U.S. Nuclear Regulatory Commission
Safety Evaluation for

Topical Report 6002-00301
“Advanced Logic System Topical Report”

ENCLOSURE 1

Table of Contents

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

TOPICAL REPORT 6002-00301, "ADVANCED LOGIC SYSTEM TOPICAL REPORT"

CS INNOVATIONS, LLC

PROJECT NO. 779

1.0 INTRODUCTION

By letter dated October 29, 2010 (Reference 1), the U.S. Nuclear Regulatory Commission (NRC) staff accepted the platform topical report 6002-00301, "Advanced Logic System Topical Report" for review. By letter dated July 29, 2010 (Reference 5), CS Innovations, LLC (CSI) submitted the "Advanced Logic System Topical Report" and an initial set of supporting documents for staff evaluation. CSI has since provided 21 subsequent submittal letters dated August 13, 2010, February 8 and 25, March 18 and 25, and November 11, 2011, February 10, April 5 and 25, May 1, July 24, August 30, November 1 and 15, and December 4, 2012, January 30, February 6 and 15, March 4, 6, and 27, 2013 (References 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, and 26). Each submittal letter contains a set of new or revised supporting documents wherein varying portions or entire documents are identified as proprietary.

The "Advanced Logic System Topical Report" identifies the scope of the requested platform safety evaluation (SE) (Reference 32). The SE of the Advanced Logic System (ALS) platform is limited to the development and test plans, specifications and procedures to design, verify and validate, and perform equipment qualification for two variants of seven circuit boards. The SE scope excludes the development, integration and test of a specific system, factory acceptance test of a system, or maintenance activities to support a fielded system. The SE also excludes any evaluation of the platform's accuracy and response time specifications to determine whether a given configuration will meet plant-specific or application-specific needs.

The ALS platform is an evolution of the development method, architecture, board suite, and communication interfaces developed and approved for use in the Wolf Creek Generating Station (Wolf Creek) main steam and feedwater isolation system (see Reference 2). The ALS platform is based on field programmable gate array (FPGA) technology and is being evaluated for general application within safety systems of current and new nuclear power generating stations. As such, this SE addresses criteria that apply to digital equipment for use in nuclear power plant safety systems.

Section 2.0 of this SE identifies the applicable regulatory bases and corresponding guidance and regulatory acceptance criteria against which the NRC staff evaluated the topical report submittals. Section 3.0 of this SE provides the instrumentation and control (I&C) technical evaluation of the topical report submittals and includes a description of the ALS platform.

Section 4.0 provides the limitations and conditions that apply to applicants or licensees referencing this SE for use of the ALS platform in a safety system of a nuclear power generating station. Section 5.0 provides a list of references and Section 6.0 provides the NRC staff conclusion.

For clarity, this SE uses the term “manufacturer” to refer to the applicant, CS Innovations, LLC, that submitted the “ALS Topical Report” for its platform while “applicant” refers to an “applicant for a license” and “licensee” refers to a holder of a license.

2.0 REGULATORY EVALUATION

NUREG-0800, “Standard Review Plan [(SRP)] for the Review of Safety Analysis Reports for Nuclear Power Plants,” Rev. 5, dated March 2007 provides the acceptance criteria for this review. NUREG-0800, which is referred to as the SRP, sets forth a method for reviewing compliance with applicable sections of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, “Domestic Licensing of Production and Utilization Facilities.” Specifically, SRP Chapter 7, “Instrumentation and Controls,” addresses the requirements for I&C systems in nuclear power plants based on light-water reactor designs. SRP Chapter 7 and Interim Staff Guidance (ISG), which augments and supplements SRP Chapter 7, principally establish the review process for digital I&C systems, which the NRC staff applied in this evaluation.

The suitability of a digital I&C platform for use in safety systems depends on the quality of its components, quality of the design process, and comprehensiveness of its equipment qualification. Suitability also considers system implementation characteristics—such as real-time performance, independence, and support of on-line surveillance requirements—that were demonstrated through the digital I&C platform’s verification, validation, and qualification efforts. Because this equipment is intended for use in safety systems and other safety-related applications, the platform topical report was evaluated against its ability to support application-specific system provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” based on the guidance contained in SRP Chapter 7, Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std 603,” which provides acceptance criteria for this standard. The platform topical report was similarly evaluated against IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” and Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std 7-4.3.2.”

SRP Chapter 7, Table 7-1, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety,” identifies design criteria and regulations from 10 CFR Part 50 applicable to I&C systems and relevant to the general review of the suitability of a digital I&C platform for use in safety-related applications. Some review criteria within the SRP depend on the design of an assembled system for a particular application, whereas this licensing topical report (LTR) presents elements of hardware and board-level FPGA programming that constitute the ALS platform, which is intended for use in a variety of applications. As such, this SE is necessarily limited to the evaluation of compliance with the relevant regulations and guidance documents to the degree that they can be met at the platform level, because ALS Topical Report scope excludes the details that would support a

plant-specific safety system application. In other words, this SE does not directly evaluate regulations and guidance at the system level and only evaluates the capabilities and characteristics of the ALS platform on a generic basis with respect to support of future evaluations of safety systems at the system level.

Determination of full compliance with the applicable regulations remains subject to a plant-specific licensing review of a full system design based on the ALS platform. Plant-specific action items have been established to identify criteria that should be addressed by applicants and licensees referencing this SE (see Section 4.2). In part this criteria is provided to facilitate an applicant's or licensee's ability to establish full compliance with the design criteria and regulations identified in SRP Chapter 7, Table 7-1 applicable to the applicant's or licensee's digital I&C system and in effect at the time of the ALS platform review. Regardless, the plant-specific action items identified in Section 4.2 do not obviate an applicant's or licensee's responsibility to adequately address new or changed design criteria or regulations that apply in addition to those to perform this SE when making a voluntary change to its facility.

The following regulations are applicable to the topical report:

- 10 CFR 50.55a(a)(1), "Quality Standards" requires structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.
- 10 CFR 50.55a(h), "Protection and Safety Systems" approves the 1991 version of IEEE Standard 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," for incorporation by reference, including the correction sheet dated January 30, 1995.

The NRC staff also considered the application-specific 10 CFR Part 50, Appendix A, General Design Criterion, when evaluating the topical report for use in safety systems, as follows:

- GDC 1, "Quality Standards and Records"
- GDC 2, "Design Bases for Protection Against Natural Phenomena"
- GDC 4, "Environmental and Dynamic Effects Bases"
- GDC 13, "Instrumentation and Control"
- GDC 20, "Protection System Functions"
- GDC 21, "Protection System Reliability and Testability"
- GDC 22, "Protection System Independence"
- GDC 23, "Protection System Failure Modes"
- GDC 24, "Separation of Protection and Control Systems"
- GDC 25, "Protection System Requirements for Reactivity Control Malfunctions"
- GDC 29, "Protection Against Anticipated Operational Occurrences"

The NRC staff evaluated the topical report using applicable portions of the following guidance:

- RG 1.22, "Periodic Testing of Protection System Actuation Functions," Revision 0, describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 1, describes a method acceptable to the NRC staff for complying with

IEEE Std 603-1991 in regard to bypassed and inoperable status indication for nuclear power plant safety systems.

- RG 1.53, “Application of the Single-Failure Criterion to Safety Systems,” Revision 2, describes a method acceptable to the NRC staff for meeting the NRC’s regulations as they apply to the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.
- RG 1.62, “Manual Initiation of Protective Actions,” Revision 1, describes methods acceptable to the NRC staff for complying with IEEE Std 603-1991 in regard to the manual initiation of protective actions.
- RG 1.75, “Criteria for Independence of Electrical Safety Systems,” Revision 3, describes a method acceptable to the NRC staff for meeting physical independence of the circuits and electrical equipment that comprise or are associated with safety systems.
- RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” Revision 4, describes a method acceptable to the NRC staff for providing instrumentation to monitor variables for accident conditions.
- RG 1.100, “Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants,” Revision 3, describes a method acceptable to the NRC staff for meeting the seismic qualification.
- RG 1.118, “Periodic Testing of Electric Power and Protection Systems,” Revision 3, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to periodic testing of electric power and protection systems.
- RG 1.152, “Criteria for Use of Computers In Safety Systems of Nuclear Power Plants,” Revision 3, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to high functional reliability and design requirements for computers used in safety systems of nuclear power plants.
- RG 1.153, ““Criteria for Safety Systems,” Revision 1, endorsed IEEE Std 603-1991 as a method acceptable to the NRC staff for meeting the NRC’s regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants prior to IEEE Std 603-1991incorporation by reference into the regulations.
- RG 1.168, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 1, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to the verification and validation of safety system software.
- RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to the configuration management of safety system software.
- RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to test documentation of safety system software.

- RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997, describes a method acceptable to the NRC staff

for complying with the NRC's regulations as they apply to the unit testing of safety system software.

- RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997, describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to preparation of software requirement specifications for safety system software.
- RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997, describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the development processes for safety system software.
- RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 1, describes a method acceptable to the NRC staff for design, installation, and testing practices to address the effects of EMI/RFI and power surges on safety-related I&C systems.
- RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," describes a method acceptable to the NRC staff for meeting the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants.
- DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues, Interim Staff Guidance," Revision 2, describes methods acceptable to the NRC staff for implementing diversity and defense-in-depth (D3) in digital I&C system designs.
- DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," Revision 1, describes methods acceptable to the NRC staff to prevent adverse interactions among safety divisions and between safety-related equipment and equipment that is not safety-related.

The NRC staff also considered applicable portions of the branch's technical positions in accordance with the review guidance established within NUREG-0800, "U.S. Nuclear Regulatory Commission Standard Review Plan (SRP)," Chapter 7, "Instrumentation and Controls", in accordance with 10 CFR 50.34(h)(3), as follows:

- Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"
- Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2"
- BTP 7-11, "Guidance on Application and Qualification of Isolation Devices"
- BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- BTP 7-17, "Guidance on Self-test and Surveillance Test Provisions"
- BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems"
- BTP 7-21, "Guidance on Digital Computer Real-Time Performance"

3.0 TECHNICAL EVALUATION

The following subsections identify and describe the ALS platform's I&C components and evaluate these components and their development against the regulatory evaluation criteria identified in Section 2.0. Section 3.1 provides a description of the ALS platform, including the

I&C components and architecture. Each of the remaining subsections provides a specific technical evaluation against the applicable regulatory evaluation criteria.

3.1 Platform Description

The ALS platform consists of standardized circuit boards and FPGA programs. As an Appendix B supplier, CSI developed this platform to implement a variety of plant systems for use in nuclear power plants. The ALS platform is FPGA logic-based and provides a configurable architecture that relies on the quality of the design and development process to produce platform components suitable for use in nuclear safety related applications. The development activities are discussed in Section 3.2, and Section 3.2.1 provides an overview of the FPGA technology as applied within the ALS platform. The platform supports redundant instrument configurations to further ensure continued safety function operability. The ALS platform provides embedded diagnostic and testing capabilities, which have been built into the ALS platform through specification. Section 3.4.3 discusses the embedded diagnostic and testing capabilities to detect and annunciate equipment failures and to support maintenance and surveillance tests.

The ALS platform is a modular design where generic standardized circuit boards can be combined in a variety of configurations. A typical configuration of the ALS platform is illustrated by Figure 3.1.1-2.

Within the set of available FPGA-based configurations are varieties that implement increasing levels of built-in design diversity to support the application-specific safety analysis required by BTP 7-19. Section 3.1.2 introduces the methods to provide built in diversity, and Sections 3.2.3 and 3.2.4 provide further details of these methods. Section 3.9 provides the NRC staff's evaluation of the overall diversity that applications can implement.

An ALS platform-based safety-related instrument would be implemented using the one or more ALS chassis and peripheral equipment consisting of cabinets, power supplies, control panels, assembly panels and a maintenance workstation. The assembly panels incorporate field terminal blocks, fuse holders, switches, and other application-specific hardware. Nevertheless, the scope of this SE includes the set of seven standardized circuit boards, an instrument chassis, backplane, and backpanel. Each instrument backplane is an application-specific vertically-mounted circuit board into which each ALS standardized circuit board is installed within an instrument chassis. Instrument backplanes provide mating connectors for the standardized circuit boards to make standardized ALS bus connections and application-specific field input and output connections.

The ALS platform supports field input and output types, including digital contacts, relay contacts, analog current, analog voltage, resistance temperature detectors and thermocouples. The ALS chassis is an industry standard 19-inch chassis and ALS circuit boards are designed to a proprietary standardized size and shape. A maximum of ten ALS circuit boards can be installed in a single chassis. However, the ALS platform has been designed to allow multiple ALS chasses to be connected together when more boards are needed. The ALS bus architecture is designed to permit up to 60 boards to be locally connected to a single ALS bus using six

different chasses (one being the main chassis and the five others being expansion chasses) where all chasses are installed within the same cabinet. Each ALS chassis is typically powered through a redundant pair of current-sharing power supplies that receive input power from a Class 1E power source. These current-sharing power supplies are external to the ALS chassis and must provide a suitably stable 48VDC to each ALS chassis. Although the ALS platform has been designed to support this configuration, the external power supplies are not included as part of the ALS platform or its equipment qualification.

The manufacturer used type testing for hardware equipment qualification. The type tested equipment included a single instrument chassis containing one of each ALS circuit board type with FPGAs of a single design variant.

CSI developed the seven FPGA-based standardized circuit boards, instrument chassis, backplane, and backpanel using the ALS platform plans identified in Table 3.1-1. Appropriate subsections of this SE discuss these ALS platform plans and evaluate them against applicable regulatory evaluation criteria.

Table 3.1-1 Docketed ALS Platform Plans

Document ID	Title	Reference
6002-00000	ALS Management Plan	33
6002-00001	ALS Quality Assurance Plan	34
6002-00002	ALS Configuration Management Plan	35
6002-00003	ALS V&V Plan	36
6002-00004	ALS EQ Plan	37
6002-00005	ALS Test Plan	38
6002-00006	ALS Security Plan	39
6002-00018	ALS Platform FPGA VV Test Plan	45

The seven standardized circuit boards provided within the “ALS Topical Report” are:

1. ALS-302 Digital Input Board (48Vdc Contact Input);
2. ALS-311 Analog Input Board (RTD and Thermocouple);
3. ALS-321 Analog Input Board (Voltage/Current);
4. ALS-402 Digital Output Board (Contact Output);
5. ALS-421 Analog Output Board (Voltage/Current);
6. ALS-601 Communications Board; and,
7. ALS-102 Core Logic Board.

Following a description of the general instrument architecture in Section 3.1.1 and an overview of the development and operational concepts in Section 3.1.2, Section 3.1.4 describes the standardized circuit board approach and the capabilities of each standardized circuit board.

3.1.1 General Instrument Architecture

The block diagram, Figure 3.1.1-1, shows the general ALS platform architecture for a single backplane instrument that uses one of each standardized circuit board (see Reference 32, Figure 2.1-2). Within Figure 3.1.1-1, only those items identified within the dashed-lines are

included as part of “ALS Topical Report” (see Reference 32). This block diagram depicts only one possible configuration rather than any specific instrument configuration. Nevertheless, the block diagram is consistent with the configuration used during equipment qualification type testing.

The circuit boards (shown as blocks within Figure 3.1.1-1) and the instrument backplane, which is implied by the busses shown as Reliable ALS Bus #1 (RAB1), Test ALS Bus (TAB), and Reliable ALS Bus #2 (RAB2) within Figure 3.1.1-1, are developed and qualified as safety-related Class 1E equipment for use in a mild environment. As such, the NRC staff evaluated these components against the criteria established for digital equipment that may be relied upon to perform a safety function when installed in a mild environment. The NRC staff performed this evaluation of the ALS platform components in a generic fashion without consideration for unique or additional criteria that might apply to an application-specific safety function or plant installation. Most of the signals shown in Figure 3.1.1-1 are evaluated against applicable safety system criteria for use in performing a safety function with the exceptions of the TxB1, TxB2, and the TAB’s connection to the maintenance workstation (shown as ‘ASU’). These interfaces are evaluated against the criteria applicable to a safety-to-nonsafety digital communications that are not relied upon to perform a safety function, where the TxB1 and TxB2 are unidirectional output-only while the TAB is bi-directional.

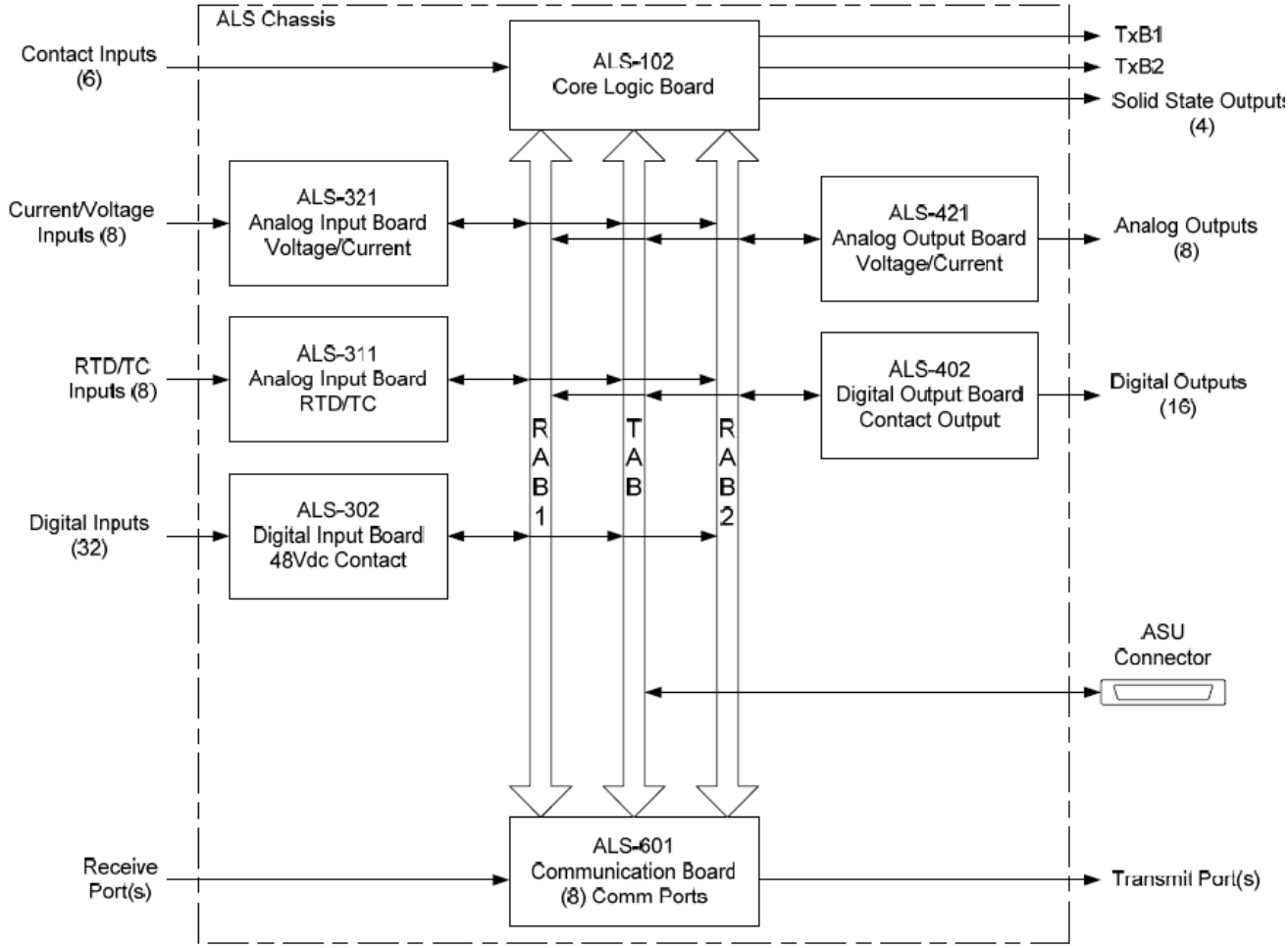

Figure 3.1.1-1 ALS Platform Architecture Block Diagram

Figure 3.1.1-2 shows a physical representation of the ALS platform for a single chassis single backplane instrument containing eight circuit boards (see Reference 32, Figure 2.1-1). Like the circuit boards, the mechanical structure and backplane of instrument were developed and qualified for use as safety-related Class 1E equipment in a mild environment. As such, the NRC staff evaluated all ALS platform components against environmental, electromagnetic compatibility and seismic qualification criteria applicable to safety-related Class 1E equipment for use in a mild environment. The depiction in Figure 3.1.1-2 is only intended to represent one possible configuration rather than any specific instrument configuration. Although similar, this depiction is not identical to the configuration used during equipment qualification type testing.

