



November 4, 2016

Docket: PROJ0769

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

SUBJECT: NuScale Power, LLC Submittal of Topical Report TR-1015-18653, "Design of the Highly Integrated Protection System Platform," Revision 1 (TAC No. RN6110)

REFERENCES:

1. Letter from NuScale Power, LLC to U.S. Nuclear Regulatory Commission, "Highly Integrated Protection System Platform Topical Report," LO-1215-19295, dated December 23, 2015 (ML15363A114).
2. NuScale Topical Report, "Highly Integrated Protection System Platform Topical Report," TR-1015-18653, Revision 0, dated December 2015 (ML15363A115).
3. Letter from U.S. Nuclear Regulatory Commission to NuScale Power, LLC, "Request for Additional Information Letter No. 3 for the Review of NuScale Topical Report (TR) 1015-18653, 'Highly Integrated Protection System Platform (HIPS),' Revision 0 (TAC No. RN6110)," dated June 22, 2016 (ML16174A464).
4. Letter from NuScale Power, LLC to U.S. Nuclear Regulatory Commission, "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)," dated August 19, 2016 (ML16235A261).

In a letter dated December 23, 2015 (Reference 1) NuScale Power, LLC (NuScale) submitted the topical report entitled "Highly Integrated Protection System Platform," Revision 0 (Reference 2). In a letter dated June 22, 2016 (Reference 3), the NRC Staff provided Requests for Additional Information (RAI) regarding the subject topical report. NuScale Power, LLC submitted the response to the RAIs in a letter dated August 19, 2016 (Reference 4). The purpose of this letter is to provide Revision 1 of the NuScale Topical Report, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report." This revision includes the changes proposed in Reference 4.

Enclosure 1 contains the proprietary version of this report. NuScale requests this enclosure be withheld from public disclosure pursuant to 10 CFR § 2.390. The enclosed affidavit (Enclosure 3) supports this request. Enclosure 1 has also been determined to contain Export Controlled Information. This information must be protected from disclosure per the requirements of 10 CFR Part 810. Enclosure 2 is the nonproprietary version of NuScale Topical Report, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," Revision 1.

This letter makes no regulatory commitments and no revisions to any existing regulatory commitments.

Please feel free to contact Jennie Wike at 541-360-0539 or at jwike@nuscalepower.com if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'T. Bergman', written over a circular stamp or seal.

Thomas A. Bergman
Vice President, Regulatory Affairs
NuScale Power, LLC

Distribution: Frank Akstulewicz, NRC, TWFN-6C20
Greg Cranston, NRC, TWFN-6E55
Omid Tabatabai, NRC, TWFN-6E55
Mark Tonacci, NRC, TWFN-6E55

- Enclosure 1: "NuScale Topical Report, TR-1015-18653, Revision 1, 'Design of the Highly Integrated Protection System Platform Topical Report'," proprietary version
- Enclosure 2: "NuScale Topical Report, TR-1015-18653, Revision 1, 'Design of the Highly Integrated Protection System Platform Topical Report'," nonproprietary version
- Enclosure 3: Affidavit, AF-1116-51718

Enclosure 1:

“NuScale Topical Report, TR-1015-18653, ‘Design of the Highly Integrated Protection System Platform Topical Report’, Revision 1” proprietary version

Enclosure 2:

“NuScale Topical Report, TR-1015-18653, ‘Design of the Highly Integrated Protection System Platform Topical Report’, Revision 1” nonproprietary version

Design of the Highly Integrated Protection System Platform

October 2016

Revision 1

Docket: PROJ0769

NuScale Power, LLC

1100 NE Circle Blvd., Suite 200

Corvallis, Oregon 97330

www.nuscalepower.com

© Copyright 2016 by NuScale Power, LLC

COPYRIGHT NOTICE

This document bears a NuScale Power, LLC and Rock Creek Innovations, LLC, copyright notice. No right to disclose, use, or copy any of the information in this document, other than by the U.S. Nuclear Regulatory Commission (NRC), is authorized without the express, written permission of NuScale Power, LLC and/or Rock Creek Innovations, LLC.

The NRC is permitted to make the number of copies of the information contained in these reports needed for its internal use in connection with generic and plant-specific reviews and approvals, as well as the issuance, denial, amendment, transfer, renewal, modification, suspension, revocation, or violation of a license, permit, order, or regulation subject to the requirements of 10 CFR 2.390 regarding restrictions on public disclosure to the extent such information has been identified as proprietary by NuScale Power, LLC, copyright protection notwithstanding. Regarding nonproprietary versions of these reports, the NRC is permitted to make the number of additional copies necessary to provide copies for public viewing in appropriate docket files in public document rooms in Washington, DC, and elsewhere as may be required by NRC regulations. Copies made by the NRC must include this copyright notice in all instances and the proprietary notice if the original was identified as proprietary.

Department of Energy Acknowledgement and Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-NE0000633.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

CONTENTS

Abstract	1
Executive Summary	2
1.0 Introduction	4
1.1 Purpose	4
1.2 Scope	5
1.3 Regulatory Acceptance Criteria	8
1.4 Abbreviations	10
2.0 Highly Integrated Protection System Platform.....	14
2.1 HIPS Chassis	14
2.2 HIPS Module	16
2.3 HIPS Backplane	17
2.4 HIPS Back Panel.....	19
2.5 HIPS Module Types.....	20
2.5.1 Safety Function Module.....	21
2.5.2 Bypass or Trip Operation.....	27
2.5.3 Communication Module.....	32
2.5.4 Equipment Interface Module	35
2.5.5 Hard-Wired Module	43
2.6 Communication Buses	44
2.6.1 Safety Data Bus	45
2.6.2 Monitoring and Indication Bus Protocol.....	47
2.6.3 Calibration and Test Bus Protocol	47
3.0 Representative Protection System Overview.....	48
3.1 Sensors and Detectors	49
3.2 Signal Conditioning	49
3.3 Trip Determination	50
3.4 Data Communication within the Representative Protection System Architecture	52
3.5 Reactor Trip System.....	55
3.6 Engineering Safety Features Actuation System	56
3.7 Protection System Gateway	58

3.8	Maintenance Workstation	58
3.9	Other Potential Architectures.....	59
4.0	Independence	60
4.1	HIPS Platform Grounding	60
4.2	Safety Function Module.....	61
4.3	Communication Modules	64
4.4	Equipment Interface Modules.....	65
4.5	Hard-Wired Module	65
4.6	HIPS Communication	67
4.6.1	Communications Independence within the Platform	67
4.6.2	Communication Independence outside the Platform.....	68
4.7	Monitoring and Indication	69
4.8	Access Control Features	69
5.0	Redundancy.....	72
5.1	Power Supply	72
5.2	Safety Function Module Internal Redundancy.....	72
5.3	Communication Redundancy	73
5.4	Equipment Interface Module Redundancy	73
5.5	Platform Internal Redundancy Summary.....	73
6.0	Diversity	75
6.1	Equipment Diversity	75
6.1.1	Field Programmable Gate Array.....	75
6.2	Design Diversity	77
6.3	Functional Diversity	80
6.3.1	Functional Diversity of a Safety Function Module	80
6.3.2	Functional Diversity of Actuation Priority Logic.....	80
6.4	HIPS Diversity Summary	80
7.0	Repeatability and Predictability	85
7.1	Input Sub-Module	86
7.1.1	Self-Test of the Analog to Digital Converter.....	86
7.2	Safety Function Modules.....	87
7.3	Communication Modules.....	87

7.4	Equipment Interface Modules	89
7.5	Bus Communications	90
7.5.1	Safety Data Bus Communication	90
7.6	HIPS Module Modes	92
7.6.1	Operation Modes	92
7.6.2	Safety Function Module MOD_OK Mode	94
7.6.3	Scheduling and Bypass Module MOD_OK Mode.....	97
7.6.4	Scheduling and Voting Module MOD_OK Mode	100
7.6.5	Equipment Interface Module MOD_OK Mode	103
7.6.6	Safety Data Bus HIPS Bus Frame.....	106
7.7	HIPS Platform Work Cycle	107
7.7.1	Safety Data Work Cycle	107
7.7.2	MIB Work Cycle.....	111
8.0	Calibration, Testing and Diagnostics	113
8.1	Calibration	113
8.2	Testing.....	113
8.2.1	Safety Function Module.....	113
8.2.2	Communication Module.....	115
8.2.3	Equipment Interface Module	115
8.2.4	Communication Buses	119
8.2.5	End-to-End Testing of Entire Platform	121
8.2.6	Built-In Self-Testing	122
8.2.7	Module Testing	123
8.3	Surveillance Requirements	124
8.4	System Diagnostics.....	125
9.0	Simplicity	127
9.1	Independence.....	127
9.2	Diversity.....	127
9.3	Redundancy	128
9.4	Predictability and Repeatability	128
10.0	Summary and Conclusions	129
11.0	References.....	131

Appendix A. IEEE Std. 603-1991 Traceability Matrix.....	133
Appendix B. IEEE Std. 7-4.3.2-2003 Traceability Matrix.....	152
Appendix C. Digital I&C Interim Staff Guidance 04 Traceability Matrix.....	163
Appendix D. SRM for SECY-93-087 Traceability Matrix	201

TABLES

Table 1-1. Abbreviations.....	10
Table 1-2. Definitions.....	13
Table 2-1. HIPS Module	20
Table 2-2. Single SFM in Maintenance Bypass.....	30
Table 2-3. Entire Division in Maintenance Bypass	30
Table 2-4. SFMs in Different Divisions in Maintenance Bypass	31
Table 2-5. Same SFM in Different Divisions in Maintenance Bypass.....	31
Table 2-6. SDB, MIB, and CTB Request and Response Structure	45
Table 6-1. Inherent Differences between FPGA Architecture Choices	76
Table 6-2. Intentional Differences between FPGA Architecture Choices.....	78
Table 6-3. Effects of Digital CCF for HIPS Diversity Strategy	84
Table 7-1. Typical SDB REQUEST and RESPONSE Packet Format	90
Table 7-2. Example Partial Trip Determination Actuation List.....	109
Table 8-1. Output Channel Test (When Contact Is Closed).....	119
Table 8-2. SDB, MIB, and CTB Request and Response Structure	119
Table 8-3. HIPS Module LEDs	125
Table 8-4. HIPS Platform Fault Classification.....	126

FIGURES

Figure 2-1. HIPS Chassis	15
Figure 2-2. Populated HIPS Chassis	16
Figure 2-3. HIPS Module	17
Figure 2-4. HIPS Backplane (Traces Not Shown)	18
Figure 2-5. HIPS Back Panel.....	19
Figure 2-6. Field Cable Connecting to Back Panel Field Connector.....	20
Figure 2-7. Safety Function Module Block Diagram	22
Figure 2-8. SFM Input Sub-Module Blocks	24
Figure 2-9. SFM FPGA Logic Blocks	25
Figure 2-10. SFM Communication	27
Figure 2-11. HIPS Chassis with Trip/Bypass Plate.....	28
Figure 2-12. Receive-Only (Fiber) Configured Communication Module	34
Figure 2-13. Transmit-Only (Fiber) Configured Communication Module	35
Figure 2-14. Equipment Interface Module Block Diagram	36
Figure 2-15. EIM FPGA Blocks	37
Figure 2-16. EIM Hard-Wired Signals Block	38
Figure 2-17. EIM APL Blocks	39
Figure 2-18. EIM Switching Output Blocks	39

Figure 2-19.	Simplified Diagram of a Single EIM Output	41
Figure 2-20.	Two EIMs Driving Two Groups of Field Components	42
Figure 2-21.	Position Feedback Blocks	43
Figure 2-22.	Hard-Wired Module	44
Figure 3-1.	Representative PS Architecture.....	49
Figure 3-2.	Representative Separation Group A Communication Architecture	51
Figure 3-3.	Representative PS Communications Architecture.....	53
Figure 3-4.	Representative RTS (Division I) Communication Architecture	55
Figure 3-5.	Representative ESFAS (Division I) Communication Architecture.....	57
Figure 3-6.	Representative PS Gateway and MWS.....	58
Figure 3-7.	Representative One or Two Division Architecture (One Division Shown)	59
Figure 6-1.	Example Transistor Configuration Comparison	76
Figure 6-2.	Difference between Transistors Used in Flash Cell and SRAM Cell	77
Figure 6-3.	FPGA Equipment Diversity Allocation in a Representative Architecture.....	83
Figure 7-1.	An Analog PS Implementation.....	86
Figure 7-2.	Example of HIPS Bus Topology in a Separation Group	88
Figure 7-3.	Example of HIPS Bus Topology in a Division of RTS or ESFAS	89
Figure 7-4.	Example SDB Master-Slave Transactions.....	91
Figure 7-5.	Module Operational Modes	92
Figure 7-6.	Safety Function Module MOD_OK Mode	96
Figure 7-7.	SBM MOD_OK Mode	99
Figure 7-8.	SVM MOD_OK – Loading 2-out-of-4 Voting Registers.....	101
Figure 7-9.	SVM MOD_OK Mode – 2-out-of-4 Voting and Transfer to EIMs	102
Figure 7-10.	EIM MOD_OK Mode	105
Figure 7-11.	SBM HIPS Bus Frame Cycle.....	106
Figure 7-12.	SVM HIPS Bus Frame Cycle.....	107
Figure 7-13.	Safety Function Group Example.....	108
Figure 7-14.	Timing Diagram for a Representative Architecture	109
Figure 7-15.	MIB-CM Work Cycle	112
Figure 8-1.	Simplified Diagram Is a Single EIM Output	118
Figure 8-2.	Overlap of Testing for the HIPS Platform.....	122

Abstract

This licensing topical report (LTR) presents key design concepts for the highly integrated protection system (HIPS) platform cooperatively developed by Rock Creek Innovations, LLC and NuScale Power, LLC (NuScale). The HIPS platform is a generic digital safety instrumentation and control (I&C) platform devoted to the implementation of safety-related and important-to-safety applications in nuclear power plants. The key design concepts describe how the HIPS platform incorporates the fundamental I&C design principles (i.e., independence, redundancy, diversity and defense-in-depth, and predictability and repeatability) that are outlined in the Nuclear Regulatory Commission (NRC) Design Specific Review Standard for NuScale, as well as important platform functionality, including the capability for test and calibration.

NuScale is requesting NRC's review and approval that the HIPS platform, as presented here, meets the applicable regulatory requirements associated with the fundamental I&C design principles. The LTR demonstrates how the HIPS platform key design concepts meet the fundamental I&C design principles of independence; redundancy; predictability and repeatability; diversity and defense-in-depth. The LTR also describes the testing and diagnostic concepts applied to the HIPS platform and how the key design concepts are implemented to achieve simplicity in the overall HIPS platform design concept. The information in the appendices provides a summary of regulatory conformance of the HIPS platform with the applicable regulatory requirements associated with the fundamental I&C design principles. The appendices also provide a cross reference to the applicable portions of the report where conformance information is presented.

Executive Summary

The highly integrated protection system (HIPS) platform is designed for use in safety-related and important-to-safety applications. This licensing topical report (LTR) presents key design concepts of the HIPS platform. The key design concepts describe how the HIPS platform incorporates the fundamental instrumentation and controls (I&C) design principles outlined in the Nuclear Regulatory Commission (NRC) Design Specific Review Standard for NuScale, as well as important platform functionality, including the capability for test and calibration.

NuScale Power is requesting NRC review and approval that the key design concepts demonstrate that the HIPS platform meets the applicable regulatory requirements associated with the fundamental I&C design principles. The LTR demonstrates how the HIPS platform key design concepts meet the fundamental I&C design principles of independence; redundancy; predictability and repeatability; diversity and defense-in-depth. The LTR also describes the testing and diagnostic concepts applied to the HIPS platform and how the key design concepts are implemented to achieve simplicity in the overall HIPS platform design concept. The information in the appendices provides a summary of regulatory conformance of the HIPS platform with the applicable regulatory requirements associated with the fundamental I&C design principles. The appendices also provide a cross reference to the applicable portions of the report where conformance information is presented.

The HIPS platform is a protection system architecture jointly developed by Rock Creek Innovations, LLC and NuScale Power, LLC. The HIPS platform design concept is based on the fundamental I&C design principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth and was developed specifically to provide a simple and reliable solution for nuclear power plant safety-related and important-to-safety I&C applications. These design principles help contribute to simplicity in both the functionality of the system and in its implementation.

The HIPS platform is a logic based platform that does not utilize software or microprocessors for operation. It is composed of logic implemented using discrete components and field programmable gate array technology. The scope of this report is limited to the HIPS platform, which consists of various components and processing modules.

The platform design was developed to support meeting the guidelines and the requirements of NRC Regulatory Guides (RGs) and Institute of Electrical and Electronics Engineers (IEEE) standards applicable to safety-related applications. The primary reference is RG 1.153, which endorse IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Since the HIPS platform is a programmable digital device, RG 1.152, IEEE Std. 7-4.3.2-2003, Digital I&C Interim Staff Guidance 04, and the Staff Requirements Memorandum for SECY-93-087 were also used to guide the general platform design.

An applicant using the approved HIPS platform topical report can reference the generic approval for all design concepts, as noted in the Appendices. For concepts with full conformance, the applicant will need to demonstrate that the requirements have been implemented. The applicant can reference the generic approval for all design concepts with partial conformance; however, additional application-specific information would be needed to show how these HIPS platform design concepts were implemented in the system design. The applicant would also need to address all other application-specific items that were not reviewed or not approved as part of the HIPS platform topical.

1.0 Introduction

1.1 Purpose

The highly integrated protection system (HIPS) platform is targeted for use in safety-related and important-to-safety applications. This licensing topical report (LTR) presents key design concepts of the HIPS instrumentation and control (I&C) platform. The key design concepts describe how the HIPS platform incorporates the fundamental I&C design principles (i.e., independence, redundancy, predictability and repeatability, and diversity and defense-in-depth) outlined in the Nuclear Regulatory Commission (NRC) Design Specific Review Standard for NuScale as well as important platform functionality including the capability for test and calibration.

NuScale Power, LLC (NuScale) is requesting NRC's review and approval that the HIPS platform key design concepts demonstrate that the HIPS platform

1. internal platform redundancy does not degrade the platform performance; augments the reliability, testability, and fault tolerance of the platform; adequately supports the capability to implement system designs that can satisfy the single failure criterion requirements of Institute of Electrical and Electronics Engineers (IEEE) Std. 603-1991 Clause 5.1 (Reference 11.1.1)
2. configuration capabilities of the HIPS platform components support conformance with application-specific completion of protective action requirements of IEEE Std. 603-1991 Clause 5.2
3. components can accomplish their safety functions under the full range of applicable conditions to support conformance with application-specific system integrity requirements of IEEE Std. 603-1991 Clause 5.5 and meets the system integrity requirements of IEEE Std. 7-4.3.2-2003 Clause 5.5 (Reference 11.1.2)
4. internal platform independence features provide the capability to implement systems designs that can satisfy system independence requirements of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003, Clause 5.6
5. test and calibration concepts adequately support conformance with specific system test and calibration requirements of IEEE Std. 603-1991 Clause 5.7
6. internal platform signal processing and bypass features support conformance with application-specific information display requirements of IEEE Std. 603-1991 Clause 5.8
7. control of access concepts adequately support conformance with application-specific system control of access requirements of IEEE Std. 603-1991 Clause 5.9
8. testing and maintenance features meet the repair requirements of IEEE Std. 603-1991 Clause 5.10

9. firmware identification features meet the identification requirements of IEEE Std. 7-4.3.2-2003, Clause 5.11
10. internal auxiliary support features concepts adequately support conformance with application-specific system auxiliary features requirements of IEEE Std. 603-1991 Clause 5.12
11. adequately provides the capability to implement application-specific automatic control requirements of IEEE 603-1991 Clauses 6.1 and 7.1
12. adequately provides the capability to implement application-specific manual control requirements of IEEE Std. 603-1991 Clauses 6.2 and 7.2
13. configuration capabilities and bypass features of the HIPS platform components support conformance with application-specific sense and command requirements of IEEE Std. 603-1991 Clause 6.3
14. configuration capabilities and deterministic performance features of the HIPS platform components support conformance with application-specific sense and command requirements of IEEE Std. 603-1991 Clause 6.4
15. adequately provides the capability to implement calibration self-testing for the input sub-modules to meet the capability for test and calibration requirements of IEEE Std. 603-1991 Clause 6.5
16. meets the maintenance bypass requirements of IEEE Std. 603-1991 Clauses 6.7 and 7.5
17. adequately supports meeting the completion of protective action requirements of IEEE Std. 603-1991 Clause 7.3
18. adequately provides the capability to implement application-specific logic to meet the Staff Positions of Digital I&C Interim Staff Guidance (DI&C-ISG)-04 (Reference 11.1.3)
19. adequately supports meeting the requirements of Staff Requirements Memorandum (SRM) for SECY-93-087 (Reference 11.1.4)

1.2 Scope

The HIPS platform is a protection system (PS) architecture jointly developed by Rock Creek Innovations, LLC and NuScale. The HIPS platform is based on the fundamental I&C design principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth and was developed specifically to provide a simple and reliable solution for nuclear power plant safety-related and important to safety I&C applications. These HIPS platform key design concepts help contribute to simplicity in both the functionality of the system and in its implementation.

The HIPS platform is a logic-based platform that does not utilize software or microprocessors for operation. It is composed of logic implemented using discrete components and field programmable gate array (FPGA) technology.

The scope of this report is limited to the HIPS platform, which consists of the following components:

- HIPS chassis
- HIPS backplane
- HIPS back panel
- safety function modules (SFMs)
- communication modules (CMs)
- hard-wired module (HWM)
- equipment interface modules (EIMs)

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 only included to support the discussion on monitoring/indication, testing, and calibration.

The focus of this report is on how the HIPS platform utilizes the fundamental key design concepts to support meeting the regulatory guidelines (Section 1.3) that are specific to the following fundamental design principles:

- independence
- redundancy
- diversity
- predictability and repeatability

The LTR also describes the testing and diagnostics concepts applied to the HIPS platform and how the key design concepts are implemented to achieve simplicity in the overall HIPS platform design concept.

In addition to the design concepts, other topics that are addressed include:

- theory of operation
- signal path independence
- functional independence
- communication
- access control features
- operational/failure modes (states)
 - startup
 - normal operation

- failure state
- testing
 - self-testing/diagnostics
 - periodic testing
 - fault detection and response
- monitoring and indication
- maintenance

This LTR provides the platform details and design requirements that are needed to verify that the fundamental I&C design principles have been satisfactorily implemented and the platform requirements are sufficient to meet the applicable regulatory guidelines. This LTR is the summary licensing document for the HIPS platform and is organized as follows:

- Section 1, Introduction – Describes the purpose, scope, and regulatory acceptance criteria for the review of the HIPS platform.
- Section 2, Highly Integrated Protection System Platform – Describes the basic HIPS platform hardware and communication bus design concepts. The key design concepts for the HIPS platform are implemented by the HIPS platform hardware.
- Section 3, Representative Protection System Overview – Describes typical applications of the HIPS platform as a protection system (PS). The architectures described are provided for reference to help describe the attributes of the HIPS platform and how it could be used in an application. It is not expected that the NRC approve these representative architectures in this LTR.
- Section 4, Independence – Describes the HIPS platform design concepts that address the fundamental design principle of independence. The grounding concepts for the platform are described. The independence concepts implemented on the individual HIPS platform modules are described. The communication independence concepts are described. The isolation concepts used to support monitoring and indication features and provide access control are described.
- Section 5, Redundancy – Describes the HIPS platform design concepts that address the fundamental design concepts of redundancy, as well as the platform redundancy features associated with power converters, safety function and equipment interface modules, and communication buses.
- Section 6, Diversity – Describes the HIPS platform design concepts that address the fundamental design principle of diversity. The platform design concepts associated with equipment diversity, design diversity, and functional diversity are described.

