features," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.12 of IEEE Std. 603-1991 are necessary.

The TR states that Clause 5.12 of IEEE Std. 7-4.3.2-2003 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.12 of IEEE Std. 7-4.3.2-2003.

3.7.1.13 Clause 5.13 Multi-Unit Stations

Clause 5.13, "Multi-Unit Stations," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.13 of IEEE Std. 603 are necessary.

The TR states that Clause 5.13 of IEEE Std. 7-4.3.2-2003 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.13 of IEEE Std. 7-4.3.2-2003.

3.7.1.14 Clause 5.14 Human Factors Consideration

Clause 5.14, "Human Factors Consideration," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.14 of IEEE Std. 603 are necessary.

The TR states that Clause 5.14 of IEEE Std. 7-4.3.2-2003 is not applicable to the generic HIPS platform. The NRC staff agrees that evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 5.14 of IEEE Std. 7-4.3.2-2003.

3.7.1.15 Clause 5.15. Reliability

When IEEE Std. 603 reliability goals are identified, Clause 5.15, "Reliability," of IEEE Std. 7-4.3.2-2003 requires the proof that goals are met, including software. Clause 5.15 also identifies two potential methods that may be used for determining reliability, which are (1) combinations of analysis, field experience, or testing, and (2) software error recording and trending in combination with analysis, field experience, or testing.

As stated in RG 1.152, Revision 2, the NRC does not endorse the concept of quantitative reliability goals as the sole means of meeting the Commission's regulations for reliability of digital computers in safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system.

The determination of the reliability of a digital safety system is an application-specific activity that requires an assessment of a full system design, its application and system software, and the software life-cycle processes. The TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures; the evaluation against this requirement is limited to considering the reliability characteristics of the digital platform and the quality of its system software. In addition, the TR cannot fully address Clause 5.15 of IEEE Std. 7-4.3.2-2003, because the IEEE Std. 603 reliability goals are application specific. Therefore, this SE does not address the evaluation against the requirement of Clause 5.15 of IEEE Std. 603-1991. ASAI-37 is necessary to establish full compliance with this regulatory requirement.

3.7.2 Clause 6 Sense and Command Features

Clause 6, "Sense and Command Features," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Section 6 of IEEE Std. 603-1991 are necessary.

The TR states that Clause 6 of IEEE 7-4.3.2-2003 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 6 of IEEE Std. 7-4.3.2-2003.

3.7.3 Clause 7 Execute Features

Clause 7, "Execute Features," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 7 of IEEE Std. 603 are necessary.

The TR states Clause 7 of IEEE 7-4.3.2 is not applicable to the generic HIPS platform. The staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 7 of IEEE Std. 7-4.3.2-2003.

3.7.4 Clause 8 Power Source Requirements

Clause 8, "Power Source Requirements," of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 8 of IEEE Std. 603 are necessary.

The TR states that Clause 8 of IEEE 7-4.3.2 is not applicable to the generic HIPS platform. The NRC staff agrees that an evaluation of this clause is not applicable because no requirements beyond IEEE Std. 603-1991 are necessary. Therefore, this SE does not address the evaluation against the requirement of Clause 8 of IEEE Std. 7-4.3.2-2003.

3.8 Review of DI&C-ISG-04 Staff Positions

The NRC Task Working Group 4, "Highly Integrated Control Rooms—Communications Issues," developed interim NRC staff guidance on the review of communications issues applicable to digital safety systems. DI&C-ISG-04, Revision 1, contains NRC staff positions on three areas of interest: (1) interdivisional communications, (2) command prioritization, and (3) multidivisional control and display stations.

Appendix C to the TR summarizes the regulatory conformance of the HIPS platform with DI&C-ISG-04. However, it was not clear to the staff how the HIPS design specifications conform to the staff positions in DI&C-ISG-04. Therefore, in RAI 3, Question 07.01 Draft DSRS-17, the staff asked the applicant to explain the basis for its claims, specifically, conformance to the staff positions in DI&C-ISG-04. In its response to RAI 3, Question 07.01 Draft DSRS-17, dated August 19, 2016 (see Ref. 6.1-20), the applicant revised Appendix B to

add the application-specific information and make other conforming changes based on the RAI responses. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-17 (see Sections 3.8.1 to 3.8.3), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Appendix C provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-17, is resolved and closed.

Although the staff determined that the HIPS platform includes features to support satisfying various sections and clauses of DI&C-ISG-04, an applicant or licensee referencing this SE must evaluate the HIPS platform-based system for full conformance against this guidance. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences.

Some of the points under the DI&C-ISG-04 staff positions are implementation specific and worded primarily in light of microprocessor-based systems. Other points are application specific and cannot be fully evaluated within the scope of the TR. The subsections below provide an evaluation of each HIPS platform communication method against the applicable points for that position. These evaluations address implementation-specific points in consideration of the HIPS platform's FPGA-based logic processing to determine the degree that the platform's approach provides equivalent assurance that the digital data communications do not adversely affect the operability of safety functions.

3.8.1 DI&C-ISG-04, Section 1—Interdivisional Communications

Staff Position 1 of DI&C-ISG-04 establishes criteria for communication interfaces between independent safety channels/divisions and between safety and nonsafety equipment. Meeting the criteria under this staff position gives reasonable assurance that these types of communications do not adversely affect the operability of safety functions. The subsections below address each point of this staff position.

3.8.1.1 Point 1

Staff Position 1, Point 1, states that a safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE Std. 603-1991. It is recognized that division voting logic must receive inputs from multiple safety divisions.

The HIPS platform is designed such that a safety division functions independently of other safety divisions. For voting purposes, divisions do share voting data with other divisions through the SVM. The division voters are not dependent on voting data from other divisions because the division voters will still be able to complete their safety function even if the SVM

voting data have errors or are not available. The division voters would apply a safe default for the missing inputs.

The staff determined that the HIPS design concepts support conformance to the guidance provided by Staff Position 1, Point 1, because no division is dependent on any information outside its own division to perform a safety function. ASAI-22, ASAI-23, and ASAI-55 are necessary to establish full conformance to this staff position.

3.8.1.2 Point 2

Staff Position 1, Point 2, states that each safety channel should use internal safety resources to protect its safety functions from being adversely influenced by resources, signals, and information that originate from outside its own safety division.

The staff determined that the HIPS platform design concepts support conformance to the guidance provided by Staff Position 1, Point 2, because the HIPS platform can be configured into an architecture that has four separation groups that are physically and electrically independent of each other, using isolation devices. ASAI-20 to ASAI-23 are necessary to establish full conformance to this staff position.

3.8.1.3 Point 3

Staff Position 1, Point 3, states that a safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. However, if receipt of information from outside the division exists, then the applicant should justify it. Furthermore, the applicant should justify receipt of information and inclusion of functions that do not support or enhance safety functions. These justifications should demonstrate that the added system/programming complexity does not significantly increase the likelihood of program specification or implementation errors and should also define and justify the term 'significantly' within the demonstration.

The HIPS platform does not identify any interdivisional communication except for voting, as discussed in Staff Position 1, Point 1. As a result, the staff determined that the HIPS platform design concepts support conformance to the guidance provided by Staff Position 1, Point 3. ASAI-22 is necessary to establish full conformance to this staff position.