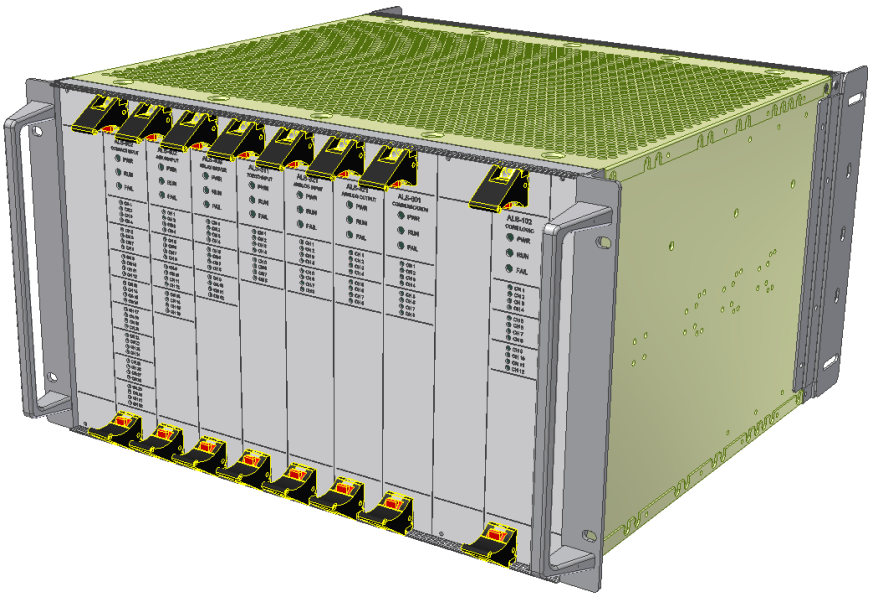

Figure 3.1.1-2 ALS Platform Instrumentation Chassis

As examples of ALS platform applications for potential digital modifications, the “ALS Topical Report” includes three proprietary appendices that show a variety of generalized equipment architectures with varying degrees of built-in diversity (see Reference 32, Appendices A thru C). This SE does not include a safety determination of adequate diversity for either the application-specific equipment or conceptual architectures provided in these appendices. Rather this SE uses the “ALS Topical Report” Appendices A thru C as examples that demonstrate the intended use of ALS platform design features in order to identify and document appropriate plant-specific action items.

The scope of this SE for diversity provides a generic SE of the design approaches to build diversity into ALS platform components and application-specific system architectures (Section 3.9). This SE also includes a plant-specific action item for the ALS platform to address applicant or licensee D3 analyses, which in part determine the degree of diversity to be specified for a given system or maintained between different systems.

Subsequent system development activities would demonstrate an ALS platform-based system implements the degree of diversity that has been specified for it. The final set of diversity and defense-in-depth considerations should address the overall plant instrumentation architecture with regard to potential plant vulnerabilities.

The isolation provided on ALS platform circuit boards is limited to that necessary for electromagnetic compatibility and circuit reliability. However, the board level provisions are not intended to ensure sufficient isolation exists between the ALS platform-based Class 1E equipment and Non-1E equipment. The “ALS Topical Report” scope excludes explicit identification of the method to ensure sufficient isolation exists between the ALS platform-based Class 1E equipment and Non-1E equipment. The “ALS Topical Report” states the

demonstration that this isolation criterion is met will be performed as part of a plant-specific application and qualified isolation devices will be used when required by the application.

The ALS platform equipment qualification applied type testing, which RG 1.209 identifies as the preferred method. This type testing used a representative instrument configuration to proof-test the platform's capabilities and to establish its qualified performance for safety-related applications in nuclear power plants.

Tables 3.1.1-1 and 3.1.1-2 identify ALS platform-level documents that apply to the entire ALS platform development and include specifications, qualification, configuration management and verification and validation (V&V) summary reports, and support information. Appropriate subsections of this SE discuss these ALS platform documents and evaluate them against applicable regulatory evaluation criteria.

Table 3.1.1-1 Docketed ALS Platform Development Documentation

Document ID	Title	Reference
6002-00007	ALS Platform Configuration Status Accounting	40
6002-00008	ALS Application Guidance	41
6002-00009	ALS Platform Requirements Traceability Matrix	42
6002-00010	ALS Platform Requirements Specification	43
6002-00011	ALS Platform Specification	44
6002-00030	ALS Design Tools	46
6002-00040	ALS Terms and Abbreviations	48
6002-00070	ALS EQ Rack System Specification	50
6002-00200	ALS Platform EQ Summary Report	51
6002-00240	ALS Platform Qualification Evaluation	52
6002-00400	ALS Platform Configuration Management Summary Report	53
6002-00500	ALS Platform VV Summary Report	54

Table 3.1.1-2 ALS Platform Development Documentation Available for Audit

Document ID	Title
6002-00019	ALS Platform VV Simulation Environment Specification
6002-00211	ALS EMC Qualification Report
6002-00212	ALS Seismic Qualification Report
6002-00213	ALS Environmental Qualification Report
6002-00214	ALS Environmental Test Procedure
6002-00215	ALS EMC Test Procedure
6002-00216	ALS Seismic Test Procedure
6002-00700	ALS Qualification Equipment Baseline Test Procedure

3.1.2 Development and Operational Concept Overview

Six of the ALS platform standardized circuit boards provide generic input or output capabilities and do not require application-specific FPGA programming. However, the seventh circuit board,

the ALS-102 Core Logic Board, does require application-specific FPGA programming. Regardless, the use of each circuit board requires configuration of its internal non-volatile memory settings to select the functionality needed to meet application specifications from the options specified to be available for the circuit board.

Each FPGA on each board provides built-in diversity through redundant hardware logic pairs, where this diversity is achieved through generation of two different hardware logic implementations from common program files by way of differing FPGA synthesis directives. The subsequent FPGA place and route operation assigns each of the two synthesized hardware logic implementations to a different physical section within a common FPGA device. Section 3.2.1 provides an overview of the FPGA technology as applied within the ALS platform, and Sections 3.2.3 and 3.2.5 provide the description and evaluation of the ALS platform's FPGA development process. These sections provide further details regarding FPGA-specific terminology.

The approach to provide built-in design diversity through generation of two different hardware logic implementations is the same approach used in the Wolf Creek MSFIS, which previously evaluated by the NRC staff (see Reference 2, Enclosure 2). Redundant and different hardware logic implementations within each FPGA device provide the capability to detect potential single-event upset conditions. The detection of a single-event upset eliminates this as a potential source of an otherwise undetectable failure, which supports equipment reliability and safety function operability. In response to the detection of a single-event upset the equipment can take application-specific actions to annunciate the failure and initiate fail-safe actions.

The FPGA on each standardized circuit board may be programmed with one of two FPGA program images (i.e., design variants) to provide an additional degree of built-in design diversity. [

] The functional requirements for each FPGA design variant are identical and either FPGA design may be programmed into the FPGA of the common circuit board design. At a higher level of instrument and system integration, different combinations of diverse FPGA programs may be integrated either within an instrument channel or division, or between redundant instrumentation channels or divisions.

Using design variants of FPGA program files adds built-in design diversity beyond that provided within the Wolf Creek MSFIS, because a common FPGA program would no longer be used within all redundant standardized circuit boards of the same type. Applying design variants of FPGA program files within redundant instrumentation channels or divisions provides mitigation against potential common-cause programming errors that might otherwise produce adverse equipment behavior. Section 3.2.4 provides the description and evaluation of the process to develop FPGA design variants.

An instrumentation chassis or set of instrumentation chasses will be defined based on application-specific system requirements. Each instrument chassis will have an associated backplane, backpanel, and circuit board set. The backplane provides signal connectivity between boards, and the backpanel provides signal connectivity to the application-specific external devices (e.g., sensors, actuators, data recorders, maintenance workstation, etc.) or

other backplanes. The system requirements will identify the application-specific approach to build-in sufficient diversity, so any plant vulnerabilities to common-cause programming failures are adequately addressed. Section 3.9 provides the description and the evaluation of the approaches to provide diversity.

Application-specific instrumentation specifications will also define the set of circuit boards and their configuration for installation into a backplane or backplanes. An application-specific ALS-102 Core Logic Board is required among the set of circuit boards within each backplane, except for backplanes accessible via a bus extension. The FPGA program within each ALS-102 Core Logic Board determines both the sequence of input/output board logical operations (i.e., processing) and frequency at which individual input/output board functions are accessed by an instrument. The general operation of the ALS-102 Core Logic Board is to acquire inputs from its set of input boards, to perform application-specific logic, and to provide outputs to its set of output boards. The ALS-102 Core Logic Board exchanges digital data with the other circuit boards that form the instrument. These circuit boards either share the same physical backplane or are accessed via the backplane bus extension. The digital data exchanges occur over a redundant bidirectional communication path provided by the backplane(s) and referred to as the RAB.

Once an ALS platform-based instrument has been programmed for plant-specific use and delivered to the applicant or licensee, ALS platform design features prevent the applicant or licensee from altering either the standardized or application-specific FPGA logic. This does not preclude a licensee from flashing a board, as part of its onsite inventory and configuration control program, with configuration controlled files that the ALS manufacturer supplied. Flashing that uses a licensee's administrative procedure could include configuring any board's non-volatile memory for specific use or loading application-specific logic into the ALS-102 Core Logic Board's FPGA. Regardless, the topical report and its evaluation do not include any licensee administrative procedures or the tooling used to perform these activities. Furthermore, ALS platform design features prevent the maintenance workstation from modifying any non-operationally adjustable settings required to remain constant so the equipment remains capable of performing its application-specific instrument functions.

3.1.3 Platform Digital Communications Overview

The ALS platform provides digital communications methods for intrachannel safety signals, unidirectional transmit-only to external equipment, bidirectional for use with a maintenance workstation, and unidirectional receive or transmit for exchanges between instrument channels or to additional nonsafety equipment.

<u>Intrachannel Safety Communications (RAB)</u> - Within an instrument, a single ALS-102 Core Logic Board acts as the sole bus master of the RAB, and the RAB forms an integral part of a safety system's safety signal path. The RAB uses a lower-level Universal Asynchronous Receiver/Transmitter (UART) protocol and a higher-level request and reply message protocol of a fixed-format at fixed-intervals. The higher-level protocol applies defined response limits for each transaction and includes time for one automatic request-and-reply retry in response to a failed transaction. Each communication transaction is initiated by the ALS-102 Core Logic

Board as bus master of the RAB and replied to by one of the remaining standardized circuit boards. The backplane(s) provide the copper medium for the point-to-point differential signaling of each redundant RAB communication path.

Unidirectional Transmit Only (TxB1 and TxB2) - Like the RAB, this method also uses the ALS-102 Core Logic Board, which provides two transmit-only digital communication interfaces to support providing plant-specific digital data to external equipment, such as to a nonsafety plant process computer or transient event recorder.

Bidirectional with Maintenance Workstation (TAB) - This method is the TAB to support connection of a maintenance workstation. The TAB provides bidirectional communications between the instrument and the maintenance workstation as a nonsafety signal path for access to individual board test and maintenance functions. The architecture supports an administratively controlled connection between the maintenance workstation and the TAB for operational, test and maintenance activities. These activities include placing a channel into bypass, performance of periodic surveillance requirements, and operational adjustments to addressable constants, setpoints, or parameters. The architecture supports the physical disconnection of the maintenance workstation from the TAB. The TAB will remain inactive when no maintenance workstation is connected, because the maintenance workstation acts as the sole bus master of the TAB. For clarity and consistency, this SE will use the term 'maintenance workstation' even though the ALS documentation interchangeably uses the term 'ALS Service Unit' (ASU).

TAB similarities with the RAB are each provides bidirectional communications, each uses a lower-level UART protocol, each has a single bus master, each uses a higher-level protocol that implements fixed-format request-and-reply messaging that applies a defined response limit for each transaction, and the backplane(s) provide a copper medium for point-to-point differential signaling. TAB differences from the RAB are a maintenance workstation—which may be nonsafety—is the TAB's master while a safety ALS-102 Core Logic Board is the RAB's master, unlike the RAB the TAB does not provide a safety signal path, unlike the RAB the TAB is not redundant, unlike the RAB the TAB interface is not always active, and unlike the RAB the TAB neither enforces a fixed-interval for messaging nor includes an automatic retry in response to a failed transaction.

Interdivisional or Additional Safety-with-nonsafety Communications (ALS-601) – This method uses the ALS-601 Communications Board, which provides eight unidirectional digital communication interfaces that may be individually configured as either transmit or receive to support safety-to-safety digital data exchanges between instruments or additional safety-to-nonsafety digital communication interfaces beyond those already provided by the ALS-102 Core Logic Board and the TAB.

As applicable to safety signal paths of digital safety systems in nuclear power plants, this SE describes and evaluates the response time, determinism and diagnostic and self-test characteristics both for the RAB and for uses of the ALS-601 Communications Board to provide interdivisional communications (see Section 3.4). This SE also separately describes and evaluates the communication independence and isolation requirements that apply to safety-

with-nonsafety and interdivisional safety-to-safety communications (see Sections 3.7 and 3.10.2.6).

3.1.4 Platform Circuit Board Set

ALS platform circuit boards are built to a standardized layout, which is shown in Figure 3.1.4-1 (see Reference 32, Figure 2.1-3). Among the standardized circuit boards, hardware design reuse is applied for the circuit blocks shown as dotted-shapes within Figure 3.1.4-1. Because the block labeled “CHANNEL CIRCUIT” is essential to provide board-specific functionality this section differs significantly among standardized circuit boards. The other blocks shown remain either similar or identical among the standardized circuit board set.

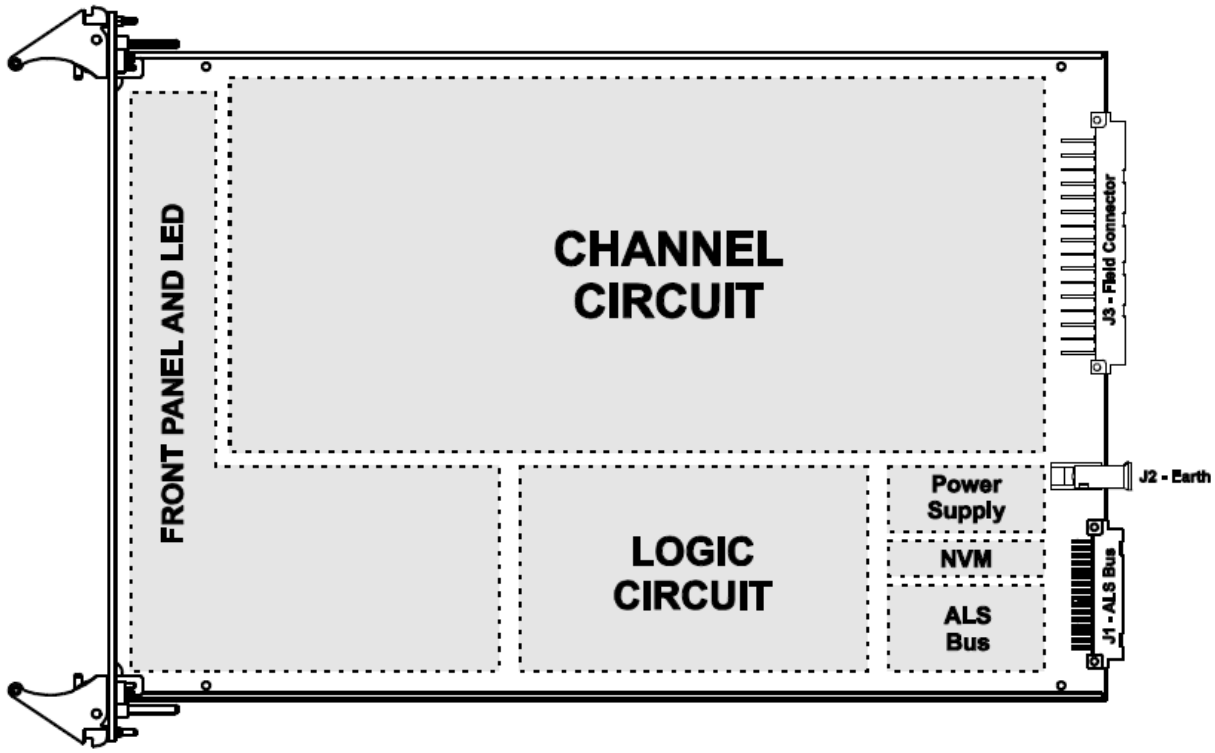

Figure 3.1.4-1 Standardized ALS Platform Circuit Board Layout

Each standardized circuit block within the standardized circuit board layout is briefly described by the following:

> The “CHANNEL CIRCUIT” block provides board-specific interfaces to the “J3 – Field Connector” and consists of a number of input and/or output channels that are directly related to the board’s type. For analog interfaces, each input channel provides signal conditioning and converts an analog signal into digital representations. Likewise each output channel converts digital representations to an analog signal to meet its analog interface specification.

The “FRONT PANEL AND LED” (Light Emitting Diode) block interfaces to the board edge LEDs and switches as shown in Figure 3.1.1-2.

The “LOGIC CIRCUIT” block contains the FPGA circuit, which is programmed to provide the board-specific functionality.

The “POWER SUPPLY” block provides on-board regulation of the power supply input to the board and power management logic.

The “NVM” (Non-Volatile Memory) block contains the non-volatile memory to store operator adjustable constants, setpoints and parameters, as well as non-operational configuration settings based on application specifications, which cannot be modified by the operator.

The “ALS Bus” block provides the backplane interface for the RAB and TAB busses using the “J1 – ALS Bus” connector.

Similar to circuit block standardization, some FPGA functions and their logic designs are standardized for reuse within each design variant , but the standardized FPGA logic designs are not shared between design variants.

The “ALS Topical Report” provides further details on the platforms approach to the use of common components and designs (see Reference 32, Section 2.1.5).

The circuit boards and the FPGAs of the ALS platform were developed and manufactured using the quality assurance, development, and manufacturing procedures identified in Tables 3.1.4-1 and 3.1.4-2. Appropriate subsections of this SE discuss these ALS platform documents and evaluate them against applicable regulatory evaluation criteria.

Table 3.1.4-1 Docketed Board and FPGA Documentation

Document ID	Title	Reference
9000-00000	CSI Quality Assurance Manual	27
9000-00311	Electronics Development Procedure	28
NA 4.50	Electronics Development Procedure	29
9000-00313	FPGA Development Procedure	30
NA 4.51	FPGA Development Procedure	31
6002-00016	FPGA Core A Common Module Design Specification	97
6002-00017	ALS FPGA Core B Common Module Design Specification	98
6002-00060	ALS Board Manufacturing Procedures	48
6002-00241	ALS FPGA Qualification Evaluation	99

Table 3.1.4-2 Platform FPGA Documentation Available for Audit

Document ID	Title
9006-00043	ALS Core A FPGA Build Procedure
9006-00071	ALS Core B FPGA Build Procedure

The following subsections provide a brief description of the functional capabilities for each ALS platform standardized circuit board within the “ALS Topical Report” scope as shown in Figure 3.1.1-1. Each subsection includes two tables that identify documentation specific to the circuit board and its diverse FPGA options. Where applicable, an appropriate technical evaluation subsection of this SE discusses the documentation types included within the set of board-specific tables.

3.1.4.1 ALS-302 Digital Input Board (48Vdc Contact Input)

The ALS-302 Digital Input Board provides 32 optically-isolated input channels to simultaneously monitor the state of up to 32 field contacts. The input channels are subdivided into groups of 16 to provide isolation between the two electrical groups. The circuit board provides galvanic isolation between external inputs and the board’s digital logic for each input channel. Each input channel contains a surge suppression circuit and filter. Each input channel also includes automated internal self-test circuits to verify the channel’s operability.

The ALS-302 Digital Input Board senses the contact change for each channel and provides the analog filtered signal at the correct voltage levels to the circuit board’s FPGA. The FPGA performs digital filtering on each enabled input channel and makes the resulting contact state available for further logic processing via the RAB. Each channel’s data is tagged with the channel’s self-test result to indicate operability.

The ALS-302 Digital Input Board includes self-test capabilities to detect single point failures in each channel, the FPGA logic circuits, the NVM configuration, and the power management logic.

The NVM configuration for each ALS-302 Digital Input Board channel can enable/disable the channel, define the channel’s input as either a normally open or normally closed contact, and

establish digital filtering constraints to control the channel’s response time from an actual contact state change until the resulting status is available to the RAB. These NVM settings cannot be adjusted in the field because these settings will have been configured to meet application specifications.

The “ALS Topical Report” provides further details on ALS-302 Digital Input Board (see Reference 32, Sections 2.1.3 and 2.2.2).

The following two tables identify ALS-302 Digital Input Board documentation. Table 3.1.4.1-1 identifies specification, analysis, verification and validation, and configuration documents for the ALS-302 FPGAs and circuitry that were docketed and evaluated by the NRC staff. Table 3.1.4.1-2 identifies lower level documents for the ALS-302 FPGAs and circuitry. The NRC staff performed a sample-based audit of ALS platform documentation as part of this SE (see References 125 and 126). These documents are identified in one or more ALS platform plans (See Table 3.1-1) or the configuration status accounting documents that apply to the ALS-302 (see References 40 and 63).