- Section 7, Repeatability and Predictability – Describes the HIPS platform design concepts that address the fundamental design principle of repeatability and predictability. The platform design concepts associated with repeatable and predictable platform behavior for each HIPS platform module and associated communication buses are described. The section also describes the HIPS platform operational modes and transitions and the standard HIPS platform work cycle and how they provide repeatable and predictable platform operation.
- Section 8, Testing and Diagnostics – Describes the calibration and testing of the HIPS platform from the inputs to the outputs using self-testing in the individual modules and traditional surveillance testing and calibration.
- Section 9, Simplicity – Describes how simplicity has been considered throughout the development of the key design concepts of the HIPS platform that address the fundamental principles: independence, redundancy, diversity, and repeatability and predictability.
- Section 10, Summary and Conclusion – Provides an overall summary and conclusion for the LTR.
- Section 11, References – Lists the reference documents for the LTR.
- Appendix A, IEEE Std. 603-1991 Traceability Matrix – This appendix provides a summary of the regulatory conformance of the HIPS platform with IEEE Std. 603-1991 and a cross reference of applicable portions of the report where conformance information is presented.
- Appendix B, IEEE Std. 7-4.3.2-2003 Traceability Matrix - This appendix provides a summary of the regulatory conformance of the HIPS platform with IEEE Std. 7-4.3.2-2003 and a cross reference of applicable portions of the report where conformance information is presented.
- Appendix C, Interim Staff Guidance 04 Traceability Matrix - This appendix provides a summary of the regulatory conformance of the HIPS platform with D&IC-ISG-04 and a cross reference of applicable portions of the report where conformance information is presented.
- Appendix D, SRM for SECY-93-087 - This appendix provides a summary of the regulatory conformance of the HIPS platform with SRM for SECY-93-087 and a cross reference of applicable portions of the report where conformance information is presented.

1.3 Regulatory Acceptance Criteria

The platform design was developed to support meeting the requirements and guidelines applicable to safety-related applications. The primary reference is RG 1.153 (Reference 11.1.5), which endorses IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Since portions of the HIPS platform are programmable digital devices, RG 1.152 (Reference 11.1.6), IEEE Std. 7-4.3.2-

2003, DI&C-ISG-04, and the Staff Requirements Memorandum for SECY-93-087 were also used to guide the general platform design.

The following NRC documents contain the regulatory acceptance criteria applicable to the review of the HIPS platform key design concepts:

- Regulatory Guide 1.153, Revision 1, “Criteria for Safety Systems” – The regulatory position in Section C states that conformance with the requirements of IEEE Std. 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations” (including the correction sheet dated January 30, 1995), provides a method acceptable to the NRC staff for satisfying the Commission’s regulations with respect to design, reliability, qualification, and testability of the power, instrumentation, and controls portion of nuclear power plants.
- Regulatory Guide 1.152, Revision 3, “Criteria for use of Computers in Safety Systems of Nuclear Power Plants” – The regulatory position stated in Section C.1 that conformance with the requirements of IEEE Std. 7-4.3.2-2003 is a method that the NRC staff has deemed acceptable for satisfying the NRC’s regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants. The NRC does not endorse Annexes B-F of IEEE Std. 7-4.3.2-2003.
- DI&C-ISG-04, Revision 1, “Task Working Group #4: Highly Integrated Control Rooms – Communications Issues (HICRc) Interim Staff Guidance” – This interim staff guidance (ISG) addresses the design and review of digital systems proposed for safety-related service in nuclear power plants. This guidance addresses selected digital aspects of such systems. Such systems are also subject to requirements germane to safety-related systems, such as requirements for separation, independence, and electrical isolation. Additional guidance applicable to such systems is provided in various other NRC and industry documents. This ISG provides acceptable methods for addressing HICRc in digital I&C system designs. This ISG also clarifies the criteria the staff uses to evaluate whether an applicant/licensee digital system design is consistent with HICRc guidelines.
- SRM for SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs” – The SRM provides direction in Section II.Q for the defense against common mode failures in digital I&C systems. Specifically, Point 1 requires defense-in-depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.

The Information in the appendices provides a summary of regulatory conformance of the HIPS platform with the applicable regulatory requirements associated with the fundamental I&C design principles. The appendices also provide a cross reference to the applicable portions of the report where conformance information is presented.

1.4 Abbreviations

Table 1-1. Abbreviations

Term	Definition
ADC	analog-to-digital converter
ALWR	advanced light water reactor
ANSI	American National Standards Institute
APL	actuation and priority logic
ASME	American Society of Mechanical Engineers
BIST	built-in self-testing
CCF	common cause failure
CFR	Code of Federal Regulation
CM	communication module
CRC	cyclic redundancy checksum
CS	control system
CTB	calibration and test bus
D3	diversity and defense-in-depth
DC	direct current
DI&C	digital instrumentation and control
DTR	digital time response
EIA	Electronics Industries Association
EIM	equipment interface module
ESD	electrostatic discharge
ESF	engineered safety feature
ESFAS	engineered safety feature actuation system
FMEA	failure modes and effects analysis
FPGA	field programmable gate array
HICRc	highly integrated control rooms – communications
HIPS	highly integrated protection system
Hp	high side (primary)
Hs	high side (secondary)
HWM	hard-wired module
I&C	instrumentation and controls
ID	identification
IDI	indication and diagnostic information
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPC	Association Connecting Electronics Industries (formerly Institute for Printed Circuits)
ISG	Interim Staff Guidance
iV&V	independent verification and validation
JTAG	joint test action group
LED	light emitting diode
Lp	low side (primary)

Term	Definition
Ls	low side (secondary)
LTR	Licensing topical report
mA	milliampere
Mbps	megabits per second
MIB	monitoring and indication bus
MIB-CM	MIB communication module
MOSFET	metal–oxide–semiconductor field-effect transistor
MSB	most significant bit
MWS	maintenance workstation
N/A	not applicable
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
NUPIC	Nuclear Procurement Issues Committee
NVM	non-volatile memory
OOS	out-of-service
OTP	one-time programmable
PCB	printed circuit board
PS	protection system
PTDA	partial trip determination actuation
PZR	pressurizer
QA	quality assurance
RCS	reactor coolant system
RG	regulatory guide
RTD	resistance temperature detector
RTS	reactor trip system
SBM	scheduling and bypass module
SC/TD	signal conditioning and trip determination
SDB	safety data bus
SDI	safety display and indication
SECY	Secretary of the Commission, Office of the (NRC)
SFG	safety function group
SFM	safety function module
SLV	slave
SRAM	static random-access memory
SVM	scheduling and voting module
TCK	test clock
TDA	trip determination actuation
TDI	test data in
TDO	test data out
TIA	Telecommunications Industry Association
{{ }} ^{2(a),(c),(e)-ECI}	{{ }} ^{2(a),(c),(e)-ECI}
TRST	test reset
TVS	transient-voltage-suppression
V	volt

Term	Definition
V _{DC}	volt (direct current)
V _{RMS}	volt (root mean square)
V&V	verification and validation
VFC	valve fully closed
VFO	valve fully open
XooY	X-out-of-Y (e.g., 2oo3 is 2-out-of-3)
μs	microsecond

Table 1-2. Definitions

Term	Definition
fundamental I&C design principle	fundamental I&C design principles have been defined by the Nuclear Regulatory Commission (NRC) in the NRC Design Specific Review Standard for NuScale as independence; redundancy; diversity and defense-in-depth; repeatability and predictability.
hard failure	An error occurrence in a computer system that is caused by the failure of a memory chip. Hard errors can appear like chip-level soft errors, but the difference is that the hard error is not rectified when the computer is rebooted. The solution to a hard error is to replace the memory chip or module entirely.
key design concepts	HIPS platform design concepts that are used to address the NRC's fundamental I&C design principles.
module	any assembly of interconnected components that constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics that permit it to be tested as a unit. A module can be a card, a drawout circuit breaker, or other subassembly of a larger device, provided it meets the requirements of this definition.
multidrop	a bus in which all components are connected to the electrical circuit
single event upset	a change of state caused by one single ionizing particle (ions, electrons, photons...) striking a sensitive node in a micro-electronic device, such as in a microprocessor, semiconductor memory, or power transistors
software CCF	A failure caused by software errors or software developed logic that could defeat the redundancy achieved by hardware architecture
versatile	Fundamental building block of an FPGA that consists of logic cells (e.g., latch with clear or set, D-flip-flop with clear or set). Versatiles are configured and interconnected, as needed, for a given application.

2.0 Highly Integrated Protection System Platform

The HIPS platform is designed to provide a robust platform for safety-related and important-to-safety functions within the commercial nuclear power plant industry. The HIPS platform provides a system of modules that are interchangeable between chassis. The platform is designed to work with different module types configured to the individual application where multiple chassis can be connected to create a larger system if needed. {{

}}^{2(a),(c),(e)-ECI} The different HIPS modules and platform inputs and outputs are connected to each other through the backplane and back panel of the chassis.

2.1 HIPS Chassis

The HIPS chassis is an industry standard 19 inch cabinet mountable card frame, as shown in Figure 2-1. The HIPS chassis is 10.5 inches tall and 15.75 inches deep. The individual HIPS modules slide in from the front providing a seamless “face plate” across the front. All permanent cabling and connectors are made on the HIPS back panel. This ensures the front view of the populated HIPS chassis is clean and not cluttered with wiring. Figure 2-2 shows a populated HIPS chassis.

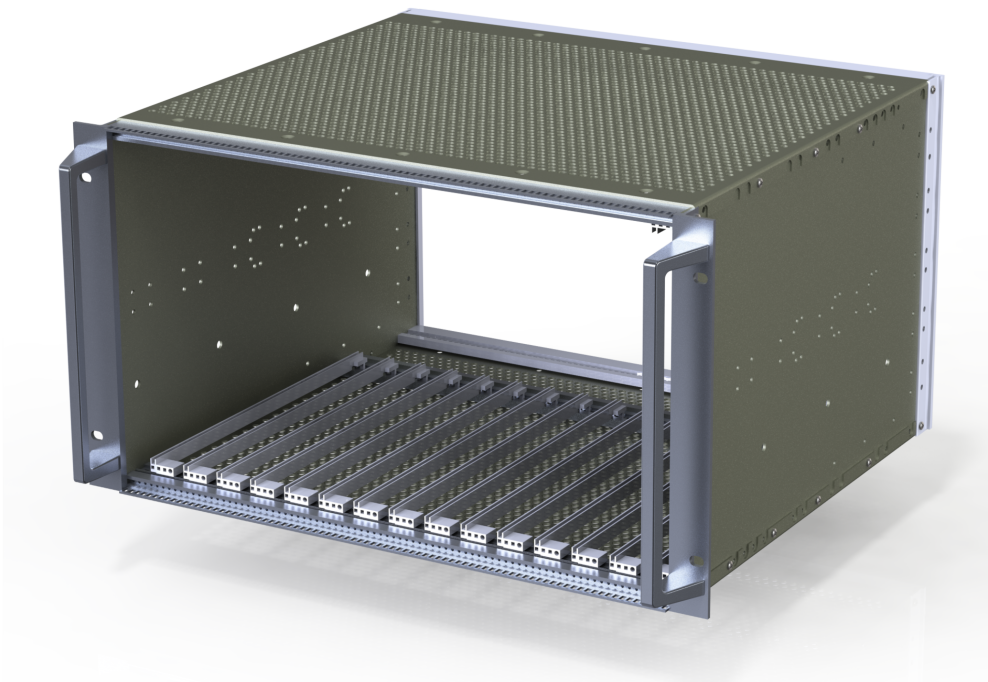


Figure 2-1. HIPS Chassis

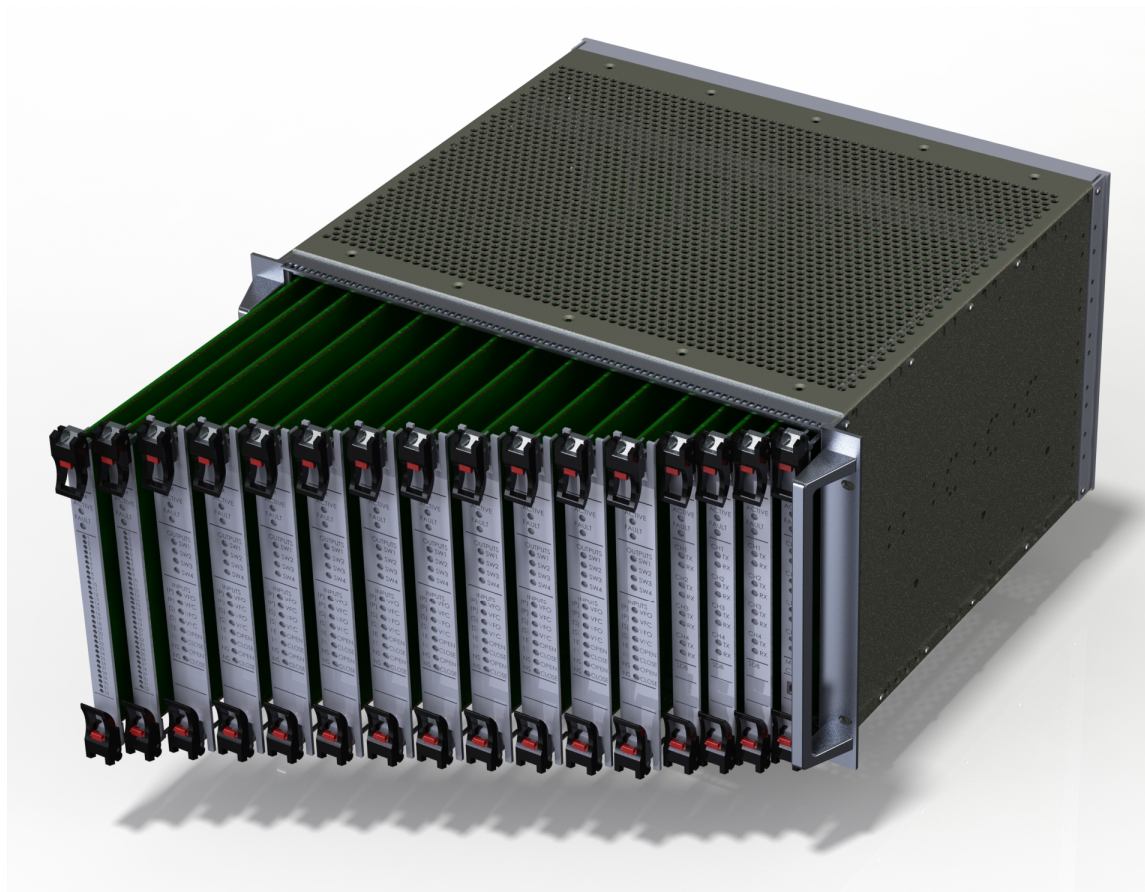


Figure 2-2. Populated HIPS Chassis

2.2 HIPS Module

The HIPS module represents a line-replaceable unit. The HIPS module consists of a base printed circuit board (PCB), a set of rear connectors, front panel, and electronic components. In some modules, additional sub-modules may be mounted to the base board (see Section 2.5.1.1). 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, etc.).

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. Self-tests are performed to assure the HIPS module is inserted in the correct location (see Section 8.2.7). Figure 2-3 shows a

HIPS module with no components mounted on the base PCB. The purpose of this image is to show the injector/ejector latches, the front panel, and the base PCB with the connectors mounted on the rear of the PCB.



Figure 2-3. HIPS Module

2.3 HIPS Backplane

The HIPS backplane is a PCB with female connectors and copper traces that is shown without traces in Figure 2-4. There are no active components on a HIPS backplane.



Figure 2-4. HIPS Backplane (Traces Not Shown)

The quantity and location of female connectors along with traces on the HIPS backplane are unique to each HIPS platform implementation. There are three types of signals that are traced on the backplane:

- power and grounding signals
- communication signals
- hard-wired module signals

The HIPS backplane is mounted at the rear of the HIPS chassis to provide 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. This is done when the number of HIPS modules exceeds the capacity of a single HIPS chassis.

The HIPS backplane is designed using Association Connecting Electronics Industries standard IPC-6012B (Reference 11.1.7).

2.4 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. Figure 2-5 shows a cutaway of a HIPS chassis with the HIPS backplane mounted to the HIPS back panel as well as an external connector. Figure 2-6 shows the field cable connections to back panel field connector that connects to the backplane.

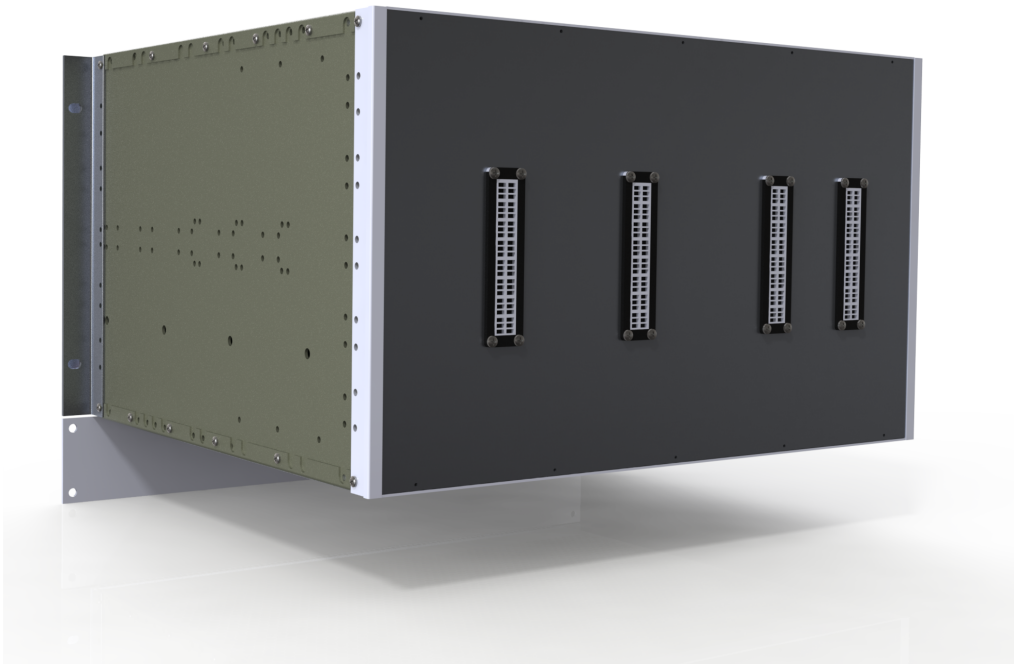


Figure 2-5. HIPS Back Panel

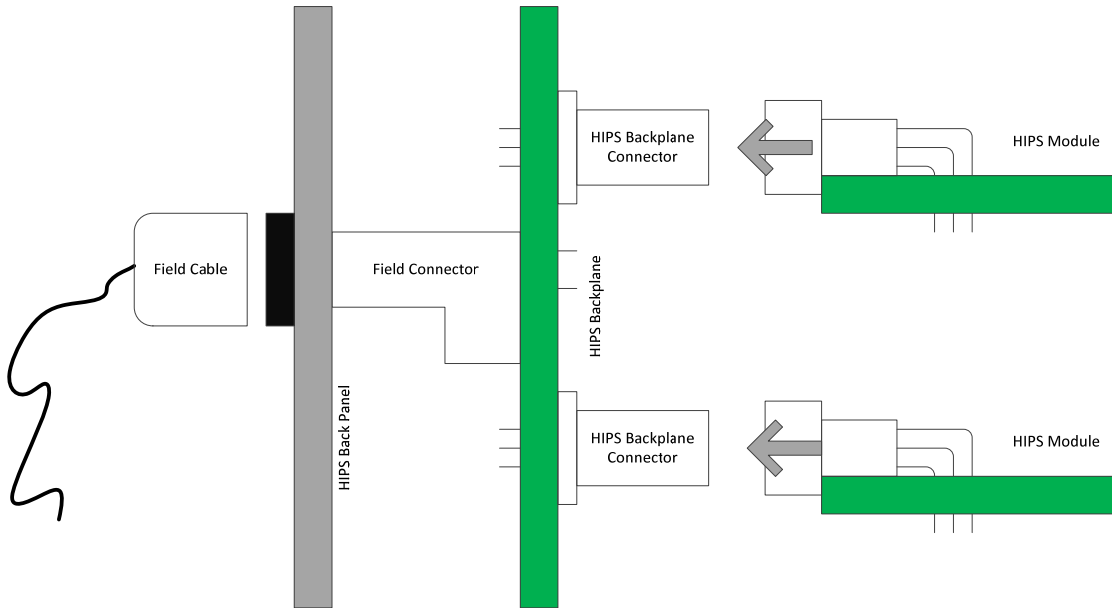


Figure 2-6. Field Cable Connecting to Back Panel Field Connector

2.5 HIPS Module Types

The HIPS platform includes four different HIPS modules capable of performing dedicated functions. Table 2-1 provides a list of the four HIPS modules.

Table 2-1. HIPS Module

Name	Acronym	Description/Use
Safety Function Module	SFM	Responsible for signal conditioning and actuation of safety function(s) from input signals. Provides scaled value of input process to nonsafety controls and safety display for monitoring purposes.
Communications Module	CM	Responsible for controlling, collecting, and transmitting information between HIPS modules or to external components.
Equipment Interface Module	EIM	<p>{{</p> <p>}}^{2(a),(c),(e)}-ECI Provides final equipment actuation output and includes priority logic circuitry for automatic and manual actuation inputs.</p>

Name	Acronym	Description/Use
Hard-Wired Module	HWM	The HWM converts hard-wired contact inputs into logic levels for direct connection on dedicated backplane traces to particular module as per the detail application design.

{{

}}2(a),(c),(e)-ECI

2.5.1 Safety Function Module

{{

}}2(a),(c),(e)-ECI

4. {{

}}2(a),(c),(e)-ECI

Figure 2-7. Safety Function Module Block Diagram

As described in Section 3.8, the safety function must be out of service, either in bypass or trip, and a temporary cable between the MWS and the MIB communication module (MIB-CM) is required to allow changing of any parameters. The MWS is used to update setpoints and tunable parameters in the SFMs when the safety function is out of service. Physical and logical controls are put in place to prevent modifications to a safety channel when it is being relied upon to perform a safety function. A temporary cable and OOS switch 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, an indication is

provided by the HIPS platform that can be used to drive an alarm in the main control room to inform the operator. Adjustments to parameters are performed in accordance with plant operating procedures, including any that establish the minimum number of redundant safety channels that must remain operable for the current operating mode and conditions.

The communication from the MWS to the SFMs to update setpoints and tunable parameters uses a message format that includes the address of a single SFM. The load switch on the front of the SFM allows loading the NVM parameters when they are changed while the SFM is out of service. These features only allow the update of a single SFM at a time.

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 define specific limitations on the use of maintenance bypasses.

2.5.1.1 Input Sub-Module

The input sub-module consists of a signal conditioning circuit, analog to digital converter (ADC), and a serial interface.