3.8.1.4 Point 4

Staff Position 1, Point 4, states that the communication processes to support interdivisional communications (i.e., the transfer of data and any associated handshaking between a safety function processor and another channel or nonsafety equipment) should be carried out by a safety-related communications processor that is separate from the processor that executes the safety function, so communications errors and malfunctions will not interfere with the successful execution of safety functions. Point 4 provides amplifying information that describes an

acceptable implementation method; this method uses a shared memory resource, such as dual-ported random-access memory. Point 4 further identifies the need to demonstrate safety function determinism with respect to the data exchange between the safety processor and the communication processor. The demonstration of safety function determinism should show that the safety function will (1) be performed within the timeframe established in the safety analysis, and (2) complete successfully without data from the communication process, including either a complete lack of access or any delays in obtaining access to a resource shared between the safety processor and the communication processor.

Communications within the HIPS platform are performed by dedicated logic within the FPGA on each of the module types: SFM, CM, and EIM. The dedicated logic for the communications is separate from the safety function logic. Communication between modules is done asynchronously. The transfer of information between the safety function logic and the communications logic is achieved through dedicated shared data registers.

The staff has reviewed the design and functionality of the communications process and has determined that the HIPS platform conforms to Staff Position 1, Point 4.

3.8.1.5 Point 5

Staff Position 1, Point 5, states that the cycle time for the safety function processor should be determined by considering the longest possible completion time for each access to the shared memory. Failure of the system to meet the limiting cycle time should be detected and alarmed.

The HIPS platform supports application-specific conformance with a fully deterministic work cycle for the safety data path from the input of the HIPS platform to the final actuated device output. The TR states the failures of the system to meet timing requirements will activate an alarm so corrective actions can be taken.

Section 3.5 discusses the HIPS platform throughput and response time.

The staff determined that the HIPS platform communication components support conformance to the guidance provided by Staff Position 1, Point 5, because the HIPS platform supports detection and alarm logic in response to a system's failure to meet its application-specific limiting cycle time. When implementing a HIPS safety system, the applicant must review its timing analyses and validation tests to verify that it satisfies its plant-specific requirements for system response and display response time presented in the accident analysis in Chapter 15 of the safety analysis report. This is ASAI-56.

3.8.1.6 Point 6

Staff Position 1, Point 6, states that the safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

The HIPS platform provides an FPGA approach that implements communication logic circuits that nonintrusively monitor safety function logic circuits so communication activities cannot delay or otherwise adversely affect the performance of the safety functions. Additionally, the TR states that communication functions do not perform communication handshaking and do not accept any interrupts from any communication devices.

The staff determined that the HIPS platform conforms to Staff Position 1, Point 6, because the safety function communication logic circuits perform no communication handshaking and do not accept interrupts.

3.8.1.7 Point 7

Staff Position 1, Point 7, states that only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the prespecified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be predetermined. Every message should have the same message field structure and sequence (e.g., message identification, status information, data bits) in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

The HIPS platform provides an FPGA approach that implements communication logic circuits that are separate and independent from safety function logic circuits without regard to whether the circuits reside in the same FPGA device. In addition, the TR states that a receiving HIPS platform will validate the data and will only accept and use data that conform to a predefined communication protocol and message format.

The staff therefore determined that the HIPS platform conforms to Staff Position 1, Point 7, because the HIPS platform supports fixed messaging structures that operate in a fully deterministic manner. The communications for the HIPS platform are continuous and remain fully deterministic at all times.

3.8.1.8 Point 8

Staff Position 1, Point 8, states that data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

The HIPS platform provides an FPGA approach that implements communication logic circuits that are separate and independent from safety function logic circuits without regard to whether the circuits reside in the same FPGA device. Therefore, the staff determined that transmit-only communications cannot adversely affect a safety function, regardless of its location.

The staff determined that the HIPS platform communication components support conformance to the guidance provided by Staff Position 1, Point 8, because the HIPS platform supports an application-specific communication architecture for data exchanges that conforms to Point 8. ASAI-22 is necessary to establish full conformance to this staff position.

3.8.1.9 Point 9

Staff Position 1, Point 9, states that incoming message data should be placed in fixed and predetermined locations of communication processor shared memory and function processor memory, both of which contain memory locations dedicated to store incoming message data. These memory locations should segregate input data from output data, such as through placement into separate memory devices or in separate prespecified physical areas of a single memory device.

The staff determined that the dual-ported memory usage within the HIPS platform conforms to Staff Position 1, Point 9, because each HIPS module has data registers with predetermined purposes and fixed locations.

3.8.1.10 Point 10

Staff Position 1, Point 10, states that safety division programs should be protected from alteration while the safety division is in operation. In other words, the safety division programs should be protected when the equipment is on line and being relied upon to perform a safety function. Point 10 identifies two acceptable implementation options to protect programming from alteration: (1) hardware interlocks and (2) physical disconnection of the MWS. Point 10 also establishes that MWSs capable of altering addressable constants, setpoints, parameters, and other settings can only do so when either (1) an interposing communication processor provides a shared-memory resource to exchange incoming and outgoing messages with the safety function processor in accordance with the entirety of the DI&C-ISG-04's interdivisional communication guidance, or (2) when the associated channel is inoperable. When such an MWS is provided, Point 10 further establishes that the maintenance activities should be physically restricted to making changes to only one redundant safety division at a time, and this restriction should be accomplished by means of physical disconnection capable of interrupting the communication signal path to all safety channels except for the one undergoing maintenance changes. Although Point 10 establishes that this restriction is to be implemented in hardware circuits, it does not preclude program monitoring of the hardware circuits for other purposes.

The staff determined that the design concepts within the HIPS platform conform to Staff Position 1, Point 10, because the HIPS platform is based on FPGA technology. The FPGA logic for the specific functions is designed during the design process and is used to configure the logic within the FPGA. This logic configuration remains fixed and cannot be changed while the equipment is on line. Any changes to this logic require the equipment to be removed from

service. TR Section 4.8 further describes such access control features as communication from the MWS to the HIPS chassis is allowed when the SFM is placed OOS by activating the OOS switch and attaching a temporary cable from the MWS and the SFM is the only module that can be modified while installed in the chassis. This capability is limited to setpoints and tunable parameters that may require periodic modification.

3.8.1.11 Point 11

Staff Position 1, Point 11, states that provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise OOS. These provisions should prevent the progress of a safety function processor through its instruction sequence from being affected by any message from outside its division. For example, there should be no possibility that interdivisional communication messages could direct a safety function processor to execute a subroutine or branch to a new instruction sequence.

The HIPS platform does not contain conventional software instructions with either subroutines or branches. Instead, the HIPS platform contains configured hardware logic circuits that are contained in the FPGA. The HIPS platform does not depend on interdivisional communications or external systems to perform its safety functions.

The staff determined that the HIPS platform conforms to Staff Position 1, Point 11, because these provisions explicitly preclude any ability to change the safety division logic circuits, which is the FPGA equivalent to conventional processor software. Furthermore, the staff determined that available HIPS platform features can be used to ensure that a HIPS platform-based instrument has been bypassed or is otherwise OOS when MWS activities are active, as described in Staff Position 1, Point 10.