Table 3.1.4.1-1 Docketed ALS-302 Documentation

Document ID	Title	Reference
6002-30201	ALS-302 Requirements Specification	61
6002-30210	ALS-302 Core A Requirements Traceability Matrix	103
6002-30211	ALS-302 Core B Requirements Traceability Matrix	104
6002-30212	ALS-302 FPA, FMEA, and Reliability Analysis	62
6002-30216	ALS-302 VV Simulation Environment Specification	105
6002-30250	ALS-302 Configuration Status Accounting	63
6002-30281	ALS-302 Configuration Management Summary Report	64
6002-30282	ALS-302 VV Summary Report	65
6002-30294	ABTS-302 Test Summary Report	66

Table 3.1.4.1-2 ALS-302 Documentation for Audit

Document ID	Title
6002-30202	ALS-302 Design Specification
6002-30203	ALS-302 Core A FPGA Design Specification
6002-30204	ALS-302 Core B FPGA Design Specification
6002-30206	ALS-302 FPGA Design Specification
6002-30220	ASE-302 Test Simulation Environment Specification
6002-30221	ASE-302 Test Design Specification
6002-30222	ASE-302 Test Case Specification
6002-30225	ASE-302 Core B Test Simulation Environment Specification
6002-30226	ASE-302 Core B Test Design Specification
6002-30227	ASE-302 Core B Test Case Specification
6002-30228	ASE-302 Core B Test Procedure
6002-30242	ALS-302 Release Test Design Specification
6002-30245	ALS-302 Release Test Procedure
6002-30261	ABTS-302 Test Design Specification
6002-30262	ABTS-302 Test Case Specification

3.1.4.2 ALS-311 Analog Input Board (RTD and Thermocouple)

The ALS-311 Analog Input Board provides eight input channels to simultaneously monitor up to eight temperature sensors. Each input channel can be individually configured for use with several types of Resistance Temperature Detectors (RTDs) and thermocouples (TCs), and the circuit board supports two-wire TC connections and both three-wire and four-wire RTD connections. Each input channel contains a surge suppression circuit and filter. Each input channel also includes automated internal self-test circuits to verify the channel's operability.

The ALS-311 Analog Input Board performs sensor signal conditioning each for each input and converts the analog signals into digital representations. These digital signals are made available to the circuit board's FPGA. The FPGA performs digital filtering on each input channel, calculates the temperature, and makes the resulting temperature data available for further logic processing via the RAB. Each channel's data is tagged with the channel's self-test

result to indicate operability. The FPGA logic calculates temperature by applying linearization constants that are specific to the type of temperature sensor. The FPGA logic also supports automatic cold junction temperature compensation for thermocouple sensors using temperature data provided via the RAB.

The ALS-311 Analog Input Board includes self-test capabilities to detect single point failures in each channel, the FPGA logic circuits, the NVM configuration, and the power management logic. The ALS-311 Analog Input Board also includes features to support calibration without affecting cabling.

The NVM configuration for each ALS-311 Analog Input Board channel can enable/disable the channel, define the channel's input as either a two-wire TC, three-wire RTD or four-wire RTD measurement, store the linearization constants based on the sensor type to convert the channel's sensor data to temperature, and control the channel's response time by establishing the frequency at which it is sampled and its temperature data is made available to the RAB. These NVM settings cannot be adjusted in the field because these settings will have been configured to meet application specifications.

The "ALS Topical Report" provides further details on ALS-311 Analog Input Board (see Reference 32, Sections 2.1.3 and 2.2.3).

The following two tables identify ALS-311 Analog Input Board documentation. Table 3.1.4.2-1 identifies specification, analysis, verification and validation, and configuration documents for the ALS-311 FPGAs and circuitry that were docketed and evaluated by the NRC staff.
Table 3.1.4.2-2 identifies lower level documents for the ALS-311 FPGAs and circuitry. The NRC staff performed a sample-based audit of ALS platform documentation as part of this SE (References 125 and 126). These documents are identified in one or more ALS platform plans (See Table 3.1-1) or the configuration status accounting documents that apply to the ALS-311 (References 40 and 69).Table 3.1.4.2-1 Docketed ALS-311 Documentation

Document ID	Title	Reference
6002-31101	ALS-311 Requirements Specification	67
6002-31110	ALS-311 Core A Requirements Traceability Matrix	106
6002-31111	ALS-311 Core B Requirements Traceability Matrix	107
6002-31112	ALS-311 FPA, FMEA, and Reliability Analysis	68
6002-31116	ALS-311 VV Simulation Environment Specification	108
6002-31150	ALS-311 Configuration Status Accounting	69
6002-31181	ALS-311 Configuration Management Summary Report	70
6002-31182	ALS-311 VV Summary Report	71
6002-31194	ABTS-311 Test Summary Report	72

Table 3.1.4.2-2 ALS-311 Documentation for Audit

Document ID	Title
6002-31102	ALS-311 Design Specification
6002-31103	ALS-311 Core A FPGA Design Specification
6002-31104	ALS-311 Core B FPGA Design Specification

6002-31106	ALS-311 FPGA Design Specification
6002-31120	ASE-311 Test Simulation Environment Specification
6002-31121	ASE-311 Test Design Specification
6002-31122	ASE-311 Core A Test Case Specification
6002-31125	ASE-311 Core B Test Simulation Environment Specification
6002-31126	ASE-311 Core B Test Design Specification
6002-31127	ASE-311 Core B Test Case Specification
6002-31128	ASE-311 Core B Test Procedure
6002-31142	ALS-311 Release Test Design Specification
6002-31145	ALS-311 Release Test Procedure
6002-31161	ABTS-311 Test Design Specification
6002-31162	ABTS-311 Test Case Specification

3.1.4.3 ALS-321 Analog Input Board (Voltage/Current)

The ALS-321 Analog Input Board provides eight input channels that are independently isolated from one another to simultaneously monitor up to eight analog signals. Each channel can be configured to measure either a voltage or current input, where each input type is supported by four ranges. The circuit board does not provide instrument loop power for the measurements. Each input channel contains a surge suppression circuit and filter. Each input channel also includes automated internal self-test circuits to verify the channel's operability.

The ALS-321 Analog Input Board performs sensor signal conditioning for each input and converts the analog signals into digital representations. These digital signals are made

available to the circuit board's FPGA. The FPGA performs digital filtering on each input channel, calculates the corresponding voltage or current, and makes the resulting voltage/current data available for further logic processing via the RAB. Each channel's data is tagged with the channel's self-test result to indicate operability.

The ALS-321 Analog Input Board includes self-test capabilities to detect single point failures in each channel, the FPGA logic circuits, the NVM configuration, and the power management logic. The ALS-321 Analog Input Board also includes features to support calibration without affecting cabling.

The NVM configuration for each ALS-321 Analog Input Board channel can enable/disable the channel, define the channel's input as either a voltage, current with internal dropping resistor or current with external dropping resistor measurement, define the channel's input range as [0 to 5V], [-5 to +5V], [0 to 10V], or [-10 to +10V] for voltage measurements or [4 to 20mA], [0 to 20mA], [10 to 50mA] or [0 to 50mA] for current measurements, define the input channel's out-of-range limits, and control the channel's response time by establishing the frequency at which it is sampled and its measurement data is made available to the RAB. These NVM settings cannot be adjusted in the field because these settings will have been configured to meet application specifications.

The “ALS Topical Report” provides further details on ALS-321 Analog Input Board (see Reference 32, Sections 2.1.3 and 2.2.4).

The following two tables identify ALS-321 Analog Input Board documentation. Table 3.1.4.3-1 identifies specification, analysis, verification and validation, and configuration documents for the ALS-321 FPGAs and circuitry that were docketed and evaluated by the NRC staff.
Table 3.1.4.3-2 identifies lower level documents for the ALS-321 FPGAs and circuitry. The NRC staff performed a sample-based audit of ALS platform documentation as part of this SE (References 125 and 126). These documents are identified in one or more ALS platform plans (See Table 3.1-1) or the configuration status accounting documents that apply to the ALS-321 (References 40 and 75).

Table 3.1.4.3-1 Docketed ALS-321 Documentation

Document ID	Title	Reference
6002-32101	ALS-321 Requirements Specification	73
6002-32110	ALS-321 Core A Requirements Traceability Matrix	109
6002-32111	ALS-321 Core B Requirements Traceability Matrix	110
6002-32112	ALS-321 FPA, FMEA, and Reliability Analysis	74
6002-32116	ALS-321 VV Simulation Environment Specification	111
6002-32150	ALS-321 Configuration Status Accounting	75
6002-32181	ALS-321 Configuration Management Summary Report	76
6002-32182	ALS-321 VV Summary Report	77
6002-32194	ABTS-321 Test Summary Report	78

Table 3.1.4.3-2 ALS-321 Documentation for Audit

Document ID	Title
6002-32102	ALS-321 Design Specification
6002-32103	ALS-321 Core A FPGA Design Specification
6002-32104	ALS-321 Core B FPGA Design Specification
6002-32106	ALS-321 FPGA Design Specification
6002-32120	ASE-321 Test Simulation Environment Specification
6002-32121	ASE-321 Test Design Specification
6002-32122	ASE-321 Test Case Specification
6002-32125	ASE-321 Core B Test Simulation Environment Specification
6002-32126	ASE-321 Core B Test Design Specification
6002-32127	ASE-321 Core B Test Case Specification
6002-32128	ASE-321 Core B Test Procedure
6002-32142	ALS-321 Release Test Design Specification
6002-32145	ALS-321 Release Test Procedure
6002-32161	ABTS-321 Test Design Specification
6002-32162	ABTS-321 Test Case Specification

3.1.4.4 ALS-402 Digital Output Board (Contact Output)

The ALS-402 Digital Output Board provides 16 output channels to open and close field contacts and each channel is capable of switching either an alternating current (AC) or a direct current (DC) resistive or low inductance load. Each output channel uses optically-isolated solid state relays that are capable of switching up to 125Vdc or 120Vac with a maximum 1 Amp load current. However, the circuit board does not provide the load current. The optical-isolation protects the ALS logic up to 1500Vrms at the channel's output. Each output channel is independently isolated from one another to 300Vrms, and the output channels are subdivided into groups of eight to provide isolation between the two electrical groups. Each output channel contains a surge suppression circuit. Each output channel also includes automated internal self-test circuits to verify the channel's operability.

The ALS-402 Digital Output Board receives commanded output states (OPEN or CLOSED) from the RAB and applies these states to the channel output signals. Each channel's operability status, which is determined by the self-test, is made available to the RAB. The ALS-402 Digital Output Board supports setting each output channel to either open, closed, or as-is upon detection of the channel's inoperability.

The ALS-402 Digital Output Board includes self-test capabilities to test the continuity of field wiring and to detect single point failures in each channel, the FPGA logic circuits, the NVM configuration, and the power management logic.

The NVM configuration for each ALS-402 Digital Output Board channel can enable/disable the channel, enable/disable continuity testing of the channel, enable/disable whether the channel

may be bypassed (i.e., may be held at its current state without further changes while in bypass), and enable/disable whether the channel may be overridden (i.e., may be set to an explicit state without regard of the normal control signal). These NVM settings cannot be adjusted in the field because these settings will have been configured to meet application specifications.

The "ALS Topical Report" provides further details on ALS-402 Analog Output Board (Reference 32, Sections 2.1.4 and 2.2.5).

The following two tables identify ALS-402 Digital Output Board documentation. Table 3.1.4.4-1 identifies specification, analysis, verification and validation, and configuration documents for the ALS-402 FPGAs and circuitry that were docketed and evaluated by the NRC staff.
Table 3.1.4.4-2 identifies lower level documents for the ALS-402 FPGAs and circuitry. The NRC staff performed a sample-based audit of ALS platform documentation as part of this SE (References 125 and 126). These documents are identified in one or more ALS platform plans (See Table 3.1-1) or the configuration status accounting documents that apply to the ALS-402 (References 40 and 81).

Table 3.1.4.4-1 Docketed ALS-402 Documentation

Document ID	Title	Reference
6002-40201	ALS-402 Requirements Specification	79
6002-40210	ALS-402 Core A Requirements Traceability Matrix	112
6002-40211	ALS-402 Core B Requirements Traceability Matrix	113
6002-40212	ALS-402 FPA, FMEA, and Reliability Analysis	80
6002-40216	ALS-402 VV Simulation Environment Specification	114
6002-40250	ALS-402 Configuration Status Accounting	81
6002-40281	ALS-402 Configuration Management Summary Report	82
6002-40282	ALS-402 VV Summary Report	83
6002-40294	ABTS-402 Test Summary Report	84

Table 3.1.4.4-2 ALS-402 Documentation for Audit

Document ID	Title
6002-40202	ALS-402 Design Specification
6002-40203	ALS-402 Core A FPGA Design Specification
6002-40204	ALS-402 Core B FPGA Design Specification
6002-40206	ALS-402 FPGA Design Specification
6002-40220	ASE-402 Test Simulation Environment Specification
6002-40221	ASE-402 Test Design Specification
6002-40222	ASE-402 Core A Test Case Specification
6002-40225	ASE-402 Core B Test Simulation Environment Specification
6002-40226	ASE-402 Core B Test Design Specification
6002-40227	ASE-402 Core B Test Case Specification
6002-40228	ASE-402 Core B Test Procedure
6002-40242	ALS-402 Release Test Design Specification
6002-40245	ALS-402 Release Test Procedure
6002-40261	ABTS-402 Test Design Specification
6002-40262	ABTS-402 Test Case Specification

3.1.4.5 ALS-421 Analog Output Board (Voltage/Current)

The ALS-421 Analog Output Board provides eight output channels within a common isolation domain to simultaneously control up to eight analog signals. Each channel can be configured as either a voltage or current output, where each output type is supported by ranges with type-specific output drive limitations. Each output channel contains circuits for surge, short circuit and over-voltage protection. Each output channel also includes automated internal self-test circuits to verify the channel's operability. Each channel's operability status, which is determined by the self-test, is made available to the RAB.

The ALS-421 Analog Output Board receives digital data representations of the output values from the RAB, and converts the digital data to filtered analog output signals. Each output channel is individually and independently calibrated for offset and span, supports out-of-range detection, and automatically recovers from overload conditions.

The ALS-421 Analog Output Board includes self-test capabilities to detect single point failures in each channel, the FPGA logic circuits, the NVM configuration, and the power management logic. The ALS-421 Analog Output Board also includes features to support calibration without affecting cabling.

The NVM configuration for each ALS-421 Analog Output Board channel can enable/disable the channel, define the channel's output as either a voltage or current, and define the channel's output range as [0 to 5V], [-5 to +5V], [0 to 10V], or [-10 to +10V] for voltage signals or [4 to 20mA] or [0 to 20mA] for current signals. These NVM settings cannot be adjusted in the field because these settings will have been configured to meet application specifications.

The "ALS Topical Report" provides further details on ALS-421 Analog Output Board (see Reference 32, Section 2.2.7).

The following two tables identify ALS-421 Analog Output Board documentation. Table 3.1.4.5-1 identifies specification, analysis, verification and validation, and configuration documents for the ALS-421 FPGAs and circuitry that were docketed and evaluated by the NRC staff.
Table 3.1.4.5-2 identifies lower level documents for the ALS-421 FPGAs and circuitry. The NRC staff performed a sample-based audit of ALS platform documentation as part of this SE (See References 125 and 126). These documents are identified in one or more ALS platform plans (See Table 3.1-1) or the configuration status accounting documents that apply to the ALS-421 (References 40 and 87).

Table 3.1.4.5-1 Docketed ALS-421 Documentation

Document ID	Title	Reference
6002-42101	ALS-421 Requirements Specification	85
6002-42110	ALS-421 Core A Requirements Traceability Matrix	115
6002-42111	ALS-421 Core B Requirements Traceability Matrix	116
6002-42112	ALS-421 FPA, FMEA, and Reliability Analysis	86
6002-42116	ALS-421 VV Simulation Environment Specification	117
6002-42150	ALS-421 Configuration Status Accounting	87
6002-42181	ALS-421 Configuration Management Summary Report	88
6002-42182	ALS-421 VV Summary Report	89
6002-42194	ABTS-421 Test Summary Report	90

Table 3.1.4.5-2 ALS-421 Documentation for Audit

Document ID	Title
6002-42102	ALS-421 Design Specification
6002-42103	ALS-421 Core A FPGA Design Specification
6002-42104	ALS-421 Core B FPGA Design Specification
6002-42106	ALS-421 FPGA Design Specification
6002-42120	ASE-421 Core Test Simulation Environment Specification
6002-42121	ASE-421 Core A Test Design Specification
6002-42122	ASE-421 Core A Test Case Specification
6002-42125	ASE-421 Core B Test Simulation Environment Specification

6002-42126	ASE-421 Core B Test Design Specification
6002-42127	ASE-421 Core B Test Case Specification
6002-42128	ASE-421 Core B Test Procedure
6002-42142	ALS-421 Release Test Design Specification
6002-42145	ALS-421 Release Test Procedure
6002-42161	ABTS-421 Test Design Specification
6002-42162	ABTS-421 Test Case Specification

3.1.4.6 ALS-601 Communication Board

The ALS-601 Communication Board provides eight channels of unidirectional digital data communications that apply differential signaling in accordance with EIA-422 over terminated point-to-point transmission lines. The circuit board provides galvanic isolation between external inputs and the board's digital logic for each input channel. The circuit board provides UART communication over a copper medium, but does not provide qualified isolation devices to ensure electrical isolation between safety and nonsafety equipment.

The ALS-601 Communication Board performs the logic associated with communication processing to either transmit or receive the data using an application-specific encoding configuration and one of two predefined communication protocols, which are referred to as Byte Mode and Packet Mode. Byte Mode treats each individually transmitted or received byte as a complete set of information that does not require either synchronization or a checksum. Packet

Mode groups data sets into small packets where each unique packet starts with a unique header that identifies its contents and ends with a checksum to ensure the integrity of the complete data transfer. Neither of these communication protocols supports automatic re-transmission in response to a data communication error.

The ALS-601 Communication Board exchanges digital data between the RAB and other equipment that do not share this ALS bus. When a channel is configured to transmit data, the ALS-601 Communication Board receives the data from the RAB, formats the data in accordance with the transmission protocol, provides the data to the associated transmitter buffer, and transmits the data. When a channel is configured to receive data, the ALS-601 Communication Board takes the data from the receiver, provides it to the associated receive data buffer, validates the integrity of the data (e.g., parity, checksum, etc.), and makes the validated data available to the RAB.

The ALS-601 Communication Board includes self-test capabilities to detect single point failures in each channel, the FPGA logic circuits, the NVM configuration, and the power management logic. Self-tests are provided to detect communication failures within the board and an application may pair a transmission channel with receive channel to support loopback testing in further support of failure detection.

The NVM configuration for each ALS-601 Communication Board channel can enable/disable the channel, define the channel as either a receiver or transmitter, define the channel's baud rate from among 4800, 9600, 19200, 34800, 57600, 115200, 230400, 460800, or 921600 bits per second, define the channel's UART encoding scheme from among: 1) 8 data bits, no parity bit,

1 stop bit, 2) 8 data bits, odd parity bit, 1 stop bit, 3) 8 data bits, even parity bit, 1 stop bit, or 4) 8 data bits, no parity 2 stop bits, and define the base communication protocol as either Byte Mode or Packet Mode. These NVM settings cannot be adjusted in the field because these settings will have been configured to meet application specifications.

The "ALS Topical Report" provides further details on ALS-601 Communication Board (see Reference 32, Section 2.2.8).

The following two tables identify ALS-601 Communication Board documentation. Table 3.1.4.6-1 identifies specification, analysis, verification and validation, and configuration documents for the ALS-601 FPGAs and circuitry that were docketed and evaluated by the NRC staff. Table 3.1.4.6-2 identifies lower level documents for the ALS-601 FPGAs and circuitry. The NRC staff performed a sample-based audit of ALS platform documentation as part of this SE (See References 125 and 126). These documents are identified in one or more ALS platform plans (See Table 3.1-1) or the configuration status accounting documents that apply to the ALS-601 (References 40 and 93).

Table 3.1.4.6-1 Docketed ALS-601 Documentation

Document ID	Title	Reference
6002-60101	ALS-601 Requirements Specification	91
6002-60110	ALS-601 Core A Requirements Traceability Matrix	118
6002-60111	ALS-601 Core B Requirements Traceability Matrix	119
6002-60112	ALS-601 FPA, FMEA, and Reliability Analysis	92
6002-60116	ALS-601 VV Simulation Environment Specification	120
6002-60150	ALS-601 Configuration Status Accounting	93
6002-60181	ALS-601 Configuration Management Summary Report	94
6002-60182	ALS-601 VV Summary Report	95
6002-60194	ABTS-601 Test Summary Report	96

Table 3.1.4.6-2 ALS-601 Documentation for Audit

Document ID	Title
6002-60102	ALS-601 Design Specification
6002-60103	ALS-601 Core A FPGA Design Specification
6002-60104	ALS-601 Core B FPGA Design Specification
6002-60106	ALS-601 FPGA Design Specification
6002-60120	ASE-601 Test Simulation Environment Specification
6002-60121	ASE-601 Test Design Specification
6002-60122	ASE-601 Core A Test Case Specification
6002-60125	ASE-601 Core B Test Simulation Environment Specification
6002-60126	ASE-601 Core B Test Design Specification
6002-60127	ASE-601 Core B Test Case Specification
6002-60128	ASE-601 Core B Test Procedure
6002-60142	ALS-601 Release Test Design Specification
6002-60145	ALS-601 Release Test Procedure
6002-60161	ABTS-601 Test Design Specification

3.1.4.7 ALS-102 Core Logic Board

The ALS-102 Core Logic Board provides a processing resource to implement application-specific safety functions, and these safety functions are programmed into the board's FPGA logic. The ALS-102 Core Logic Board determines the order and frequency to process the application-specific set of ALS boards within an instrument backplane. The ALS-102 Core Logic Board will acquire system inputs from input boards, perform application-specific logic, and provide system outputs to output boards to meet the application-specific performance requirements.