Each SFM can handle up to four input sub-modules (i.e., separate smaller PCBs that are mounted to the base board) and the input type can be any combination of standard analog signals (e.g., resistance temperature detector (RTD), thermocouple, 4-20 milliampere (mA), 10-50 mA, 0-10 Volt (V)). The HIPS platform input sub-module can accept inputs from digital sensors that are transmitted as analog signals (e.g., voltage or current signal loop or binary input signals). The HIPS platform is not designed to decode or use the digital signal superimposed on top of the conventional analog signal by a "smart" device or transmitter.

The HIPS platform can process nonsafety-related inputs to the protection system, as described in Section 4.2. The SFM input sub-module blocks are shown in Figure 2-8.

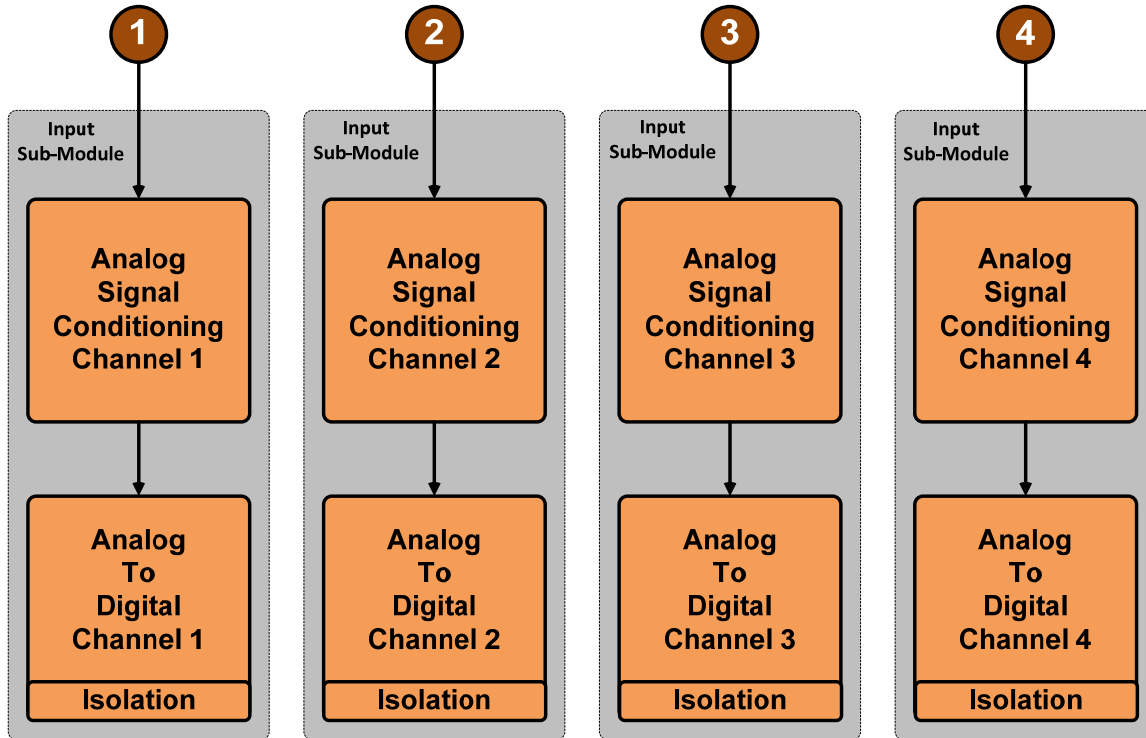


Figure 2-8. SFM Input Sub-Module Blocks

2.5.1.2 Safety Function Module Logic Functions

{{

}}^{2(a),(c),(e)-ECI}

{{

}}2(a),(c),(e)-ECI

Figure 2-9. SFM FPGA Logic Blocks

2.5.1.3 Communication Engine

{{

}}2(a),(c),(e)-ECI

Each communication engine is connected to an RS-485¹ 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. The SFM communication blocks are shown in Figure 2-10.

However, while physically configured in a multi-drop 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. Additional information on the request and response packet can be found in Section 2.6.1.2.

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.

¹ The RS-485 standard was originally developed by the Electronics Industries Association (EIA). EIA has disbanded and the standard is now maintained by the Telecommunications Industry Association (TIA) as the TIA-485 standard; however, RS-485 is still a common term used to refer to this standard. This report uses the common term.

}}

}}2(a),(c),(e)-ECI

Figure 2-10. SFM Communication

2.5.2 Bypass or Trip Operation

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 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, as discussed in Section 7.6.3. 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 out of service. It also provides the appropriate alarm output. The decision to put a channel in either bypass or trip is specific to the application.

The bypass or trip operation is implemented for each SFM on a plate below the chassis with the SFMs, as shown in Figure 2-11. Any time an SFM module is placed in an out of service condition, the module that is master to the SFM reads the state of the trip or bypass switch to determine if the SFM channel should be bypassed or treated as a trip when continuing the flow of data through the system.



Figure 2-11. HIPS Chassis with Trip/Bypass Plate

The trip/bypass features are illustrated by the following example:

Division A			
SFM	SFM Trip/Bypass Switch Position	Input(s)	Safety Function
1	Bypass	Power range flux signal	<ul style="list-style-type: none"> Reactor trip on high power

2	Bypass	Containment pressure	<ul style="list-style-type: none"> • Reactor trip on high containment pressure • Decay heat removal actuation on high containment pressure • Containment isolation on high containment pressure
3	Bypass	Steam pressure Steam temperature	<ul style="list-style-type: none"> • Reactor trip on high steam pressure • Reactor trip on low steam pressure • Reactor trip on high steam superheat • Decay heat removal actuation on high steam superheat • Decay heat removal actuation on high steam pressure • Decay heat removal actuation on low steam pressure
4	Trip	Pressurizer pressure	<ul style="list-style-type: none"> • Reactor trip on high pressurizer pressure

If an SFM has only one safety function, that function could be individually bypassed or tripped when that SFM out of service switch is activated (i.e., SFM #1 or SFM #4).

If an SFM has more than one safety function, it is not possible to trip/bypass only one of those functions when that SFM out of service switch is activated. For example, it is not possible to only trip or bypass 'Reactor Trip on High Containment Pressure' on SFM #2 when the SFM #2 out of service switch is activated. Instead, all of the SFM #2 safety functions are placed into maintenance bypass when the SFM #2 out of service switch is activated. Assuming that only the SFM #2 out of service switch is activated, all of the other functions in SFM #1, SFM #3, and SFM #4 are available for that division.

The number of safety divisions determines how the application-specific implementation meets the single-failure criterion even with portions of the system in maintenance bypass. For example, a two-out-of-four voting scheme has a relatively simpler method of satisfying the single-failure criterion with portions of the system in maintenance bypass.

Because individual SFMs can be placed into maintenance bypass, Table 2-2 shows SFM #2 in Division A taken to maintenance bypass (shown in yellow). If the failure of all SFMs in Division C is assumed (shown in red), there are still enough SFMs for a minimum two-out-of-four coincidence vote.

Table 2-2. 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

If it is assumed that all of the SFMs in Division A are taken into maintenance bypass (shown in yellow) and all of Division C SFMs fail (shown in red), there are still at least two SFMs available for a minimum two-out-of-four vote, as shown in Table 2-3.

Table 2-3. 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

As long as the same SFM across more than one division is not taken to maintenance bypass (shown in yellow), multiple SFMs can be placed out of service across different divisions and still satisfy the single-failure criterion, as shown in Table 2-4.

Table 2-4. 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

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. Without such administrative controls, the application-specific implementation would not be able to satisfy the single-failure criterion, as shown in Table 2-5.

Table 2-5. 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

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 forced trip input from the OOS switch, an additional trip input on any of the other divisions results in actuation (e.g., one-out-of-three of the remaining divisions). With a bypass input, a trip input on two of the other divisions results in actuation (e.g., two-out-of-three of the remaining divisions).

The typical plant technical specifications require plant operators to put plant protection system channels in the trip condition or allow protection system channels to be put in bypass. The HIPS platform OOS and trip/bypass switch allows a system to be configured to comply with either of these technical specifications requirements.

2.5.3 Communication Module

The CM is a base module that supports inter- and intra-divisional data communication.

The CM also supports hard-wired signal inputs via logic level backplane signals from the HWM. If used, these hard-wired signals are connected directly from the HWM within the same chassis or connected chassis.

The basic CM is composed of the following circuits:

- FPGA
 - scheduling and communication logic
 - indication and diagnostic information
 - CM logic functions
- hard-wired signals
- communication physical layers

The CM utilizes an FPGA device to implement the logic circuits based on the specific functions the CM performs. The logic implemented in the FPGA includes the scheduling logic, any functions that the CM is to perform, and IDI logic circuits.

{{

}}^{2(a),(c),(e)-EC}

{{

}}2(a),(c),(e)-ECI

{{

}}2(a),(c),(e)-ECI

Figure 2-12. Receive-Only (Fiber) Configured Communication Module

{{

}}2(a),(c),(e)-ECI

Figure 2-13. Transmit-Only (Fiber) Configured Communication Module

The use of the CMs in a representative system context is illustrated in Section 3.

2.5.4 Equipment Interface Module

The EIM is the final actuating device of the HIPS platform and is composed of the following functions as shown in Figure 2-14.

{{

}}2(a),(c),(e)-ECI

Figure 2-14. Equipment Interface Module Block Diagram

The EIM is composed of the following circuits:

- FPGA block

– {{

}}2(a),(c),(e)-ECI

- hard-wired signals logic
- actuation and priority logic (APL)
- switching output
- position feedback

2.5.4.1 FPGA Block

{{

}}^{2(a),(c),(e)-ECI}

Figure 2-15. EIM FPGA Blocks

{{

}}^{2(a),(c),(e)-ECI}

2.5.4.2 Hard-wired Signals Logic

Similar to the hard-wired signal circuit on a CM, hard-wired signals from the back panel that originate from the HWM (See Section 2.5.5) are distributed to the primary and secondary APL, as shown in Figure 2-16.

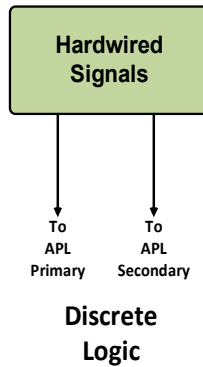


Figure 2-16. EIM Hard-Wired Signals Block

2.5.4.3 Actuation and Priority Logic

{{

}}2(a),(c),(e)-ECI

{{

}}2(a),(c),(e)-ECI

Figure 2-17. EIM APL Blocks

2.5.4.4 Switching Output

{{

}}2(a),(c),(e)-ECI

Figure 2-18. EIM Switching Output Blocks

{{

}}2(a),(c),(e)-ECI

{{

}}^{2(a),(c),(e)}-ECI

Figure 2-19. Simplified Diagram of a Single EIM Output

{{

}}^{2(a),(c),(e)}-ECI

{{

}}2(a),(c),(e)-ECI

Figure 2-20. Two EIMs Driving Two Groups of Field Components

2.5.4.4.1 Position Feedback

The position feedback block consists of inputs from the field component (e.g., valve fully open (VFO), valve fully closed (VFC), breaker closed/open). This equipment feedback is utilized for indication of the component position for the operator and for determining 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, as shown in Figure 2-21. The position feedback can also be fed into the HWM to be used in other modules as needed for some specific applications.



Figure 2-21. Position Feedback Blocks

2.5.5 Hard-Wired Module

The HWM is a module that receives signals from the manual switches in the main control room and the trip/bypass switch panel, as shown in Figure 2-22. 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:

- trip/bypass (each redundant SFM)
- manual actuation (main control room)
- enable nonsafety control (main control room)
- operational overrides (main control room)
- non-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.

There is also a trip/bypass switch for each SFM (see Section 2.5.2) that is located in the cabinet containing the HIPS chassis. The switches are connected to the HWM that places the trip or bypass position on the backplane of the chassis for the CMs.

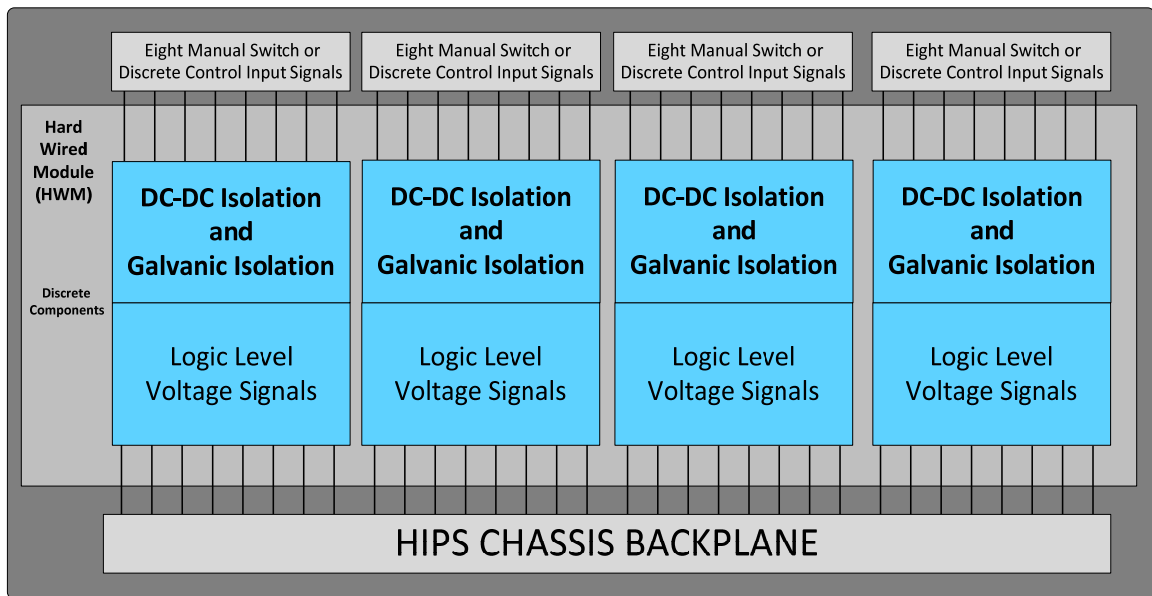


Figure 2-22. Hard-Wired Module

2.6 Communication Buses

{{

}}2(a),(c),(e)-ECI

2.6.1 Safety Data Bus

2.6.1.1 Safety Data Path Bus Architecture

{{

}}^{2(a),(c),(e)-ECI}

2.6.1.2 Safety Data Path Packet Contents

{{

}}^{2(a),(c),(e)-ECI}

Table 2-6. SDB, MIB, and CTB Request and Response Structure

{{

}}^{2(a),(c),(e)-ECI}

2.6.1.3 Safety Data CRC Algorithm

{{

}}^{2(a),(c),(e)-ECI}

2.6.1.4 Safety Data Bus Self-Test

{{

}}^{2(a),(c),(e)-ECI}

2.6.1.5 Safety Data Bus Protocol

{{

}}2(a),(c),(e)-ECI

2.6.2 Monitoring and Indication Bus Protocol

{{

}}2(a),(c),(e)-ECI

2.6.3 Calibration and Test Bus Protocol

{{

}}2(a),(c),(e)-ECI

3.0 Representative Protection System Overview

This section provides a typical application of the HIPS platform as a protection system. The architecture described is provided for reference to help describe the attributes of the HIPS platform and how it could be used in an application. NuScale does not seek NRC approval of this representative architecture with this LTR.

The primary purpose of the representative PS is to provide automatic actuation signals, manual actuation and control signals, and monitoring display information to mitigate the consequences of off-normal conditions. The design basis of the PS is to automatically actuate the reactor trip system (RTS) and/or the engineered safety feature actuation system (ESFAS) whenever it is necessary to

- prevent core damage from an anticipated transient
- limit core damage from infrequent faults
- preserve the integrity of the reactor coolant pressure boundary during limiting fault conditions
- limit site radiological releases to acceptable limits

The PS monitors process variables that are directly related to equipment mechanical limitations such as pressurizer pressure and water level, and variables that directly affect the heat transfer capability of the reactor, such as reactor coolant flow and temperatures. Upon coincidence that multiple redundant directly measured process variables or calculated variables exceed setpoints, the reactor is shut down to protect against damage to the fuel cladding or loss of system integrity that could lead to the release of radioactive fission products. The ESFAS actuates various equipment that perform protective actions to mitigate the consequences of postulated accidents.

{{

}}2(a),(c),(e)-ECI

{

}}2(a),(c),(e)-ECI

Figure 3-1. Representative PS Architecture

3.1 Sensors and Detectors

Redundant sets of sensors and detectors feed each separation group and provide inputs to the signal conditioning block. The interconnections of the process sensors and neutron flux detectors to the signal conditioning block are dedicated copper wires.

3.2 Signal Conditioning

The signal conditioning function is composed of input sub-modules that are part of the SFM and is responsible for conditioning, measuring, filtering, and sampling field inputs. Each input module is dedicated to a specific input type (e.g., resistance temperature detector (RTD), thermocouple, 4-20 mA, 10-50 mA, 0-10 V).

A signal conditioning function is composed of an analog circuit and a digital circuit. The analog circuit is responsible for converting analog voltages or currents into a digital representation.

The digital portion performs all input module control, sample and hold filtering, integrity checks, self-testing, and digital filtering functions.

The digital representation of the process sensor signal is communicated from the signal conditioning block to the trip determination block using a serial interface.

3.3 Trip Determination

{{

}}^{2(a),(c),(e)-ECI}

{{

}}2(a),(c),(e)-ECI

Figure 3-2. Representative Separation Group A Communication Architecture

{{

}}2(a),(c),(e)-ECI

3.4 Data Communication within the Representative Protection System Architecture

{{

}}2(a),(c),(e)-ECI

{

}}2(a),(c),(e)-ECI

Figure 3-3. Representative PS Communications Architecture

{{

}}2(a),(c),(e)-ECI

3.5 Reactor Trip System

{{

}}2(a),(c),(e)-ECI

Figure 3-4. Representative RTS (Division I) Communication Architecture

{{

}}2(a),(c),(e)-ECI

{{

}}^{2(a),(c),(e)}-ECI

3.6 Engineering Safety Features Actuation System

{{

}}^{2(a),(c),(e)}-ECI

{{

}}2(a),(c),(e)-ECI

Figure 3-5. Representative ESFAS (Division I) Communication Architecture

{{

}}2(a),(c),(e)-ECI

3.7 Protection System Gateway

{{

}}^{2(a),(c),(e)-ECI}

Figure 3-6. Representative PS Gateway and MWS

{{

}}^{2(a),(c),(e)-ECI}

3.8 Maintenance Workstation

Each division of PS 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 is connected through the PS gateway for its division and is 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 out of service. Physical and logical controls are put in place to prevent modifications to a safety channel when it is being relied upon to perform a safety function. A temporary cable and OOS switch 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, an indication is provided by the HIPS platform that can be used to drive an alarm in the main control room to inform the operator. Adjustments to parameters are performed in accordance with plant operating procedures, including any that establish the minimum number of redundant safety channels that must remain operable for the plant operating mode and conditions.

3.9 Other Potential Architectures

Figure 3-7 shows an example of an architecture that could be used where only one or two divisions are needed. {{

}}2(a),(c),(e)-ECI

Figure 3-7. Representative One or Two Division Architecture (One Division Shown)

4.0 Independence

This section describes the HIPS platform design concepts that address the fundamental design principle of independence. The grounding concepts used for the platform are described in Section 4.1. The independence concepts implemented on the individual HIPS platform modules are described in Sections 4.2 through 4.5. The communication independence concepts are described in Section 4.6. The isolation concepts used to support monitoring and indication features and provide access control are described in Sections 4.7 and 4.8, respectively.

4.1 HIPS Platform Grounding

There are four different isolation domains in the HIPS platform:

1. **DGND:** the DGND reference originates in the power converters. It is fed through the HIPS backplane bus connector as the supply ground for the HIPS modules. The DGND domain is normally a floating domain in order to provide immunity against a single point failure.
2. **CHASSIS:** CHASSIS is used as protective ground for the HIPS chassis and is a supplementary safeguard to protect personnel. Chassis also functions as an electrostatic discharge protection barrier for the HIPS module.
3. **EARTH:** Same potential as CHASSIS, but used to decouple noise and protect against surge voltages.
4. **FIELD:** Isolated input or output channels with independent reference. A HIPS chassis typically has multiple isolated field domains.

Isolation between DGND and FIELD: DGND shall be galvanically isolated from FIELD and capable of withstanding $1500 V_{RMS}$ or $1500 V_{DC}$ test voltage for 1 minute without failure when tested in accordance with International Electrotechnical Commission (IEC) 60950-1 Section 5.2 (Reference 11.1.7).

Isolation between DGND and CHASSIS or EARTH: DGND shall be galvanically isolated from CHASSIS and EARTH and capable of withstanding $750 V_{RMS}$ or $750 V_{DC}$ test voltage for 1 minute without failure when tested in accordance with IEC 60950-1 Section 5.2.

Isolation between FIELD and CHASSIS or EARTH: FIELD shall be galvanically isolated from CHASSIS or EARTH and capable of withstanding $750 V_{RMS}$ or $750 V_{DC}$ test voltage for 1 minute without failure when tested in accordance with IEC 60950-1 Section 5.2.

Separation of CHASSIS and EARTH: CHASSIS and EARTH do not require isolation, but separation must be maintained to ensure noise currents are not coupled onto the CHASSIS from noise filters.

Isolation between FIELD and FIELD: FIELD shall be galvanically isolated from FIELD and capable of withstanding 750 V_{RMS} or 750 V_{DC} test voltage for 1 minute without failure when tested in accordance with IEC 60950-1 Section 5.2.

4.2 Safety Function Module

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

The analog RPS that is discussed in Section 7 is based on independent channels for each safety function. This is an example of functional independence. The fundamental design objective for the HIPS platform is to preserve the functional independence of the safety function as in the analog architecture. The HIPS platform implements each SFG on a different SFM, unlike a microprocessor based system where the functions are consolidated and the loss of the central processing board causes the loss of all functions. Also, see Section 6.3 on functional diversity.

Each SFM can handle up to four input sub-modules. The analog and temperature input sub-modules contain an isolation device (channel isolator) that at a minimum meets the independence requirements as described in Regulatory Guide (RG) 1.75 (Reference 11.1.9). 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 analog or discrete signal from the field sensor or detector is converted to a digital signal with an ADC (channel domain). The serial interface of the ADC is the input to the channel isolator that isolates the channel domain from the digital domain. {{

}}^{2(a),(c),(e)-ECI}

The HIPS platform can process nonsafety-related inputs to the protection system (e.g., anticipatory turbine or main feedwater trip signals required by 10 CFR 50.34(f)(2)(xxiii)). The HIPS platform is protected from adverse impacts from the nonsafety-related field input signals by the galvanic isolation features on the SFM. The SFM isolation capabilities for the use of non-1E input signals address IEEE Std. 384-1992 Section 7.2.2.1 requirements by the FIELD to FIELD testing described in Section 4.1 above. These input signals are processed by the SFM

and the trip determination is transmitted on the {{
}}2(a),(c),(e)-ECI

The HIPS platform can transmit nonsafety-related status and bypass indication information required by IEEE Std. 603-1991 Clauses 5.8.2 and 5.8.3. The nonsafety-related status information is processed by the MIB logic and transmitted over the MIB, which is a completely separate communication bus and functionally different than the SDB logic and buses to prevent adverse impacts to the SDB signal paths. Interdivision communication from the MIB uses fiber optic cables to provide galvanic isolation and prevent adverse impacts to the SFM safety functions from modules or devices outside the division of the MIB.