3.8.1.12 Point 12

Staff Position 1, Point 12, states that communication faults should not adversely affect the performance of required safety functions in any way. Point 12 includes 12 examples of credible communication faults for consideration, as applicable.

The HIPS platform provides an FPGA approach that implements communication logic circuits that are separate and independent from safety function logic circuits without regard to whether the circuits reside in the same FPGA device. The HIPS platform's communication protocol and implementation checks, detects, and annunciates communication failures.

As discussed in Staff Position 1, Point 10, the HIPS platform provides design features (monitoring and indication capabilities) to alert operators when a safety channel/division is bypassed; these design features are intended to detect and indicate when the interface that supports the MWS is either enabled or active.

The staff determined that communications faults, including the 12 examples contained in Staff Position 1, Point 12, will not adversely affect the performance of the required safety functions and that the HIPS platform supports conformance to the guidance provided by Staff Position 1, Point 12. ASAI-57 is necessary to establish full conformance to this staff position.

3.8.1.13 Point 13

Staff Position 1, Point 13, states that vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Testing should demonstrate and verify the effectiveness of these provisions. Point 13 further establishes that vital interdivisional communications should include provisions to handle corrupt, invalid, untimely, or otherwise questionable data. Any error detection or error correction processing should not adversely affect the operation of the safety function processor.

The staff determined that the HIPS platform communication components support conformance to the guidance provided by Staff Position 1, Point 13, because the HIPS platform provides that methods to detect data corruption during transmission include the use of parity bits and/or CRC message checksums. The protocol includes a feature for encoding messages, and this feature ensures the originator of any received message is correct. Use of this feature applies to messaging protocols that include the CRC checksum, is directly supported by the HIPS platform's restriction to use of a point-to-point communication architecture for all interdivisional communications, and will result in the complete rejection of a message originating from an unexpected source. The transmit interval for messages is fixed, so the HIPS platform communication protocol supports detection of untimely messages (too early or too late). The communications logic circuits detect and handle communication errors. ASAI-32 is necessary to establish full conformance to this staff position.

3.8.1.14 Point 14

Staff Position 1, Point 14, states that vital communications should be point-to-point by means of a dedicated medium without intervening nodes between the transmitter and the receiver. Point 14 further establishes that alternative methods, if proposed, should be justified and demonstrated as providing equivalent reliability.

The staff determined that the HIPS platform conforms to Staff Position 1, Point 14, because vital communications are achieved through a "point-to-point" connection, as described in TR Sections 2.6, "Communication Buses; 4.3; and 7.7.

3.8.1.15 Point 15

Staff Position 1, Point 15, establishes that vital interdivisional communications for safety functions provide a fixed dataset at regular intervals, whether data values in the set have

changed or not. This fixed dataset should reflect the equipment state in support of equipment safety functions.

The NRC staff determined the HIPS platform conforms to the guidance provided by Staff Position 1, Point 15, because the protocol can be used to transmit predefined fixed datasets at prescribed intervals and without regard to the data values, as described in TR Sections 2.5.3; 7.6.6, "Safety Data Bus HIPS Bus Frame"; 7.7; and 8.2.4.

3.8.1.16 Point 16

Staff Position 1, Point 16, states that network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol.

Point 16 is application specific, because meeting it is dependent upon the safety functions of the application and the installed communication architecture.

The staff determined that the HIPS platform supports conformance to the guidance provided by Staff Position 1, Point 16, because the protocol can be used to ensure the connectivity, liveness, and real-time properties of vital communication processes. The staff further determined that ASAI-20 to ASAI-23 should verify that Point 16 is met by ensuring that application specifications identify provisions to detect untimely messages and provide an indication of this type of communication failure to operators when it occurs.

3.8.1.17 Point 17

Staff Position 1, Point 17, establishes that the medium used for vital interdivisional communications should be qualified for the anticipated normal and postaccident environments associated with its installation.

The TR states that the generic HIPS platform design concepts do not address Staff Position 1, Point 17. The staff agrees with the evaluation of Position 17, because it is dependent upon the plant installation and the safety application. Although the HIPS platform supports both copper and fiber-optic mediums, the TR scope excludes the medium used for interdivisional communication and identifies this to be application specific. Therefore, this SE does not address the evaluation against Point 17 of Staff Position 1. ASAI-17 is necessary to establish full conformance to this staff position.

3.8.1.18 Point 18

Staff Position 1, Point 18, states that provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complexity.

Point 18 is dependent upon the plant safety application because the plant's application establishes potential hazards, and application-specific needs establish the required

performance, the needed functionality, and the interdivisional communication architecture to support the needed functionality. Application specifications for each use of a digital data communication channel must be analyzed and designed to meet plant and system hazard and performance specifications. This analysis will occur as part of the application-specific development process. This analysis will assess unneeded functionality and complexity to ensure no hazards or performance deficits are produced from the inclusion of unneeded functionality or increases in complexity that result from including these functions.

Based on the evaluations in Sections 3.5 and 3.6.2.7, the staff determined that the HIPS platform supports conformance to the guidance provided by Staff Position 1, Point 18, because the HIPS platform supports the performance of application-specific hazard and performance analyses in considering an application's specified functionality and inherent level of complexity. The staff further determined that application-specific items should verify that Point 18 is met by ensuring an application-specific analysis has been performed to assess unneeded functionality and complexity. The results of this analysis should demonstrate that any resultant hazards or performance deficits have been addressed. ASAI-12 and ASAI-58 are necessary to establish full compliance with this staff position.

3.8.1.19 Point 19

Staff Position 1, Point 19, states that all vital interdivisional communication links and nodes should have sufficient capacity to support the safety functions. Point 19 further establishes the need to identify the true data rate (including overhead) and ensure the communication bandwidth is sufficient for proper performance of all safety functions. Safety system sensitivity to potential communication throughput issues should be confirmed by testing to demonstrate each specified minimum communications throughput threshold associated with a safety function performance is reliably met.

Point 19 is dependent upon the plant safety application, because the plant's application establishes the minimum communications throughput threshold for each vital interdivisional communication link and node required to reliably meet each application-specific safety function's limiting performance requirement.

The staff determined that the HIPS platform supports conformance to the guidance provided by Staff Position 1, Point 19 because, as described in TR Sections 2.5.3, 4.3, 7.6.6, 7.7, and 8.2.4, the HIPS bus frame cycle time is fixed for a given application and does not change once the system has been implemented and has sufficient diagnostic capabilities. Interdivisional communications are through four fiber-optic communication channels on each CM that can provide one-way isolated communications to another CM or system, or receive one-way data from another CM or system. Each communication channel can be configured as transmit only or receive only. Further, the staff evaluated the repeatability and predictability of the safety function performance in Section 3.5 of this SE. ASAI-19 and ASAI-59 are necessary to establish full conformance to this staff position.

3.8.1.20 Point 20

Staff Position 1, Point 20, states that the safety system response time calculations should assume a data error rate greater than or equal to a design-basis error rate, which is supported by error rates observed during design and qualification testing.