The ALS-102 Core Logic Board provides on-board input/output capabilities that may be used within a system and provides galvanic isolation between the input/output signals and the board's digital logic to withstand 1500Vrms. The ALS-102 Core Logic Board provides six contact input

channels, four solid-state output channels, and two transmit-only digital data communication channels. As examples, a contact input can provide a reset to clear alarms, a solid-state output can provide alarm indication, and a digital data communication channel can provide plant-specific data to a nonsafety plant process computer or transient event recorder. The content and format of the digital data communications are to be included in application specifications for each system that uses either an on-board digital data communication channel or one provided by the ALS-601 Communication Board.

The ALS-102 Core Logic Board includes self-test capabilities to detect single point failures in each channel, the FPGA logic circuits, the NVM configuration, and the power management logic. Self-tests are provided to detect communication failures within the board.

The ALS-102 Core Logic Board contains an NVM device to store operator adjustable settings for application-specific functions. Examples of such settings include delay times, time constants, and trigger-thresholds (i.e., set and reset points). Unlike these operator adjustable settings but similar to the NVM settings that have been discussed for the other ALS boards, additional settings that cannot be adjusted in the field because the setting is associated with a configuration required to meet an application specification may exist.

The "ALS Topical Report" provides further details on ALS-102 Core Logic Board (see Reference 32, Sections 2.1.2 and 2.2.1).

The following two tables identify ALS-102 Core Logic Board documentation. Table 3.1.4.7-1 identifies specification, analysis, verification and validation, and configuration documents for the ALS-102 FPGAs and circuitry that were docketed and evaluated by the NRC staff.
Table 3.1.4.7-2 identifies lower level documents for the ALS-102 FPGAs and circuitry. The NRC staff performed a sample-based audit of ALS platform documentation as part of this SE (See References 125 and 126). These documents are identified in one or more ALS platform plans (See Table 3.1-1) or the configuration status accounting documents that apply to the ALS-102 (References 40 and 57).

Table 3.1.4.7-1 Docketed ALS-102 Documentation

Document ID	Title	Reference
6002-10201	ALS-102 Requirements Specification	55
6002-10210	ALS-102 Core A Requirements Traceability Matrix	100
6002-10211	ALS-102 Core B Requirements Traceability Matrix	101
6002-10212	ALS-102 FPA, FMEA, and Reliability Analysis	56
6002-10216	ALS-102 VV Simulation Environment Specification	102
6002-10250	ALS-102 Configuration Status Accounting	57
6002-10281	ALS-102 Configuration Management Summary Report	58
6002-10282	ALS-102 VV Summary Report	59
6002-10294	ABTS-102 Test Summary Report	60

Table 3.1.4.7-2 ALS-102 Documentation for Audit

Document ID	Title
6002-00047	ALS-102 FPGA Equipment Qualification Requirements Specification
6002-10202	ALS-102 Design Specification
6002-10203	ALS-102 Core A FPGA Design Specification
6002-10204	ALS-102 Core B FPGA Design Specification
6002-10206	ALS-102 FPGA Design Specification
6002-10220	ASE-102 Test Simulation Environment Specification
6002-10221	ASE-102 Test Design Specification
6002-10222	ASE-102 Core A Test Case Specification
6002-10225	ASE-102 Core B Test Simulation Environment Specification
6002-10226	ASE-102 Core B Test Design Specification
6002-10227	ASE-102 Core B Test Case Specification
6002-10228	ASE-102 Core B Test Procedure
6002-10242	ALS-102 Release Test Design Specification
6002-10245	ALS-102 Release Test Procedure
6002-10261	ABTS-102 Test Design Specification
6002-10262	ABTS-102 Test Case Specification

3.2 Development Process

The following subsections provide an overview of the ALS platform's use of the FPGA technology and the NRC staff's evaluation of the manufacturer's development processes.

3.2.1 Overview of the ALS Platform's Use of the FPGA Technology

An FPGA is a very large scale high speed integrated circuit that provides user programmable logic through the configuration and interconnection of elemental circuit building blocks within the device. The 'field programmable' portion of FPGA refers to the ability of an end-user to program the device after it has left the device manufacturer's foundry. The 'gate array' portion of FPGA refers to the collection (an 'array') of elemental digital building blocks ('gates') within the device.

Elemental digital building blocks typically include inputs/outputs, registers, memory, and a basic logic element.

For the FPGA used within the ALS platform, the basic logic element is a NAND2 gate. A NAND2 gate provides a two-input AND gate with an inverted output. NAND2 logic produces a binary logic '0' output when both of its inputs are binary logic '1,' produces a binary logic '1' output for any other combination of its inputs. This description of the NAND2 gate demonstrates the basic logic element itself does not contribute much to the understanding of application-specific logic circuit implementations in support of system safety functions.

Comparisons between typical discrete large-scale integrated circuits, which may be more familiar, to FPGAs, which may be less familiar, can help to understand the FPGA technology and provide further insights despite a fundamental difference between the two. This

fundamental difference is the party responsible to define and verify the digital circuit's functionality. For FPGAs the end-user becomes responsible for these efforts rather than the device manufacturer, and this fundamental difference arises directly from the FPGA's programmability. For discrete large-scale integrated circuits, the manufacturer defines, verifies, and tests the digital circuit functionality and performance that it has specified for the logic-specific device. However, an FPGA manufacturer only establishes and verifies the device's underlying performance characteristics and programmability limitations, because the FPGA has no equivalent specified logic function. Therefore, within the processes to produce an FPGA-based design, the FPGA end-user should define, verify, and test the digital circuit's functionality, including its conformance to the manufacturer's prescribed FPGA characteristics and limitations.

Before programming end-user functionality into an FPGA, the elemental digital building blocks remain an array of isolated internal devices. There are no interconnections or connections to input/output pins. This view is analogous to a large discrete integrated circuit breadboard that has been populated with integrated circuits, power and ground signals, but has neither any interconnection between integrated circuits nor from integrated circuits to input or output connectors of the breadboard. The functionality cannot exist for either the FPGA circuits or the breadboard circuits until specific and appropriate interconnections between devices are made. The FPGA contains a series of reconfigurable interconnects to allow elemental digital building blocks to be interconnected to form a digital circuit with user-defined functionality.

The FPGA's configurability allows creation of lower-level logic beyond the NAND2 (e.g., AND, OR, Inverter, and XOR, etc.). This configurability also allows creation of higher-level and more complex digital circuits from flip-flops (e.g., JK, D, and SR, etc.), to adders and counters, and beyond to logic circuits of even greater complexity (e.g., bus arbiters, serial data controllers, etc.). The logic circuits are then combined to provide application-specific functions that will conform to specified behavior while meeting required performance characteristics. Regardless of the degree of complexity represented within an end-user's application-specific FPGA design, the quantities of available elemental digital building blocks, dedicated input/output pins, and configurable input/output pins remain fixed. Along with the basic logic element's type, the quantities of elemental digital building blocks, dedicated input/output pins, and configurable input/output pins are defined by the FPGA manufacturer and the FPGA part number.

Typical discrete large-scale integrated circuits contain a defined quantity of the same digital logic circuit, which is established by its part number. Within a large-scale integrated circuit, each like digital logic circuit operates independently via dedicated input and output pins, and only power and ground signals are shared. FPGAs provide significantly greater digital logic density than their discrete integrated circuit counterparts. However, unlike typical discrete large-scale integrated circuits, the FPGA leaves the manufacturer as a blank slate of digital functionality.

For a typical printed circuit board that contains several discrete large-scale integrated digital circuits, the connections between individual integrated circuits are made by copper traces or wiring, and the characteristics of these interconnections limit the equipment's performance. Additionally, the oscillator's clock tree, which is associated with synchronous logic designs, is

supported by separate integrated circuits and associated copper traces within protected layers of the printed circuit board. In contrast to this approach, the FPGA's internal logic connections overcome the performance limitations of printed circuit board external traces and wiring by substantially reducing external connections and by eliminating external clock tree circuits. The FPGA embeds logic connections and clock tree circuits within the device.

When a digital circuit board is built from discrete integrated circuits, various design tools are used in the development of its populated printed circuit board. For example, schematic capture tools and timing analysis tools are used by designers to verify the performance of the board and its digital circuits prior to the generation of a parts list and the printed circuit board drawings needed to manufacture the board. Vendors of schematic capture and timing analysis tools embed models of available devices and their performance characteristics to support in-process design evaluations. Some of these performance characteristics are dependent on the device's packaging (e.g., dual-in line, surface mount, etc.) and grade (e.g., commercial, industrial, military, etc.). Electronics vendors use design guidelines, standards, and procedures to help ensure a circuit board layout and its signal routing will operate correctly. Additionally, formal equipment qualification testing of a pre-production hardware product is typically performed following engineering proof-of-design tests.

The use of tools to perform FPGA logic circuit synthesis, simulation and timing analysis are analogous to those used for discrete integrated digital circuit designs. Nevertheless, four significant differences exist between FPGA designs and tools when compared to discrete integrated digital circuit designs and tools. First, the FPGA manufacturer provides the complete set of performance characteristics for circuit modeling and simulation rather than individual integrated circuit manufacturers providing the performance characteristics for their devices. Second, FPGA designs eliminate the vast majority of circuit board connections between components, because logic circuit interconnections are made internally. This reduces the scope but does not eliminate the need to use other board layout tools in support of high speed digital logic designs. During the circuit synthesis process, FPGA tools produce a '*netlist*' similar to non-FPGA digital circuit design tools. A '*netlist*' is a list that identifies each logic circuit, its connection points, and the associated connections that are made to it. Most of an FPGA's '*netlist*' typically identifies internal devices and connections while the entirety of discrete integrated digital circuit design tool's '*netlist*' explicitly identifies each available digital logic circuit and the external connections made to each device. Third, FPGA tools will layout the logic

circuits within the FPGA device in a manner specific to the FPGA device and user directives rather than relying on a generically applicable drafting tool to place large-scale integrated digital circuits onto a printed circuit board. Fourth, FPGA programming tools are required and these tools are manufacturer and device specific. Furthermore, once programmed some FPGAs do not have a read-back capability to verify the programmed content. When this is the case, the device programming is verified by attempting to program the device a second time with the same file. The programming activity confirms the resultant FPGA configuration after the second programming is identical to the configuration after the first time it was programmed. In contrast, discrete large-scale integrated digital printed circuit boards do not require programming tools and can be laid out to support the use of independent test tools to verify the integrity of the resultant connections after the board is manufactured. Once an FPGA is programmed, the use

of independent test tools to verify the integrity of the resultant connections becomes largely impractical. Therefore, manufacturers that embed FPGA products on circuit boards typically use other techniques to ensure the device continues to reflect its initial programming.

The ALS platform uses a '*flash*' method to program its FPGA device and this method is non-volatile. Non-volatile FPGAs do not lose their internal configuration when power is removed. The '*flash*' method allows the device to be reprogrammed, which supports potential engineering change and corrective actions to the FPGA's logic design. Reprogramming '*flash*' interconnects is similar to what occurs when reprogramming an electronically erasable programmable read only memory to alter an embedded microprocessor's program.

The definition and verification of digital circuits that are programmed into an FPGA is similar to the definition and verification of individual software programs that are integrated and executed by a microprocessor. As is the case for all electronic circuits (and for software), specifications must first establish the desired functionality of the circuit (or software). The ALS platform uses natural language in its requirement specifications. The ALS platform then uses a text-based high level language to specify the functionality of its FPGA-based digital circuits. The ALS platform FPGA designers use the HDL as the high level language to specify functionality. This is the same high level language that the manufacturer used within the Wolf Creek MSFIS development.

The use of HDL is analogous to a standard software programming language, such as Ada or C, to develop a system's software component. The HDL language uses standard text-based expressions to govern the structural and behavioral aspects of the desired digital circuit. In this way, HDL can be considered a method that refines the natural language requirements into specifications of a more precise set of formatted requirements. The use of HDL allows a simulation program to model, explore and test the behavior of the resultant circuit before establishing the use of specific elemental digital building blocks and device interconnections. Therefore, HDL simulation does not require a physical FPGA device. This stage of simulation program is generally integral to the FPGA circuit developer's test bench. In this way, HDL simulation is analogous to a software developer's Integrated Development Environment (IDE) cross-compiler, which is performed without the target microprocessor or hardware. At this point in an FPGA circuit development, because it is only HDL being simulated, the testing validates the designer's intent rather than an actual circuit. HDL simulation and validation are independent of the underlying FPGA device technology. This independence is similar to

portable standard language software that excludes all target and compiler specific directives, and similarly leads to greater portability of the HDL from one device to another. The ALS platform development includes use of HDL simulation and validation with formally established and configuration controlled test vectors to verify acceptable FPGA circuit design behavior. This HDL simulation and validation is integral to ALS platform FPGA program development plans.

The HDL specification can include standardized directives to govern circuit behavior. Directives can include RTL as an underlying digital circuit implementation approach to provide a synchronous (versus asynchronous) digital logic design. The ALS platform circuit designs use RTL for a synchronous digital logic design. In contrast to an asynchronous design, RTL-based

synchronous designs result in circuits with behaviors that are more readily predictable and deterministic. Because the resultant circuit is more readily predictable and deterministic, improved efficacy and efficiency of automatic testing can be realized. The predictability and determinism of RTL-based synchronous designs facilitate the generation of rigorous test vectors with expected results. Rigorous test vectors can increase equipment test coverage and improve the ability of equipment V&V efforts to detect design errors. These test vectors can subsequently be re-used during regression testing throughout the equipment's life-cycle.

HDL allows for FPGA circuit modules to be developed independently and validated through simulation. This type of development is analogous to a modular software development, where the beneficial heuristics of high cohesion and loose coupling aggregate software functionally within a compilation unit (i.e., module). This type of development approach improves overall in-process validation, systematic reuse opportunities, and has the potential to reduce life-cycle maintenance burdens. Systematic reuse of common FPGA circuit modules is important to create a platform that conforms to a specified architecture and set of communication protocols. Reuse of common FPGA circuit modules necessitates full consideration of life-cycle approaches presently applicable to modular software development. HDL modular FPGA circuit development should include appropriate life-cycle configuration control and maintenance (regression testing) activities. After individual modular FPGA circuits have been validated, the next step in an FPGA-based circuit development can include the integration and HDL simulation and validation of new individual circuit modules with previously integrated ones. Again, this simulation validates the designer's intent rather than an actual circuit. The ALS platform development includes standard and application-specific FPGA circuit modules which are integrated into an overall FPGA circuit.

Either on a single circuit module basis or after integration of multiple FPGA circuit modules for inclusion in a specific FPGA, the next step to realize an FPGA-based circuit is the synthesis of the circuit implementation from the high level description. A software-based development tool, which is referred to as a "*synthesizer*," determines the required FPGA elemental digital building blocks and their interconnections from the HDL statements using synthesizer directives. Similar to a software cross-compiler with directives to optimize resultant machine code for speed or memory use of the target processor, the synthesizer produces the '*netlist*' of elemental digital building blocks and interconnects from the HDL based on its directives. An FPGA circuit developer selects the directive(s) to be used per HDL module for the FPGA from a list of available digital circuit implementation techniques. During synthesis per the directives, the specific digital circuit building blocks and required interconnections are identified. Some of

these building blocks will be standardized implementations of digital logic circuits such as flip-flops, adders and counters as provided by the synthesizer tool. As previously mentioned, the FPGA *'netlist'* is analogous to a proposed schematic of the discrete integrated circuits where the specific digital logic device family, manufacturer(s) and circuit board locations have not yet been determined. The FPGA-based circuit, as described by the '*netlist*' can again be simulated and validated for proper operation, and the determination that the circuit will correctly perform the specified functions can be reached. The simulation and validation of the synthesis output includes an additional level of circuit detail, but does not yet represent all performance characteristics that are specific to the target FPGA device.

After acceptable performance of the synthesis output has been determined, the synthesized circuits undergo a '*place and route*' operation. The '*place and route*' operation uses an FPGA device manufacturer specific software-based development tool. During the '*place and route*' operation, each proposed logic element is assigned to an actual elemental digital building block within the targeted FPGA device. The place and route operation also determines the specific physical interconnections required between the elemental digital building blocks. Through these determinations, the place and route operation adds an additional level of detail to the circuit definition. These details include device specific timing characteristics, propagation delays, and input or output pin assignments that are associated with the specific circuit design, target FPGA device, and location of the circuit within the FPGA. Once again, the described circuit can be simulated and validated before programming it into the FPGA device. This simulation is referred to as "gate-level simulation." Similar to an embedded software development's use of an in-circuit emulator, this state of FPGA design validation requires use of specialized software-based development tools to emulate the FPGA's overall characteristics. One output of the '*place and route*' tool is a '*flash*' (or burn) list. The '*flash*' list is the record with which an FPGA device is programmed. The '*flash*' list is analogous to the hex file(s) programmed into a software-based system's read only memory device(s).

For the ALS platform circuit designs, the programmed FPGAs will be limited to combinatorial logic and finite state machine (FSM) designs. For the ALS platform circuit designs, the programmed FPGAs prohibit the implementation of latches and limit the use of the static random access memory (SRAM) type of elemental digital building block. Where SRAM is used, additional design features are implemented to ensure a SEU does not prevent a board from performing its safety function. An SEU is a non-destructive temporary error caused by a single, energetic particle. The temporary error typically appears as a transient pulse in logic or support circuitry, or as a bit-flip within a memory cell or register. As previously mentioned, for the ALS platform circuit designs, the programmed FPGAs will be RTL synchronous designs. With each of these constraints the behavior of the programmed FPGA becomes more predictable and more deterministic, and thereby promotes more effective testing and functional reliability.

Predictable and deterministic FSMs exhibit certain desirable characteristics. First, each FSM within the FPGA should operate independent from one another using hardware digital logic resources that are dedicated to that FSM and that are not shared with any other FSM. Second, no FSM should support an undefined state. Third, for a given state, only one transition to a new state should occur per cycle. Fourth, for each input event applicable to the current state, there

should be one and only one associated transition to the next state. These characteristics should be present in each as-designed and as-tested FSM logic circuit.

As an example, for an overall trip decision circuit, one FSM might periodically acquire the sensor input data. This sensor input data may be provided to a second FSM to perform the comparison of the sensor input against its set and reset points. A third FSM may receive the trip decision and subsequently transmit the result to the final actuator. A parallel FSM, independent and not connected to the trip decision FSMs, may monitor an equipment rack door latch and the bypass switch to determine an alarm status when the door is opened and the channel is not in bypass. Each FSM's underlying digital logic circuit remains in a quiescent and

well-defined state until an appropriate input event that requires a response occurs. While some FSMs will repeat cyclically, such as sampling sensor inputs, other FSMs operate only in response to a specific event.

The ability to produce FSM behavior can equally be achieved using discrete integrated circuits when similar constraints are applied. Furthermore, regardless of whether the technology is FPGA or discrete integrated circuits, the underlying complexity of an overall circuit design will still depend on the overall functionality required, The differences between FPGAs and discrete integrated circuits rest not in the behavior, but rather rest in the feasibility to realize an acceptable implementation in terms of size, power, and reliability, along with an increased reliance on tools to achieve the beneficial characteristics. FPGAs offer beneficial characteristics of reduced size, less power consumption and improved hardware reliability when compared to discrete integrated circuits. FPGAs can produce functionally equivalent circuits using fewer physical devices, less material and less touch labor than discrete integrated circuit designs. By using fewer physical devices, less material and less touch labor, FPGA-based designs derive improved reliability when compared to discrete integrated circuit designs.

Programming with HDL has the potential to create latent defects in a manner similar to other software programming languages. Errors may exist in the requirements or program source code which could propagate through the development. The source of the error can be introduced in the HDL source text or during the tool transformations that are required by the development process. Typical of most FPGA developments and for the ALS platform, transformations occur during the requirements review, HDL modeling, synthesis, place and route, and device programming. To detect errors for the ALS platform, the manufacturer performs in-process V&V at each stage of transformation, as well as a formal test of the functioning programmed circuit in its final form.

FPGA programming presents similar configuration control, quality assurance and other issues as those presently associated with traditional software programming. For this reason, the NRC staff review of HDL is similar to the NRC staff review of an application that uses a software programming language for a microprocessor-based system. The potential for programming errors creates the need for a well-defined high quality design process. Rigorous V&V should be integral to this process to provide reasonable assurance that the resulting system will perform its safety function in a predictable and reliable manner. The methods, constraints, and reduced complexity of FPGAs act to simplify the overall determination of reasonable assurance when compared to microprocessors. Nevertheless, the NRC staff performs its review of FPGA logic

program development process, including a regulatory audit of design products, to make a reasonable assurance determination that the development process is of a high quality and suitable to produce items for use in nuclear power plants.