The HIPS platform can process post-accident monitoring signals that are classified as nonsafety-related. These signals meet the design requirements specified for them [e.g., Regulatory Guide 1.97 and 10 CFR 50.34(f)(2)(xi)] and may be routed through the HIPS platform to achieve a simpler overall I&C system design for a plant. The HIPS platform is protected from adverse impacts from the nonsafety-related field input signals by the galvanic isolation features on the SFM. 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 to the SDB signal paths. The MIB communicates with other modules or devices using fiber optic cables to provide galvanic isolation and prevent adverse impacts to the SFM safety functions and MIB-CM communication functions.

The discrete Input sub-module is protected from excessive positive voltages by two unidirectional transient-voltage-suppression (TVS) diodes. An optocoupler is used to isolate the FPGA from the input signal. The TVS diodes ensure that the channel circuit does not experience voltages above the maximum collector to emitter voltage specified for the optocoupler.

{{

}}2(a),(c),(e)-ECI

The logic functions are part of the programmable portion (i.e., FPGA) of the SFM.
{{

}}2(a),(c),(e)-ECI

Two redundant power sources are provided to the HIPS chassis backplane. The power converters within the HIPS platform are designed as safety-related equipment. The redundant power provided is auctioneered once it is on the board and converted to the needed voltages of the FPGA. There are voltage and current monitoring circuits on each SFM that protect the module from voltage and current transients. The power sources to the HIPS platform are not required to be independent, because they provide power to a single division in a multi-division system. These power sources are provided to improve reliability and maintainability. The redundant power feeds are auctioneered once it is on the SFM and either power source can power the board.

The FPGA is a hardware logic device and each core logic function and communication engine is implemented with logic gates that are unique for each path. {{

}}2(a),(c),(e)-ECI

The MIB and CTB logic functions and communication engines are separate and cannot affect the core logic functions. During the FPGA synthesis and place and route process, the logic functions are defined and assigned to the actual logic elements.

The monitoring and indication data use registers in the MIB logic and are independent of the safety data and are processed by the MIB logic separately. The CTB logic coordinates updating the NVM from the MWS and can only be performed when the SFM is removed from service.

The OOS switch on the SFM allows removing the SFM from service. Activating the switch physically closes a contact to allow modification of setpoints and tunable parameters in the NVM. A temporary cable is also required to be connected from the MWS to the MIB-CM CTB input. Activating the OOS switch also informs the SBM to place the affected trip and actuate signals for that safety function to either bypass or trip based on the position of the trip/bypass switch for that SFM.

The NVM used for the HIPS platform as internal memory devices (e.g., electrically erasable programmable read-only memory or flash memory chips) is a type of computer memory that can retrieve stored information even after having been power cycled (i.e., turned off and back on). The NVM is used to store the setpoints and tunable parameters for modules with both the SRAM-based FPGA and the one-time programmable (OTP) or flash-based FPGA. The NVM is also used to store the FPGA configuration for modules with SRAM-based FPGAs. The NVM chips used for the HIPS platform do not require power to maintain the memory state. The NVM is designed to not change states in response to the changing operating states of the HIPS platform.

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. To change the functional logic, the SFM and all other HIPS platform modules must be removed from the chassis and installed in a special

device to allow modification of the logic of the FPGA for an SRAM-type FPGA or replacement of an OTP or flash-type FPGA. The functionality for the SRAM-type FPGAs is stored in the FPGA configuration files stored in the NVM.

The source of setpoints and tunable parameters is the NVM for all logic paths. The setpoint and tunable parameters that can be modified with the SFM installed are defined during the application-specific design phase. 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 they do not access the NVM while the SFM is in service. If the setpoints or tunable parameters are updated in the 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 out of service.

The one-way isolated data from the HIPS platform to the MWS includes the setpoint and tunable parameter information for each SFM. When the setpoint or tunable parameter information in the NVM is modified, the data that is loaded into the NVM through the CTB can be verified by reading this information back through the one-way data path to the MWS. The SFM verifies that the data that is sent from the MWS is valid using the CRC for the data packet sent. {{

}}2(a),(c),(e)-ECI

A nonsafety-related input that is connected to the SFM input sub-module is galvanically isolated from the other inputs on that SFM and all of the other SFMs in the chassis by the channel isolator. The logic developed for the nonsafety-related inputs would be developed as safety-related and be qualified to the same level as the safety-related logic. The nonsafety-related inputs that are used for indication only would only be sent to the monitoring and indication logic function for processing. Because the signal path is not connected to the SDB communication engines, it cannot affect the safety data on the SDBs.

4.3 Communication Modules

The CM is a base module that can be programmed and configured for different functions depending on where it is used in the platform (see Section 3 for an example of application-specific uses). There are 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 or receive only. When the communication channel is configured for transmit only, the receive capability is physically disabled by hardware. When the communication channel is configured for receive only, the transmit capability is physically disabled by hardware.

The channel isolator at the minimum meets the independence requirements as described in RG 1.75.

The communication ports are protected against transients and over-currents.

The CMs are functionally independent from the SFMs and EIMs.

4.4 Equipment Interface Modules

{{

}}^{2(a),(c),(e)-ECI}

The APL circuit on the EIM is part of the EIM and qualified to the same requirements.

- The APL circuit is constructed of discrete components and is not part of the FPGA.
- {{

}}^{2(a),(c),(e)-ECI}

- The manual actuation signal connects directly to the APL and is downstream of the FPGA logic.
- All inputs and outputs are individually isolated from the EIM discrete logic circuitry.

4.5 Hard-Wired Module

The HWM is an analog component with no digital functions that is designed as a safety-related component. The HWM receives signals from manual switches, nonsafety-related discrete control signals, and the manual trip/bypass switches.

- trip/bypass switches for each SFM
- manual actuation
- reset switch
- enable nonsafety control switch
- operational bypasses switches
- nonsafety-related control signals

All input signals to the HWM are isolated from the field and traced on the backplane to those modules that use the analog logic-level signals (i.e., not data communication). As such, the HWM performs a safety-related function to provide electrical isolation of nonsafety-related input signals.

The HWM provides electrical isolation for the backplane and modules from the external manual switches and the nonsafety-related control signals. An optocoupler is used to electrically isolate the input signal. TVSs ensure that the channel circuit does not experience voltages above the maximum collector to emitter voltage specified for the optocoupler.

The enable nonsafety control switch concept is designed to allow a plant operator to control components with an analog binary control signal that is nonsafety-related. The enable nonsafety control switch concept could be used in various ways: 1) an enable nonsafety control switch for each safety-related component, 2) an enable nonsafety control switch for a group of safety-related components within a division, or 3) an enable nonsafety control switch for an entire division of safety-related components. The closed enable nonsafety control switch allows an analog binary control signal from the HWM to be used. Otherwise, the nonsafety-related component control signal input is ignored in the APL logic when the enable nonsafety control switch is open. The APL is designed to provide priority to safety-related signals over nonsafety related signals. The specific use and switch configuration details are application-specific. The HIPS platform design concept for the enable nonsafety control switch envisions the use of a limited number of enable nonsafety control switches (i.e., one per division) to support the human factors engineering aspects associated with using an integrated operator workstation for normal plant control by the nonsafety-related control system. The actual number of enable nonsafety control switches used is application-specific. The limit to the number of enable nonsafety control switches that can be used has a practical value that is dependent on the number of available inputs into the HWM and associated dedicated traces on the backplane. An enable nonsafety control switch for an entire division of safety-related components uses the least amount of inputs into the HWM and associated traces on the backplane, while an enable nonsafety control switch for each safety-related component uses the most.

The enable nonsafety control switch provides an input to the priority logic for a component. This priority logic is located in the non-digital APL portion of the EIM. This logic is made from discrete components; it is not a programmed (i.e., software) feature.

The enable nonsafety control switch is a safety-related device that can be used to prevent spurious nonsafety-related control signals from adversely affecting safety-related components as part of an application-specific design to provide independence features that satisfy IEEE Std. 603-1991 Clause 5.6.3 requirements.

The HIPS platform can detect certain HWM failures during operation by self-tests; specifically, the slot/board identification (ID) test, board latch test, LED test, and input channel test described in Section 8.2.7.

4.6 HIPS Communication

{{

}}^{2(a),(c),(e)-ECI}

4.6.1 Communications Independence within the Platform

{{

}}^{2(a),(c),(e)-ECI}

- {{

}}^{2(a),(c),(e)-ECI}

4.6.2 Communication Independence outside the Platform

The HIPS platform can be configured into an architecture that has four separation groups that are physically and electrically independent of each other (see Figure 3-1). The communication from the four separation groups to the RTS and ESFAS is {{

}}^{2(a),(c),(e)-ECI} 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.

{{

}}^{2(a),(c),(e)-ECI} The four communication ports on each SVM are configured as fiber-optic receive-only ports and received the trip and actuate information from the four separation groups (see Figure 3-4 and Figure 3-5).

Where redundant divisions communicate, such as voting logic inputs (e.g., SVM) from independent measurement channels, isolation devices are employed to preserve electrical independence of the divisions.

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 fiber optic cables are incapable of transmitting electrical faults and therefore meet IEEE Std. 384-1992 electrical isolation requirements. {{

}}^{2(a),(c),(e)-ECI}

4.7 Monitoring and Indication

The status and diagnostic information is obtained by the IDI circuitry on the SFM (core logic function), CM, and EIM and is sent to the MIB communication port on each module. The MIB-CM is the bus master for the MIB and coordinates gathering this information from all of the modules and sending it out to other systems. The data going out of the chassis is one-way and sent over fiber optic cables and isolated as described above.

The diversity features of the HIPS platform described in Section 6 can be used to ensure monitoring and indication information is available even if a digital CCF affects one FPGA technology.

4.8 Access Control Features

The HIPS platform design considers the concepts-phase guidance from RG 1.152. The HIPS platform contains design features that reduce the susceptibility to inadvertent access. 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-related systems or equipment are generally dependent on the application. This topical report addresses platform features to control access to both hardware and software.

The HIPS platform is a modular, rack-mounted platform 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 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 HIPS platform has design concepts that provide a secure operating environment that supports the IEEE Std. 603-1991 requirement for access control and isolation.

- {{

}}^{2(a),(c),(e)-ECI}

- The only time communication from the MWS to the HIPS chassis is allowed is when the SFM is placed out of service by activating the OOS switch and a temporary cable is attached from the MWS to the MIB-CM for that separation group.
- 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.
- The FPGA on any of the modules (i.e., SFM, CMs, and EIM) cannot be modified (for SRAM type) or replaced (for OTP or flash types) while installed in the HIPS platform chassis. To change the functional logic, a HIPS platform module must be removed from the chassis and installed in a special device to allow modification of the logic of the FPGA for an SRAM type FPGA or replacement of an OTP or flash-type FPGA. {{

}}^{2(a),(c),(e)-ECI}

- The CM communication ports that are for communication outside of the HIPS chassis implement the one-way communication with hardware.
- The HIPS platform design does not have the capability for remote access to the safety system.

Each division of an I&C system based on the HIPS platform has a nonsafety-related MWS for the purpose of online monitoring and offline maintenance and calibration. The HIPS platform MWS supports online monitoring using the MIB-CM through one-way isolated communication ports over point-to-point fiber-optic cables. The HIPS platform MWS serves as a maintenance workstation that supports offline, OOS management (e.g., troubleshooting, calibration, and surveillance testing). The MWS is used to update setpoints and tunable parameters in the SFMs when the safety function is out of service. Physical and logical controls are put in place to prevent modifications to a safety channel when it is being relied upon to perform a safety function. A temporary cable and OOS switch 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, an indication is provided by the HIPS platform that can be used to drive an alarm in the main control room to inform the operator. Adjustments to parameters are performed in accordance with plant operating procedures, including any that

establish the minimum number of redundant safety channels that must remain operable for the plant operating mode and conditions.

5.0 Redundancy

Redundancy is commonly used in I&C safety systems to achieve system reliability goals and conformity with the single-failure criterion. The HIPS platform is designed to support separation group and divisional redundancy. The specific system architecture that is chosen for the application needs to be evaluated separately to determine if it meets the single failure criterion. Internal platform redundancy is used to improve availability and error detection and supplements redundancy at the system level to satisfy the single failure criterion. This section describes the internal platform redundancy.

5.1 Power Supply

The HIPS platform and modules are designed to accept a redundant pair of DC power feeds to its internal circuits. The DC power feeds are auctioneered and down converted on the HIPS modules to the voltage domains required for the module circuitry. The HIPS modules use a general logic supply and an FPGA core supply. The redundant DC supplies are diode auctioneered and fuse protected immediately after entering the board. The fuse cannot be replaced and is designed to operate (open) in case of severe overcurrent (due to an overvoltage condition) or severe board failure.

5.2 Safety Function Module Internal Redundancy

The SFM input sub-modules convert the analog or discrete input signal to a digital signal. {{

}}2(a),(c),(e)-ECI

5.3 Communication Redundancy

{{

}}^{2(a),(c),(e)}-ECI

5.4 Equipment Interface Module Redundancy

With only one EIM supplying power to the coil of the end device, a failure or removal of the EIM would cause the field component to be actuated. To allow replacing an EIM without actuating the end device, a second EIM switching output is placed in parallel with a second EIM so that either EIM can keep the output energized. This configuration also allows for more thorough testing of the EIM circuits (see Section 8).

{{

}}^{2(a),(c),(e)}-ECI

5.5 Platform Internal Redundancy Summary

The HIPS platform internal redundancy is summarized as follows:

- Redundant power supply feeds to all of the HIPS modules improves availability.
- {{

}}^{2(a),(c),(e)}-ECI

-
- {{
}}^{2(a),(c),(e)-ECI}
 - The internal redundancy in the HIPS platform design provides fault tolerant capabilities which, coupled with self-testing, provides a high-level of integrity.
 - The HIPS platform has internal redundancy that simplifies the self-testing circuitry.
 - Redundancy in the safety data communications and the EIM configuration allows for on-line maintenance without the need to remove equipment from service.
 - Internal platform redundancy supplements redundancy at the system level to satisfy the single failure criterion.

6.0 Diversity

A software CCF is a failure caused by software errors or software developed logic that could defeat the redundancy achieved by hardware architecture. Two basic forms of preventing CCFs in a system are either to reduce the causal influences or to increase the system's ability to resist those influences. Two primary strategies for preventing CCFs in a system are quality and diversity.

Safety systems are designed to high quality requirement; however, as noted in Multinational Design Evaluation Program Generic Common Position DICWG-01, "demonstrating adequate software quality only through verification and validation activities and controls on the development process has proved to be problematic" (Reference 11.1.10). Branch Technical Position 7-19 notes that using a diversity strategy is considered sufficient to eliminate consideration of software CCFs (Reference 11.1.11).

The following sub-sections discuss the minimum diversity attributes required within the HIPS platform design to eliminate consideration of software CCFs.

6.1 Equipment Diversity

6.1.1 Field Programmable Gate Array

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 architectures are different and inherently create differences in how the FPGA is configured and how it operates once it has been configured, as shown in Figure 6-1 and Figure 6-2. Inherent differences between the two architectures are:

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 re-configures itself with the "lookup" table obtained from the external memory or configuration chip.

The inherent differences are summarized in Table 6-1.

Table 6-1. 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

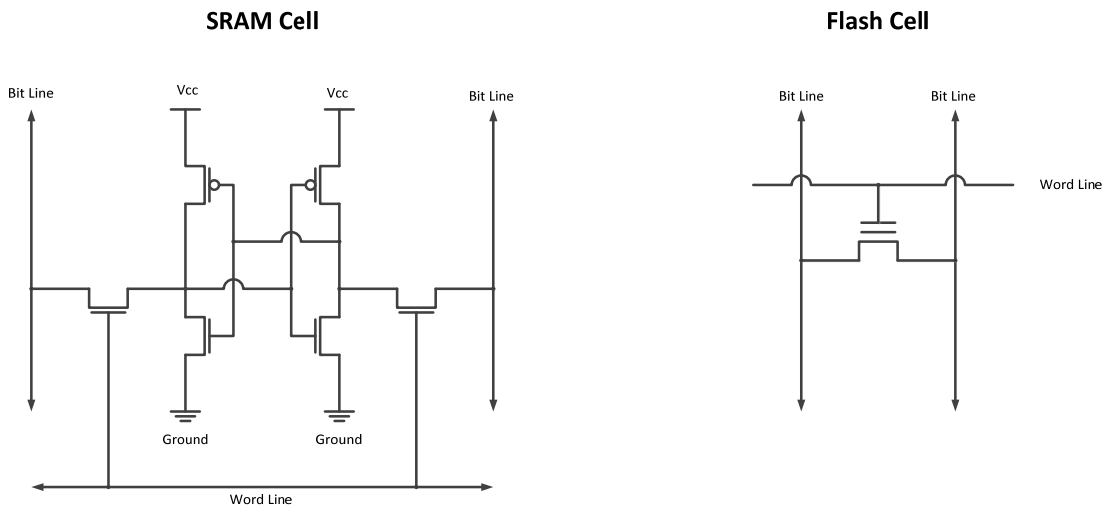


Figure 6-1. Example Transistor Configuration Comparison

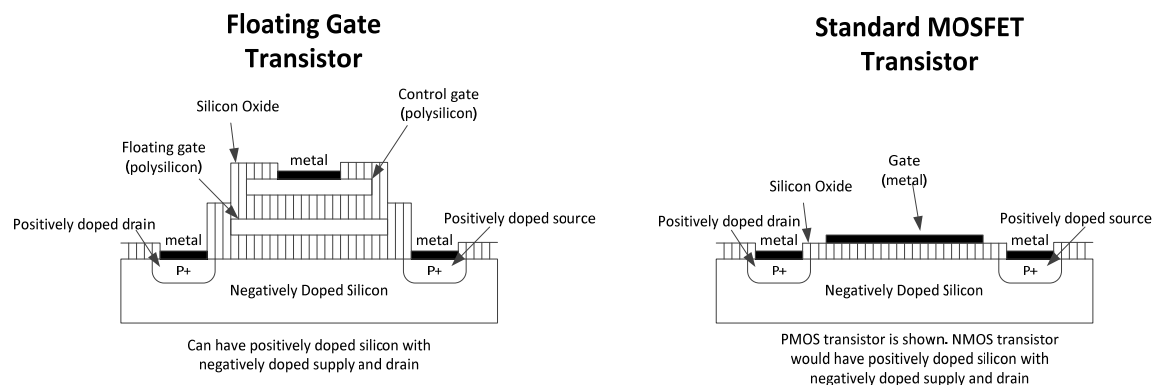


Figure 6-2. Difference between Transistors Used in Flash Cell and SRAM Cell

At the chip level, the two FPGA technologies operate in different ways during operation and programming.

6.2 Design Diversity

NUREG/CR-6303 defines design diversity as the use of different approaches, including both software and hardware, to solve the same or similar problem (Reference 11.1.12). The diverse FPGA technologies described in Section 6.1 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 collections of development tools used for an FPGA architecture is considered a suite of tools. It should be noted that human diversity is an implicit attribute of the FPGA equipment, chip design, and software tool diversity; however, it is not explicitly defined nor verified for the HIPS platform diversity strategy.

Intentional differences are required in the following 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 utilized 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. The intentional differences are summarized in Table 6-2.

Table 6-2. 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 purpose of the iV&V effort is to check the development of the FPGAs by the design team. Required independence is the attribute most effective in identifying errors that might be introduced by a flaw in FPGA design development. The purpose of required diversity in the iV&V design simulation tool is to check the development of the FPGAs with a tool that is diverse from the development tool. This diversity compensates for errors that might be introduced by a flaw in either of the development tools. The use of a single iV&V tool allows 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 consideration of errors introduced by one of the iV&V tools as a potential source of error.

{{
 }}^{2(a),(c)} is based on insights drawn from a recent Massachusetts Institute of Technology research report on hazards analysis (Reference 11.1.13) sponsored by the NRC (i.e., independently developed software is very likely to still contain CCF modes). The research report noted that “almost all serious accidents caused by software have involved errors in the requirements, not in the implementation of those requirements in software code.” The report noted that the software requirements have had missing cases or incorrect assumptions about the behavior of how the system operated. These problems were attributed to misunderstandings 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. Software may be considered “correct” if 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 that specified in the requirements. The report noted that redundancy or even

multiple versions of the implementations of the requirements does not help in these cases.

The National Research Council was asked by the NRC to conduct a study on application of digital I&C technology to commercial nuclear power plant operations (Reference 11.1.14). 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 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 not likely to be effective in achieving diversity (i.e., none of these methods is a proof of independence of failures). The report noted that there is 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.

{{

}}^{2(a),(c)} The paper suggested that excessive reliance on software diversity may be a case of diminishing returns (i.e., high conformity to the wrong specification). As such, it might make more sense to utilize diversity at a higher level so there is some defense-in-depth against faults in the requirements.

{{

}}^{2(a),(c)}

{{

}}2(a),(c),(e)-ECI

6.3 Functional Diversity

6.3.1 Functional Diversity of a Safety Function Module

The HIPS platform supports functional diversity by requiring segregation of safety functions by their inputs. For example, two SFMs within a division of the HIPS platform each monitor 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.

6.3.2 Functional Diversity of Actuation Priority Logic

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 capability for hard-wired signals into each EIM supports the capability for additional 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.

6.4 HIPS Diversity Summary

The HIPS platform uses two diverse FPGA technologies to achieve equipment diversity. The diverse FPGA technologies results in an associated level of chip design diversity, since different development tools are developed by the FPGA vendors to provide the final configured FPGAs. These tools have inherent

diversity related to the differences in FPGA chip architectures and programming methods. The diversity in FPGA equipment, chip designs, and software 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 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, 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 are implemented on separate SFM hardware boards within the same division (or separation group). The functional diversity approach directly mitigates a set of CCFs associated with a specific FPGA platform.

Human diversity is not specifically credited in the HIPS platform for mitigating the potential for digital CCFs. The HIPS platform meets requirements for having a design team and an independent verification and validation team; however, the HIPS platform does not require an additional independent design or verification and validation team since it would provide minimal benefits in eliminating digital CCFs. The basis for not crediting human diversity is consistent with the view that independently developed software is very likely to contain CCF modes, as discussed in recent Massachusetts Institute of Technology research report on hazards analysis. It should be noted that human diversity is an implicit attribute of the FPGA equipment, chip design, and software tool diversity; however, it is not explicitly defined nor verified for the HIPS platform strategy.

The HIPS platform diversity solution is an acceptable regulatory solution for the digital CCF vulnerabilities present in the HIPS platform. NRC Branch Technical Position (BTP) 7-19, Revision 6, states that there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF: diversity or testability. With respect to the diversity option, BTP 7-19 specifies that when sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action. It includes an example that was the genesis for the HIPS platform diversity strategy:

Example: An RPS design in which each safety function is implemented in two channels that use one type of digital system and another two channels that use a diverse digital system. If a D3 analysis performed consistent with the guidance in NUREG/CR-6303 determines that the two diverse digital systems are not subject to a CCF, then, in this case, no additional diversity would be necessary in the safety system.

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. For example, a four division protection system can be implemented with one FPGA technology in two divisions and the other FPGA technology in two divisions. In this arrangement, a CCF associated with one FPGA technology would not defeat the safety function, since two divisions would be unaffected due to the FPGA diversity and would accomplish the safety function.

The HIPS platform diversity strategy represents a stronger diversity case (i.e., more diversity attributes) than others accepted by NRC for systems based on FPGA technology.