The TR states that the generic HIPS platform design concepts do not apply to Staff Position 1, Point 20. The staff agrees that an evaluation of Point 20 is not applicable because the TR does not address equipment qualification, since these are application-specific activities that depend on the equipment vendor to be used to implement the HIPS system. Therefore, this SE does not address the evaluation against Point 20 of Staff Position 1. ASAI-18, ASAI-19, and ASAI-59 are necessary to establish full conformance to this staff position.

3.8.2 DI&C-ISG-04, Section 2—Command Prioritization

Section 2 of DI&C-ISG-04 provides guidance applicable to a priority module. A priority module is a shared resource capable of receiving device actuation commands from multiple sources, which may originate from different safety divisions or from both safety and nonsafety divisions but that responds by only sending the command having the highest priority to the actuating device. Priority modules should be developed as safety-related devices for use with safety-related actuators.

Section 2 of DI&C-ISG-04 provides ten points; these points govern (1) the development, configuration, and testing of any priority module, (2) its functional performance and behavior, and (3) its connection to safety components. Testing guidance includes consideration of (1) the impact of software-based development tools, (2) conditions where the scope should include every possible combination of inputs and every possible sequence of device states to verify all outputs for every case, and (3) uses of automated test tools. A priority module must be shown to execute to completion the associated protective actions, such that completion of any protective action is not interrupted by commands, conditions, or failures outside the priority module's safety division.

3.8.2.1 Point 1

Staff Position 2, Point 1, states that a priority module is a safety-related device or software function and must meet all of the requirements in 10 CFR Part 50, Appendices A and B (e.g., design, qualification, quality), applicable to safety-related devices or software.

The TR states that the generic HIPS platform design concepts do not apply to Point 1 of Staff Position 2. The staff agrees that an evaluation of Point 20 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology) and the TR does not address quality as stated in Appendix A, IEEE Section 5.3. Therefore, this SE does not address the evaluation against Point 1 of Staff Position 2.

3.8.2.2 Point 2

Staff Position 2, Point 2, states that priority modules used for diverse actuation signals should be independent of the remainder of the digital system and should function properly, regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.

The TR states that the generic HIPS platform design concepts do not apply to Point 2 of Staff Position 2. The staff agrees that an evaluation of Point 2 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology), and no priority modules have been used for diverse actuation signals. Therefore, this SE does not address the evaluation against Point 2 of Staff Position 2.

3.8.2.3 Point 3

Staff Position 2, Point 3, states that safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but that only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a CCF in the primary system that erroneously forces the plant equipment to a state that is different from the designated "safe state") and that do not directly support any safety function have lower priority and may be overridden by other commands. In some cases, such as a containment isolation valve in an auxiliary feedwater line, there is no universal "safe state"; the valve must be open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of ISG-04. The reasoning behind the proposed priority ranking should be explained in detail. The staff should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority rankings and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.

The TR states that the generic HIPS platform design concepts do not apply to Point 3 of Staff Position 2. The NRC staff agrees that an evaluation of Point 3 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology). Therefore, this SE does not address the evaluation against Point 3 of Staff Position 2.

3.8.2.4 Point 4

Staff Position 2, Point 4, states that a priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.

The TR states that the generic HIPS platform design concepts do not apply to Point 4 of Staff Position 2. The staff agrees that an evaluation of Point 4 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology). Therefore, this SE does not address the evaluation against Point 4 of Staff Position 2.

3.8.2.5 Point 5

Staff Position 2, Point 5, states that communication isolation for each priority module should be as described in the guidance for interdivisional communications.

The TR states that the generic HIPS platform design concepts do not apply to Point 5 of Staff Position 2. The staff agrees that an evaluation of Point 5 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology). Therefore, this SE does not address the evaluation against Point 5 of Staff Position 2.

3.8.2.6 Point 6

Staff Position 2, Point 6, states that software used, for example, in the design, testing, and maintenance of a priority module is subject to all of the applicable guidance in RG 1.152, which endorses IEEE Std. 7-4.3.2-2003. This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices, programmable gate arrays, or other such devices. Clause 5.3.2 of IEEE Std. 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100 percent tested before being released for service. The 100 percent testing requirement means that every possible combination of inputs and every possible sequence of device states is tested and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (e.g., quality requirements, V&V, documentation) applicable to safety-related software.

The TR states that the generic HIPS platform design concepts do not apply to Point 6 of Staff Position 2. The staff agrees that an evaluation of Point 6 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology). Therefore, this SE does not address the evaluation against Point 6 of Staff Position 2.

3.8.2.7 Point 7

Staff Position 2, Point 7, states that any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software and should be developed, maintained, and controlled accordingly.

The TR states that the generic HIPS platform design concepts do not apply to Point 7 of Staff Position 2. The staff agrees that an evaluation of Point 7 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology). Therefore, this SE does not address the evaluation against Point 7 of Staff Position 2.

3.8.2.8 Point 8

Staff Position 2, Point 8, states that, to minimize the probability of failures because of common software, the priority module design should be fully tested.

The TR states that the generic HIPS platform design concepts do not apply to Point 8 of Staff Position 2. The staff agrees that an evaluation of Point 8 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology). Therefore, this SE does not address the evaluation against Point 8 of Staff Position 2.

3.8.2.9 Point 9

Staff Position 2, Point 9, states that automatic testing within a priority module, whether initiated from within the module or triggered from outside and including the failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute a CCF if it were to result in disabling the module safety function.

The TR states that the generic HIPS platform design concepts do not apply to Point 9 of Staff Position 2. The staff agrees that an evaluation of Point 9 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology). Therefore, this SE does not address the evaluation against Point 9 of Staff Position 2.

3.8.2.10 Point 10

Staff Position 2, Point 10, states that the priority module must ensure that the completion of a protective action as required by IEEE Std. 603-1991 is not interrupted by commands, conditions, or failures outside the module's own safety division.

The TR states that the generic HIPS platform design concepts do not apply to Point 10 of Staff Position 2. The staff agrees that an evaluation of Point 10 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components (i.e., analog technology). Therefore, this SE does not address the evaluation against Point 10 of Staff Position 2.

3.8.3 DI&C-ISG-04, Section 3—Multidivisional Control and Display Stations

Section 3 of DI&C-ISG-04 provides guidance concerning operator workstations used to control plant equipment in more than one safety division and to display information from sources in more than one safety division and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

The TR scope excludes the control and display stations.

3.8.3.1 DI&C-ISG-04, Section 3.1—Independence and Isolation

Section 3.1 of DI&C-ISG-04 provides guidance applicable to multidivisional control and display stations. These guidance provisions do not apply to conventional hardwired control and indicating devices (e.g., hand switches, indicating lamps, analog indicators).

3.8.3.1.1 Point 1

Staff Position 3, Point 1, states that all communications with safety-related equipment should conform to the guidelines for interdivisional communications.

The TR states that the generic HIPS platform design concepts do not apply to Point 1 of Staff Position 3. The staff agrees that an evaluation of Point 1 is not applicable because it does not include multidivisional control and display stations. Therefore, this SE does not address the evaluation against Point 1 of Staff Position 3.

3.8.3.1.2 Point 2

Staff Position 3, Point 2, states that all communications with equipment outside the station's own safety division, whether that equipment is safety related or not, should conform to the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself.