A software-based microprocessor (µP) system operates on principles fundamentally different than an FPGA. In general, a µP executes external instructions and should maintain an overall program flow control to perform the required functionality. A simple program flow control might cyclically repeat a single loop of instructions at a prescribed interval. More complicated program flow control might involve multiple tasks, task switching and interrupts. Regardless, all

microprocessor program flow control types involve repetitive retrieval and storage from memory devices. Internal to the µP, microcode uses dedicated registers to manipulate data, execute low-level operations, and produce result values. The memory and the circuitry within the µP are shared resources for the overall software program. Although individual software modules may exist, when they execute on a single µP they share its resources. Resource sharing increases the ability for a latent error or other event to propagate, which can result in unpredictable behavior. An unplanned interruption of any portion of the software can affect the larger set of software-enabled functionality, and may cause the µP or its program(s) to enter undefined states. These µP characteristics differ from the ALS platform FPGAs, because ALS platform FPGA circuit modules always use dedicated resources, are designed and verified to preclude undefined states, and the ALS platform design directives constrain the use of memory in support of continued safety function capability.

For a typical µP design, dedicated diagnostic routines execute in an attempt to detect failures. The ALS platform FPGAs implement dedicated FSMs to perform diagnostics. SEUs and Single Event Latch-ups (SELs) can corrupt a memory location or other internal register within a µP and result in unpredictable behavior. This characteristic is undesirable from a safety assessment perspective. To address this concern, µP-based designs typically include a separate and distinct watchdog timer circuit, which is reset at a prescribed program control point, as a mechanism to ensure and restore normal program control flow when it is lost. This kind of watchdog timer is not applicable to FPGAs developed with constraints similar to the ALS platform FPGAs. However, FPGA logic can include watchdog timer-like functionality to ensure other FPGA logic satisfies specified timing requirements. The ALS platform FPGAs implement parallel FSMs with diversity to perform functions redundantly and include watchdog timer-like logic. These features ensure continued functional operability or result in annunciation of an alarm for operator action, similar to a µP's watchdog timer timeout.

Unlike FPGAs, for µPs an additional operating system software layer and set of device drivers may exist to support the application-specific software functions and processes. The additional software is often commercial-off-the-shelf, proprietary or developed by a third party. The additional software typically has very limited or no design disclosure documentation. Like this software, the internal designs of commercial µPs are proprietary and lack design disclosure documentation. Lack of transparency into the design is undesirable from a SE perspective, because it restrains the ability to perform root-cause analysis and perform corrective actions as part of the equipments life-cycle. When using µPs, a degree of uncertainty is typically accepted and mitigated by broad use of a commercial product and its successful operating history. These mitigations represent a compromise from the SE perspective. However, a similar compromise

is not required for FPGAs, as proposed for the ALS platform. In contrast to typical commercial software and µP designs, an FPGA's internal design details are transparent and available for review and evaluation. For the ALS platform FPGAs, full transparency into the design documentation exists to enable SEs for reasonable assurance purposes.

3.2.1.1 Technology Comparison

Table 3.2.1.1-1 identifies general characteristics that affect a SE based on the technology with which a safety system is implemented. For each general characteristic, the table presents a relative comparison of four alternative implementation technologies: Relay Logic, Discrete Large Scale Integrated (LSI) Circuits, µP, and FPGA. The table also summarizes attributes of the ALS platform FPGA development that the manufacturer has included to enhance the base FPGA technology and provide a degree of mitigation against perceived weaknesses.

Table 3.2.1.1-1 Comparison of General Characteristics of Alternative Implementations

General Characteristic	**Implementation Technology**				**ALS Platform FPGA Mitigations**
	Relay Logic	**Discrete LSI Circuits**	**µP**	**FPGA**	
Who specifies the logic within the device, the manufacturer or implementer	Manufacturer	Manufacturer	Manufacturer	Implementer	Development plan includes: • Requirements review • In-process developer simulation
Who verifies the logic within the device, the manufacturer or implementer?	Manufacturer	Manufacturer	Manufacturer	Implementer	Development plan: • Formally establishes test vectors • Includes in-process independent simulation: HDL, RTL , and gate level • Uses verifiers and testers who are independent from designers • Uses diverse and independent test setups • Final as-programmed in-circuit testing

Is the device's programmable or fixed?	Fixed	Fixed	Programmable	Programmable	Management plan: • Addresses life-cycle needs • Precludes on-site programming of devices
Are the device's processing resources generally dedicated or shared?	Dedicated	Dedicated	Shared	Dedicated	ALS platform finite state machine RTL FPGA designs result in dedicated hardware implementations that eliminate shared resources among functions.
What is the degree of design disclosure provided by the technology full or limited?	Full	Full	Limited	Full	Applicants, licensees, and NRC audits of complete set of FPGA design products.
Once manufacture is complete, to what degree does the technology allow the logic's state to be observed, maximum, moderate or minimum?	Maximum	Maximum	Minimum	Moderate	FPGA designs include standard JTAG port to provide visibility into devices internal states during development. ALS platform supports a maintenance interface to provide visibility into device internal states when fielded.
To what degree does the technology rely on software-based tools, minimum, moderate or maximum?	Minimum	Moderate	Maximum	Maximum	Development plan includes in-process review, verification and validation of each transformation: • Requirements • HDL modeling • Synthesis • Place and route • Device programming FPGA designs include redundant diverse logic implementations derived through varying synthesizer directives.

Table 3.2.1.1-1 shows an FPGA implementation retains the desirable characteristics of dedicated logic with independence and full visibility into design disclosure information. Conventional discrete relay and LSI circuit based systems also exhibit these characteristics. However, these characteristics are generally lacking in typical µP-based systems.

Additionally, Table 3.2.1.1-1 shows an FPGA with appropriate development methods and constraints can overcome the undesirable characteristic of a fixed design by providing programmability. This programmability characteristic is a critical enabler of any standard platform architecture. This programmability characteristic is one benefit that µP-based systems have traditionally possessed over discrete relay and LSI circuit based systems.

Table 3.2.1.1-1 also shows an FPGA with appropriate development methods and constraints overcomes undesirable characteristic of a µP-based system by providing dedicated resources and improved visibility into the logic's behavior and present state. Furthermore, the FPGA provides greater visibility into and disclosure of its full design when compared to µP-based systems, because large portions of µP proprietary design features typically lack full transparency.

In summary, the NRC staff determined the ALS platform's FPGA implementation, with its development methods and constraints, provides the following:

- Programmability that cannot be modified in the field;
- Dedicated embedded logic resources;
- Transparency into the design and design process;
- In-process V&V of each design transformation within the design and development and V&V activities;
- Diverse testing within in-process V&V as mitigation against undetected common-mode tool errors; and,
- Redundant diverse logic to address difficulties in performing 100percent testing.

Additionally, the NRC staff confirmed the ALS platform development processes support implementation of each of these development methods and constraints by applicants or licensees referencing this SE.

3.2.2 Standardized Circuit Boards

An NRC staff review of a digital safety system requires a system description to explain how the components of the system interact to accomplish the design function from the perspective of integrated hardware and FPGA logic programs. This description facilitates subsequent NRC staff reviews and evaluations against applicable acceptance criteria. The "ALS Topical Report" (Reference 32) limits the components to seven standardized circuit boards, a backplane, and chassis. Section 3.1 of this SE provides descriptions of these components and their intended use in consideration of the "ALS Topical Report" appendices that depict notional applications of these components for several safety-related digital safety systems.

As discussed within Section 3.10.2.3 of this SE, the manufacturer produced the ALS platform components as an Appendix B supplier and will continue to produce ALS-based systems using

the “Westinghouse Quality Management System,” which had been reviewed and approved by the NRC staff separate from this SE.

Within the “ALS Platform Requirements Specification” (Reference 43), the manufacturer specified the top level platform requirements for the ALS platform, its architecture, its backplane and its chassis. In addition to these platform requirements, the manufacturer specified top level requirements for each standardized circuit board within the set of “ALS-xxx Requirements Specification,” where “xxx” represents a unique board identifier (References 55, 61, 67, 73, 79, 85, and 91). The manufacturer used a requirements management tool to support traceability of from these top level requirements specifications into lower level product specifications, including hardware. The manufacturer used a configuration management tool to maintain and control top level requirements specifications, lower level product specifications, and other design, development and implementation products. The manufacturer identifies its documentation and products, including hardware, by name, revision and date within its configuration status accounting documents (References 40, 57, 63, 69, 75, 81, 87, and 93). The manufacturer identifies the requirements and the lower level product specifications within its requirements traceability matrices (References 42, 100, 101, 103, 104, 106, 107, 109, 110, 112, 113, 115, 116, 118, and 119). Within these requirements traceability matrices, the manufacturer also maps requirements and specification identifiers to V&V activities (e.g., inspection, simulation, board test, etc.) that include hardware components.

The manufacturer provided an “ALS EQ Plan” (Reference 37) to guide equipment qualification efforts. The manufacturer also provided an “ALS V&V Plan” (Reference 36) and an “ALS Test Plan” (Reference 38) to guide hardware design verification and FPGA logic program V&V integration testing activities. For the platform, the manufacturer provided an “ALS Platform EQ Summary Report” (Reference 51) that documents completion of the platform’s equipment qualification activities. For each standardized circuit board, the manufacturer provided a “VV Summary Report” (References 59, 65, 71, 77, 83, 89, and 95) that documents completion of board-specific FPGA program verification and validation activities identified in the requirements traceability matrices. For each standardized circuit board, the manufacturer also provided an “ABTS Test Summary Report” (References 60, 66, 72, 78, 84, 90, and 96) that documents successful completion of the identified board-specific hardware design verification and integration test (board-specific FPGA programs with hardware) activities. Additionally, the manufacturer provided ALS platform summary reports for configuration management (Reference 53) and V&V (Reference 54).

Although the NRC staff did not perform an independent design review of the ALS platform products, the NRC staff did review the ALS platform design and the development process to determine whether it meets or supports an applicant’s or licensee’s ability to meet regulatory requirements, and whether the hardware process is of sufficiently high quality to produce systems, hardware, and FPGA logic programs that are suitable for use in safety-related applications in nuclear power plants. The NRC staff also performed thread audits to confirm the implementation activities were consistent with planning activities, as these activities evolved over the execution of the project. This section of the SE is limited to the NRC staff’s evaluation of the hardware design and development process, because later sections provide the NRC staff’s evaluations against other specific regulatory requirements, including the FPGA logic

program design and development. The NRC staff reviewed the hardware development process, and the associated implementation, to determine whether the process described was followed and applied in a manner that produced hardware suitable for use in safety-related applications at nuclear power plants.

The NRC staff reviewed the manufacturer's "ALS Topical Report," "ALS Platform Requirements Specification," board "Requirements Specifications," and the "ALS Platform EQ Summary Report" and determined the manufacturer's information provided descriptions of its ALS platform components, explained how the integrated hardware and FPGA logic programs support safety functions, identified specific platform functions that support safety, and performed equipment qualification and V&V to ensure the continued operability and performance of platform functions. The manufacturer's explanations of the ALS platform components supported the NRC staff's detailed reviews and evaluations against specific regulatory evaluation criteria, which are documented in the balance of this SE. Furthermore, the NRC staff determined the manufacturer's information is suitable for use by applicants or licensees referencing this SE.

The NRC staff reviewed the manufacturer's "ALS EQ Plan," "ALS V&V Plan," "ALS Test Plan," "ALS Platform Requirements Specification," board "Requirements Specifications," platform and board/FPGA-specific "Requirements Traceability" matrices, platform and board "Configuration Status Accounting" sheets, board specific "VV Summary Reports" and "ABTS Test Summary Reports," "ALS Platform Configuration Management Summary Report," "ALS Platform VV Summary Report," and "ALS Platform EQ Summary Report." The NRC staff also performed a regulatory thread audit of the ALS platform documentation. Based on the NRC staff's review and audit, the NRC staff determined the ALS platform hardware components were designed and developed with a sufficiently high quality process and in a manner that produced hardware suitable for use in safety-related applications at nuclear power plants, because the manufacturer's information provides a comprehensive explanation of its hardware development process and the hardware development process is subordinate to top level quality assurance program activities to meet Appendix B to 10 CFR Part 50.

3.2.3 Standardized FPGAs

As described in Section 3.1 of this SE, six of the seven standardized circuit boards (ALS-302, ALS-311, ALS-321, ALS-402, ALS-421, and ALS-601) provide non-application-specific FPGA logic programs. Therefore, the "ALS Topical Report" scope encompasses the entire FPGA logic program development for these six boards. This section provides a summary description of the manufacturer's FPGA logic program development process and the NRC staff's evaluation to ensure it is of sufficiently high quality to produce FPGA logic programs that are suitable for use in safety-related applications in nuclear power plants.

The NRC staff evaluated the ALS platform FPGA logic program development using the set of regulatory guidance applicable to a computer software development, because no equivalent regulatory guidance exists specific to an FPGA logic program development. This NRC staff evaluation considered differences between FPGA logic program development activities and typical computer software development activities when applying the following guidance:

- BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems;”
- RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants;"
- RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants;"
- RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants;"
- RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants;"
- RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants;”
- RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

This NRC staff evaluation excluded consideration of guidance that applies at the system level, such as system-specific requirements development, hazards analysis, and all activities associated with project life-cycle stages from production manufacturing, to system integration, and onward because the “ALS Topical Report” and ALS platform efforts only cover the development of a set of components rather than the production of a system.

The manufacturer’s plans defined the design development process to start with top-level platform and standardized circuit card requirements development. The design development process then proceeded to successively lower levels through specifications development and design implementation. The ALS platform developments address only the life-cycle stages of planning and development for the ALS platform components (see Reference 32, Section 6). To meet portions of BTP 7-14 that are applicable to the ALS platform scope for life-cycle planning, the manufacturer also provided a mapping between its documentation and information identified within DI&C-ISG-06 and committed to follow the guidance specified in BTP 7-14 for the applicable life-cycle activities (see Reference 32, Sections 6.2 and 12.4).

The manufacturer’s processes include lower level specifications, which the manufacturer refers as “Design Specifications,” to govern FPGA logic program development. The manufacturer produced multiple FPGA design specifications, because the manufacturer specified the requirement of “Core Diversity” and decomposed FPGA logic functionality between that common to all boards and board-specific. The manufacturer explained these design specifications fulfill the role of “Software Requirements Specifications” for its FPGA development. Furthermore, the manufacturer provided its “FPGA Development Procedure” to govern this design activity (see References 30 and 31).

The manufacturer performed independent verification, validation, review, and audit activities throughout the development of the ALS platform components and FPGA logic programs. The manufacturer defined its organization and approach to provide IV&V in the “ALS V&V Plan.” Within this plan the manufacturer identifies and clarifies its segregation of life-cycle activities applicable to an ALS platform standardized circuit board versus an ALS-based system and identifies content for ALS-based systems to be guidance (see Reference 36). The manufacturer

defined further details of its approach to provide IV&V for FPGA logic programs in the “ALS Platform FPGA Test VV Plan” (Reference 45) and for the FPGA logic’s integration with its standardized circuit board in the “ALS Test Plan.” Within these plans, the manufacturer identifies review and testing activities applicable to configuration controlled items within the planning and development life-cycle stages. These activities include requirements and specification reviews and the generation of requirements traceability matrices. These activities validate lower level specifications meet parent requirements and verify the requirements and specifications have been implemented, as specified.

The manufacturer established a configuration management plan as part of its quality plan for use throughout the ALS platform life-cycle (see Reference 32, Section 12.2.10). The manufacturer’s “ALS Quality Assurance Plan” establishes the quality assurance team as independent from the development organization in terms of financial and schedule performance and identifies its role throughout the ALS platform life-cycle. The “ALS Quality Assurance Plan” also identifies the manufacturer’s anomaly reporting and corrective action processes, as applied throughout the ALS platform life-cycle (see Reference 34). The anomaly reporting and corrective action processes are further detailed within the “ALS V&V Plan” (Reference 36, Appendix B). The manufacturer’s “ALS Configuration Management Plan” identifies the items subject to configuration management activities, defines project milestones related to these activities, and explains the manufacturer’s application of a configuration management tool, as applied throughout the ALS platform life-cycle. These configuration management activities include provisions to track the resolution of reported anomalies to the item or items that implement a corrective action (see Reference 35).

For its FPGA programs, the manufacturer created test documentation that includes plans, test environment and design specifications, test case specifications, test procedures, and documented test results, all of which the manufacturer maintains under configuration management. These documents include applicable acceptance criteria for the reviews and tests along with an evaluation of conformance against the established acceptance criteria.

In addition to Equipment Qualification type-testing, the following testing activities, which are part of FPGA logic verification, represent that which the manufacturer has characterized as “exhaustive testing using advanced test environments” (see Reference 32, Section 2.1.5.1).

The manufacturer’s approach to FPGA logic program V&V includes incremental releases of FPGA circuit module designs and evaluations of candidate releases before they are formally released. The manufacturer’s approach subjects subsequent releases to full regression testing, which will include any previous incremental releases in addition to the most recent modifications. The manufacturer reviews tool outputs associated with the generation of an FPGA logic program including synthesis, place and route, and simulation results as part of its IV&V activities. The IV&V activities also include RTL simulations of the FPGA logic and post-simulation coverage analyses. The manufacturer uses a constrained-random test generation approach that targets the function of the device as defined by its requirements and specifications to perform “black box” tests on the FPGA logic programs. The manufacturer performs coverage analysis to ensure each FPGA HDL statement that can be tested during RTL simulations has been successfully exercised and performed as expected. Should additional

constrained-random tests fail to exercise HDL statements, the manufacturer applies a “white box” test approach to identify additional constraints. Regardless, the manufacturer may reach a final determination that a specific HDL statement cannot be reached through simulation, and in these limited cases the manufacturer performs a manual inspection and authors a formal justification that explains why coverage of a particular HDL statement during simulation is not feasible. The manufacturer summarized the results of its IV&V activities within individual board-specific “ALS-xxx VV Summary Reports” and the “ALS Platform VV Summary Report” (see References 59, 65, 71, 77, 83, 89, 95, and 54). These documents state the manufacturer achieved 100percent statement coverage when the manual evaluation and justification are considered to provide coverage in addition to the RTL simulations. In addition to the RTL simulation, the manufacturer’s IV&V personnel review of the gate level simulations, which have been performed by the design team, and also perform a reduced-scope gate level simulation. Finally, the released FPGA logic program is installed on its standardized circuit card and subjected to automatic and manual testing.

The NRC staff reviewed the manufacturer’s plans that governed the ALS platform FPGA logic program development, which include its “ALS Management Plan,” “ALS Quality Assurance Plan,” “ALS Configuration Management Plan,” “ALS V&V Plan,” “ALS Test Plan,” “ALS Platform FPGA VV Test Plan” (References 33, 34, 35, 36, 38, and 45). The NRC staff also performed a regulatory audit of the design, IV&V, and test products produced using these plans. This NRC staff effort audited traceability of requirements through lower specifications and to the IV&V activity that verified the requirement. This NRC staff also audited the manufacturer’s configuration management and anomaly reporting and tracking (see Reference 127). Additionally, the NRC staff reviewed the board-specific and platform V&V summary reports.

Based on the NRC staff reviews of ALS platform plans, specifications, and reports, along with the results from the NRC staff’s regulatory audit, the NRC staff determined the ALS platform FPGA logic program development process is of sufficiently high quality to produce FPGA logic programs that are suitable for use in safety-related applications in nuclear power plants because the manufacturer’s process is consistent with the portions of the guidance within BTP 7-14, RG 1.168, RG 1.169, RG 1.170, RG 1.171, RG 1.172, and RG 1.173 that are applicable to an FPGA development for a component through completion of its development.

3.2.4 FPGA Design Variants

The manufacturer developed two designs of each FPGA logic program for each standardized circuit card within the “ALS Topical Report” scope. Although U.S. NRC regulations do not include any specific requirement for independently developed FPGA logic programs, 10 CFR Part 50, Appendix A, General Design Criteria for Nuclear Power Plants, Criterion 22, Protection system independence states, in part, the diversity in component design shall be used to the extent practical to prevent loss of the protection function. This section of the SE provides the NRC staff evaluation for aspects of the development process that are unique to the ALS platform production of two FPGA design variants while Section 3.2.3 of this SE provides the NRC staff evaluation for aspects the development process that apply to all FPGA logic programs. Section 3.9 of this SE separately provides the NRC staff’s evaluation of the ALS platform’s overall diversity characteristics.

The manufacturer identified development processes and procedures to provide [ ] diversity between its independent developments of two FPGA design variants for each standardized circuit card. As discussed within Section 3.9 of this SE, the manufacturer refers to the use of two independently developed FPGA design variants as “Embedded Design Diversity” and the independent designs as “Core A” and “Core B.” The manufacturer has indicated “Embedded Design Diversity” will be used within more complex safety applications to mitigate potential sources of common-cause programming errors from being adverse to public health and safety. Furthermore, the manufacturer expects applicants and licensees referencing this SE will document and consider any application of “Embedded Design Diversity” within plant-specific D3 analyses.