The diversity approach provides other benefits by simplifying the overall I&C systems designs, since a separate diverse actuation system is not required to mitigate digital CCFs. The HIPS platform diversity strategy leads to a simpler overall I&C architecture than other platform-based diverse technology solutions (e.g., addition of a separate diverse actuation system). The HIPS platform diversity strategy eliminates the complex intersystem design coordination analysis of two actuation systems controlling safety components. The HIPS platform diversity strategy leads to simpler integration and timing analyses than other internal diversity solutions, since the response time of the two types of FPGAs is more similar than if microprocessor or relay technology was used.

The key diversity attributes credited with reducing the CCF vulnerabilities in the HIPS platform design (i.e., diverse FPGA equipment and associated different development tools) simplifies verification that the credited FPGA equipment diversity attributes are present in the installed system. The FPGA equipment-based diversity attributes are also easier to maintain during the lifecycle of the installed system.

The HIPS platform diversity 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. This capability is illustrated in Figure 6-3, which shows 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.

The use of FPGA equipment diversity in the form of two different FPGA technologies (i.e., SRAM based FPGA and the OTP or flash-based FPGA) when coupled with the different development tools used for the two FPGA technologies is an effective solution for the digital CCF vulnerabilities present in the HIPS platform. This diversity solution is targeted at mitigating the CCF vulnerabilities unique to the FPGAs (i.e., chip-programming interactions during configuration with the development tools; need for special skills for implementing the hardware description language requirements into the FPGA-specific architecture,

synthesis, place and route and bitstream generation; and special FPGA chip circuit behavior considerations).

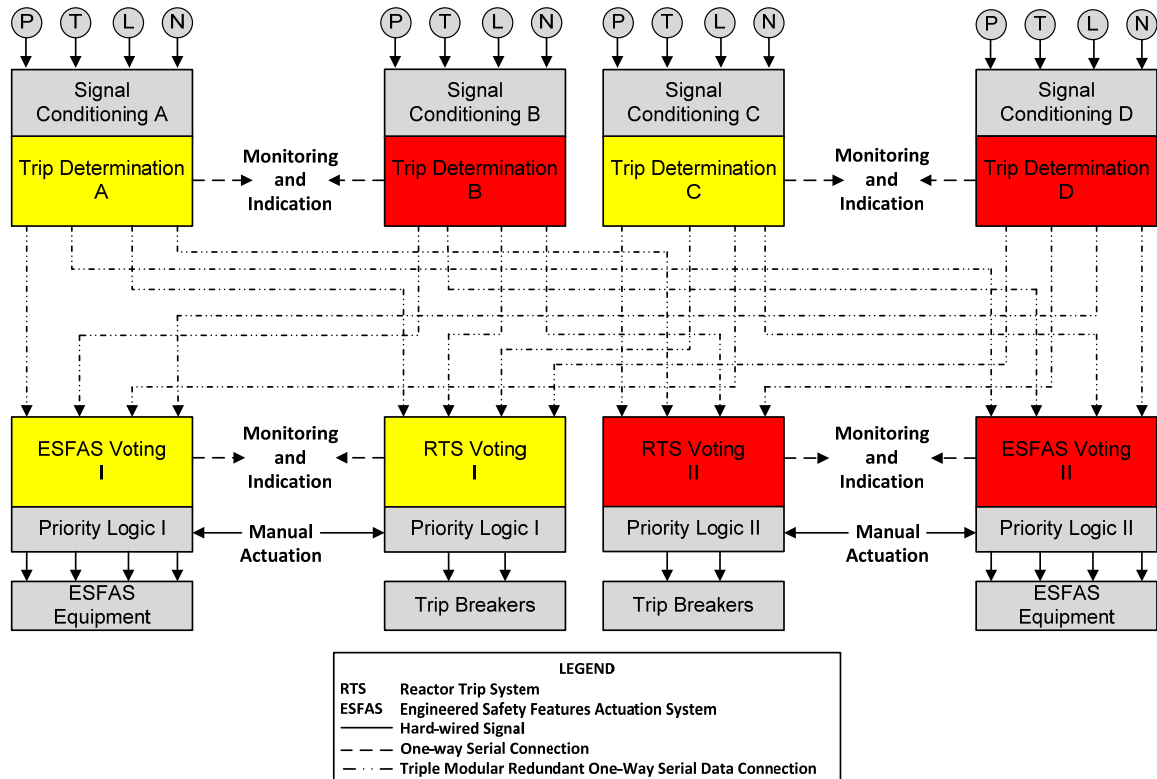


Figure 6-3: FPGA Equipment Diversity Allocation in a Representative Architecture

The effects of digital CCF for a system using the HIPS diversity strategy is illustrated for two cases in Table 6-3. 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 6-3. 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.

7.0 Repeatability and Predictability

Repeatable and predictable 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. 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. This is also referred to as deterministic behavior.

The fundamental design objective for the HIPS platform is to take advantage of the benefits of analog architectures installed within the existing commercial nuclear power plants. The discussion below summarizes this notion of the existing architecture and how the HIPS platform models this approach.

Figure 7-1 shows an example of an analog PS architecture that has four independent trip determination channels (e.g., pressurizer pressure A, B, C, D) within the top level of the architecture. Each of these channels is within a separate division, also referred to as separation group. Each of the trip determination channels operates independently of the others within their own division and independently from the other divisions. This design approach creates an individual channel that does not rely on any other channels to perform its intended safety function.

Independent trip channels provide the trip decision to the lower level of the architecture, referred to as the voter level. These trip determinations are provided to the voter level via isolated physical point-to-point connections. The actuation of ESF components is achieved by use of a master relay and slave relay approach where the master relay is connected to multiple slave relays and each slave relay actuates an ESF component. The master relay to slave relay connections are arranged as a point-to-multipoint connection.

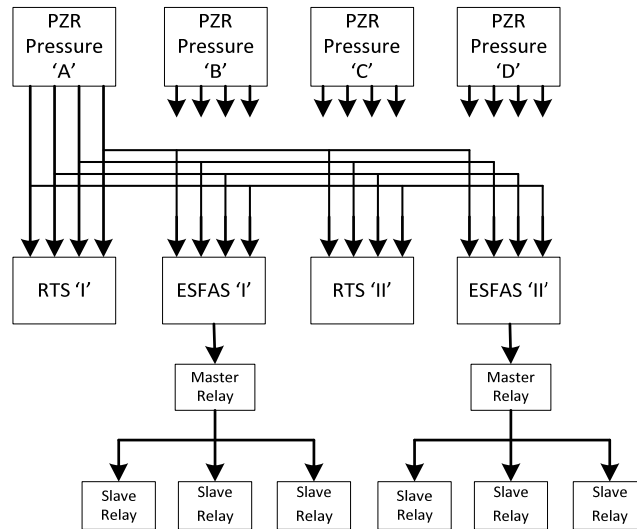


Figure 7-1. An Analog PS Implementation

The HIPS platform supports the independent trip determination channels in the same manner as in the analog architecture. The HIPS platform utilizes a virtual point-to-point connection of the trip decision to the voter level of the architecture. It also utilizes the point-to-multipoint arrangement achieved within the master relay to slave relay connection. This summary provides a perspective on the fundamental design genesis for the HIPS platform. This section of the LTR provides detailed information that supports the predictability and repeatability attributes of the HIPS platform using a representative PS that is described in Section 3 and illustrates how the traditional analog architecture can be implemented with the HIPS platform.

7.1 Input Sub-Module

The input sub-module 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.

7.1.1 Self-Test of the Analog to Digital Converter

Continuous self-test and calibration checks are performed on the analog input sub-module ADCs. These tests verify the input sub-module is working and the calibration of the analog portion. The continuous calibration check verifies the ADC is within the desired accuracy and that it has not drifted out of calibration. This supports the platform design fundamental of predictable and repeatable. Details of the self-testing are in Section 8.

7.2 Safety Function Modules

A single clock base is used for all logic on the SFM as well as being used 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, due to the bus architecture.

{{

}}^{2(a),(c),(e)-ECI}

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 is in the operate position. The OOS switch in the out of service position connects the CTB to the SFM and allows changing of setpoints and tunable parameters that are stored in the NVM. On module startup, the NVM parameters are loaded into the logic functions. The load switch on the front of the SFM allows loading the NVM parameters when they are changed while the SFM is out of service.

For detailed information on the SFM, see Section 2.5.1.

7.3 Communication Modules

{{

}}^{2(a),(c),(e)-ECI}

{{

}}^{2(a),(c),(e)-ECI}

Figure 7-2. Example of HIPS Bus Topology in a Separation Group

{{

}}^{2(a),(c),(e)-ECI}

Figure 7-3. Example of HIPS Bus Topology in a Division of RTS or ESFAS

7.4 Equipment Interface 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.

{{

}}^{2(a),(c),(e)-ECI}

The EIM is equipped with four high drive switching outputs. {{

}}^{2(a),(c),(e)-ECI}

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

7.5 Bus Communications

{{

}}^{2(a),(c),(e)-ECI}

7.5.1 Safety Data Bus Communication

{{

}}^{2(a),(c),(e)-ECI}

Table 7-1. Typical SDB REQUEST and RESPONSE Packet Format

{{

}}^{2(a),(c),(e)-ECI}

{{

}}^{2(a),(c),(e)-ECI}

Figure 7-4. Example SDB Master-Slave Transactions

{{

}}^{2(a),(c),(e)-ECI}

7.6 HIPS Module Modes

{{

}}2(a),(c),(e)-ECI

7.6.1 Operation Modes

{{

}}2(a),(c),(e)-ECI

Figure 7-5. Module Operational Modes

{{

}}2(a),(c),(e)-ECI

{{

}}^{2(a),(c),(e)}-ECI

7.6.2 Safety Function Module MOD_OK Mode

{{

}}^{2(a),(c),(e)}-ECI

{{

}}2(a),(c),(e)-ECI

{{

}}^{2(a),(c),(e)-ECI}

Figure 7-6. Safety Function Module MOD_OK Mode

7.6.3 Scheduling and Bypass Module MOD_OK Mode

The operation of a CM that is configured as an SBM in the representative architecture shown in Section 3 is illustrated below. {{

}}2(a),(c),(e)-ECI

{{

}}2(a),(c),(e)-ECI

{{

}}^{2(a),(c),(e)-ECI}

Figure 7-7. SBM MOD_OK Mode

7.6.4 Scheduling and Voting Module MOD_OK Mode

The operation of a CM that is configured as an SVM in the representative architecture shown in Section 3 is illustrated below. {{

}}2(a),(c),(e)-ECI

{{

}}^{2(a),(c),(e)}-ECI

Figure 7-8. SVM MOD_OK – Loading 2-out-of-4 Voting Registers

{{

}}^{2(a),(c),(e)}-ECI

{{

}}^{2(a),(c),(e)}-ECI

Figure 7-9. SVM MOD_OK Mode – 2-out-of-4 Voting and Transfer to EIMs

{{

}}^{2(a),(c),(e)}-ECI

{{

}}2(a),(c),(e)-ECI

7.6.5 Equipment Interface Module MOD_OK Mode

{{

}}2(a),(c),(e)-ECI

{{

}}2(a),(c),(e)-ECI

{{

}}2(a),(c),(e)-ECI

Figure 7-10. EIM MOD_OK Mode

7.6.6 Safety Data Bus HIPS Bus Frame

The SBM is the bus master and requests information from each slave device in a round robin fashion at a fixed rate that is determined by the transaction time. The SBM requests and receives information for each slave device once every HIPS bus frame cycle.

The HIPS bus frame cycle time is fixed for a given application and does not change once the system has been implemented. It is based on the number of slave devices and the transaction time. There are no specific signals or flags to indicate the start or end of an HIPS bus frame cycle.

{{

}}2(a),(c),(e)-ECI

Figure 7-11. SBM HIPS Bus Frame Cycle

The SVM HIPS bus frame cycle is illustrated in Figure 7-12. {{

}}2(a),(c),(e)-ECI

Figure 7-12. SVM HIPS Bus Frame Cycle

7.7 HIPS Platform Work Cycle

7.7.1 Safety Data Work Cycle

Each SFM is dedicated to implementing one SFG. Each SFG may consist of a single safety function or multiple safety functions. An example of a single safety function SFG is a reactor trip from low RCS flow generated from an RCS flow sensor signal. An example of multiple safety function SFG is a pressurizer pressure channel that has multiple trips and actuations (i.e., low pressure reactor trip, high pressure reactor trip, high pressure decay heat removal actuation, etc.).

Figure 7-13 shows an example SC/TD chassis for separation group A with a set of SFMs and a single SBM communicating with an ESFAS chassis for division II with a set of EIMs and a single SVM. Each of the SFMs contains a specific SFG. The SFG is assigned a unique digital address for identification within the communications protocol. The first SFM, SFM1A contains SFG1A. This SFG1A represents a partial SFG as there is also an SFG1B, SFG1C, and SFG1D to complete the four separation groups of the same SFG. SFG1A produces a set of PTDA data. This set of PTDA data is based on the number of safety functions contained within the SFG.

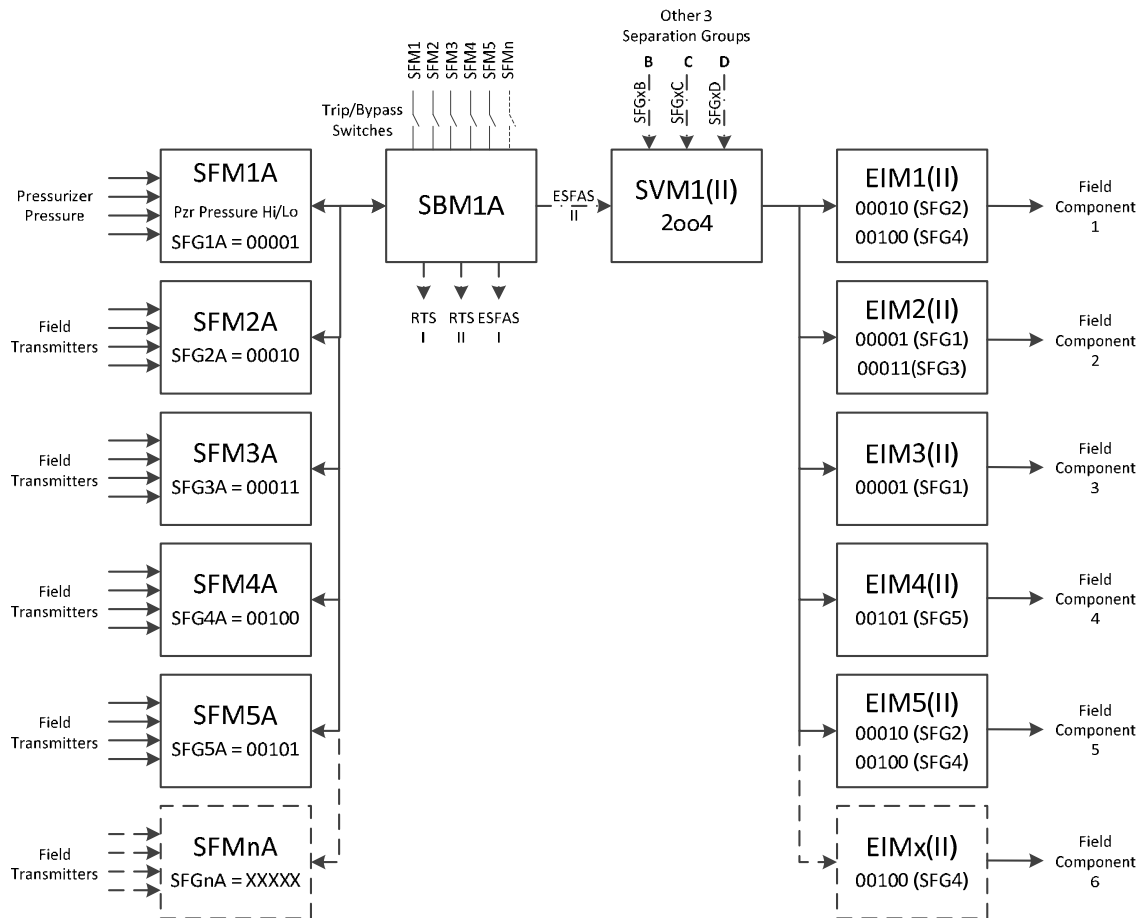


Figure 7-13. Safety Function Group Example

Table 7-2 shows the PTDA list for SFG1A. In this example SFG1A is Pressurizer Pressure Hi/Lo. The list of actions for SFG1A is: 1) no action, 2) ESFAS Hi Pressure actuation, 3) ESFAS Lo Pressure actuation, 4) RTS Hi Pressure actuation, 5) RTS Lo Pressure actuation, and 6) All Actuate. The most significant bit (MSB) of the payload represents an OOS state for the SFM. This bit is utilized by the SBM to determine the OOS state for all of the safety functions within a given SFG. The PTDA is communicated as the payload of the communication transmission from the SFM to the SBM.

Table 7-2. Example Partial Trip Determination Actuation List

<p>SFG1A = Pzr Pressure Hi/Lo Partial Trip Determination Action (PTDA): 00000 = No Action 00001 = ESFAS Hi Pressure Actuation 00010 = ESFAS Lo Pressure Actuation 00100 = RTS Hi Pressure Actuation 01000 = RTS Lo Pressure Actuation 01111 = All Actuate 1XXXX = OOS</p>
--

Figure 7-14 shows the timing of transferring the SFG PTDA from the SFM to the EIM. The timing diagram is focused on the digital portion. ^{2(a),(c),(e)-ECI} 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 regards to the communications timing; as such, they are added as an element in the worst case timing calculation.

{{

^{2(a),(c),(e)-ECI}

Figure 7-14. Timing Diagram for a Representative Architecture

{{

}}2(a),(c),(e)-ECI

{{

}}^{2(a),(c),(e)-ECI}

7.7.2 MIB Work Cycle

The MIB provides monitoring and indication information for all of the modules in the chassis. The MIB-CM coordinates gathering this information to send to other systems. The MIB work cycle is asynchronous and independent from the SDB work cycle {{
}}^{2(a),(c),(e)-ECI}

The MIB is a master/slave bus structure where the MIB-CM bus master initiates all communications to multiple slave devices very similar to the SBM communication. The MIB bus master (MIB-CM) requests information from each slave device in a round robin fashion at a fixed rate that is determined by the transaction time and the number of slave devices. The MIB bus master requests and receives information for each slave device once every HIPS bus frame cycle, as shown in Figure 7-15.

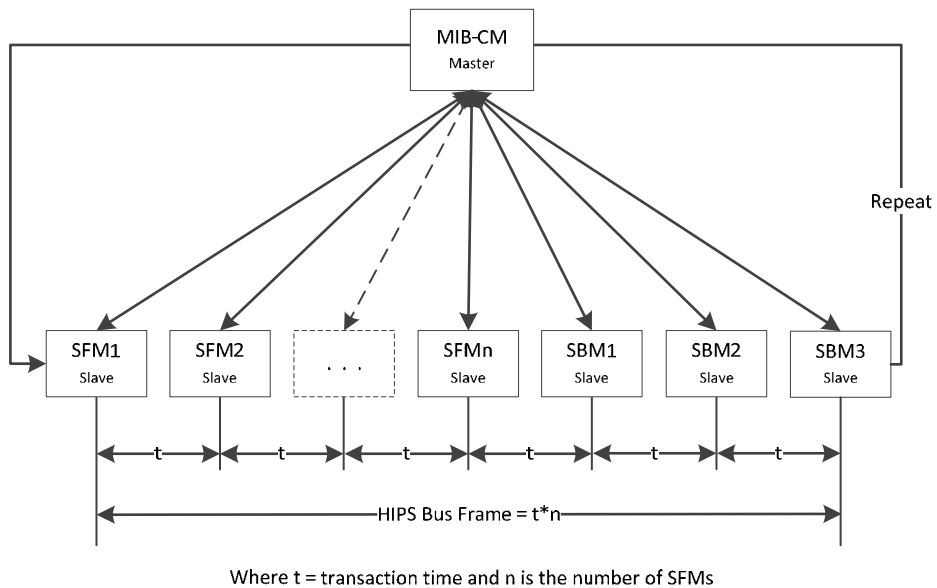


Figure 7-15. MIB-CM Work Cycle

8.0 Calibration, Testing and Diagnostics

The goal of calibration, testing, and diagnostics from the inputs at the SFM to the output of the EIM is to

1. increase reliability of input measurements
2. identify faults by either self-testing or period surveillance testing
3. provide high self-test coverage for immediate detection and diagnosis of faults

8.1 Calibration

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.

Calibration of the SFM involves the temperature and analog input sub-modules. The discrete input sub-module does not require calibration. The calibration is done using the MWS as the primary interface.

8.2 Testing

The goal of testing is to verify the functionality of the HIPS platform with minimal interruption of the normal flow of system process. Self-test has the capability to operate in unison with the normal operation of the system while verifying the functionality. The self-testing features of the HIPS modules do not affect the ability of any module to perform its safety function.

Surveillance testing methods share a similar goal of verifying functionality, but are performed with the HIPS module out of service.

8.2.1 Safety Function Module

The SFM input sub-module self-testing and auto-calibration features are designed to detect failures and faults related to the FPGA-related portions of an instrument channel.

8.2.1.1 Input Sub-Module

The testing of the SFMs varies depending on the type of input into the sub-module (i.e., analog, temperature, or discrete).

All analog and temperature inputs are converted into a voltage at the input to the input sub-module. 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.

{{

^{2(a),(c),(e)-ECI} In the event that a failure is detected, the SFM transitions into a fault mode and no longer transmits any information onto the data path.

The surveillance testing on analog and temperature input sub-module types is done using the MWS as the primary test interface.

Self-testing for an SFM with a discrete input sub-module is sufficient for checking performance of the sub-module, since there are no calibration requirements. The self-testing for a discrete input sub-module verifies all pins for 'stuck low', 'stuck high', 'shorts' or 'open.' In the event that a failure is detected, the module transitions into a fault mode and no longer transmits any information onto the data path.

8.2.1.2 Safety Function Algorithms

The FPGAs include built-in self-testing (BIST) to ensure that unannounced failures do not build up without plant personnel being notified by alarms. See Section 8.2.6 for a description of BIST.

{{

}}^{2(a),(c),(e)-ECI}

8.2.2 Communication Module

The CMs do not require surveillance testing or calibration. There are no setpoints and tunable parameters in the CM that need monitoring. Self-testing of the logic is incorporated into the BIST feature provided by the FPGA the logic is built into (see Section 8.2.6 for a description of the BIST). The data message error checking also detects failures that may occur in the communication module, as described in Section 8.2.4.

8.2.3 Equipment Interface Module

8.2.3.1 FPGA Testing

The FPGAs on the EIM use the BIST feature provided by the FPGA (see Section 8.2.6 for a description of the BIST). The data message error checking also detects any failures that may occur in the EIM, as described in Section 8.2.4.

8.2.3.2 Discrete Input Operation

The discrete input circuit senses the state of the field contact by its ability to source a wetting current through a closed contact by performing an open contact test and a closed contact test. If the detected current is less than a minimum value (or zero), the contact state is determined to be open. Otherwise, the contact state is determined to be closed.

The state of the input is provided to the logic on the input signals, where the input is high if the corresponding contact is closed.

To allow for self-testing of the input, each input is equipped with two test inputs which can be used by the logic to ensure that key components in the channel are functional.

8.2.3.2.1 Open Contact Test

{{

}}^{2(a),(c),(e)-ECI}

8.2.3.2.2 Closed Contact Test

{{

}}^{2(a),(c),(e)-ECI}

8.2.3.3 Actuation and Priority Logic

The individual transistors and logic gates in the EIM actuation and priority logic are simple discrete components that are designed to be tested for functionality by periodic surveillance tests. Testing the APL on an EIM is performed through periodic surveillance testing.