The TR states that the generic HIPS platform design concepts do not apply to Point 2 of Staff Position 3. The staff agrees that an evaluation of Point 2 is not applicable because the TR does not address cross divisional communications or communications from nonsafety systems. These are application-specific activities that depend on the application of the architecture to be implemented in the HIPS-based system. Therefore, this SE does not address the evaluation against Point 2 of Staff Position 3. ASAI-60 is necessary to establish full conformance to this staff position.

3.8.3.1.3 Point 3

Staff Position 3, Point 3, states that nonsafety stations may control the operation of safety-related equipment, provided the following restrictions are enforced: (1) the nonsafety station should access safety-related plant equipment only by way of a priority module associated with that equipment, (2) the nonsafety station should not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function, and (3) the nonsafety station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.

The TR states that the generic HIPS platform design provides an enable nonsafety switch concept that is designed to allow an analog nonsafety-related component binary control signal input into the HWM when the switch is closed by a plant operator and is otherwise ignored.

The staff determined that the HIPS platform supports conformance to the guidance provided by Staff Position 3, Point 3, because the enable nonsafety switch only allows control by the plant operator of a safety-related component; however, it does not override the priority logic capability should a safety trip signal occur. Nevertheless, ASAI-61 is necessary to establish full conformance to this staff position.

3.8.3.1.4 Point 4

Staff Position 3, Point 4, states that safety-related stations controlling the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that control the operation of safety-related equipment.

The TR states that the generic HIPS platform design concepts do not apply to Point 4 of Staff Position 3. The staff agrees that an evaluation of Point 4 is not applicable because the control capability is outside the scope of the TR. Therefore, this SE does not address the evaluation against Point 4 of Staff Position 3.

3.8.3.1.5 Point 5

Staff Position 3, Point 5, states that the result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant.

The TR states that the generic HIPS platform design concepts do not apply to Point 5 of Staff Position 3. The staff agrees that an evaluation of Point 5 is not applicable because the control capability is outside the scope of the TR. Therefore, this SE does not address the evaluation against Point 5 of Staff Position 3.

3.8.3.2 DI&C-ISG-04, Section 3.2—Human Factors Considerations

Section 3.2 of DI&C-ISG-04 provides guidance regarding various human factors engineering requirements.

The TR states that the generic HIPS platform design concepts do not apply to Section 3.2 of DI&C-ISG-04. The staff agrees that an evaluation of Section 3.2 of DI&C-ISG-04 is not applicable because human factors engineering requirements are outside the scope of the TR. Therefore, this SE does not address the evaluation against Section 3.2 of DI&C-ISG-04.

3.8.3.3 DI&C-ISG-04, Section 3.3—Diversity and Defense-in-Depth Considerations

Section 3.2 of DI&C-ISG-04 provides D3 considerations that may influence the number and disposition of operator workstations and possibly of backup controls and indications that may or may not be safety related. D3 considerations may also impose qualification or other measures or guidelines upon equipment addressed in this ISG. Finally, the consideration of other aspects of D3 is outside the scope of this guidance. Additional guidance concerning D3 considerations is provided separately.

The TR states that the generic HIPS platform design concepts do not apply to Section 3.3 of DI&C-ISG-04. The staff agrees that an evaluation of Section 3.3 of DI&C-ISG-04 is not applicable because the TR scope excludes the control and display stations. Therefore, this SE does not address the evaluation against Section 3.3 of DI&C-ISG-04.

3.9 Review of Staff Requirements Memorandum to SECY-93-087

The SRM to SECY-93-087 describes the NRC position on D3 requirements to compensate for potential common-cause programming failure. This requires that the applicant assess the D3 of the proposed I&C system, and if a postulated CCF could disable a safety function, then a diverse means, with a documented basis where the diverse means is unlikely to be subject to the same CCF, shall be required to perform either the same function or a different function.

Appendix D to the TR summarizes the regulatory compliance of the HIPS platform with the SRM to SECY-93-087. However, it was not clear to the staff how the HIPS design specifications

comply with the SRM to SECY-93-087. Therefore, in RAI 3, Question 07.01 Draft DSRS-18, the staff asked the applicant to explain the basis for its claims; specifically, compliance with the SRM to SECY-93-087. In its response to RAI 3, Question 07.01 Draft DSRS-18, dated August 19, 2016 (see Ref. 6.1-20), the applicant revised Appendix D to add the application-specific information and make other conforming changes based on the RAI responses. Based on its review of the applicant's response to RAI 3, Question 07.01 Draft DSRS-18 (Sections 3.9.1 to 3.9.4 of this SE), the staff found the applicant's response acceptable. The staff also reviewed the markup of TR Appendix D provided with the response and found it acceptable. The applicant subsequently incorporated the proposed changes into Revision 1 of the TR (Ref. 6.1-3). Therefore, RAI 3, Question 07.01 Draft DSRS-18, is resolved and closed.

Although the staff determined that the HIPS platform includes features to support satisfying various sections of the SRM to SECY-93-087, an applicant or licensee referencing this SE must evaluate the HIPS platform-based system for full compliance against these requirements. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences.

3.9.1 SRM Section 1

Section 1 of the SRM to SECY-93-087 requires D3 of the proposed I&C system to demonstrate that vulnerabilities to CCFs have been adequately addressed.

The determination of D3 to compensate for potential common-cause programming failures is an application-specific activity that requires an assessment of a full system design. Section 3.4 addresses the staff review of the approaches to build diversity into a HIPS-based system. Although the TR cannot fully address Section 1 of the SRM to SECY-93-087, the NRC staff determined that the HIPS platform supports meeting Section 1 of the SRM to SECY-93-087. This determination is based on the platform design features, deterministic behavior, built-in diversity, and adequate closure of ASAI-62.

3.9.2 SRM Section 2

Section 2 of the SRM to SECY-93-087 requires the vendor or applicant to analyze each postulated CCF for each event that is evaluated in the accident analysis section of the safety analysis report using best estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

The determination of D3 to compensate for potential common-cause programming failures is an application-specific activity that requires an assessment of a full system design. Section 3.4 addresses the staff review of the approaches to build diversity into a HIPS-based system. Although the TR cannot fully address Section 2 of the SRM to SECY-93-087, the staff determined that the HIPS platform supports meeting Section 2 of the SRM to SECY-93-087.

This determination is based on the diverse technologies, modular nature of the HIPS platform equipment, and adequate closure of ASAI-62 and ASAI-63.

3.9.3 SRM Section 3

Section 3 of the SRM to SECY-93-087 requires that, if a postulated CCF could disable a safety function, then a diverse means, with a documented basis where the diverse means is unlikely to be subject to the same CCF, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

The determination of D3 to compensate for potential common-cause programming failures is an application-specific activity that requires an assessment of a full system design. Section 3.4 contains the staff review of the approaches to build diversity into a HIPS-based system. Although the TR cannot fully address Section 3 of the SRM to SECY-93-087, the staff determined that the HIPS platform supports meeting Section 3 of the SRM to SECY-93-087. This determination is based on the diverse technologies, the modular nature of the HIPS platform equipment, and the adequate closure of ASAI-63 and ASAI-64.