The manufacturer specified the following approach and constraints to provide [ ] diversity through “Embedded Design Diversity” within its development of two FPGA design variants per standardized circuit board:[

1.

2.

3.

4.

]

The NRC staff performed a sample-based review of the manufacturer’s design and IV&V products, including a regulatory thread audit of these products, to confirm the manufacturer developed, verified, and validated “Core A” and “Core B” FPGA logic programs in accordance the constraints it identified to provide [ ] diversity. [

]

Based on the sample-based NRC staff review and regulatory audit, the NRC staff determined the manufacturer developed the ALS platform in accordance with the approach and constraints that the manufacture specified to provide diversity through “Embedded Design Diversity.” The NRC staff further determined this provides a degree of diversity in FPGA logic program design consistent with 10 CFR Part 50, Appendix A, General Design Criteria for Nuclear Power Plants, Criterion 22, Protection system independence, because the ALS platform has demonstrated it to be practical and this form of diversity can contribute to the prevention of lost protection functions.

3.2.5 Application-Specific FPGAs

As described in Section 3.1 of this SE, one of the seven standardized circuit boards, the ALS-102, requires application-specific FPGA logic programming, and no ALS-based safety system is possible without at least one application-specific ALS-102 board. Therefore in contrast to the other ALS platform standardized circuit boards, each ALS-102 FPGA development requires efforts beyond the “ALS Topical Report” scope. Nevertheless, the manufacturer has indicated the application-specific FPGA development processes for each standardized ALS-102 circuit board will be equivalent to those described and evaluated in Section 3.2.3 of this SE. The manufacturer identifies an “Application Requirements Specification” in the “ALS Topical Report” as the source of top level application specifications from which to derive application-specific ALS-102 design specifications (see Reference 32, Table 12.7-1, Item 1.12). Similarly, the manufacturer has indicated the “Application Requirements Specification” will identify whether the application requires any FPGA design variants, as described in Section 3.2.4 of this SE. When an applicant or licensee identifies FPGA design variants within its specifications, the manufacturer has indicated the application-specific FPGA development processes applied to each standardized ALS-102 FPGA variant will follow a development process equivalent to the one described and evaluated in Section 3.2.4 of this SE.

Regardless, the manufacturer has indicated each ALS-102 FPGA logic program will be based on one of the two available FPGA design variants. The manufacturer has indicated each application-specific ALS-102 FPGA logic program will derive top level requirements from the “Application Requirements Specification” while maintaining conformance to the previously established “ALS Platform Requirements Specification” and “ALS-102 Requirements Specification“ (References 43 and 55, respectively). Additionally, the manufacturer reuses previously developed FPGA logic components and supports this reuse through its segregation of FPGA design specifications between FPGA logic functions components common to multiple standardized circuit cards (including the ALS-102) and those specific to a single card. The FPGA common module design specifications are unique to each FPGA design variant (see References 97 and 98). Consequently, the requirements traceability matrices for the ALS-102 are also FPGA design variant dependent (see References 100 and 101).

In Sections 3.2.3 and 3.2.4 of this SE, the NRC staff evaluated the development processes applicable to ALS platform FPGAs and FPGA design variants, so no further NRC staff conclusion is required. However, three plant-specific actions result from the application-specific ALS-102 FPGA logic programming. First, applicants and licensees referencing this SE should

demonstrate it has provided application specification(s) to govern each unique ALS-102 FPGA logic program's development (see Section 4.2, Item 1). Second, applicants and licensees referencing this SE should demonstrate the development of its application-specific ALS-102 FPGA logic programs followed a development process equivalent to the one described and evaluated in Section 3.2.3 of this SE. When the application uses only a single FPGA design variant, this demonstration should identify the associated design variant (either "Core A" or "Core B") and address the production and configuration control of the related life-cycle development products, including those identified in Table 3.2.5-1 for that design variant, where "xxxx" represents a project specific identifier or may directly refer to "6002" if that document may be used without application-specific modification (see Section 4.2, Item 2). Third, when both FPGA design variants are specified, applicants and licensees referencing this SE should demonstrate the FPGA design variants followed equivalent development processes to those described and evaluated in Section 3.2.4 of this SE. This demonstration should address the production and configuration control of the related life-cycle development products, including those identified in Table 3.2.5-1 for both "Core A" and "Core B" (see Section 4.2, Item 3).

Table 3.2.5-1 Plant-Specific ALS-102 Documentation

Document ID	Title
xxxx-10202	ALS-102 Design Specification
xxxx-102(03 / 04)	ALS-102 Core (A / B) FPGA Design Specification
xxxx-102(10 / 11)	ALS-102 FPGA Core (A / B) Requirements Traceability Matrix
xxxx-10206	ALS-102 FPGA Design Specification
xxxx-10216	ALS-102 VV Simulation Environment Specification
xxxx-102(20 / 25)	ASE-102 Core (A / B) Test Simulation Environment Specification
xxxx-102(21 / 26)	ASE-102 Core (A / B) Test Design Specification
xxxx-102(22 / 27)	ASE-102 Core (A / B) Test Case Specification
xxxx-102(23 / 28)	ASE-102 Core (A / B) Test Procedure
xxxx-10242	ALS-102 Release Test Design Specification
xxxx-10245	ALS-102 Release Test Procedure
xxxx-10250	ALS-102 Configuration Status Accounting
xxxx-10261	ABTS-102 Test Design Specification
xxxx-10262	ABTS-102 Test Case Specification
xxxx-10281	ALS-102 Configuration Management Summary Report
xxxx-10282	ALS-102 VV Summary Report
xxxx-10294	ABTS-102 Test Summary Report

3.3 Equipment Qualification

Two objectives of the ALS platform equipment qualification testing are: 1) to establish a bounding operating envelope for temperature, humidity, power source, electromagnetic compatibility, and seismic conditions; and 2) to demonstrate the ALS platform equipment continues to reliably perform its safety function(s) when exposed to conditions within this bounding operating envelope. The manufacturer has indicated its equipment qualification conditions will encompass typical installed operational environments at licensee sites

characterized as mild environments. A mild environment is an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences.

Criteria for environmental qualifications of safety-related equipment are provided in 10 CFR Part 50, Appendix A, "General Design Criterion (GDC) 2, "Design Bases for Protection Against Natural Phenomena," and GDC 4, "Environmental and Dynamic Effects Design Bases." Additionally, 10 CFR 50.55a(h) incorporates IEEE Std 603-1991, which addresses both system-level design issues and quality criteria to qualify components. Section 5.4 of IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," states the equipment qualification requirements for the safety systems shall be in accordance with IEEE Standard 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

To comply with the requirements of GDC 4, 10 CFR 50.49 ("Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants"), and IEEE Std 603-1991, each applicant or licensee should establish an environmental qualification program that demonstrates safety-related equipment will remain functional during and following design basis events. Environmental qualifications are necessary to ensure I&C systems meet design-basis and performance requirements when the equipment is exposed to the normal and adverse environments associated with its location.

For the uses of the ALS platform, the normal and adverse environments should at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences. This eliminates consideration of more severe conditions that apply to equipment in environments that are materially affected by design basis events. Nevertheless, to demonstrate compliance with the requirements of GDC 4, 10 CFR 50.49 ("Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants"), and IEEE Std 603-1991, an applicant or licensee using the ALS platform should demonstrate the equipment qualifications performed on the ALS platform envelope its plant-specific application as installed in its mild environment. This necessitates a plant-specific action to confirm the adequacy of the ALS platform's qualification in full consideration of the plant-specific ALS-based I&C system and its installation.

The manufacturer identified equipment interface/boundary conditions and installation limitations in its "ALS Platform EQ Summary Report" based on its equipment qualification tests (see Reference 51, Section 7). Additionally, within its "ALS Application Guidance," the manufacturer

identified generic restrictions applicable to ALS projects and a means for projects to specify implementation of applicable restrictions. The manufacturer identifies these restrictions to address requirements that have not been met and known issues with certain ALS platform configurations that have been identified during the ALS product qualification activities. Furthermore, the manufacturer recommends each ALS project formally review the restrictions and identify and justify any deviation from conforming to these restrictions. The "ALS Application Guidance" generic restrictions incorporate or reference "ALS Platform EQ Summary Report" conditions and limitations. The "ALS Application Guidance" generic restrictions additionally include statements relating to the restricted use of Common Q components (see

Reference 41). Although the application of Common Q components may have been evaluated by the NRC staff elsewhere, restrictions relating to Common Q components are not evaluated by the NRC staff in this SE, because the Common Q components are not within scope of the "ALS Topical Report."

For clarity and to ensure full coverage, the NRC staff created two plant-specific actions to address the installation conditions and limitations in the "ALS Platform EQ Summary Report" and the generic restrictions in the "ALS Application Guidance" (see Section 4.2, Items 4 and 5, respectively).

Section 4 of the "ALS Topical Report" (Reference 32) summarizes the manufacturer's equipment qualification for temperature/humidity, seismic, and electromagnetic compatibility. The "ALS EQ Plan" (Reference 37) provides guidelines to ensure the ALS platform equipment is suitably qualified for Class 1E operation in a mild environment installation. The manufacturer has indicted each applicant or licensee will reference the "ALS EQ Plan" for each application specific safety-related system built from ALS platform components.

The "ALS Platform EQ Summary Report" (Reference 51) provides further details of the equipment qualification tests, the results, and manufacturer conclusions derived from equipment qualification type testing.

The "ALS Platform Qualification Evaluation" (Reference 52) provides manufacturer analyses to support extension or exclusion of platform capabilities that the "ALS Topical Report" describes. These analyses address the number and nature of signals used during equipment qualification. They also address the limited configuration of the standardized circuit boards for processing these signals. These analyses were performed, because the single chassis Equipment Under Test (EUT) for the type tests neither exercised and loaded the full complement of available signals nor included all unique configurations of signals that each standardized circuit board supports. In consideration of the limited EUT configuration, the "ALS Platform Qualification Evaluation" provides manufacturer analyses of platform capabilities considered qualified through the efforts summarized in the "ALS Platform EQ Summary Report" and other board-specific testing (i.e., the ABTS-xxx Test Summary Reports").

The "ALS EQ Rack System Specification" (Reference 50) is the manufacturer's specification for the EUT used in the equipment qualification type tests. Additionally, the "ALS FPGA Qualification Evaluation" (Reference 99) provides manufacturer analyses of differences between

FPGA programs used within the EUT and the final production versions of the FPGAs, because EUT used only one FPGA program design variant of an earlier version than the final production versions.

This SE does not include plant-specific determinations for a specific application or installation. Instead, the NRC staff evaluated the equipment qualification type testing that the manufacturer performed on the seven ALS platform standardized circuit boards, representative backplane, and chassis, against applicable equipment qualification regulations, standards and guidance. Additionally, this SE includes a plant-specific action for applicants and licensees referencing this SE to demonstrate the adequacy of the ALS platform's qualification in consideration of the

applicant's or licensee's environmental qualification program, ALS-based I&C system, and installed operational environment (see Section 4.2, Item 6). This plant-specific action is consistent with GDC 4, 10 CFR 50.49, IEEE Std 603-1991, and the final conclusion of the "ALS Platform EQ Summary Report." The manufacturer's "ALS Platform EQ Summary Report" concludes "Plant specific applications shall reconcile differences between the qualified and installed configurations in order to extend the EMC, environmental, and seismic qualifications for specific applications" (see Reference 51, Section 8).

The next subsection provides an overview the type testing and the test configuration. It also provides NRC staff evaluations generally applicable to the manufacturer's equipment qualification activities. Each of the subsequent three subsections provides an NRC staff evaluation of a specific ALS platform equipment qualification test against its applicable regulatory evaluation criteria.

3.3.1 Test Overview and Type Test Configuration

The "ALS EQ Plan" requires each equipment qualification test procedure to provide a detailed description of the test to be performed and to document the specific test setup and acceptance/performance criteria to be applied during the test. The "ALS EQ Plan" also requires the test procedures provide a description of the safety functions of the EUT and the measurements and methods to demonstrate the safety functions are not affected by the test.

The manufacturer created three specific test procedures to address its equipment qualification: 1) the "ALS Environmental Test Procedure," 2) the "ALS Seismic Test Procedure," and 3) the ALS EMC Test Procedure;" along with a supporting baseline test procedure, the "ALS Qualification Equipment Baseline Test Procedure." The "ALS Platform Configuration Status Accounting" document (Reference 40) identifies these test procedures by name, revision, and date.

The baseline test procedure supports the individual equipment qualification test procedures. In part, performing the baseline test procedure demonstrates continued operability of the identified EUT safety functions. Although the test procedures were not submitted to the NRC for staff review, the manufacturer's "ALS Topical Report" provides a high level summary of the individual qualification tests, and its "ALS Platform EQ Summary Report" provides a more detailed summary of the individual qualification tests along with acceptance and performance criteria.

To demonstrate identified safety functions remain operable during testing, the manufacturer required the ALS platform meet the safety function acceptance criteria and performance criteria outlined in the "ALS EQ Plan" and further described in its "ALS Platform EQ Summary Report" (see Reference 37, Section 3, and Reference 51, Section 3, respectively). The performance criteria apply before, during and after performance of an environmental test cycle, each step within the seismic test sequence, or applicable EMC tests. The manufacturer established the performance criteria to be "no operational degradation, loss of function, or structural damage to EUT" for each of its equipment qualification tests except in some cases when performing tests not identified by NRC staff regulations, considered optional to obtain Conformite Europeene (CE) Mark certification, or where the testing standard allows relaxation of the performance

criteria. The NRC staff did not evaluate optional CE Mark-related tests. However, it notes the additional tests provide some degree of additional assurance.

The manufacturer's "ALS EQ Plan" similarly identifies an individual test report for each test procedure. And likewise, the manufacturer's "ALS Platform Configuration Status Accounting" identifies three specific test reports that correspond to the test procedures for its equipment qualification: 1) the "ALS Environmental Qualification Report," 2) the "ALS Seismic Qualification Report," and 3) the "ALS Electromagnetic Compatibility Qualification Report." The "ALS Platform Configuration Status Accounting" also identifies an additional supplemental test report, "ALS Electromagnetic Compatibility Qualification Report - Supplemental 1." Unlike the test procedures, the "ALS Topical Report" does not provide a high level summary of the individual qualification results. However, similar to the individual test procedures, the manufacturer did not submit the individual qualification reports for NRC staff review but the manufacturer's "ALS Platform EQ Summary Report" references the individual qualification reports and summarizes the test results. Although initial equipment qualification tests identified some non-compliance, following supplemental testing of the equipment with modifications, the "ALS Platform EQ Summary Report" states each equipment qualification test met the established acceptance and performance criteria.

The "ALS EQ Rack System Specification" (Reference 50) is the manufacturer's specification of the ALS platform instrument configuration used during equipment qualification type testing. This configuration installed one each of the seven standardized circuit boards within a single equipment qualification backplane and chassis. The "ALS EQ Rack System Specification" identifies the configuration of each board within the EUT. The "ALS EQ Rack System Specification" also identifies the signals monitored by and generated from the EUT and the safety functions of the ALS platform type test configuration (see Reference 50, Figure 3-1 and Table 8-1, respectively).

The EUT used only one FPGA design variant (Core A). The "ALS Platform EQ Summary Report" summarizes the "ALS FPGA Qualification Evaluation." This summary addresses changes made to the EUT's FPGA program revisions to make the Core A 's production revisions and differences between the EUT's FPGA program revisions and the second design variant (Core B's) production FPGA program revisions (see Reference 51, Section 6.2). The "ALS Platform EQ Summary Report" identifies the revisions of EUT FPGA programs along with

the Core A and Core B production FPGA program revisions that the manufacturer considers qualified by its similarity analyses (see Reference 51, Table 6-3).

The NRC staff reviewed the "ALS Topical Report," "ALS EQ Plan," and "ALS Platform EQ Summary Report" and determined the manufacturer's equipment qualification conforms to Regulatory Position 1's preference for type testing, as provided in the RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," because the ALS platform manufacturer performed type testing on seven standardized circuit boards, a backplane, and a chassis using a set of FPGA programs representative of production FPGA programs. The NRC staff further determined the manufacturer documented its equipment qualification in a manner that supports evaluations by applicants and licensees to determine whether the ALS platform equipment qualification meets

its environmental qualification program and demonstrates its plant-specific safety equipment's safety functions will remain functional during and following its design basis events. However, the NRC staff's SE does not eliminate the need to perform application-specific system and installation testing (see Section 4.2, Item 23). Furthermore, the NRC staff's SE does not preclude an applicant or licensee from performing supplemental equipment qualification on its plant-specific system application (see Section 4.2, Item 6).

3.3.2 Environmental Testing

RG1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," endorses and provides guidance for compliance with IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." RG 1.209 describes a method acceptable to the NRC staff for meeting the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants.

The manufacturer committed to perform its environmental qualification in accordance with IEEE Std 323 -1974 as endorsed by RG 1.89 and IEEE Std 323-2003 as endorsed by RG 1.209 (see Reference 37, Section 3, and Reference 51, Section 1.2). As discussed in Sections 3.3 and 3.3.1 of this SE, the manufacturer produced configuration controlled specifications, plans, procedures with acceptance and performance criteria to perform environmental type testing on seven standardized circuit boards, a backplane, and a chassis. The manufacturer justified the configuration of its type tested equipment through its choice of board configurations (e.g., least filtering, highest baud rate, etc.) with the potential to be most susceptible to environmental effects and therefore most likely to reveal unacceptable performance. The manufacturer's "ALS EQ Plan" (Reference 37) defines its environmental qualification approach and the "ALS Platform EQ Summary Report" (Reference 51) provides a detailed summary of the environmental qualification testing and results. The manufacturer performed initial environmental type tests at the Westinghouse Electric Company (Westinghouse) test facility in New Stanton, Pennsylvania, between January 30, 2012, and February 20, 2012. The manufacturer performed supplemental environmental type tests at the same facility between December 6, 2012, and December 19, 2012. This testing included baseline verification tests and performance monitoring during synergistic environmental conditions that combined maximum and minimum specified

temperatures, humidity and DC input voltage. The "ALS Platform EQ Summary Report" states the environmental qualification performed on the ALS platform equipment met the technical requirements of the IEEE Std 323-1974 as endorsed by RG 1.89 and IEEE Std 323-2003 as endorsed by RG 1.209 (see Reference 51, Section 8).

The NRC staff reviewed the "ALS Topical Report," "ALS EQ Plan," and "ALS Platform EQ Summary Report" and determined the manufacturer's environmental qualification conforms to the RG 1.209, Regulatory Position 1, inclusion of potential synergistic effects, because the ALS platform manufacturer specified an environmental envelope consistent with a typical mild environment that included potential synergistic effects between temperature, humidity and input voltage on the seven standardized circuit boards (see Reference 37, Table 3-2 and Figure 3-1; and Reference 51, Table 4-4). The manufacturer determined the worst-case synergistic effect for the technology of the standardized circuit boards was high temperature and high voltage

based on the performance of on-board power supply circuitry. The manufacturer also performed supplemental tests at high temperature and low voltage to evaluate potential adverse synergistic effects on data communications and response time. Additionally, the NRC staff determined the manufacturer's environmental qualification conforms to the RG 1.209, Regulatory Position 2, because the manufacturer performed its qualification testing on functioning equipment with FPGA programming and diagnostics that are representative of those intended to be used in the operation of an ALS-based system while subjecting the EUT to the manufacturer's specified environmental envelope. Furthermore, this testing exercised the portions of the equipment that the manufacturer identified as necessary to accomplish safety functions or whose failure could impair a safety function within a configuration that the manufacturer justified as most susceptible to environmental effects and therefore most likely to reveal unacceptable performance. The NRC staff further determined the manufacturer's environmental qualification conforms to the RG 1.209, Regulatory Position 4, because the environmental conditions are based on the manufacturer's prior analyses of licensee mild environments and the manufacturer has retained evidence of its mild environment qualification by placing its environmental qualification plans, procedures and reports under configuration control.

Additionally, the NRC staff agrees with the manufacturer identified installation limitation concerning temperature envelope for the platform (see Reference 51, Section 7.2, Item 9). The manufacturer designed its equipment to allow for a temperature rise within the cabinet. However, the type testing did not include a cabinet configuration or generate the maximum specified temperature rise. Instead, the manufacturer tested the equipment at a maximum ambient temperature. This maximum ambient temperature was derived by adding a typical maximum plant ambient temperature for operating conditions in nuclear power plant control rooms to the manufacturer's specified maximum internal cabinet temperature rise for the ALS platform.

Therefore, applicants and licensees referencing this SE should ensure the maximum temperature within an ALS cabinet does not exceed either the manufacturer specified or qualified design temperatures. Applicants and licensees referencing this SE should demonstrate the maximum temperature rise within each cabinet containing ALS components does not exceed the platform specification. Applicants and licensees referencing this SE should also demonstrate the maximum ambient temperature at each ALS platform installation location will not exceed the maximum qualified temperature during normal plant operation, including anticipated operational occurrences. Licensees should evaluate the adequacy of design basis temperature margin in full consideration of the actual temperature rise within its plant-specific cabinet and the maximum ambient temperature at the installed cabinet's location during normal plant operation, including anticipated operational occurrences (see Section 4.2, Item 6).