8.2.3.4 High Drive Output Testing

{

}}2(a),(c),(e)-ECI

{{

}}2(a),(c),(e)-ECI

Figure 8-1. Simplified Diagram Is a Single EIM Output

Table 8-1. Output Channel Test (When Contact Is Closed)

{{

}}2(a),(c),(e)-ECI

8.2.4 Communication Buses

{{

}}2(a),(c),(e)-ECI

Table 8-2. SDB, MIB, and CTB Request and Response Structure

{{

}}2(a),(c),(e)-ECI

1. {{

}}2(a),(c),(e)-ECI

2. Synchronization/Timing failure detection:

a. {{

}}2(a),(c),(e)-ECI

3. CRC failure detection

- a. Tx: CRC generation failure - source issue
- b. Rx: CRC calculation failure or data comparison not matching – destination issue
- c. Rx: Signal corruption due to noise
- d. Rx: Multiple transmitters on the line
- e. Rx: Detection of wrongly synchronized HIPS bus transaction, CRC did not compare at the time it was required.

4. Protocol failure

- a. Rx: The HIPS bus packet synchronization (SYNC) detection circuit detects the lack of signal or inaccurate SYNC words. Successful SYNC detection is required for any HIPS bus transaction; therefore, communications on the HIPS bus do not occur with SYNC failures
- b. Rx: Lack of response following a request from a master: attempt to access a board that has been removed
- c. Rx: Invalid access such as: for master: attempt to access an invalid board or invalid register; for slaves: attempt to write to a read-only address, etc.

The performance of the core logic within the safety function module FPGA and the SDB communications buses can be monitored by reviewing the results of the periodic injection of a PTDA test signal into one core logic within the safety function module 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 by the MIB. The test injection can be used to confirm the core logic and the SDBs are functioning correctly from the SFM output through the {{ }}^{2(a),(c),(e)-ECI} in the EIM. The periodic injection of the PTDA test signal has no adverse impact on the safety function of the division because the other two core logics and SDBs not being tested remain fully functional and can process PTDA decisions made in the SFM logic.

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. The detecting module transitions into a fault mode depending on the class of failure depicted in Table 8-4. What is done with the failure after it has cleared is application-specific.

8.2.5 End-to-End Testing of Entire Platform

End to end testing of the HIPS platform is performed through overlap testing. The individual self-tests on the different components of the HIPS platform ensure that the entire platform is functioning correctly. All of the components, minus the discrete logic of the EIM, have self-testing capabilities that ensure the information passed on to the following step in the data path is correct. For the discrete logic, periodic surveillance testing is used to ensure that it retains the correct functionality. Self-testing of the platform ensures that errors in the system shall be detected in the order of minutes whereas periodic surveillance is subject to the frequency of the surveillance testing. Figure 8-2 shows the different components and the test coverage that each performs. In the overlap method, the modules ensure that they are each functioning correctly and the error checking on the communication buses ensure that transfer of data is correct.

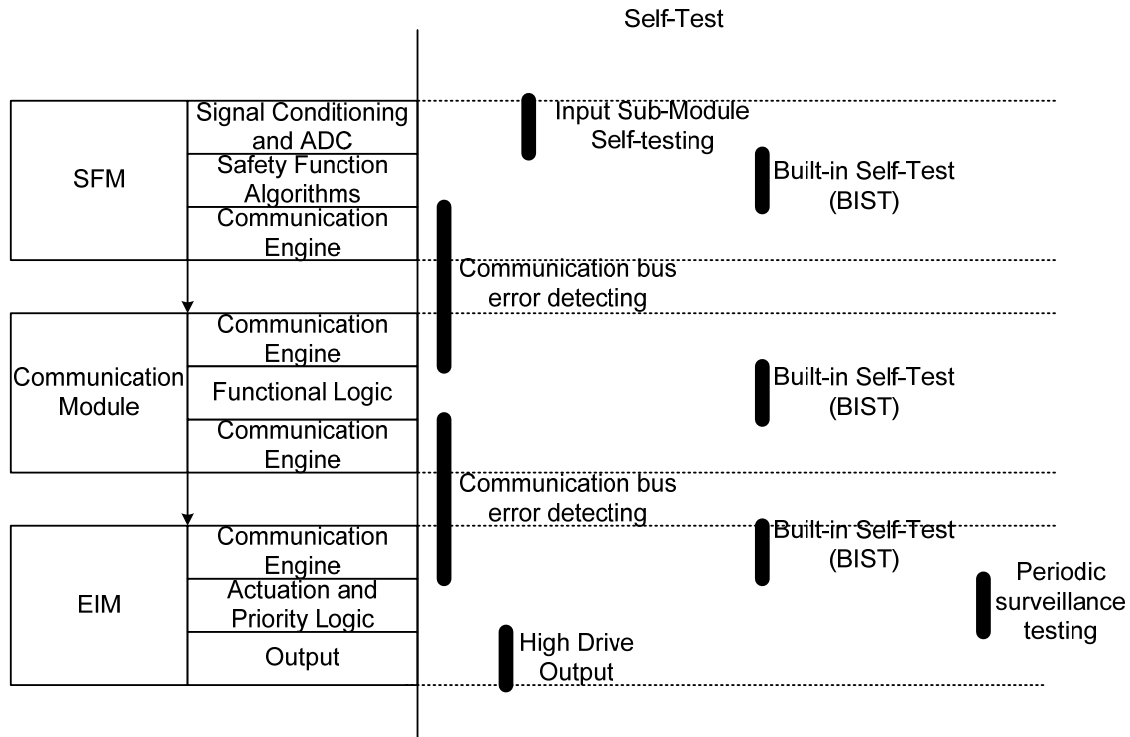


Figure 8-2. Overlap of Testing for the HIPS Platform

8.2.6 Built-In Self-Testing

{{

}}2(a),(c),(e)-ECI

{{

}}^{2(a),(c),(e)-ECI}

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.

8.2.7 Module Testing

The HIPS platform incorporates self-testing of the individual modules that is designed to continuously verify the operation of the board. These tests are performed in the background continuously. If any of these tests fail, the module transitions to the fault mode, which cannot be cleared without manual interaction.

{{

}}^{2(a),(c),(e)-ECI}

These detected failures would not affect a safety function due to the required redundancy in safety-related I&C systems.

The MWS can be used to retrieve identification information from the NVMs. For modules using an SRAM-based FPGA, file identification and CRC information can be retrieved for both the setpoint and tunable parameter file, and the FPGA configuration file. For modules using an OTP or flash-based FPGA, file identification and CRC information can be retrieved for the setpoint and tunable parameters file. The MWS can also be used to retrieve build version identification information from the FPGAs.

8.3 Surveillance Requirements

The HIPS platform testing and calibration features can be integrated in the typical set of technical specification surveillance requirements.

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

The HIPS platform self-testing features can take the place of technical specification surveillance requirements (e.g., channel functional tests) that are performed during power operation to verify setpoints and protection systems actuation capability. The MWS can also be used to retrieve identification information from the NVMs and FPGAs to verify that the electronic designs and setpoints are the correct versions. The associated CRC checks verify the files have not been corrupted.

Periodic surveillance testing of the equipment interface module APL would need to be integrated with other actuation logic tests.

The self-testing features of the EIM supplement the typical channel operational tests.

The self-testing features of the SFM analog and temperature input sub-modules supplement the typical channel calibration surveillance requirement by continuously testing performing calibration checks. The channel calibration surveillance requirement of the entire instrument loops would be supported by the MWS interface.

8.4 System Diagnostics

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. Table 8-3 shows the LED indications and function that each status represents.

Table 8-3. HIPS Module LEDs

LED Name	Indication type	Green	Red	Off
ACTIVE	Board power indicator	Board powered Latches closed	Board powered One latch open	Board is OFF Both latches open
FAULT	HIPS module fault indicator	Solid - module not in FAULT Flashing – non-vital fault	Module in FAULT	Module in FAULT

The classification of HIPS faults and how the two LEDs for status indication indicate each type of fault are shown in Table 8-4.

Table 8-4. HIPS Platform Fault Classification

Class of Failure	Description	Active LED	Fault LED
Fatal	Fatal faults refer to a severe type of fault that compromises the control function of the HIPS module. The most obvious fatal fault is the complete loss of input power to the HIPS chassis. The result is a loss of all HIPS module functionality and status indication.	Off	Off
Vital	Vital faults refer to the class of errors that compromise the HIPS module and cause it to become inoperable for the performance of one or more safety functions. The occurrence of a vital fault requires immediate maintenance.	Green	Red
Non-vital	Non-vital faults refer to the class of errors that do not affect the overall HIPS module performance or integrity. Following one or more non-vital faults, the HIPS module is still operable and its integrity has not been compromised. Maintenance is required and is performed by the station in accordance with the work management system. For example, the loss of one redundant power supply input is regarded as a non-vital failure.	Green	Green (flashing)

9.0 Simplicity

Simplicity has been considered throughout the development of the key design concepts of the HIPS platform that address the NRC's fundamental design principles: independence, diversity, redundancy, and predictability and repeatability. The HIPS platform architecture is developed with consideration of proven analog PS architectures found in existing nuclear power plants. Section 3 provides an implementation of a representative PS. The HIPS platform is based on only five core components: SFM, input sub-module, CM, EIM, and hard-wired HWM.

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

9.1 Independence

Functions within the FPGA of each module are implemented with finite state machines in order to achieve deterministic behavior. The HIPS platform does not rely on complex system/platform 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.

Dedicating safety function modules to a function or group of functions based on its 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 utilized throughout a division of a HIPS platform implementation.

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

9.2 Diversity

The use of diversity within a digital system is a strategy for eliminating the concern of software CCFs. Use of different FPGA architectures provides a simple and verifiable approach to equipment and design diversity. Inherent differences between FPGA architectures are supplemented by intentional software tool differences.

By simply implementing safety functions on an SFM based on its inputs, safety functions can be segmented to provide functional diversity. The discrete and digital logic circuits on an EIM provide a clear distinction between those portions that are and are not vulnerable to a software CCF. The discrete circuits handle multiple inputs (e.g., automatic digital signals, operator manual signals) and can be fully tested. These diversity attributes may simplify a plant's I&C systems design by not having to install a separate diverse actuation system to address software CCF concerns.

9.3 Redundancy

{{

}}2(a),(c),(e)-ECI

9.4 Predictability and Repeatability

Functions within the FPGA of each module are implemented with finite state machines in order to achieve deterministic behavior. Deterministic behavior allows implementation of a simple communication protocol using a predefined message structure with fixed time intervals. This simple periodic communication scheme is used throughout the architecture. Communication between SFMs and CMs is implemented through a simple and well established RS-485 physical layer. The configurable transmit-only or receive-only 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.

10.0 Summary and Conclusions

The HIPS is a protection system architecture jointly developed by Rock Creek Innovations, LLC and NuScale Power, LLC. The HIPS platform is a logic based platform that does not utilize software or microprocessors for operation. It is composed of logic implemented using discrete components and field programmable gate array technology. The scope of this report is limited to the HIPS platform, which consists of various components and processing modules. The HIPS platform is designed for use in safety-related and important-to-safety applications.

The HIPS platform is based on the fundamental I&C design principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth and was developed specifically to provide a simple and reliable solution for nuclear power plant safety-related and important-to-safety I&C applications. These key design concepts help contribute to simplicity in both the functionality of the system and in its implementation.

This LTR presented key design concepts of the safety I&C platform. The LTR demonstrated how the HIPS platform key design concepts meet the fundamental I&C design principles of independence; redundancy; predictability and repeatability; and diversity and defense-in-depth outlined in the NRC Design Specific Review Standard for NuScale. The LTR also describes testing and diagnostic concepts applied to the HIPS platform and how the key design concepts are implemented to achieve simplicity in the overall HIPS platform design concept.

The platform design was developed to support meeting the guidelines and the requirements of NRC RGs and IEEE standards applicable to safety-related applications, including RG 1.153, which endorse IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Since the HIPS platform is a programmable digital device, RG 1.152, IEEE Std. 7-4.3.2-2003, DI&C-ISG-04, and the Staff Requirements Memorandum for SECY-93-087 were also used to guide the general platform design. The LTR also demonstrated that the key design concepts of the HIPS platform meet the applicable regulatory requirements.

NuScale Power submitted this LTR to the NRC for review and generic approval that the HIPS platform key design concepts satisfy the review guidance in NRC Design Specific Review Standard for NuScale.

An applicant using the approved HIPS platform topical report can reference the generic approval for all design concepts, as noted in the Appendices. For concepts with full conformance, the applicant needs to demonstrate that the requirements have been implemented. The applicant can reference the generic approval for all design concepts with partial conformance; however, additional application-specific information would be needed to show how these HIPS platform design concepts were implemented in the system design. The applicant

would also need to address all other application-specific items that were not reviewed or not approved as part of the HIPS platform topical.

11.0 References

- 11.1.1 Institute of Electrical and Electronics Engineers, IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.
- 11.1.2 Institute of Electrical and Electronics Engineers, IEEE Std. 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Piscataway, NJ.
- 11.1.3 DI&C-ISG-04, Revision 1, Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc) Interim Staff Guidance.
- 11.1.4 U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," SRM SECY-93-087, July 21, 1993.
- 11.1.5 U.S. Nuclear Regulatory Commission, "Criteria for Safety Systems," Regulatory Guide 1.153, Revision 1.
- 11.1.6 U.S. Nuclear Regulatory Commission, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, Revision 3.
- 11.1.7 Institute for Printed Circuits, "Qualification and Performance Specification for Rigid Printed Boards," IPC-6012B, Amendment 1, Bannockburn, IL, December 2006.
- 11.1.8 IEC 60950-1:2005, Information Technology Equipment – Safety – Part 1: General requirements.
- 11.1.9 U.S. Nuclear Regulatory Commission, "Criteria for Independence of Electrical Safety Systems," Regulatory Guide 1.75, Revision 3, February 2005.
- 11.1.10 Multinational Design Evaluation Program Generic Common Position DICWG No. 1, Common Position on the Treatment of Common Cause Failure Caused By Software within Digital Safety Systems.
- 11.1.11 Branch Technical Position 7-19, Revision 6, Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems.
- 11.1.12 U.S. Nuclear Regulatory Commission, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," NUREG/CR-6303, 1994.

- 11.1.13 John Thomas, Francisco Luiz de Lemos, and Nancy Leveson, Research Report: NRC-HQ-11-6-04-0060, Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants, November, 2012.
- 11.1.14 National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Final Report," Washington, DC, 1997.
- 11.1.15 Bishop, P. G., Adelard LLC, "*Review of Software Design Diversity*," December 1994.
- 11.1.16 Sedra, A. S., and K. C. Smith, Microelectronic Circuits, Oxford University Press, New York, NY, 2004.

Appendix A. IEEE Std. 603-1991 Traceability Matrix

This appendix provides for a summary of regulatory conformance of the HIPS platform with IEEE Std. 603-1991. Conformance is described in four ways:

Full Conformance: The generic HIPS platform design concepts fully satisfy the IEEE Std. 603-1991 requirement.

HIPS Platform Supports Application Specific Conformance: The generic HIPS platform design concepts provide the capability to implement application-specific design that can fully satisfy the IEEE Std. 603-1991 requirement.

Application Specific Item: The generic HIPS platform design concepts do not address the IEEE Std. 603-1991 requirements.

Not Applicable: The IEEE Std. 603-1991 requirement does not apply to the generic HIPS platform.

The appendix also provides a cross reference to the applicable portions of the report where conformance information is presented.

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
1	Scope			
2	Definition			
3	References			
4	Safety System Design			
5	Safety System Criteria			

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.1	Single-Failure Criterion	<p>The HIPS platform supports application-specific conformance based on the modular nature of the HIPS platform equipment and HIPS platform design features that provide electrical and communication independence features and diagnostic, self-test, and calibration capabilities.</p>	<p>An applicant or licensee referencing the HIPS platform topical report should perform a system-level failure modes and effects analysis (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-related 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.</p> <p>The applicant or licensee referencing the HIPS platform topical report should demonstrate the application-specific diagnostic, self-test, and manually initiated test and calibration features do not adversely affect channel independence, system integrity, or the system ability to meet the single-failure criterion.</p> <p>An applicant or licensee referencing the HIPS platform topical report must review the actions defined to be taken when failures and errors are detected</p>	Sections 2, 4, 5, and 8

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
			<p>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 should confirm that this information is provided in the single failure analysis for the plant-specific application.</p>	
5.2	Completion of a Protective Action	<p>The HIPS platform supports-application-specific conformance based on HIPS platform design features to implement coincidence logic and the platform response time characteristics.</p>	<p>The applicant or licensee will demonstrate that the application-specific logic satisfies the completion of protective action requirements.</p>	Section 2.5.4
5.3	Quality	<p>The HIPS platform topical report does not address quality assurance because these are application-specific activities that depend on the equipment vendor used to implement the HIPS system.</p>	<p>An applicant or licensee referencing HIPS platform topical report must confirm that the HIPS platform manufacturer is currently on the Nuclear Procurement Issues Committee (NUPIC) list or confirm that the HIPS manufacturing quality processes conform to the applicant's 10 CFR 50, Appendix B compliant program (i.e., vendor is included in the applicant's approved vendor list). The applicant will need to demonstrate that the HIPS software and associated development lifecycle conform to applicable regulatory requirements.</p>	N/A

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.4	Equipment Qualification	The HIPS platform topical report does not address equipment qualification because these are application-specific activities that depend on the equipment vendor used to implement the HIPS system.	An applicant or licensee referencing the HIPS platform topical report must confirm that the HIPS platform equipment is qualified to the applicable regulatory requirements.	N/A
5.5	System Integrity	The HIPS platform supports application-specific conformance based on platform integrity characteristics and design features that ensure a safe state can be achieved in the presence of failures.	<p>An applicant or licensee referencing the HIPS platform topical report 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.</p> <p>An applicant or licensee referencing the HIPS platform topical report must confirm that system real-time performance is adequate to ensure completion of protective action within critical time frames required by the plant safety analyses.</p>	Sections 7 and 8

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.6	Independence			
5.6.1	Between Redundant Portions of a Safety System	The HIPS platform supports application-specific conformance based on platform design features that provide equipment electrical isolation and digital communication independence features.	An applicant or licensee referencing the HIPS platform topical report 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. An applicant or licensee referencing the HIPS platform topical report must provide redundant power sources to separately supply the redundant power conversion features within the HIPS platform.	Section 4
5.6.2	Between Safety Systems and Effects of Design Basis Event	The HIPS platform supports application-specific conformance based on platform design features that provide equipment electrical isolation and digital communication independence features.	An applicant or licensee referencing the HIPS platform topical report must confirm that the HIPS platform equipment is qualified to the applicable regulatory requirements.	N/A
5.6.3	Between Safety Systems and Other Systems			

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.6.3.1	Interconnected Equipment	The HIPS platform supports application-specific conformance based on platform design features that provide equipment electrical isolation and digital communication independence features.	<p>An applicant or licensee referencing the HIPS platform topical report must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety to nonsafety-related systems.</p> <p>An applicant or licensee referencing the HIPS platform topical report should perform an FMEA to demonstrate 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.</p>	Section 4
5.6.3.2	Equipment in Proximity	The HIPS platform supports application-specific conformance based on platform design features that provide equipment electrical isolation and digital communication independence features.	An applicant or licensee referencing the HIPS platform topical report must perform isolation testing on the HIPS platform equipment to demonstrate the capability to satisfy the Class 1E to non-Class 1E isolation requirements,	Section 4

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
			consistent with the provisions of IEEE Std. 384-1992.	
5.6.3.3	Effects of a Single Random Failure	The HIPS platform supports application-specific conformance based on platform design features that provide equipment electrical isolation and digital communication independence features.	An applicant or licensee referencing the HIPS platform topical report should perform a system-level FMEA to demonstrate 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.	Section 4
5.6.4	Detailed Criteria	The HIPS platform supports application-specific conformance based on platform design features that provide equipment electrical isolation and digital communication independence features.	An applicant or licensee referencing the HIPS Platform Topical Report 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 provisions of IEEE Std. 384-1992.	Section 4

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.7	Capability for Test and Calibration	<p>The HIPS platform supports application-specific conformance based on platform design features that provide the capability to perform diagnostics and self-testing. The HIPS platform diagnostic and self-test capabilities are thorough and provide automatic detection of most identified failure modes at the platform level. 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 implementation of application-specific diagnostic logic and confirmation of continued execution via the MWS.</p>	<p>An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment is used for testing and calibration of safety-related features.</p> <p>An applicant or licensee referencing the HIPS platform topical report 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.</p> <p>An applicant or licensee referencing the HIPS platform topical report will need to 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.</p>	Section 8
5.8	Information Displays			
5.8.1	Displays for Manually Controlled Action	<p>The HIPS platform supports application-specific conformance with design features that provide the capability to transmit field sensor signals for use in display systems associated with</p>	<p>An applicant or licensee referencing the HIPS platform topical report must describe any manual controls and associated displays used to support</p>	Sections 2.5.2 and 4.7

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		manually controlled actions, receive manual demand signals, and perform the required safety actions.	manually controlled safety actions necessary to accomplish a safety function for which no automatic control is provided.	
5.8.2	System Status Indication	The HIPS platform supports application-specific conformance with design features that provide the capability to perform the protective actions and provide status both locally with discrete front panel indicators and remotely to display instrumentation.	An applicant or licensee referencing the HIPS platform topical report 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.	Sections 2.5.2 and 4.7
5.8.3	Indication of Bypasses	The HIPS platform supports application-specific conformance with design features that provide the capability to provide indication of bypass for application-specific protective actions and provide indication of bypass both locally with discrete front panel indicators and remotely to display instrumentation. The HIPS platform supports the actuation of the bypass or inoperable condition of a safety group 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. The HIPS platform topical report describes the platform maintenance features, which address the behavior of bypass and inoperable status indications.	An applicant or licensee referencing the HIPS platform topical report 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.	Sections 2.5.2 and 4.7

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.8.4	Location	<p>The HIPS platform supports application-specific conformance with design features that provide the capability to locally monitor protective action states with discrete front panel indicators and initiate manually controlled protective actions with front panel toggle switches.</p>	<p>An applicant or licensee referencing the HIPS platform topical report must describe how the information displays are located accessible to the operator and are visible from the location of any controls used to effect a manually controlled protective action provided by front panel controls of a HIPS-based system.</p>	<p>Sections 2.5.2 and 4.7</p>
5.9	Control of Access	<p>The HIPS platform supports application-specific conformance. 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-related systems or equipment are generally dependent on the application. The HIPS platform topical report addresses platform features to control access to both hardware and software.</p> <p>The HIPS platform is a modular, rack mounted</p>	<p>An applicant or licensee referencing the HIPS platform topical report must provide additional control of access features to address the system-level aspects for a safety-related system using the HIPS platform.</p>	<p>Sections 4.8, 7.2, and 8.1</p>

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>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 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.</p> <p>The HIPS platform MWS serves as a maintenance workstation that supports offline, out-of-service 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 the HIPS platform topical report. Nevertheless, it is noted that the base platform architecture described in the HIPS platform topical report does not provide for direct or network connection of the MWS to the HIPS platform for online maintenance.</p>		
5.10	Repair	<p>The HIPS platform supports application-specific conformance based on the platform design features to implement coincidence logic, deterministic performance characteristics, capability to transmit field sensor signals for use in nonsafety-related systems, and the use</p>	<p>An applicant or licensee referencing the HIPS platform topical report must provide additional diagnostics or testing functions (self-tests or periodic surveillance tests) to address any system-level failures that are identified</p>	<p>Sections 2.2 and 8.2</p>