3.9.4 SRM Section 4

Section 4 of the SRM to SECY-93-087 requires the applicant to provide a set of displays and controls located in the main control room for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Sections 1 and 3 of the SRM.

The determination of D3 to compensate for potential common-cause programming failures is an application-specific activity that requires an assessment of a full system design. Section 3.4 discusses the staff review of the approaches to build diversity into a HIPS-based system. Although the TR cannot fully address Section 4 of the SRM to SECY-93-087, the staff determined that the HIPS platform supports meeting Section 4 of the SRM to SECY-93-087. This determination is based on the diverse technologies, modular nature of the HIPS platform equipment, and adequate closure of ASAI-65.

4.0 LIMITATIONS AND CONDITIONS

For each generic open item and application-specific action item that applies to their use of the HIPS platform, applicants and licensees referencing this SE should demonstrate that they have satisfactorily addressed the applicable items. The set of applicable items contains limitations and conditions for the use of a HIPS platform, as reviewed by the staff and documented within this SE.

4.1 Generic Open Items

Beyond the application-specific action items that follow, the staff did not identify any generic open items to be addressed by an applicant or licensee referencing this SE for installation of a safety-related system based on the HIPS platform.

4.2 Application-Specific Action Items

The application-specific, or plant-specific, actions provided in Table 4-1 must be performed when requesting NRC approval of the HIPS platform for safety-related applications in NPPs.

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
1	2.0	An applicant or licensee referencing this SE must establish full compliance with the design criteria and regulations identified in NuScale DSRS Chapter 7, Table 7.1, that are relevant to the specific application(s) of the HIPS platform as a safety-related I&C system in an NPP.
2	2.0 3.0	An applicant or licensee referencing this SE must demonstrate that the HIPS platform used to implement the application-specific or plant-specific system is unchanged from the base platform addressed in this SE. Otherwise, the applicant or licensee must clearly and completely identify any modification or addition to the base HIPS platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes.
3	3.6	Although the staff determined that the HIPS platform supports satisfying various sections and clauses of IEEE Std. 603-1991, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std. 603-1991. Because this SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences, an applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 603-1991 clause to its application-specific HIPS platform-based safety system or component. Furthermore, the applicant or licensee must demonstrate that the plant-specific and application-specific use of the HIPS platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.
4	3.7	Although the staff determined that the HIPS platform supports satisfying various sections and clauses of IEEE Std. 7-4.3.2-2003, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std. 7-4.3.2-2003. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. The applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 7-4.3.2-2003 clause to its application-specific HIPS platform-based safety system or component. Furthermore, the

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
		applicant or licensee must demonstrate that the plant-specific and application-specific use of the HIPS platform satisfies the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.
5	3.8	Although the staff determined that the HIPS platform includes features to support satisfying various sections and clauses of DI&C-ISG-04, an applicant or licensee referencing this SE must evaluate the HIPS platform-based system for full conformance against this guidance. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences.
6	3.9	Although the staff determined that the HIPS platform includes features to support satisfying various sections of the SRM to SECY-93-087, an applicant or licensee referencing this SE must evaluate the HIPS platform-based system for full compliance against this requirement. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences.
7	3.1.4.3	An applicant or licensee referencing this SE must provide administrative controls (e.g., procedures, technical specifications) to prevent an operator from placing the same SFM across more than one division into maintenance bypass concurrent with a single failure of a different division.
8	3.2	An applicant or licensee referencing this SE should verify having appropriate physical independence between nonsafety-related and safety-related equipment to satisfy the Class 1E to non-Class 1E separation requirements, consistent with the guidelines of RG 1.75, Revision 3.
9	3.4	An applicant or licensee referencing this SE must provide the basis for the allocation of safety functions between the two diverse divisions to mitigate the effects of a postulated CCF concurrent with Chapter 15 events in the final safety analysis report.

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
10	3.4	An applicant or licensee referencing this SE must verify that all diversity attributes of a HIPS platform (i.e., equipment diversity, design diversity, and functional diversity) conform to the diversity design details provided in the TR.
11	3.4	An applicant or licensee referencing this SE must verify that the diverse FPGA technologies have unique identification.
12	3.6.2.1 3.6.2.5 3.6.2.6.3.1 3.6.2.6.3.3 3.8.1.18	An applicant or licensee referencing this SE should perform a system-level FMEA to demonstrate that the application-specific use of the HIPS platform identifies each potential failure mode and determines the effects of each failure. The FMEA should demonstrate that single failures, including those with the potential to cause a nonsafety system action (i.e., a control function) resulting in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions, as applicable.
13	3.6.2.1	An applicant or licensee referencing this SE should demonstrate that the application-specific diagnostic, self-test, and manually initiated test and calibration features will not adversely affect channel independence, system integrity, or the system's ability to meet the single-failure criterion.
14	3.6.2.1	An applicant or licensee referencing this SE must review the actions to be taken when failures and errors are detected during tests and self-tests and ensure that these actions are consistent with system requirements. In addition, the applicant should review how errors and failures are indicated and managed after they are detected. The applicant or licensee should confirm that this information is provided in the single-failure analysis for the plant-specific application.
15	3.6.2.2 3.6.4.3	An applicant or licensee referencing this SE must demonstrate that the application-specific logic satisfies the completion of protective action requirements.
16	3.6.2.3 3.7.1.3	An applicant or licensee referencing this SE must confirm that the HIPS platform manufacturer is currently on the Nuclear Procurement Issues Committee list or confirm that the HIPS manufacturing quality processes conform to the applicant's or licensee's program that is compliant with 10 CFR Part 50, Appendix B (i.e., vendor is included in the applicant's Approved Vendor List). The

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
		applicant or licensee will need to demonstrate that the HIPS software and associated development life cycle conform to applicable regulatory requirements.
17	3.6.2.4 3.6.2.6.2 3.7.1.4 3.8.1.17	An applicant or licensee referencing this SE must confirm that the HIPS platform equipment is qualified to the applicable regulatory requirements.
18	3.6.2.5 3.7.1.5.1 3.8.1.20	An applicant or licensee referencing this SE must identify the safe states for protective functions and the conditions that require the system to enter a fail-safe state. The applicant or licensee must also demonstrate system qualification for installation and operation in mild environment locations.
19	3.6.2.5 3.7.1.5.1 3.8.1.19 3.8.1.20	An applicant or licensee referencing this SE must confirm that system real-time performance is adequate to ensure completion of protective actions within critical time frames required by the plant safety analyses.
20	3.6.2.6.1 3.8.1.2 3.8.1.16	An applicant or licensee referencing this SE must demonstrate that the full system design, any use of a shared component, the equipment's installation, and the power distribution architecture provide the required independence.
21	3.6.2.6.1 3.8.1.2 3.8.1.16	An applicant or licensee referencing this SE must provide redundant power sources to separately supply the redundant power conversion features within the HIPS platform.
22	3.2.2 3.6.2.6.3.1 3.8.1.1 3.8.1.2 3.8.1.3 3.8.1.8	An applicant or licensee referencing this SE must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety- to nonsafety-related systems.