3.3.3 Seismic Testing

RG 1.100, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," Revision 3, describes a method acceptable to the NRC staff for meeting seismic qualification. RG 1.100 currently endorses, with exceptions and clarifications, IEEE Std 344-2004 and ASME QME-1-2007, and

the prior revision of RG 1.100 endorsed IEEE Std 344-1987. IEEE Std 344 is the "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."

The manufacturer committed to perform its seismic qualification in accordance with the technical requirements of IEEE Std 344-1987 as endorsed by RG 1.100, Revision 2, and the technical requirements of IEEE Std 344-2004 as endorsed by RG 1.100, Revision 3 (see Reference 37, Section 5, and Reference 51, Section 1.2). As discussed in Sections 3.3 and 3.3.1 of this SE, the manufacturer produced configuration controlled specifications, plans, procedures with acceptance and performance criteria to perform seismic type testing on seven standardized circuit boards, a backplane, and a chassis. The manufacturer's "ALS EQ Plan" (Reference 37) defines its seismic qualification approach and the "ALS Platform EQ Summary Report" (Reference 51) provides a detailed summary of the seismic qualification testing and results. The manufacturer performed seismic type tests at the Westinghouse test facility located in New Stanton, Pennsylvania, between February 7, 2012, and February 12, 2012. This testing included baseline verification tests and performance monitoring during seismic conditions. The "ALS Platform EQ Summary Report" states the seismic qualification performed on the ALS platform equipment met the technical requirements of IEEE Std 344-1987 as endorsed by RG 1.100, Revision 2, and IEEE Std 344-2004 as endorsed by RG 1.100, Revision 3 (see Reference 51, Section 8).

The NRC staff reviewed the "ALS Topical Report," "ALS EQ Plan," and "ALS Platform EQ Summary Report" and determined the manufacturer's seismic qualification conforms to the RG 1.100 endorsements of IEEE Std 344. This determination is based on the manufacturer's establishment and documentation of a Safe Shutdown Earthquake (SSE) Required Response Spectra (RRS) for use by applicants and licensees referencing this SE, and the manufacturer's seismic testing in accordance with the technical requirements of the industry standards, as endorsed by NRC staff regulatory guidance. The NRC staff's conclusion is further based on its confirmation that these seismic qualification activities included a resonance search on the EUT, subjected the equipment to five Operating Basis Earthquakes and one Safe Shutdown Earthquake based on the established SSE RRS, and verified the type tested equipment maintained its physical integrity and capability to perform the manufacturer identified platform safety functions before, during and after each seismic test.

3.3.4 Electromagnetic Compatibility Testing

RG 1.209 identifies RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 1, which describes a method acceptable to the NRC staff for design, installation, and testing practices to address the effects of EMI/RFI and power surges on safety-related I&C systems.

RG 1.180 endorses the MIL-STD-461E and IEC 61000 series of tests to evaluate conducted and radiated EMI/RFI and power surges on safety-related I&C systems. In its discussion section, RG 1.180 states both RG 1.180 and EPRI TR-102323 present acceptable means for demonstrating electromagnetic compatibility (EMC), and the applicant or licensee has the freedom to choose either method. It should be noted the maximum acceptable limits for

emissions or susceptibility are different for some types of testing and, therefore, it is possible for equipment to meet the requirements and limits of one test method, but not meet the corresponding requirements and limits of the equivalent test from another test method. RG 1.180 states this is acceptable, as long as the requirements of a complete suite of EMI/RFI emissions and susceptibility criteria are met, with no mixing and matching of test criteria and methods.

EPRI TR-102323, "Guideline for Electromagnetic Interference Testing in Power Plants," provides alternatives to perform site-specific EMI/RFI surveys to qualify digital plant safety I&C equipment in a plant's electromagnetic environment. In a SE issued in 1996, the NRC staff concluded the recommendations and guidelines in EPRI TR-102323 provide an adequate method for qualifying digital equipment for a plant's electromagnetic environment without the need for plant-specific EMI/RFI surveys if the plant-specific electromagnetic environment is confirmed to be similar to that identified in EPRI TR-102323. Although allowed by regulatory guidance, both plant-specific EMI/RFI surveys and the confirmation of a plant-specific electromagnetic environment are outside scope of the “ALS Topical Report.”

As discussed in Sections 3.3 and 3.3.1 of this SE, the manufacturer produced configuration controlled specifications, plans, procedures with acceptance and performance criteria to perform EMC type testing on seven standardized circuit boards, a backplane, and a chassis. The manufacturer justified the configuration of its type tested equipment through its choice of board configurations (e.g., least filtering, highest baud rate, etc.) with the potential to be most susceptible to electromagnetic effects and most prone to generate electromagnetic emissions, and therefore most likely to reveal unacceptable performance. The manufacturer’s “ALS EQ Plan” (Reference 37) defines its EMC qualification approach, and the “ALS Platform EQ Summary Report” (Reference 51) provides a detailed summary of the EMC qualification testing and results. As a Westinghouse commercially dedicated test service provider, Elite Electronic Engineering performed initial EMC type tests at its Downers Grove, Illinois facility between January 30, 2012, and February 20, 2012. Also as a Westinghouse commercially dedicated test service provider, Washington Laboratories, Ltd. performed supplemental EMC type tests at the Westinghouse test facility in New Stanton, Pennsylvania, between August 8, 2012, and September 13, 2012. Westinghouse personnel were present to support the tests, to assure testing was performed in accordance with its procedure, and to resolve any issues that arose during the tests. The testing included baseline verification tests and performance monitoring during EMC conditions excluding emissions testing. Each of the following four subsections provides an NRC staff evaluation of the ALS platform against a specific type of EMC qualification test and its applicable regulatory evaluation criteria.

3.3.4.1 Radiated and Conducted Emissions

The manufacturer committed to perform its electromagnetic emission testing in accordance with the MIL-STD-461E set of tests as endorsed by RG 1.180. The manufacturer performed additional emissions tests to meet CE Mark certification rather than NRC regulatory guidance (see Reference 37, Section 4, Table 4-1 and Figures 4-1 through 4-4). The manufacturer identified the emissions tests it performed and the test results within the “ALS Platform EQ Summary Report” (see Reference 51, Tables 5-3 and Section 5.1.7 for initial tests; and

Table 5-6 and Section 5.2.9 for supplemental tests). The manufacturer identified non-compliant results during initial tests and performed supplemental tests. Upon the conclusion of the supplemental tests, the manufacturer stated it complied with all electromagnetic emission tests identified in MIL-STD-461E as endorsed by RG 1.180.

During initial testing, the manufacturer identified the power supplies that energized the EUT as the contributing factor to non-compliance to CE101 testing. However, these power supplies are not within the scope of the "ALS Topical Report." Therefore, the CE101 testing represents a baseline of the ALS platform rather than a demonstration that an ALS-based system, with the power supplies used during EMC testing, would meet the CE101 emission limits. Regardless, supplemental testing of CE101 demonstrated the exception allowed within RG 1.180 had been met.

The "ALS Platform EQ Summary Report" states the emissions qualification performed on the ALS platform equipment met the technical requirements of MIL-STD-461E as endorsed by RG 1.180, Revision 1 (see Reference 51, Section 8).

The NRC staff reviewed the "ALS Topical Report," "ALS EQ Plan," and "ALS Platform EQ Summary Report" and determined the manufacturer's EMC emissions qualification conforms to the RG 1.180 endorsement of MIL-STD-461E. This determination is based on the manufacturer's documentation of each emissions test, testing in accordance with the technical requirements of the military standard, as endorsed by NRC staff regulatory guidance, and documentation of the equipment's emission levels for use by applicants and licensees referencing this SE.

3.3.4.2 Radiated and Conducted Susceptibility

The manufacturer committed to perform its electromagnetic susceptibility testing in accordance with the IEC suite of tests as endorsed by RG 1.180. Additionally, the manufacturer performed

broader susceptibility testing than identified in RG 1.180 to meet CE Mark certification rather than NRC regulatory guidance. The manufacturer also performed the RS103 test to cover the 1 to 10 GHz frequency range (see Reference 37, Section 4, Tables 4-2 through 4-4). The manufacturer identified the susceptibility tests it performed and the test results within the "ALS Platform EQ Summary Report" (see Reference 51, Table 5-3 and Sections 5.1.6.2 and 5.1.7.5, for initial tests; and Table 5-6 and Sections 5.2.7.2 and 5.2.7.5 through 5.2.7.8, for supplemental tests). The manufacturer's initial testing identified non-compliant results that required corrective actions to achieve compliance and did not include all planned tests. Subsequently, the manufacturer performed supplemental tests. Upon the conclusion of the supplemental tests and with all modifications incorporated, the manufacturer stated it complied with all electromagnetic susceptibility tests identified in the IEC suite of tests as endorsed by RG 1.180. Furthermore, to address some of the modifications, the manufacturer identified installation limitations (see Reference 51, Section 7.2).

The "ALS Platform EQ Summary Report" states the susceptibility qualification performed on the ALS platform equipment met the technical requirements of the IEC suite of tests as endorsed by RG 1.180, Revision 1 (see Reference 51, Section 8).

The NRC staff reviewed the “ALS Topical Report,” “ALS EQ Plan,” and “ALS Platform EQ Summary Report” and determined the manufacturer’s EMC susceptibility qualification conforms to the RG 1.180 endorsed IEC suite of tests. This determination is based on the manufacturer’s documentation of each susceptibility test, testing in accordance with the technical requirements of the industry standard, as endorsed by NRC staff regulatory guidance, verification of the equipment’s continued ability to perform the identified safety functions, and documentation of installation limitations for use by applicants and licensees referencing this SE. These installation limitations are consistent with the modifications performed during susceptibility testing to achieve successful test results.

3.3.4.3 Surge and Electrical Fast Transient Withstand Capability

The manufacturer committed to perform surge and electrical fast transient testing in accordance with the IEC suite of tests as endorsed by RG 1.180 (see Reference 37, Section 4, Table 4-5). The manufacturer identified the surge and electrical fast transient testing it performed and the test results within the “ALS Platform EQ Summary Report” (see Reference 51, Table 5-3, Sections 5.1.6.3 and 5.1.6.4, for initial tests; and Table 5-6 and Sections 5.2.7.3 and 5.2.7.4, for supplemental tests). The manufacturer performed supplemental tests to address modifications made to the ALS since the initial tests. Upon the conclusion of the supplemental tests and with all modifications incorporated, the manufacturer stated it complied with all surge and electrical fast transient tests identified in the IEC suite of tests as endorsed by RG 1.180.

The “ALS Platform EQ Summary Report” states surge and electrical fast transient qualification performed on the ALS platform equipment met the technical requirements of the IEC suite of tests as endorsed by RG 1.180, Revision 1 (see Reference 51, Section 8).

The NRC staff reviewed the “ALS Topical Report,” “ALS EQ Plan,” and “ALS Platform EQ Summary Report” and determined the manufacturer’s EMC surge and electrical fast transient qualification conforms to the RG 1.180 endorsed IEC suite of tests. This determination is based on the manufacturer’s documentation of each surge and electrical fast transient withstand test, testing in accordance with the technical requirements of the industry standard, as endorsed by NRC staff regulatory guidance, and verification of the equipment’s continued ability to perform the identified safety functions.

3.3.4.4 Electrostatic Discharge Withstand Testing

The manufacturer committed to electrostatic discharge testing to meet CE Mark certification rather than NRC regulatory guidance (see Reference 37, Section 4, Table 4-5). The manufacturer identified the electrostatic discharge tests it performed and the test results within the “ALS Platform EQ Summary Report” (see Reference 51, Table 5-3 and Section 5.1.6.1 for initial tests; and Table 5-6 and Section 5.2.7.1 for supplemental tests). The manufacturer performed supplemental tests to address modifications made to the ALS since the initial tests. Upon the conclusion of the supplemental tests and with all modifications incorporated, the manufacturer stated it complied with electrostatic discharge testing identified by IEC/EN 61000-4-2. Furthermore, to address the potential for electrostatic discharge to degrade equipment reliability, the manufacturer identified an installation limitation to use preventative techniques

during equipment installation, operation, and maintenance (see Reference 51, Section 7.2, Item 8).

The NRC staff reviewed the “ALS Topical Report,” “ALS EQ Plan,” and “ALS Platform EQ Summary Report” and agrees the manufacturer’s electrostatic discharge testing and installation limitation are consistent with RG 1.180’s reference to IEC 61000-4-2. This determination is based on the manufacturer’s documentation of its electrostatic discharge testing, testing in accordance with the technical requirements of the industry standard, verification of the equipment’s continued ability to perform the identified safety functions, and documentation of installation limitations for use by applicants and licensees referencing this SE. These installation limitations are consistent with protecting equipment from damage due to electrostatic discharge that could degrade component reliability.

3.4 Platform Integrity Characteristics

SRP Chapter 7, Appendix 7.1-C, Section 5.5, “System Integrity,” states a special concern for digital computer-based systems is confirmation that the real time performance of the system is adequate to ensure completion of protective actions within the critical time periods identified within Clause 4.10 of IEEE Std 603-1991. SRP BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” provides supplemental guidance to evaluate the real-time performance of digital systems and architectures, and discusses the identification of bounding real-time performance specifications and the verification of these specifications to demonstrate real-time performance. The establishment of predictable performance and behavior for a platform supports the future evaluation of a safety system based on the platform. The following subsections evaluate the ALS platform in terms of its response time characteristics, deterministic behavior, and fault management capabilities to support future evaluations of safety systems based on the ALS platform.

3.4.1 Response Time

GDC 20, 21, 23, and 25 (of Appendix A to 10 CFR Part 50) constitute general requirements for timely operation of the protection features. To support these requirements, SRP BTP 7-21 provides the following guidance:

- The feasibility of design timing may be demonstrated by allocating a timing budget to components of the system architecture to ensure an entire system meets its timing requirements.
- Timing requirements should be met by design commitments.

Two regulations provide bases for this guidance, where the first is 10 CFR 50.55a(h) and its incorporation of IEEE Std 603-1991 by reference. The second is 10 CFR 50.36(c)(1)(ii)(A), which provides the basis for timing requirement commitments by requiring the inclusion of limiting safety system settings for nuclear reactors in the plant technical specifications, “so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded."

Each licensee should provide its plant-specific and application-specific safety function response time design bases as response time performance requirements to be met by an ALS platform-based system (see Reference 32, Section 2.7). The actual response time of an ALS platform-based system is determined by its overall configuration. Therefore, each licensee must determine the ALS platform response time characteristics are suitable for its plant-specific application. The following information and staff evaluation addresses the ALS platform response time characteristics and use of these characteristics in support of future plant-specific suitability determinations, because the ALS platform is a set of components to which response time budgets are allocated.

The ALS platform response time performance characteristics are described in general terms within the "ALS Topical Report" (see Reference 32, Section 2.7), and the "ALS Topical Report" also identifies configuration settings that affect response time performance (see Reference 32, Sections 2.2.2.1 and 2.3.1). To meet a typical response time performance requirement, an ALS platform-based system must acquire the input signal that represents the start of a response time performance requirement, perform logic processing associated with the response time performance requirement, and generate an output signal that represents the end of a response time performance requirement. These ALS platform response time components exclude: 1) the earlier plant process delays through the sensor input to the platform and 2) the latter delays through a final actuating device to affect the plant process. Therefore, the applicant's or licensee's plant-specific and application-specific safety function response time design bases should address these response time components separate from the response time performance requirements specified for the applicant's or licensee's ALS platform-based system.

The "ALS Topical Report" Figure 2.7-1 depicts the typical ALS platform response time as a chain of high level delays that includes three board types (Input Board, Core Logic Board, and Output Board) where:

- Any of the input boards, ALS-302, ALS-311, or ALS-321, may acquire an input signal and perform some initial signal conditioning/processing (see Reference 32, Figure 2.7-1, "Input Delay");
- The ALS-102 Core Logic Board performs plant-specific and application-specific logic processing functions on the inputs to control an output signal (see Reference 32, Figure 2.7-1, "Logic Delay"); and,
- Any of the output boards, ALS-402, or ALS-421, may perform some final signal conditioning before generating the output signal (see Reference 32, Figure 2.7-1, "Output Delay").

However, an ALS-601 Communications Board may also be used within a system to transfer digital data as part the safety signal path in direct support of response time performance requirements, although this is not directly discussed in Section 2.7 of the "ALS Topical Report." Nevertheless, this capability is consistent with other discussions in the "ALS Topical Report" (see Reference 32, Section 2.2.8). When an ALS-601 Communications Board is used as part of the safety signal path in direct support of response time performance requirement, the chain of delays would include a minimum of six boards (Input Board, Core Logic Board, Communication Board #1, Communications Board #2, Core Logic Board #2, and Output Board) where additional component response time delays beyond those depicted in "ALS Topical Report" Figure 2.7-1

would exist. The first ALS-102 Core Logic Board would perform plant-specific and application-specific logic. However, its “Logic Delay” would now be associated with providing digital data to the first ALS-601 Communications Board. The first ALS-601 Communications Board would transmit digital data to the second communications board to produce a “Data Transfer Delay.” Then the second ALS-601 Communications Board would provide successfully received digital data to the second ALS-102 Core Logic Board to produce a “Data Reception Delay.” Finally, the second ALS-102 Core Logic Board would perform additional plant-specific and application-specific logic to produce another “Logic Delay.”

Each ALS platform input board has a defined propagation delay from the point in time when an input signal changes until the digital representation of the input signal reflects the new value and is available via the RAB for access by the ALS-102 Core Logic Board. Each ALS platform output board has a similarly defined propagation delay from the point in time when the ALS-102 Core Logic Board provides a new digital representation for an output signal via the RAB until the output signal reflects 50percent of the difference between the original value and the new value. In addition to these defined propagation delays, either an input or output board may apply configuration data to establish application-specific filtering, and this filtering can produce additional response time delays. Plant-specific and application-specific response time performance budgets should account for the input and output delays, including propagation delays and any additional application-specific digital filtering delays, as applicable.

Like an input board, the ALS-601 Communications Board has a defined propagation delay from the point in time when digital data reception successfully completes until the digital data is

available via the RAB for access by the ALS-102 Core Logic Board. Like an output board, the ALS-601 Communications Board has another defined propagation delay from the point in time when digital data is provided by the ALS-102 Core Logic Board via the RAB until the ALS-601 makes this digital data available for transmission. Regardless, the plant-specific and application-specific configuration of the ALS-601 Communications Board establishes the interval between digital data transmissions and the worst-case transmission duration. Furthermore, consistent with DI&C-ISG-04, Staff Position 1, Point 20 the safety system response time calculations should assume a data error rate greater than or equal to a design basis error rate, which is supported by the error rates observed during design and qualification testing (see Section 3.7.2.1.20). Plant-specific and application-specific response time performance budgets should account for the ALS-601 Communications Board digital data communications delays, as applicable. Furthermore, because the ALS-601 program does not incorporate logic to detect and a communication timeout (i.e., failure to successfully received valid data), when an ALS application must take action (e.g., go to a fail-safe state or initiate an alarm indication) based on lost communication or an excessive communication delay, a project-specific ALS application specification must include an appropriate requirement to address this application-specific system behavior. The manufacturer identified this application-related restriction within its “ALS Application Guidance” (see Reference 41, Table 2.3-1, Item A4).

The ALS platform does not establish a propagation delay from digital input to digital output for the ALS-102 Core Logic Board, because the logic for each ALS-102 Core Logic Board is both plant-specific and application-specific. In accordance with the “ALS Topical Report,” each ALS-102 Core Logic Board controls the instrument frame time, which is the interval between

accessing each specific board so information will have been read once from all application input boards and written once to all application output boards. For some applications the ALS-102 Core Logic Board propagation delay could be relatively small in comparison to the RAB transfer time and application-specific frame time. However, similar to the application-specific digital filtering on input or output boards, plant-specific and application-specific logic within the ALS-102 Core Logic Board may produce additional response time delays which are not small in comparison to the RAB transfer time and application-specific frame time. Plant-specific and application-specific response time performance budgets should account for the ALS-102 Core Logic Board processing delays, as applicable.

The “ALS Platform Specification” specifies a single crystal oscillator for use with each FPGA and performance requirements for the oscillator (see Reference 44, Section 3.3.7.1). For all ALS platform’s FPGA-based digital logic, the digital logic delays are fixed at design time and the maximum digital delay is a function of the as-built logic (i.e., as-designed and as-configured) and the frequency of the local oscillator. The FPGA logic of the ALS-102 Core Logic Board includes the logic that establishes the ALS platform board access time, which is a fixed interval allocated to exchange data with an individual board using the RAB protocol, and the application-specific frame time, which is the interval between accessing each specific board so information will have been read once from all application input boards and written once to all application output boards. The same oscillator that establishes the board access time and the frame time also establishes the timing of the ALS-102 Core Logic Board’s logic for control of the RAB as the bus master. Use of a single crystal local oscillator on the master ALS-102 Core Logic Board

and one each slave ALS platform standardized circuit board allows verification of the ALS-102 Core Logic Board’s local oscillator as a method to bound the digital system response time of the FPGA logic, because the RAB protocol logic bounds oscillator drift between boards.