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>of the MWS for calibration. The timely identification and location of malfunctioning HIPS platform components is facilitated by platform (hardware and software) features. The majority of HIPS platform hardware is rack mounted. It is designed to be replaced rather than repaired, which greatly facilitates timely return to service. The HIPS platform boards contain indicating lights to provide a visual indication of functional status of the modules.</p> <p>The HIPS platform digital communication buses are a {{ }}^{2(a),(c),(e)-ECl} design. The {{ }}^{2(a),(c),(e)-ECl} architecture is designed to allow continued system operation in the presence of any single point of failure within the system. This feature allows the HIPS platform to detect individual faults online and allow repair without interruption of monitoring, control, and protection capabilities. The HIPS platform is designed to allow online, hot replacement of any module, under power while the system is running, with no impact on the operation of the system. The HIPS platform automatic diagnostics and self-test features and the specified periodic surveillance requirements are designed to detect and identify most failures of the platform.</p>	<p>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.</p>	

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.11	Identification	<p>The HIPS platform topical report does not address equipment identification requirements because it is an application-specific design activity. 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 for the HIPS platform can contribute to fulfillment of this requirement. In addition to faceplate identification of module type, the HIPS platform provides physical labels on the printed circuit board of each module to uniquely identify the hardware module and installed firmware.</p> <p>The HIPS platform contains features that include FPGA firmware version identifiers, which may be viewed using maintenance equipment to confirm the configuration of the installed equipment. 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 board configuration. These features address the second portion of IEEE Std. 7-4.3.2-2003, Clause 5.11.</p>	<p>An applicant or licensee referencing the HIPS platform topical report must establish the identification and coding requirements for cabinets and cabling for a safety system.</p>	Section 8.2.7

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.12	Auxiliary Features	The HIPS platform supports application-specific conformance based on the platform design features to implement coincidence logic, deterministic performance characteristics, capability to transmit field sensor signals for use in nonsafety-related systems, and the use of the MWS for calibration.	An applicant or licensee referencing the HIPS platform topical report must demonstrate the application-specific system design implemented with the HIPS platform meets the applicable regulatory requirements for auxiliary features.	Sections 2.5.1, 4.8, and 8.1
5.13	Multi-Unit Stations	The HIPS platform topical report does not address multi-unit stations requirements because it is an application-specific design activity.	An applicant or licensee referencing the HIPS platform topical report must demonstrate the application-specific system design implemented with the HIPS platform meets the applicable regulatory requirements for shared systems.	N/A
5.14	Human Factors Considerations	The HIPS platform topical report does not address human factor consideration because it is an application-specific activity that depends on the equipment vendor used to implement the HIPS system. The HIPS platform supports application-specific conformance based on the platform design features to provide local equipment status displays and system status information to other plant systems.	An applicant or licensee referencing the HIPS platform topical report must confirm the HIPS platform equipment meets any specified human factors requirements.	N/A
5.15	Reliability	The HIPS platform topical report does not address reliability because it is an application-specific activity that depends on the equipment vendor used to implement the HIPS system.	An applicant or licensee referencing the HIPS platform topical report must confirm the HIPS platform equipment meets any specified quantitative or qualitative reliability goals.	N/A

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
6	Sense and Command Features			
6.1	Automatic Control	The HIPS platform supports application-specific conformance based on the platform design features to implement coincidence logic, deterministic performance characteristics, and methods to build-in diversity.	An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment provides automatic safety system sense and command features for required safety functions.	Sections 2.5.1 and 2.5.4
6.2	Manual Control	The HIPS platform supports application-specific conformance based on the platform design features that support the implementation of manual controls and connectivity to information displays.	An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment provides manual safety system sense and command features for required safety functions	Sections 2.5.5 and 4.5
6.3	Interaction Between the Sense and Command Features and Other Systems	The HIPS platform supports application-specific conformance based on built-in diversity feature and platform design features to implement coincidence logic, and maintenance features to either bypass or trip channels.	An applicant or licensee referencing the HIPS platform topical report will need to 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.	Sections 2.5.2 and 6

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
6.4	Derivative of System Inputs	The HIPS platform supports application-specific conformance based on platform design features to acquire and condition field sensor measurements of the required variables.	An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment acquires and conditions field sensor measurements of the required variables.	Section 2.5.1
6.5	Capability for Testing and Calibration	<p>The HIPS platform supports application-specific conformance based on platform design features that provide the capability to perform diagnostics and self-testing.</p> <p>The HIPS platform diagnostic and self-test capabilities are thorough and provide automatic detection of most identified failure modes at the platform level. 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 implementation of application-specific diagnostic logic and confirmation of continued execution via the MWS.</p>	<p>An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment is used for testing and calibration of safety-related features.</p> <p>An applicant or licensee referencing the HIPS platform topical report must provide additional diagnostics or testing functions (self-tests or periodic surveillance tests) to address system-level failures that are identified as detectable only through periodic surveillance.</p> <p>An applicant or licensee referencing the HIPS platform topical report will need to 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.</p>	Section 8.2.1.1

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
6.6	Operating Bypasses	The HIPS platform supports application-specific conformance based on HIPS platform design features to implement coincidence logic response time characteristics, self-test features, and calibration capabilities.	An applicant or licensee referencing the HIPS Platform Topical Report will need to describe how the HIPS platform equipment is used for operating bypasses.	Sections 2.5.1, 2.5.3, 7, and 8
6.7	Maintenance Bypass	The HIPS platform supports application-specific conformance based on HIPS platform OOS switch options, self-test features, and calibration capabilities.	An applicant or licensee referencing the HIPS platform topical report will need to describe and provide the technical specification requirements for how the HIPS platform equipment is used for maintenance bypasses.	Section 2.5.2
6.8	Setpoints	The HIPS platform topical report does not address setpoints, setpoint methodologies, or HIPS platform module accuracies because these are application-specific activities that depend on the equipment vendor used to implement the HIPS system. The HIPS platform supports application-specific conformance on the platform design features to implement coincidence logic and deterministic performance characteristics.	An applicant or licensee referencing the HIPS platform topical report will need to describe the setpoints, setpoint methodologies, or HIPS platform module accuracies used for a safety system implemented with the HIPS platform equipment.	Sections 2.5.1, 2.5.3, and 7
7	Execute Features			

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
7.1	Automatic Control	The HIPS platform supports application-specific conformance based on the platform design features to implement coincidence logic, deterministic performance characteristics, and methods to build-in diversity.	An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment is used to provide automatic safety system sense and command features for required safety functions.	Section 2.5.4
7.2	Manual Control	The HIPS platform supports application-specific conformance based on the platform design features that support the implementation of manual controls and connectivity to information displays.	An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment is used to provide manual safety system sense and command features for required safety functions.	Section 2.5.5
7.3	Completion of a Protective Action	The HIPS platform supports application-specific conformance based on HIPS platform design features to implement coincidence logic and the platform response time characteristics.	The applicant or licensee will demonstrate that the application-specific logic satisfies the completion of protective action requirements.	Section 2.5.4
7.4	Operating Bypass	The HIPS platform supports application-specific conformance based on HIPS platform design features to implement coincidence logic, response time characteristics, self-test features, and calibration capabilities.	An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment is used for operating bypasses.	Sections 2.5.1, 2.5.3, 7, and 8
7.5	Maintenance Bypass	The HIPS platform supports application-specific conformance based on the HIPS platform OOS switch options, self-test features, and calibration capabilities.	An applicant or licensee referencing the HIPS platform topical report will need to describe how the HIPS platform equipment is used for maintenance bypasses.	Section 2.5.2

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
8	Power Source Requirements	The HIPS platform topical report does not address the power sources for a specific safety system application.	An applicant or licensee referencing the HIPS platform topical report will need to describe power sources to the HIPS platform equipment and how it meets applicable regulatory requirements.	N/A

Appendix B. IEEE Std. 7-4.3.2-2003 Traceability Matrix

This appendix provides for a summary of regulatory conformance of the HIPS platform with IEEE Std. 7-4.3.2-2003. Conformance is described in four ways:

Full Conformance: The generic HIPS platform design concepts fully satisfy the IEEE Std. 7-4.3.2-2003 requirement.

HIPS Platform Supports Application Specific Conformance: The generic HIPS platform design concepts provide the capability to implement application-specific design that can fully satisfy the IEEE Std. 7-4.3.2-2003 requirement.

Application Specific Item: The generic HIPS platform design concepts do not address the IEEE Std. 7-4.3.2-2003 requirements.

Not Applicable: The IEEE Std. 7-4.3.2-2003 requirement does not apply to the generic HIPS platform.

The appendix also provides a cross reference to the applicable portions of the report where conformance information is presented.

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
1	Scope			
2	References			
3	Definitions and Abbreviations			
4	Safety System Design Basis			
5	Safety System Criteria			

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.1	Single Failure Criterion	N/A		N/A
5.2	Completion of a Protective Action	N/A		N/A
5.3	Quality	The HIPS platform topical report does not address quality assurance because these are application-specific activities that depend on the equipment vendor to be used to implement the HIPS system.	An applicant or licensee referencing HIPS platform topical report must confirm that the HIPS platform manufacturer is currently on the NUPIC list or confirm that the HIPS manufacturing quality processes conform to the applicant's 10 CFR 50, Appendix B compliant program (i.e., vendor is included in the applicant's approved vendor list). The applicant will need to demonstrate that the HIPS software and associated development lifecycle conform to applicable regulatory requirements.	N/A
5.4	Equipment Qualification	The HIPS platform topical report does not address equipment qualification because these are application-specific activities that depend on the equipment vendor used to implement the HIPS system.	An applicant or licensee referencing the HIPS platform topical report must confirm that the HIPS platform equipment is qualified to the applicable regulatory requirements.	N/A
5.5	System Integrity			

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.5.1	Design for Computer Integrity	<p>The HIPS platform supports application-specific conformance based on platform integrity characteristics and design features that assure a safe state can be achieved in the presence of failures. The HIPS platform is designed 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 HIPS platform has defined the operating modes and states, classification of failures, and the effect of failures on the system. The HIPS platform digital communication design contains provisions to address conditions with the potential to defeat a safety function.</p> <p>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 a general use computer platform. The HIPS platform restart operation occurs much faster than a microprocessor-based computing system because the HIPS platform FPGA logic does not rely on an operating system, software drivers for peripheral devices, or an executable software program. Additionally, the HIPS platform FPGA logic</p>	<p>An applicant or licensee referencing the HIPS platform topical report 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.</p> <p>An applicant or licensee referencing the HIPS platform topical report must confirm that system real-time performance is adequate to ensure completion of protective action within critical time frames required by the plant safety analyses.</p>	Sections 7 and 8.2

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>self-diagnostics that run on restart complete much faster than a typical microprocessor-based computer's startup diagnostics.</p> <p>{{</p> <p>}}^{2(a),(c),(e)-ECI} The OTP or flash-based FPGA is a fixed configuration and does not function like the SRAM-based FPGA; therefore, this type of testing is not applicable for the OTP or flash-based FPGA.</p> <p>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. Through its requirements and specifications, the HIPS platform contains provisions to enter a fail-safe state defined by the plant-</p>		

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>specific configuration and to force a channel's output to a defined state using the OOS switch. 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 multi-divisional workstation and contains provisions to ensure 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, etc.). 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.</p>		
5.5.2	Design for Test and Calibration	<p>The HIPS platform supports application-specific conformance based on platform design features that assure test and calibration functions do not create any adverse effect on the ability of the HIPS platform to perform its safety function. The HIPS platform scope does not include a separate computer to provide the verification of test and calibration data. The HIPS platform scope does not establish whether a licensee might rely</p>	<p>An applicant or licensee referencing the HIPS platform topical report 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.</p> <p>An applicant or licensee referencing the HIPS platform topical report that relies on a separate computer for the sole verification of test and calibration data</p>	Section 8

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>solely on separate computer to provide the verification of test and calibration data for a future HIPS-based safety system.</p> <p>For each standardized circuit board, test and calibrations features are discussed in the specifications for that board. The HIPS platform incorporates test and calibration features to provide a means to bypass channels during surveillance testing, setpoint changes, and calibration. The HIPS platform also incorporates features to provide a means to force a channel's output to a defined state. The HIPS platform allows a MWS to access configuration data, which includes setpoint and calibration data, when a channel is bypassed. The HIPS platform design for the test and calibration functions does not impede the safety functions of a system.</p> <p>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, etc.). Instead, a HIPS platform standardized circuit board performs individual functions supported through distinct FPGA logic and each individual function does not share its FPGA</p>	<p>should ensure adequate iV&V, configuration management, and quality assurance for the test and calibration functions of the separate computer.</p>	

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>logic resources with other functions. Within the HIPS platform, test and calibration function logic neither uses the safety signal path communication buses nor competes with safety function logic for FPGA logic resources.</p> <p>The HIPS platform test and calibration features do not impede the safety function of a HIPS-based safety system. The self-diagnostic functions do not compete with safety functions for the safety signal path or FPGA programming resources.</p>		
5.5.3	Fault Detection and Self-diagnostics	<p>The HIPS platform supports application-specific conformance based on platform design features that assure self-diagnostic functions do not create an adverse effect on the ability of the HIPS platform to perform its safety function.</p> <p>The HIPS platform incorporates self-diagnostic features to provide a means to detect and alert a 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.</p> <p>Unlike microprocessor-based computer systems, to which Clause 5.5.3 of IEEE</p>	<p>An applicant or licensee referencing the HIPS platform topical report 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.</p> <p>An applicant or licensee referencing the HIPS platform topical report must verify that the manufacturer included the self-diagnostic functions within its type testing of the HIPS platform standardized circuit boards during equipment qualification.</p> <p>An applicant or licensee referencing the HIPS platform topical report must demonstrate that the combination of</p>	Section 8.2

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>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, etc.). Instead, a HIPS platform standardized circuit board 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.</p> <p>The HIPS platform self-diagnostics do not impede the safety function of the system. The self-diagnostic functions do not compete with safety functions for FPGA programming resources. Equipment qualification will demonstrate continued operability of the HIPS platform's safety functions and safety signal path while the self-diagnostics are operable. The specifications define the self-diagnostic functions at power-up and periodically along with failure result reporting capabilities.</p> <p>The HIPS platform design does not use reliability requirements of the safety system to establish the need and scope of self-diagnostic capabilities. Instead, the</p>	<p>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.</p>	

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		HIPS platform design goal is to provide self-test coverage of all critical platform functions included in the generic HIPS platform design.		
5.6	Independence	The HIPS platform supports application-specific conformance based on platform design features that provide digital communication independence features. These features can prevent adverse interactions among safety divisions and between safety-related equipment and equipment that is not safety-related.	An applicant or licensee referencing the HIPS platform topical report must demonstrate that the full system design, any use of a shared component, the equipment installation, and the communication bus architecture provide the required independence. An applicant or licensee referencing the HIPS platform topical report must verify that the safety network provides communications independence and security requirements for communication from safety-related to nonsafety-related systems.	Sections 2.6, 4.6, and 8.2
5.7	Capability for Test and Calibration	N/A		N/A
5.8	Information Displays	N/A		N/A
5.9	Control of Access	N/A		N/A
5.10	Repair	N/A		N/A

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.11	Identification	<p>The HIPS platform topical report does not address equipment identification requirements because it is an application-specific design activity. 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 for the HIPS platform can contribute to fulfillment of this requirement. In addition to faceplate identification of module type, the HIPS platform provides physical labels on the printed circuit board of each module to uniquely identify the hardware module and installed firmware.</p> <p>The HIPS platform contains features that include FPGA firmware version identifiers, which may be viewed using maintenance equipment to confirm the configuration of the installed equipment. 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 board configuration. These features address IEEE Std. 7-4.3.2-2003, Clause 5.11.b.</p>	<p>An applicant or licensee referencing the HIPS platform topical report 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.</p>	Section 8.2.7

IEEE Std. Section Number	Section	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
5.12	Auxiliary Features	N/A		N/A
5.13	Multi-Unit Stations	N/A		N/A
5.14	Human Factors Consideration	N/A		N/A
5.15	Reliability	The HIPS platform topical report does not address reliability because it is an application-specific activity that depends on the equipment vendor used to implement the HIPS system.	An applicant or licensee referencing the HIPS platform topical report must confirm that the HIPS platform equipment meets any specified quantitative or qualitative reliability goals.	N/A
6	Sense and Command Features	N/A		N/A
7	Execute Features	N/A		N/A
8	Power Source Requirements	N/A		N/A

Appendix C. Digital I&C Interim Staff Guidance 04 Traceability Matrix

This appendix provides for a summary of regulatory conformance of the HIPS platform with DI&C-ISG-04. Conformance is described in four ways:

Full Conformance: The generic HIPS platform design concepts fully satisfy the DI&C-ISG-04 requirement.

HIPS Platform Supports Application Specific Conformance: The generic HIPS platform design concepts provide the capability to implement application-specific design that can fully satisfy the DI&C-ISG-04 requirement.

Application Specific Item: The generic HIPS platform design concepts do not address the DI&C-ISG-04 requirements.

Not Applicable: The DI&C-ISG-04 requirement does not apply to the generic HIPS platform.

The appendix also provides a cross reference to the applicable portions of the report where conformance information is presented.

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
1	Interdivisional Communications			
SP 1	A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE Std. 603. It is recognized that division voting logic must receive inputs from	The HIPS platform supports application-specific conformance with IEEE Std. 603-1991 Clause 5.6 based on platform design features that provide equipment electrical isolation and digital communication independence features. The HIPS modules that have capabilities for communication are the SFM, CM, and the IM.	An applicant or licensee referencing the HIPS platform topical report 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.	Sections 2.5.1.1 and 2.5.1.3

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	multiple safety divisions.	<p>Each SFM can handle up to four input sub-modules. The HIPS platform input sub-module can accept inputs from digital sensors that are transmitted in analog (e.g., voltage or current signal loop or binary input signals). Inputs must be from the same safety division or a nonsafety-related entity. If from a nonsafety entity, the applicant or licensee must demonstrate how the SFM is not dependent on the nonsafety entity to accomplish its safety-related function. The five separate and logically independent communication buses of the SFM use bi-directional communication and are designed for intradivisional communication.</p> <p>The EIM has four separate and logically independent communication buses designed for intradivisional communication. As a result, the EIM has no capabilities for direct inter-divisional communications.</p> <p>The CM supports intradivisional and, depending on how it is configured within the overall safety system architecture, interdivisional communication. The RS-485 ports</p>	<p>An applicant or licensee referencing the HIPS platform topical report 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 provisions of IEEE Std. 384-1992.</p> <p>An applicant or licensee referencing the HIPS platform topical report must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety to nonsafety-related systems.</p>	

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>are designed for intradivisional communication. The fiber optic ports support inter- and intradivisional communication. A CM that has fiber optic ports either disabled or configured for transmit only would not be dependent on information outside its own safety division. If there is any fiber optic port configured for receive only, the licensee or applicant must demonstrate the acceptability of using this information. Some acceptable reasons are: 1) the receive-only ports on the CM are used to support divisional voting; 2) the receive-only port is only utilized when the safety channel is not being relied upon to perform its safety-related function (see Staff Position 10); and 3) information received is not used to perform a safety-related function.</p>		

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 2	<p>The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.</p>	<p>The HIPS platform supports application-specific conformance because it 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. This 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.</p> <p>As mentioned in Staff Position 1, the modules which may have information or signals originating outside its safety division are the SFMs and CMs. Demonstrating compliance with this staff position requires a review of SFM inputs and of receive-only ports on the CM. Specifically, if the SFM input or the receive-only port on a CM is of the same safety division, this staff position doesn't apply.</p> <p>Otherwise, the applicant or licensee will demonstrate how each safety channel is protected from adverse influence from outside the division of</p>	<p>An applicant or licensee referencing the HIPS platform topical report must demonstrate that the full system design, any use of a shared component, the equipment installation, and the power distribution architecture provide the required independence.</p> <p>An applicant or licensee referencing the HIPS platform topical report 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 provisions of IEEE Std. 384-1992.</p> <p>An applicant or licensee referencing the HIPS platform topical report must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety to nonsafety-related systems.</p>	<p>Sections 4.6 and 7</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>which that channel is a member. Some of the HIPS design features that can be utilized are the deterministic communication protocols, asynchronous communication between modules, error detection and error handling (see Staff Position 12), dedicated logic for communication engines with no handshaking or interrupts, and placing a module in bypass so that it is not being relied upon to perform its safety function (see Staff Position 10).</p>	<p>An applicant or licensee referencing the HIPS platform topical report must provide redundant power sources to separately supply the redundant power conversion features within the HIPS platform.</p>	
SP 3	<p>A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed</p>	<p>The HIPS platform supports application-specific conformance because the safety data work cycle provides the complete set of communications for the HIPS platform to perform a safety function. The HIPS platform supports simple safety function execution by ensuring there are no functions other than those required by the safety function. The HIPS platform provides a one-way isolated transmit only data connection to provide information from the safety channel to other systems for performing functions such as online monitoring. This one-</p>	<p>An applicant or licensee referencing the HIPS Platform topical report must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety to nonsafety-related systems.</p>	<p>Sections 4.6, 4.7, and 7.7.1</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, on-line monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system.</p> <p>Receipt of information from outside the division, and the performance of functions not directly related to</p>	<p>way data connection is completely independent from data communications required by the safety data work cycle.</p>		

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of “significantly” used in the demonstration.</p>			
SP 4	<p>The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is</p>	<p>The HIPS platform conforms because the 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.</p> <p>Communication between modules is done asynchronously. The transfer of information between the safety function logic and the communications logic is achieved via dedicated shared data registers.</p>	None required.	Sections 2.5.1.2, 2.5.1.3, 2.5.3, 2.5.4, 2.6, 4.6, and 7.7.1

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such</p>	<p>These data registers are dedicated to the function of transferring the trip/not trip information and may not be utilized for any other purpose.</p> <p>All logic and supporting circuits for the communications of the safety data within the HIPS platform are performed by safety-related equipment.</p> <p>The access to the shared data registers is performed in a fully deterministic manner. The safety function logic and the communications logic are implemented on a single FPGA for each module type. The FPGA utilizes a single clock source to ensure all interactions between independent logic are fully deterministic.</p> <p>The HIPS platform work cycle ensures a fully deterministic communications from the input of the HIPS platform to the final actuated device output.</p>		

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.</p>			
SP 5	<p>The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should</p>	<p>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.</p>	<p>An applicant or licensee referencing the HIPS platform topical report must confirm that system real-time performance is adequate assuming longest possible completion time to ensure completion of protective action within critical time frames required by the plant safety analyses.</p>	Section 7.7.1

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	be detected and alarmed.			
SP 6	The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	The HIPS platform conforms because it does not use communications handshaking or interrupts to perform any of its safety function logic communications.	None required.	Section 4.6
SP 7	Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system	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. The description of the HIPS platform safety data work cycle in Section 7.7.1 discusses how the full safety data work cycle ensures fully deterministic communications from the input of the HIPS platform to the final actuated device output. The communications within the safety data work cycle are continuous and remain fully deterministic at all times.	None required.	Sections 7.6.6, 7.7, and 8.2.4