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
	3.8.1.16	
23	3.6.2.6.3.2 3.6.2.6.4 3.8.1.1 3.8.1.2 3.8.1.16	An applicant or licensee referencing this SE must perform isolation testing on the HIPS platform equipment to demonstrate the capability to satisfy the Class 1E to non-Class 1E isolation requirements, consistent with the guidelines of RG 1.75, Revision 3.
24	3.6.2.7 3.6.3.5	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for testing and calibration of safety-related features.
25	3.6.2.7 3.6.3.5	An applicant or licensee referencing this SE must provide additional diagnostics or testing functions (i.e., self-tests or periodic surveillance tests) to address any system-level failures that are identified as detectable only through periodic surveillance.
26	3.6.2.7 3.6.3.5	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for any automatic sensor cross-check as a credited surveillance test function and the provisions to confirm the continued execution of the automatic tests during plant operations.
27	3.6.2.8.1	An applicant or licensee referencing this SE must describe any manual controls and associated displays used to support manually controlled safety actions necessary to accomplish a safety function for which no automatic control is provided.
28	3.6.2.8.2	An applicant or licensee referencing this SE must describe how the HIPS platform safety system status information is used in displays to provide unambiguous, accurate, complete, and timely status of safety system protective actions.
29	3.6.2.8.3	An applicant or licensee referencing this SE must describe how the HIPS platform bypass status information is used to automatically actuate the bypass indication for bypassed or inoperable conditions, when required, and provide the capability to manually activate the bypass indication from within the control room.

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
30	3.6.2.8.4	An applicant or licensee referencing this SE must describe how the information displays are accessible to the operator and are visible from the location of any controls used to effect a manually controlled protective action provided by the front panel controls of a HIPS-based system.
31	3.6.2.9	An applicant or licensee referencing this SE must provide additional control of access features to address the system-level aspects for a safety system using the HIPS platform.
32	3.6.2.10 3.8.1.13	An applicant or licensee referencing this SE must provide additional diagnostics or testing functions (self-tests or periodic surveillance tests) to address any system-level failures that are identified as detectable only through periodic surveillance. The applicant or licensee must also ensure that failures detected by these additional diagnostics or testing functions are consistent with the assumed failure detection methods of the application-specific single-failure analysis.
33	3.6.2.11	An applicant or licensee referencing this SE must establish the identification and coding requirements for cabinets and cabling for a safety system.
34	3.6.2.12	An applicant or licensee referencing this SE must demonstrate that the application-specific system design implemented with the HIPS platform meets the applicable regulatory requirements for auxiliary features.
35	3.6.2.13	An applicant or licensee referencing this SE must demonstrate that the application-specific system design implemented with the HIPS platform meets the applicable regulatory requirements for shared systems.
36	3.6.2.14	An applicant or licensee referencing this SE must confirm that the HIPS platform equipment meets any specified human factors requirements.
37	3.6.2.15 3.7.1.15	An applicant or licensee referencing this SE must confirm that the HIPS platform equipment meets any specified quantitative or qualitative reliability goals.
38	3.6.3.1 3.6.4.1	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide automatic safety system sense and command features for required safety functions.

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
39	3.6.3.2 3.6.4.2	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide manual safety system sense and command features for required safety functions.
40	3.6.3.3	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for sense and command features to provide protection against the resulting condition of a nonsafety system action that has been caused by a single credible event, including its direct and indirect consequences.
41	3.6.3.4	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to acquire and condition field sensor measurements of the required variables.
42	3.6.3.6 3.6.4.4	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for operating bypasses.
43	3.6.3.7	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for maintenance bypasses and provide the technical specification requirements.
44	3.6.3.8	An applicant or licensee referencing this SE must describe the setpoints, setpoint methodologies, or HIPS platform module accuracies used for a safety system implemented with the HIPS platform equipment.
45	3.6.4.5	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for maintenance bypasses.
46	3.6.5	An applicant or licensee referencing this SE must describe power sources to the HIPS platform equipment and how they meet applicable regulatory requirements.
47	3.7.1.5.2	An applicant or licensee referencing this SE must confirm that the manufacturer followed the same design, development, and iV&V processes for test and calibration functions as for all other HIPS platform functions.

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
48	3.7.1.5.2	An applicant or licensee referencing this SE that relies on a separate computer for the sole verification of test and calibration data should ensure adequate iV&V, configuration management, and quality assurance for the test and calibration functions of the separate computer.
49	3.7.1.5.3	An applicant or licensee referencing this SE must confirm that the manufacturer followed the same design, development, and iV&V processes for self-diagnostics functions as for all other HIPS platform functions.
50	3.7.1.5.3	An applicant or licensee referencing this SE must verify that the manufacturer included the self-diagnostic functions within its type testing of the HIPS platform standardized circuit boards during EQ.
51	3.7.1.5.3	An applicant or licensee referencing this SE must demonstrate that the combination of HIPS platform self-tests and system surveillance testing provide the necessary test coverage to ensure that there are no undetectable failures that could adversely affect a required safety function.
52	3.7.1.6	An applicant or licensee referencing this SE must demonstrate that the full system design, any use of a shared component, the equipment's installation, and the communication bus architecture provide the required independence.
53	3.7.1.6	An applicant or licensee referencing this SE must verify that the safety network provides communications independence and security requirements for communication from safety- to nonsafety-related systems.
54	3.7.1.11	An applicant or licensee referencing this SE must establish the identification and coding requirements for cabinets and components for a safety system and the methods to verify that the correct firmware or software is installed in the correct hardware component.
55	3.8.1.1	An applicant or licensee referencing this SE must demonstrate that a full system design does not, with the exception of division voting logic, depend on any information or resource originating or residing outside its own safety division to accomplish its safety function.

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
56	3.8.1.5	An applicant or licensee referencing this SE must confirm that system real-time performance is adequate, assuming the longest possible completion time to ensure the completion of protective actions within the critical time frames required by the plant safety analyses.
57	3.8.1.12	An applicant or licensee referencing this SE must configure the slave modules to alarm and assume a fail-safe state.
58	3.8.1.18	An applicant or licensee referencing this SE should verify having appropriate physical, logical, and programmatic controls during the system development phases to ensure that unwanted, unneeded, and undocumented functionality is not introduced into digital safety systems.
59	3.8.1.19 3.8.1.20	An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide a deterministic communication structure for required safety functions.
60	3.8.3.1.2	An applicant or licensee referencing this SE must demonstrate that the full system design supports cross-divisional and nonsafety communication with the appropriate independence and isolation.
61	3.8.3.1.3	An applicant or licensee referencing this SE must demonstrate that the application-specific use of an enable nonsafety switch and its configuration details will not adversely affect the channel independence nor the operation of safety-related equipment when the safety-related equipment is performing its safety function. In addition, the applicant or licensee must demonstrate that the application-specific use of an enable nonsafety switch should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.
62	3.9.1 3.9.2	An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide FPGA diversity between redundant portions of the systems to eliminate HIPS platform digital CCF vulnerabilities.
63	3.9.2 3.9.3	An applicant or licensee referencing this SE must address any other digital CCF vulnerabilities in the application-specific D3 analysis.

Table 4-1 HIPS Platform Topical Report Application-Specific Action Items

ASAI No.	SER Referenced Section(s)	Description
64	3.9.3	An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide FPGA diversity between redundant portions of the system architecture (e.g., in each of two redundancies in a four-fold redundant system or in one redundancy in a two-fold redundant system) to ensure HIPS platform safety performance in the presence of a digital CCF.
65	3.9.4	An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide diversity for indication and component control signals to ensure HIPS platform monitoring and control performance in the presence of a digital CCF.

5.0 CONCLUSIONS

The staff determined that the four HIPS platform modules and their design features support meeting the applicable regulatory requirements for plant-specific and application-specific use within safety-related I&C systems when each plant-specific and application-specific use meets the limitations and conditions delineated in Section 4.0 of this SE. The staff determined that the HIPS platform can be used in safety-related systems to provide reasonable assurance of adequate protection of public health, safety, and security based on the evaluation in Section 3.0, which applies the current and applicable regulatory evaluation criteria identified in Section 2.0. On this basis, the staff determined that the HIPS platform is acceptable for use in safety-related I&C systems.

Principal Contributors: Luis Betancourt
 Dinesh Taneja
 Joseph Ashcraft

6.0 REFERENCES

- 6.1-1 Topical Report 1015-18653, "Highly Integrated Protection System Platform," Revision 0, NuScale Power, LLC, Ltd. (NuScale), December 2015 (Agency Document Access and Management Systems (ADAMS) Accession No. ML15363A107).
- 6.1-2 U.S. Nuclear Regulatory Commission (NRC) letter to NuScale, "Acceptance Letter for the Review of Topical Report 1015-18653, 'Highly Integrated Protection System Platform,' Revision 0, (PROJ. 0769)," February 19, 2016 (ADAMS Accession No. ML16048A135).
- 6.1-3 Topical Report 1015-18653, "Design of Highly Integrated Protection System Platform," Revision 1, NuScale, November 4, 2016 (ADAMS Accession No. ML16312A137).
- 6.1-4 NRC letter to NuScale, "NRC Staff's Report for the July 2016 Audit of NuScale's Highly Integrated Protection System (HIPS) Platform (Project 0769)," August 1, 2016 (ADAMS Accession No. ML16208A427).
- 6.1-5 NRC letter to NuScale, "Audit Plan for Factory Acceptance Testing of NuScale Prototype Highly Integrated Protection System Platform (Project 0769)," December 19, 2016 (ADAMS Accession No. ML16351A128).
- 6.1-6 NRC, "Design Specific Review Standard for NuScale Small Modular Reactor Design, Chapter 7—Instrumentation and Controls," U.S. Nuclear Regulatory Commission, Washington, DC, August 5, 2016 (ADAMS Accession No. ML15355A295).
- 6.1-7 U.S. *Code of Federal Regulations* (10 CFR), "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter 1, Title 10, "Energy."
- 6.1-8 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."
- 6.1-9 Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet dated January 30, 1995,
- 6.1-10 IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,"
- 6.1-11 NRC, Staff Requirements Memorandum on SECY-93-087, dated July 21, 1993 (ADAMS Accession No. ML003708056).
- 6.1-12 NRC, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," SECY-93-087, April 2, 1993 (ADAMS Accession No. ML003708021).

- 6.1-13 NRC, "Criteria for Use of Computers In Safety Systems of Nuclear Power Plants," Regulatory Guide (RG) 1.152, Revision 3, July 2011 (ADAMS Accession No. ML102870022).
- 6.1-14 NRC, "Criteria for Safety Systems of Nuclear Power Plants," RG 1.153, Revision 1, Jun 1996 (ADAMS Accession No. ML003740022).
- 6.1-15 NRC, "Criteria for Independence of Electrical Safety Systems," RG 1.75, Revision 3, February 2005 (ADAMS Accession No. ML043630448).
- 6.1-16 NRC, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," NUREG/CR-6303, December 1994 (ADAMS Accession No. ML071790509).
- 6.1-17 NRC, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," DI&C-ISG Interim Staff Guidance-04, Revision 1, (ADAMS Accession No. ML083310185).
- 6.1-18 Association Connecting Electronics Industries standard IPC-6012B, "Qualification and Performance Specification for Rigid Printed Boards."
- 6.1-19 NRC letter to NuScale, "Request for Additional Information Letter No. 3 for the Review of NuScale Topical Report (TR) 1015-18653, 'Highly Integrated Protection System Platform (HIPS),' Rev. 0. (TAC No. RN6110)," June 22, 2016 (ADAMS Accession No. ML16174A464).
- 6.1-20 NuScale letter to NRC, "NuScale Power, LLC Submittal of Response to Request for Additional Information Letter No. 3 for the Review of NuScale Topical Report, TR-1015-18653, 'Highly Integrated Protection System Platform Topical Report,' Revision 0 (TAC No. RN6110)," August 19, 2016 (ADAMS Accession No. ML16235A420).
- 6.1-21 IEEE 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."
- 6.1-22 International Electrotechnical Commission Std. 60950-1: 2005, "Information Technology Equipment—Safety—Part 1: General Requirements."
- 6.1-23 NRC, "Task Working Group #2: Diversity and Defense-in-Depth Issues," DI&C-ISG-02, Revision 2, June 2009 (ADAMS Accession No. ML091590268).
- 6.1-24 IEEE Std. 308-1980, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations."

6.1-25 IEEE/Electronics Industry Association Standard 12207.0-1996, "Standard for Information Technology—Software Life Cycle Processes."

7.0 LIST OF ACRONYMS

ADAMS	Agency Document Access and Management System
ADC	analog-to-digital
APL	actuation and priority logic
ASAI	application-specific action item
BIST	built-in self-testing
CCF	common-cause failure
CFR	<i>Code of Federal Regulations</i>
cm	centimeter(s)
CM	communication module
CRC	cyclic redundancy checksum
CTB	calibration and test bus
D3	diversity and defense in depth
DBE	design-basis event
dc	direct current
DI&C	digital instrumentation and control
DGND	digital ground
DSRS	design-specific review standard
EIM	equipment interface module
EQ	equipment qualification
ESF	engineering safety features
ESFAS	engineering safety features actuation system
FMEA	failure mode and effects analysis
FPGA	field programmable gate array
FSM	finite-state machine
HWM	hardwired module
HIPS	highly integrated protection system
I&C	instrumentation and control
IDI	indication and diagnostic information
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
in.	inch(es)
ISG	interim staff guidance
iV&V	independent verification and validation
LED	light-emitting diode
MIB	monitoring and indication bus
MWS	maintenance workstation
NRC	U.S. Nuclear Regulatory Commission
NPP	nuclear power plant
NVM	nonvolatile memory
NuScale	NuScale Power, LLC
OOS	out of service
OTP	one-time programmable

PCB	printed circuit board
PS	protection system
PTDA	partial trip determination actuation
QA	quality assurance
RAI	request for additional information
RCS	reactor coolant system
RTD	resistance temperature detector
RTS	reactor trip system
SBM	scheduling and bypass module
SDB	safety data bus
SDI	safety display and indication
SE	safety evaluation
SFG	safety function group
SFM	safety function module
SMR	small modular reactor
SR	surveillance requirements
SRAM	static random-access memory
SRM	staff requirements memorandum
Std.	standard
SVM	scheduling and voting module
TMR	triple modular redundant
TR	topical report
TS	technical specification(s)
V&V	verification and validation