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	behavior.			
SP 8	Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.	<p>The HIPS platform supports application-specific conformance because it enables communications between safety divisions through point-to-point one way interfaces. Deterministic communication protocols are used with predefined message structures and fixed time intervals.</p> <p>All communication between modules is done asynchronously without the use of handshaking or interrupts. The HIPS modules can be configured to assume safe-states upon errors or faults detected. Error detecting features are further discussed in Staff Position 12.</p> <p>The HIPS platform provides a one-way isolated transmit only data connection to provide information from the safety channel to other systems for performing functions such as online monitoring. This one-way data connection is completely independent from data communications required by the safety data work cycle.</p>	An applicant or licensee referencing the HIPS platform topical report must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety-related to nonsafety-related systems.	Sections 4.6, 4.7, 4.8, and 7.7

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 9	Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.	The HIPS platform conforms because each HIPS module has data registers with pre-determined purposes and fixed locations. The exchange of information from the safety function logic module to the communications logic and from the communications logic to the safety function logic of the next module is achieved through dedicated shared data registers. These data registers are dedicated to the function of transferring the trip/not trip information and may not be used for any other purpose.		Sections 2.5.1.2, 2.5.1.3, 2.5.3, 2.5.4, and 4.6
SP 10	Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hard-wired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g., engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor /	The HIPS platform conforms because it does not rely on software execution. The HIPS platform is based on FPGA technology. The FPGA logic for the specific functions required by the HIPS platform and the application are 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 online. Any changes to this logic require the equipment to be removed from service.	None required.	Sections 4.8, 6.1.1, and 8.1

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hard-wired logic. "Hard-wired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety</p>	<p>When an SFM is removed from service, the HIPS platform is no longer dependent on the SFM to perform the safety function and the HIPS platform enables a MWS to update setpoints and tunable parameters, such as setpoints, using a temporary connection that can only be connected to one division at a time.</p>		

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.			
SP 11	Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.	<p>The HIPS platform conforms because it does not rely on software execution. The HIPS platform is based on FPGA technology. The FPGA logic for the specific functions required by the HIPS platform and the application are 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 online. Any changes to this logic require the equipment to be removed from service.</p> <p>When an SFM is removed from service, the HIPS platform is no longer dependent on the SFM to perform the safety function and the HIPS platform enables a MWS to update setpoints and tunable parameters, such as setpoints, using a temporary connection that can only be connected to one division at a time.</p>	None required.	Sections 4.8, 6.1.1, and 8.1

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 12	<p>Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute “single failures” as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:</p>	<p>The HIPS platform conforms because all communications are implemented with a combination of the following attributes. These attributes ensure that communication faults do not adversely affect the performance of the required safety functions.</p> <ul style="list-style-type: none"> • configurable uni-directional fiber optic communications • hard-wired point-to-point connection • cyclic redundancy checksum protection • deterministic state-machines on CMs • fixed periodic communications • predetermined packet structure and packet length are fixed • master/slave communication protocol • OOS switch • administrative controls 	None required.	Sections 2.6, 4.6 5.3, and 8.2.4

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<ul style="list-style-type: none"> Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise. 	<p>All HIPS platform communications are implemented with an error detection scheme. The HIPS platform safety data work cycle implements the transfer of the safety data in a {{ }}^{2(a),(c),(e)-ECI} ensuring an error occurring {{ }}^{2(a),(c),(e)-ECI} does not impact the ability to perform the safety function. {{</p> <p style="text-align: right;">}}^{2(a),(c),(e)-ECI}</p>	<p>An applicant or licensee referencing the HIPS platform topical report must configure the slave modules to alarm and assume a fail-safe state.</p>	<p>Sections 2.6, 4.6 5.3, and 8.2.4</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>{{</p> <p style="text-align: center;">}}2(a),(c),(e)-ECI</p>		
	<ul style="list-style-type: none"> Messages may be inserted into the communication medium from unexpected or unknown sources. 	<p>Interdivisional communication over hard-wired point-to-point fiber optic connections means that messages cannot be inserted into the communication medium from unexpected or unknown sources, and cannot be sent to the wrong destination.</p>	<p>None required.</p>	<p>Sections 2.6, 4.6 5.3, and 8.2.4</p>
	<ul style="list-style-type: none"> Messages may be sent to the wrong destination, which could treat the message as a valid message. 	<p>All HIPS platform interdivision communications are “point-to-point” meaning that all messages are passed directly from a sending node to a receiving node.</p>	<p>None required.</p>	<p>Sections 2.6, 4.6 5.3, and 8.2.4</p>
	<ul style="list-style-type: none"> Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption. 	<p>{{</p> <p style="text-align: center;">}}2(a),(c),(e)-ECI</p>	<p>None Required.</p>	<p>Sections 2.6, 4.6 5.3, and 8.2.4</p>
	<ul style="list-style-type: none"> Messages may contain data that is outside the expected range. 	<p>The HIPS platform safety data work cycle transfers the safety data from the SFM to a CM and from a CM to the EIM. The safety data being transferred is simply a trip or not trip</p>	<p>None required.</p>	<p>Sections 2.6, 4.6 5.3, and 8.2.4</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
		signal. There are no complex values being transferred eliminating the need for complex data bounds checking algorithms.		
	<ul style="list-style-type: none"> Messages may appear valid, but data may be placed in incorrect locations within the message. 	<p>{{</p> <p style="text-align: right;">}}2(a),(c),(e)-ECI</p>	None required.	Sections 2.6, 4.6 5.3, and 8.2.4

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<ul style="list-style-type: none"> Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm). 	<p>{{</p> <p style="text-align: right;">}}2(a),(c),(e)-ECI</p>	None required.	Sections 2.6, 4.6 5.3, and 8.2.4

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<ul style="list-style-type: none"> Message headers or addresses may be corrupted. 	<p>{{</p> <p style="text-align: right;">}}2(a),(c),(e)-ECI</p>	None required.	Sections 2.6, 4.6 5.3, and 8.2.4

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.	sending node to a receiving node without the involvement of any equipment outside the division.		
SP 15	Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.	<p>{{</p> <p style="text-align: center;">}}^{2(a),(c),(e)-ECI}</p>	None required.	Sections 7.6.6, 7.7, and 8.2.4

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 16	<p>Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock.</p> <p>(Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria (“GDC”) 24, which states, “interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.”; and (2) IEEE Std. 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.)</p>	<p>The HIPS platform supports application-specific conformance based on platform design features that provide equipment electrical isolation and digital communication independence features.</p> <p>The HIPS platform safety data work cycle implements the transfer of the safety data in a {{ }}^{2(a),(c),(e)-ECI} ensuring an error occurring {{ }}^{2(a),(c),(e)-ECI} does not impact the ability to perform the safety function.</p>	<p>An applicant or licensee referencing the HIPS platform topical report must demonstrate that the full system design, any use of a shared component, the equipment installation, and the power distribution architecture provide the required independence.</p> <p>An applicant or licensee referencing the HIPS platform topical report 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 provisions of IEEE Std. 384-1992.</p> <p>An applicant or licensee referencing the HIPS platform topical report must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety to nonsafety-related systems.</p>	Sections 5.5 and 7.7.1

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
			An applicant or licensee referencing the HIPS platform topical report must provide redundant power sources to separately supply the redundant power conversion features within the HIPS platform.	
SP 17	Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.	The HIPS platform topical report does not address equipment qualification because these are application-specific activities that depend on the equipment vendor used to implement the HIPS system.	An applicant or licensee referencing the HIPS platform topical report must confirm that the HIPS platform equipment is qualified to the applicable regulatory requirements.	N/A

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 18	Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	The HIPS platform supports application-specific conformance because all HIPS platform communications are designed specifically for the function they are assigned to implement. There are no unneeded capabilities or functions.	An applicant or licensee referencing the HIPS Platform topical report should perform a system-level FMEA to demonstrate the application-specific use of the HIPS platform identifies each potential failure mode and determines the effects of each. An applicant or licensee referencing the HIPS platform topical report 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.	Section 8.2.4
SP 19	If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that	<p>{{</p> <p>}}^{2(a),(c),(e)}-ECI</p>	<p>An applicant or licensee referencing the HIPS Platform topical report will need to describe how the HIPS platform equipment is used to provide a deterministic communication structure for required safety functions.</p> <p>An applicant or licensee</p>	Sections 7.6.6, 7.7, and 8.2.4

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.</p>		<p>referencing the HIPS platform topical report must confirm that system real-time performance is adequate to ensure completion of protective action within critical time frames required by the plant safety analyses.</p>	
SP 20	<p>The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.</p>	<p>The HIPS platform topical report does not address equipment qualification because these are application-specific activities that depend on the equipment vendor used to implement the HIPS system.</p>	<p>An applicant or licensee referencing the HIPS Platform topical report will need to describe how the HIPS platform equipment is used to provide a deterministic communication structure for required safety functions.</p> <p>An applicant or licensee referencing the HIPS platform topical report 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.</p> <p>An applicant or licensee</p>	N/A

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
			referencing the HIPS Platform Topical Report must confirm that system real-time performance is adequate to ensure completion of protective action within critical time frames required by the plant safety analyses.	
2	Heading	Command Prioritization		
SP 1	A priority module is a safety related device or software function. A priority module must meet all of the 10 C.F.R. Part 50, Appendix A and B requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.	Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology) and will meet all of the 10 CFR Part 50, Appendix A and B requirements applicable to safety-related components.	N/A	Sections 2.5.4.3 and 6.3.2
SP 2	Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.	Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).	N/A	Sections 2.5.4.3 and 6.3.2

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 3	<p>Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a common-cause failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated “safe state.”), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as a containment isolation valve in an auxiliary feedwater line, there is no universal “safe state:” the valve must be open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be</p>	<p>Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).</p>	<p>N/A</p>	<p>Sections 2.5.4.3 and 6.3.2</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.</p>			
SP 4	<p>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.</p>	<p>Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).</p>	N/A	<p>Sections 2.5.4.3 and 6.3.2</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 5	Communication isolation for each priority module should be as described in the guidance for interdivisional communications.	Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).	N/A	Sections 2.5.4.3 and 6.3.2
SP 6	Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in RG 1.152, which endorses IEEE Std. 7-4.3.2-2003 (with comments). This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices, programmable gate arrays, or other such devices. Section 5.3.2 of IEEE Std. 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states	Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).	N/A	Sections 2.5.4.3 and 6.3.2

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.</p>			
SP 7	<p>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</p>	<p>Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).</p>	N/A	<p>Sections 2.5.4.3 and 6.3.2</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	controlled accordingly.			
SP 8	<p>To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or</p>	<p>Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).</p>	<p>N/A</p>	<p>Sections 2.5.4.3 and 6.3.2</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the “all possible combinations” criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either “TRUE” or “FALSE” and then can be ignored in the “all possible combinations” testing.</p>			
SP 9	<p>Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and including failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute common-cause failure if it were to result in the disabling of the module safety function.</p>	<p>Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).</p>	N/A	<p>Sections 2.5.4.3 and 6.3.2</p>

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 10	The priority module must ensure that the completion of a protective action as required by IEEE Std. 603 is not interrupted by commands, conditions, or failures outside the module's own safety division.	Not applicable. All priority logic capability within the HIPS platform is performed by discrete logic components (analog technology).	N/A	Sections 2.5.4.3 and 6.3.2
3	Heading	Multidivisional Control and Display Systems		
3.1	Heading	Independence and Isolation		
SP 1	Nonsafety stations receiving information from one or more safety divisions:	Not applicable. The generic HIPS platform does not include multidivisional control and display stations. Therefore, the requirements for multidivision controls in this section of DI&C-ISG-04 do not apply.	N/A	N/A
SP 2	Safety-related stations receiving information from other divisions (safety or nonsafety):	Not applicable. The HIPS platform does not address cross divisional communications or communications from nonsafety systems because these are application-specific activities that depend on the application of the architecture to be implemented in the HIPS system.	An applicant or licensee referencing the HIPS platform topical report must demonstrate that the full system design supports any cross divisional and nonsafety communication with the appropriate independence and isolation.	N/A

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 3	Nonsafety stations controlling the operation of safety-related equipment:	<p>The HIPS platform supports application-specific conformance with an enable nonsafety control 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. Otherwise, the nonsafety-related component control signal input is ignored in the APL when the switch is open. The specific use and switch configuration details would be an application-specific item.</p> <p>The enable nonsafety control witch can be used to prevent spurious nonsafety-related control signals from adversely affecting safety-related components, as part of an application-specific design to provide independence features that satisfy IEEE Std. 603-1991 Clause 5.6.3 requirements. The HWM provides isolation for the nonsafety-related signal path when the enable nonsafety control switch is closed.</p>	The specific use of an enable nonsafety control switch and its configuration details would be an application-specific item.	Sections 4.4 and 4.6.2

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
SP 4	Safety-related stations controlling the operation of equipment in other safety-related divisions:	Not applicable. The generic HIPS platform does not provide this control capability.	N/A	N/A
SP 5	Malfunctions and Spurious Actuations	Not applicable. The generic HIPS platform does not provide this control capability.	N/A	N/A
3.2	Various human factors engineering requirements.	Not applicable. The generic HIPS platform does not address nonsafety controls, which are considered outside of the scope of the HIPS platform.	N/A	N/A
3.3	<p>D3 considerations may influence the number and disposition of operator workstations and possibly of backup controls and indications that may or may not be safety-related. The guidance provided herein is not dependent upon such details.</p> <p>D3 considerations may also impose qualification or other measures or guidelines upon equipment addressed in this ISG. The guidance presented herein does not include such considerations.</p> <p>Consideration of other aspects of D3 is outside the scope of this</p>	Not applicable. The generic HIPS platform does not address nonsafety controls, which are considered outside of the scope of the HIPS platform.	N/A	N/A

ISG-04 Section Number	Requirement	HIPS/PS Conformance	Application-Specific Information	Topical Report Applicable Sections
	guidance. Additional guidance concerning D3 considerations is provided separately.			

Appendix D. SRM for SECY-93-087 Traceability Matrix

This appendix provides for a summary of regulatory conformance of the HIPS platform with SRM for SECY-93-087. Conformance is described in four ways:

Full Conformance: The generic HIPS platform design concepts fully satisfy the SRM for SECY-93-087 requirement.

HIPS Platform Supports Application Specific Conformance: The generic HIPS platform design concepts provide the capability to implement application-specific design that can fully satisfy the SRM for SECY-93-087 requirement.

Application Specific Item: The generic HIPS platform design concepts do not address the SRM for SECY-93-087 requirements.

Not Applicable: The SRM for SECY-93-087 requirement does not apply to the generic HIPS platform.

The appendix also provides a cross reference to the applicable portions of the report where conformance information is presented.

SRM Section Number	Requirement	HIPS Conformance	Application-Specific Information	Topical Report Applicable Sections
1	The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed. The staff considers software design errors to be credible common-mode failures that must specifically be included in the evaluation. An acceptable method of performing analyses is described in NUREG-0493, "A	The HIPS platform supports application-specific conformance with SRM section 1 by using two diverse FPGA technologies to achieve equipment diversity. The diverse FPGA technologies result in an associated level of chip design diversity because different development tools are developed by the FPGA vendors to provide the final configured FPGAs. These tools have inherent diversity related to the differences in FPGA chip	An applicant or licensee referencing the HIPS platform topical report 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.	Section 6

SRM Section Number	Requirement	HIPS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979. Other methods proposed by an applicant will be reviewed individually.</p>	<p>architectures and programming methods.</p> <p>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, programmable logic design for an SFM is different when compared to the protection logic for any other SFM. In addition, the safety function or SFG are implemented on separate SFM hardware boards within the same division (or separation group). The functional diversity approach directly mitigates a set of CCFs associated with a specific FPGA platform.</p> <p>The reliance on FPGA technology diversity for defense against digital CCFs aligns with one example outlined in BTP 7-19.</p> <p>The discrete and digital logic circuits on an EIM provide a clear distinction between those portions that are and are not vulnerable to a software CCF. The discrete circuits handle</p>		

SRM Section Number	Requirement	HIPS Conformance	Application-Specific Information	Topical Report Applicable Sections
		<p>multiple inputs (e.g., automatic digital signals, operator manual signals) and can be fully tested.</p> <p>The HWM is constructed of discrete logic components only (i.e., there are no programmable devices). The HWM receives signals from the manual switches in the main control room and can be fully tested.</p> <p>The HIPS platform diversity strategy can be implemented in system I&C architectures ensure that system-level safety functions are not defeated by a CCF in one or the other type of FPGAs. For example, a four-division protection system can be implemented with one FPGA technology in two divisions and the other FPGA technology in two divisions. In this arrangement, a CCF associated with one type of FPGA would not defeat the safety function because two divisions would be unaffected due to the FPGA diversity and would accomplish the safety function.</p> <p>The diversity of the FPGA technologies is readily verifiable during implementation verification</p>		

SRM Section Number	Requirement	HIPS Conformance	Application-Specific Information	Topical Report Applicable Sections
		inspections.		
2	In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR). The vendor or applicant shall demonstrate adequate diversity within the design for each of these events. For events postulated in the plant SAR, an acceptable plant response should not result in a non-coolable geometry of the core, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment.	The HIPS platform supports application-specific conformance with SRM section 2 based on the diverse technologies and the modular nature of the HIPS platform equipment. These features support system architectures that can eliminate HIPS platform digital CCF vulnerabilities associated with system actuations.	An applicant or licensee referencing the HIPS platform topical report 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. An applicant or licensee referencing the HIPS platform topical report must address any other digital CCF vulnerabilities in the application-specific defense-in-depth and diversity analysis.	Section 6.4
3	If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if	The HIPS platform supports application-specific conformance with SRM section 3 based on the diverse technologies and the modular nature of the HIPS platform equipment. These features support system architectures that can eliminate HIPS platform digital CCF vulnerabilities associated with system actuations.	An applicant or licensee referencing the HIPS platform topical report 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	Section 6.4

SRM Section Number	Requirement	HIPS Conformance	Application-Specific Information	Topical Report Applicable Sections
	<p>the system is of sufficient quality to perform the necessary function under the associated event conditions. Diverse digital or nondigital systems are considered acceptable means. Manual actions from the control room are acceptable if adequate time and information are available to the operators. The amount and types of diversity may vary among designs and will be evaluated individually.</p>		<p>redundant system) to ensure HIPS platform safety performance in the presence of a digital CCF. An applicant or licensee referencing the HIPS platform topical report must demonstrate adequate mitigation or coping capability for any other digital CCF vulnerabilities in the application-specific defense-in-depth and diversity analysis.</p>	
4	<p>A set of safety-grade displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above. The specific set of equipment shall be evaluated individually, but shall be sufficient to monitor the plant states and actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown</p>	<p>The HIPS platform supports application-specific conformance with SRM section 4 based on the diverse technologies and the modular nature of the HIPS platform equipment. The diverse FPGA technology features support system architectures that can eliminate HIPS platform digital CCF vulnerabilities associated with providing monitoring signals to display equipment. The non-digital HWM and portions of an EIM support system architectures by providing manual control capability not vulnerable to digital CCFs.</p>	<p>An applicant or licensee referencing the HIPS platform topical report 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.</p>	<p>Manual Control: Sections 2.5.4, 2.5.5, 4.4, and 4.5 Monitoring: Section 6 and Sections 2.5.1, 2.6, and 4.7</p>

SRM Section Number	Requirement	HIPS Conformance	Application-Specific Information	Topical Report Applicable Sections
	condition. In addition, the specific equipment should be intended to control the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.			



LO-1116-51717

Enclosure 3:

Affidavit, AF-1116-51718

NuScale Power, LLC

AFFIDAVIT of Thomas A. Bergman

I, Thomas A. Bergman, state as follows:

- (1) I am the Vice President of Regulatory Affairs of NuScale Power, LLC (NuScale), and as such, I have been specifically delegated the function of reviewing the information described in this Affidavit that NuScale seeks to have withheld from public disclosure, and am authorized to apply for its withholding on behalf of NuScale
- (2) I am knowledgeable of the criteria and procedures used by NuScale in designating information as a trade secret, privileged, or as confidential commercial or financial information. This request to withhold information from public disclosure is driven by one or more of the following:
 - (a) The information requested to be withheld reveals distinguishing aspects of a process (or component, structure, tool, method, etc.) whose use by NuScale competitors, without a license from NuScale, would constitute a competitive economic disadvantage to NuScale.
 - (b) The information requested to be withheld consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), and the application of the data secures a competitive economic advantage, as described more fully in paragraph 3 of this Affidavit.
 - (c) Use by a competitor of the information requested to be withheld would reduce the competitor's expenditure of resources, or improve its competitive position, in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product.
 - (d) The information requested to be withheld reveals cost or price information, production capabilities, budget levels, or commercial strategies of NuScale.
 - (e) The information requested to be withheld consists of patentable ideas.
- (3) Public disclosure of the information sought to be withheld is likely to cause substantial harm to NuScale's competitive position and foreclose or reduce the availability of profit-making opportunities. The accompanying report reveals distinguishing aspects about the process and methods by which NuScale develops its Highly Integrated Protection System Platform.

NuScale has performed significant research and evaluation to develop a basis for this process and methods and has invested significant resources, including the expenditure of a considerable sum of money.

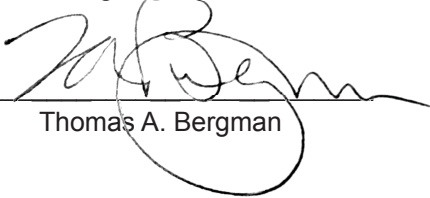
The precise financial value of the information is difficult to quantify, but it is a key element of the design basis for a NuScale plant and, therefore, has substantial value to NuScale.

If the information were disclosed to the public, NuScale's competitors would have access to the information without purchasing the right to use it or having been required to undertake a similar expenditure of resources. Such disclosure would constitute a misappropriation of NuScale's intellectual property, and would deprive NuScale of the opportunity to exercise its competitive advantage to seek an adequate return on its investment.

- (4) The information sought to be withheld is in the enclosed report entitled "Design of the Highly Integrated Protection System Platform Topical Report." The enclosure contains the designation "Proprietary" at the top of each page containing proprietary information. The information considered by NuScale to be proprietary is identified within double braces, "{{ }}" in the document.

- (5) The basis for proposing that the information be withheld is that NuScale treats the information as a trade secret, privileged, or as confidential commercial or financial information. NuScale relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC § 552(b)(4), as well as exemptions applicable to the NRC under 10 CFR §§ 2.390(a)(4) and 9.17(a)(4).
- (6) Pursuant to the provisions set forth in 10 CFR § 2.390(b)(4), the following is provided for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld:
- (a) The information sought to be withheld is owned and has been held in confidence by NuScale.
 - (b) The information is of a sort customarily held in confidence by NuScale and, to the best of my knowledge and belief, consistently has been held in confidence by NuScale. The procedure for approval of external release of such information typically requires review by the staff manager, project manager, chief technology officer or other equivalent authority, or the manager of the cognizant marketing function (or his delegate), for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside NuScale are limited to regulatory bodies, customers and potential customers and their agents, suppliers, licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or contractual agreements to maintain confidentiality.
 - (c) The information is being transmitted to and received by the NRC in confidence.
 - (d) No public disclosure of the information has been made, and it is not available in public sources. All disclosures to third parties, including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or contractual agreements that provide for maintenance of the information in confidence.
 - (e) Public disclosure of the information is likely to cause substantial harm to the competitive position of NuScale, taking into account the value of the information to NuScale, the amount of effort and money expended by NuScale in developing the information, and the difficulty others would have in acquiring or duplicating the information. The information sought to be withheld is part of NuScale's technology that provides NuScale with a competitive advantage over other firms in the industry. NuScale has invested significant human and financial capital in developing this technology and NuScale believes it would difficult for others to duplicate the technology without access to the information sought to be withheld.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 4, 2016



Thomas A. Bergman