To ensure response time performance is maintained, the RAB protocol includes within its timing budget one retry and the assertion of a bus communication failure upon a failed transaction within the ALS platform board access time. Furthermore, qualification testing of the ALS platform continuously exercised the RAB and did not result in the observation of a failed RAB transaction. For the qualification test configuration, the unit under test performed 20 RAB transactions [ ], and test equipment monitored the unit under test for RAB transaction errors but did not detect any RAB transaction errors (see Reference 51, Section 3.2.1.7). For the qualification test configuration, the observed error rate of zero will support future safety system response time calculations that assume an error rate greater than or equal to a design basis error rate. Therefore, the qualification testing demonstrated the RAB protocol’s ability to reliably assure continued response time performance. The qualification tests also included representative time response testing from a digital input signal change to a corresponding digital output signal change. This manufacturer documented the observed minimum and maximum time response after repeating the test twenty times (see Reference 51). The documented time response is consistent with time response associated with digital input board’s minimum filtering configuration, negligible board logic propagation delays, and expected variations that result from the point in time that the initiating event asynchronously occurs with respect to the RAB transaction sequence and the specified frame time. The maximum time response is also less than the sum of maximum time responses for the digital input channel and the digital output channel.

The ALS platform provides features to monitor an ALS-102 Core Logic Board's application-specific frame time to address the concern that an oscillator's drift could remain undetected and negatively affect response time performance. An application should consider the inclusion of features to monitor ALS-102 Core Logic Board oscillator drift when the application implements delays, either though application-specific logic or a digital filter configuration that extends a board's response time beyond its propagation delay. Plant-specific application specifications for the ALS-102 Core Logic Board would be required to include features to monitor an ALS-102 Core Logic Board's application-specific frame time, because these features are not included in the "ALS Platform Specification." When application specifications for the ALS-102 Core Logic Board include features to monitor an ALS-102 Core Logic Board's application-specific frame time, the continued performance of its local oscillator can be independently verified as part of technical specification surveillance requirements. In turn, this independent clock verification can be extended to the indirect verification of the oscillators on each RAB slave standardized circuit board (i.e., ALS-302, ALS-311, ALS-321, ALS-402, ALS-421, and ALS-601), because RAB protocol design features bound the oscillator logic drift between the master ALS-102 board and each slave board.

The NRC staff determined surveillance measurements of the ALS-102s' oscillator performance may be used by applicants or licensees to confirm the application-specific instrument's digital response time performance requirements continue to be met when NIST traceable independent

clock verifications bound the system's digital response time performance. The NRC staff further determined the worst-case board access and frame times, which are application-specific, may be used by licensees when determining whether the ALS platform response time characteristics are sufficient for the applicant's or licensee's plant-specific application.

The NRC staff also determined the worst-case RAB digital data transaction time may be used by applicants and licensees when determining whether the ALS platform response time characteristics are sufficient for the applicant's or licensee's plant-specific application. This determination is based on the results of qualification testing. The manufacturer did not observe any failed RAB transaction during qualification testing. The RAB protocol includes provisions to bound oscillator logic drift between boards and provides operator notification for a failed RAB transaction.

Based on the preceding evaluation of the ALS platform and staff determinations, the NRC staff determined the response time performance for each safety-related system based on the ALS platform requires a plant-specific action item to address system timing requirements and the timing budget among system components. Applicant and licensees referencing this SE should:

1. Establish application-specific design timing requirement(s) for the system;
2. Perform application-specific analysis to budget the timing requirement(s) to associated components of the system architecture;
3. Validate the most restrictive timing requirement for each ALS platform component used within the system architecture has been bounded by the qualified performance envelope for that ALS platform component;
4. Perform verification testing that demonstrates the integrated ALS platform-based system meets each design timing requirement and performs as expected; and

5. Include appropriate technical specification surveillance requirements to confirm the equipment's digital response time characteristics, as applicable.

These plant-specific actions should ensure the ALS platform-based system meets its requirements in direct support of plant-specific and application-specific system response time design bases (see Section 4.2, Item 7).

When performing the application-specific analysis to budget the timing requirement(s) as depicted "ALS Topical Report" Figure 2.7-1, each response time performance requirement should be analyzed to address the following response time delay elements, as applicable:

1. The maximum as-built and as-configured Input Delay time for the Input Board;
2. The maximum time between consecutive accesses to the Input Board;
3. The maximum RAB transaction time to acquire the input data;
4. The maximum as-built and as-configured Logic Delay time for the Core Logic Board;
5. The maximum time between consecutive accesses to the Output Board;
6. The maximum RAB transaction time to provide the output data; and,
7. The maximum as-built and as-configured Output Delay time for the Output Board.

When performing the application-specific analysis to budget the timing requirement(s) when the ALS-601 Communications Board is in the safety signal path, each response time performance

requirement should be analyzed to address the following response time delay elements, as applicable:

1. The maximum as-built and as-configured Input Delay time for the Input Board;
2. The maximum time between consecutive accesses to the Input Board;
3. The maximum RAB transaction time to acquire the input data;
4. The maximum as-built and as-configured Logic Delay time for Core Logic Board #1;
5. The maximum time between consecutive accesses to the Communications Board #1;
6. The maximum RAB transaction time to provide the digital data for transmission;
7. The maximum as-built and as-configured Transmission Delay time for Communications Board #1;
8. The maximum time until the digital data transmission by Communications Board #1 contains the response time dependent data;
9. The maximum digital data transmission duration time, including a design basis error rate supported by the error rates observed during design and qualification testing;
10. The maximum as-built and as-configured Reception Delay time for Communications Board #2;
11. The maximum time between consecutive accesses to Communications Board #2;
12. The maximum RAB transaction time to acquire the received digital data;
13. The maximum as-built and as-configured Logic Delay time for Core Logic Board #2;
14. The maximum time between consecutive accesses to the Output Board;
15. The maximum RAB transaction time to provide the output data; and,
16. The maximum as-built and as-configured Output Delay time for the Output Board.

In addition to confirming each system-level design commitment timing requirement has been met, verification testing should also evaluate the test results against the expected minimum and maximum response times predicted for the equipment's performance to validate the response time analyses. This approach is consistent with ALS platform tests for the standardized circuit

boards. The design tests for the ALS platform standardized circuit boards document both a maximum response time acceptance criteria and an expected worst-case design response time. The demonstration that actual ALS platform-based system response time performance falls between the predicted minimum and maximum response times should provide objective evidence of the determinism of the ALS platform and its components.

3.4.2 Determinism

The review guidance of SRP Chapter 7, Appendix 7.1-C, Section 6.1, “Automatic Control,” identifies considerations that address digital computer-based systems for the evaluation of the automatic control capabilities of safety system command features. This review guidance advises the evaluation should confirm the system’s real time performance is deterministic and known. SRP BTP 7-21 discusses design practices for computer-based systems that should be avoided, and these practices include non-deterministic data communications, non-deterministic computations, interrupts, multitasking, dynamic scheduling, and event-driven design. SRP BTP 7-21 further states methods for controlling the associated risk to acceptable real time performance should be described when such practices are employed.

EPRI TR-107330 provides specifications and guidance intended to achieve a deterministic execution cycle with deterministic behavior that ensures an application and its constituent tasks will be completed within specified time limits. In particular, EPRI TR-107330, Section 4.4.1.3, “Program Flow Requirements,” specifies that, where scanning of the inputs and application program execution are performed in parallel, methods should assure the input scan and application program execution are completed each cycle. EPRI TR-107330 does not directly apply to the ALS platform, because the ALS platform is entirely FPGA-based and does not include a software executive or software programming. Regardless, the EPRI report provides specifications and guidance that promotes a continuous and essentially non-interruptible operating cycle as the preferred environment in which to execute safety functions and this is applicable to the ALS platform and architecture.

The following subsections describe the deterministic characteristics of the ALS platform and architecture and evaluate these characteristics using criteria applicable to the FPGA technology.

3.4.2.1 Deterministic and Known Real Time Performance (Deterministic Computation)

The discussion and evaluation in Section 3.4.1 address the establishment and confirmation of response time performance requirements for ALS platform-based systems so the real time performance is known. Furthermore, as described in Section 3.4.1, the application-specific analysis to budget real time requirement(s) to the response time performance of each component and data transaction is founded upon deterministic propagation delays, a deterministic board access time, and a deterministic frame time in accordance with the design of the ALS platform and architecture

The “ALS Topical Report” describes the deterministic nature of the ALS platform (see Reference 32, Sections 2.3 and 3.1). The ALS platform and architecture provide design features to ensure the ALS-102 Core Logic Board will perform its functions to completion within

the board access time and frame time. The board access time is the fixed interval allocated to exchange data with an individual board using the RAB protocol. The frame time is the interval between accessing each specific board so information will have been read once from all application input boards and written once to all application output boards. Although the ALS platform establishes a fixed board access time, other aspects—including the number times a board is accessed per frame, the number of boards accessed per frame, the sequence of board accesses per frame, and the frame time itself—are determined during the application-specific design phase. All of these design aspects establish the fixed interval for each safety function performed. The ALS platform RAB protocol ensures each RAB transaction occurs within its timing budget, and each ALS platform board that responds to RAB requests contains monitoring logic to ensure it continues to be successfully accessed. Therefore, the ALS platform provides design features to alert operators to the system's condition when the RAB transaction time, board access time, or frame time is not met. The ALS platform provides the capability to activate alarms when a failure to meet timing is detected. This capability can identify to operators when timing is not being met so operators can take corrective actions.

The NRC staff determined the ALS platform supports deterministic and known real time performance through deterministic computation, because the discussions and evaluation in Section 3.4.1 demonstrate the allocation of time delays to elements of the platform and architecture, and the ALS platform provides the capability to activate alarms to notify operators of failures to meet timing so operators can take corrective actions.

3.4.2.2 Deterministic Digital Communication for Safety Signals

The ALS platform limits the digital communications for safety signals to serial data transfers over the "RAB: Reliable ALS Bus" within each safety division. Each divisional RAB provides a redundant digital data exchange, which forms part of the overall safety signal path. A second bus, "TAB: Test ALS Bus," for each safety division is used for maintenance, diagnostics, and test data (see the separate evaluation of interdivisional communications under Section 3.7). The TAB cannot adversely affect the safety signal path. Each bus follows a master-slave protocol where an ALS-102 Core Logic Board is the bus master of the RAB. When connected, the Maintenance Workstation will act as the bus master of the TAB (see Reference 44, Section 5).

As part of the NRC staff's prior SE (see Reference 2, Enclosure 2, Section 3.1.1.5.5), the NRC staff reviewed the documentation that described the RAB and TAB protocol details and determined communications independence within an ALS platform-based system is maintained between these two separately controlled busses. The NRC staff previously concluded communication independence exists because: 1) the RAB segregates the operational safety signal path from the TAB that provides the maintenance and troubleshooting diagnostic signal path, 2) independent digital logic circuits in the form of separate finite state machines implement the bus logic, and 3) operation of the TAB does not affect operation of the RAB or other safety logic.

The ALS platform boards are connected using an application-specific backplane in each instrumentation rack, and the backplane contains copper signal traces that are the signal paths

for the RAB and TAB. These busses are based on the EIA-485 differential standard and each is half-duplex, which does not allow simultaneous data transmission and reception. Each half-duplex communication is controlled by its bus master to allow one and only one active bus transmitter at a given point in time. The serial communication protocol for each bus uses predefined messages of a fixed size to establish fixed and predictable bandwidth use and data transfer delays. The serial communication protocol for each bus also uses Cyclic Redundancy Checks (CRCs) to ensure the integrity of data transfers between boards. Each bus master (ALS-102 Core Logic Board or Maintenance Workstation) controls its serial data bus resource (RAB or TAB), which is shared among boards, so two boards cannot simultaneously access the same bus. Regardless, both busses may be simultaneously active, because the busses operate independently.

The bus master controls all bus access, and a slave only communicates when enabled by and upon a request from the bus master. Each slave board listens for broadcast messages, which do not require an acknowledgement. For other than broadcast messages, the slave has a fixed

time to respond to the master after the master makes a data exchange request with the slave board. At a fixed cycle the bus master repeats sequential bus transactions with each installed board where each transaction must complete within the protocol's fixed transaction time. This fixed transaction time is designed to be less than the fixed board access time. Although multiple transactions may be performed per frame with an individual board and multiple boards are accessed per frame, each transaction is specified to complete within the fixed board access time. The RAB protocol includes redundant communication paths and time for one retry within the fixed board access time to support reliable communication performance. The bus master will also perform one additional retry with a slave after an unsuccessful slave response. If this additional retry also fails, then the bus master will declare the slave board as failed. When a board is declared as failed, an alarm can be activated for operator notification and action. For the RAB communications, when a failed board is taken out of the cyclic communication sequence, this state of inactive RAB communications remains until intervention by an operator. This intervention would typically include the operator resetting the rack after completing a repair.

Each slave board can detect a communication failure on the RAB or TAB, and can isolate itself from further communications on the RAB until the communication failure is corrected. Each RAB slave implements a communication watchdog time-out and "HALT" function for RAB communications. This watchdog function detects a condition where the elapsed time since a successful access to the slave board exceeds a prescribed limit that has been defined to be common for all slave boards and applications. As such, this failure detection time is fixed and does not depend on the application-specific configuration. The prescribed limit for this failure detection is set to nominally two and one-half times the maximum frame time specified for the ALS platform (see Reference 44, Section 5.1.5), and this failure detection time corresponds to the RAB error resilience specification that restricts the number of error free RAB transactions between the RAB Master and the RAB Slave (see Reference 43, PR0721.6).

The NRC staff reviewed the "ALS Topical Report" description of safety function determinism, which is tied to the ALS platform architecture and internal communication protocol, and for internal communications determinism, the NRC staff determined the characteristics have not changed since the NRC staff's prior SE review in Reference 2. This prior SE applied criteria to

the internal digital data communications similar to that provided in the twenty points under DI&C-ISG-04 Staff Position 1 Interdivisional Communications, as applicable to the FPGA technology and ALS platform approach (see Section 3.7.2.1 herein). The prior SE determined the ALS platform provides deterministic point-to-point communications and error detection to preclude the use of invalid data in accordance with IEEE 7-4.3.2-2003 (see Reference 2, Enclosure 2, Section 3.1.1.5.5).

The NRC staff determined the ALS platform does not include non-deterministic data communications and the prior staff determination established an applicable precedent. The ALS platform communications description provided in the "ALS Topical Report" remains consistent with that previously described, evaluated and determined to meet the NRC staff's evaluation criteria governing deterministic communications.

3.4.2.3 Exclusion of Software-based System Characteristics

The ALS platform uses independent FPGAs which contain digital logic in the form of separate finite state machines to implement individual functions. The ALS platform neither implements a microprocessor nor embeds executable software. As such, the ALS platform does not use operating system or software executive, and the design approach inherently precludes the ALS platform from implementing software interrupts, multitasking, or dynamic scheduling.

The NRC staff determined the ALS platform does not include risks to real time performance that would otherwise be associated with the potential software programming practices of interrupts, multitasking, or dynamic scheduling. The operational characteristics that result from the ALS platform's design approach inherently preclude the ALS platform from implementing these programming practices.

3.4.2.4 Exclusion of an Event-Driven Design

The "ALS Topical Report" describes a cyclic sampling of inputs, processing, and refreshing of outputs. This logic processing sequence does not vary based on the context or timing of individual data transactions.

The NRC staff in part determined the ALS platform is not an event-driven design, because the sequence of processing logic is fixed, periodically repeats, and does not change as a result of either the context or timing of individual data transactions. The NRC staff further determined the ALS platform is not an event-driven design, because the evaluation of the internal communications against the points under DI&C-ISG-04 Staff Position 1, Interdivisional Communications, as applicable to the ALS platform's use of FPGA technology, confirmed the data communication protocols are deterministic.

3.4.2.5 Summary Staff Determination for Determinism

As discussed in the preceding subsections, the NRC staff determined the ALS platform supports meeting the criteria for deterministic performance contained within SRP Chapter 7, Appendix 7.1-C, Section 6.1, SRP BTP 7-21, and EPRI TR-107330, Section 4.4.1.3 when the plant-specific and application-specific logic conforms to ALS platform architecture described

within the “ALS Topical Report.” The NRC staff also determined the ALS platform does not introduce non-deterministic computations or a non-deterministic digital data communication protocol, because the ALS platform supports deterministic data communications and the FPGA logic does not implement a microprocessor or executable software.

Based on the preceding evaluation of the ALS platform and staff determinations, the NRC staff has identified a plant-specific action item to confirm the application specifications identify the board access sequence, frame time, and design features that activate alarms upon detection of a failure to meet timing requirements. The plant-specific action should also verify the application-specific logic does not introduce non-deterministic computations or non-deterministic digital data communications (see Section 4.2, Item 8).

3.4.3 Self-Diagnostics, Test and Calibration Capabilities

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

IEEE Std 603-1991 Clause 5.7 references IEEE Std 338-1987, “Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems” for the testing of Class 1E systems, and RG 1.118, “Periodic Testing of Electric Power and Protection Systems,” endorses with exceptions IEEE Std 338-1987 as a method acceptable to the NRC staff for meeting the Commission's regulations with respect to periodic testing of electric power and protection systems. Furthermore, RG 1.22, ““Periodic Testing of Protection System Actuation Functions,” describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.

SRP, Chapter 7, Appendix 7.1-C, Section 5.7, "Capability for Test and Calibration," provides acceptance criteria for IEEE Std 603-1991, Clause 5.7. Capability should be provided to permit testing during power operation and when this capability is achieved by overlapping tests, the test scheme must ensure the tests do, in fact, overlap from one test segment to another. Section 5.7 further states test procedures requiring disconnection of wires, installation of jumpers, or other similar modifications to installed equipment are not acceptable test procedures for use during power operation. Section 5.7 further states for digital computer based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup.

SRP BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” states automatic diagnostics and self-test features should preserve channel independence, maintain system integrity, and meet the single-failure criterion during testing. Additionally, the benefits of diagnostics and self-test features should not be compromised by additional complexity that may

result from the implementation of diagnostics and self-test features. In particular, the scope and extent of interfaces between safety software and diagnostic software such as self-test routines should be designed to minimize the complexity of the integrated software. SRP BTP 7-17 only partially applies to the ALS platform, because the ALS platform is entirely FPGA-based and does not include a software executive or software programming. The ALS platform diagnostic and self-test FPGA logic is separate and independent of the FPGA safety function logic, thus the programming of the safety function FPGA logic is not made more complex by the inclusion of the diagnostic and self-test FPGA logic. Regardless, SRP BTP 7-17 provides other guidance directly applicable to the ALS platform and architecture.

EPRI TR-107330 provides guidance and requirements applicable to PLC-based system's diagnostics and test capability to help ensure the combination of self-diagnostics and surveillance testing will detect all failures that could prevent a PLC from performing its intended safety function. The range of conditions for which diagnostics or test capabilities are to be provided includes processor stall, executive program error, application program error, variable memory error, module communications error, module loss of configuration, excess scan time detection, application not executing, and field device (e.g., sensor, actuator) degradation or fault. The means of detection include watchdog timer, checksum for firmware and program integrity, read/write memory tests, communications monitoring, configuration validation, heartbeat, and self-diagnostics or surveillance test support features. EPRI TR-107330 identifies diagnostics that are executed upon power-up and diagnostics that run continuously thereafter. EPRI TR-107330 only partially applies to the ALS platform, because the ALS platform is entirely FPGA-based and does not include a software executive or software programming. Regardless, the concepts provided through EPRI TR-107330's specifications and guidance to detect all failures that could prevent performance of a safety function through the combination of self-diagnostics and surveillance testing are applicable to the ALS platform and architecture.

The regulation 10 CFR Part 50, Appendix A, GDC 21, "Protection system reliability and testability," requires, in part, the protection system be designed for in-service testability commensurate with the safety functions to be performed. It also requires a design that permits periodic testing of its function when the reactor is in operation, including the capability to test channels independently to determine failures and losses of redundancy that may have occurred.

The regulation 10 CFR 50.36(c)(3), "Technical specifications," states surveillance requirements are requirements relating to test, calibration, or inspection to assure the necessary quality of systems and components is maintained, the facility operation will be within safety limits, and the limiting conditions for operation will be met. RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," which endorses IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," states the protection system must be capable of accomplishing the required protective function in the presence of any single detectable failure concurrent with all identifiable, but non-detectable, failures. Consequently, self-testing and periodic testing are important elements in the design's ability to meet the single-failure criterion. SRP BTP 7-17 describes additional considerations in the evaluation of test provisions in digital computer based systems.

The “ALS Topical Report” describes the diagnostics and maintenance features provided by ALS platform and directly addresses IEEE Std 603-1991 Clause 5.7 (see Reference 32, Sections 3 and 12.1.8). The ALS platform supports test and calibration from field input to instrument output without lifting of leads or installation of jumpers, because design features for maintenance allow an individual instrument input or output channel to be disabled, placed into bypass or placed into calibration, and the field terminal block design allows the injection of test signals without lifting leads to field wiring. With this approach, the test signal is injected at the field terminal blocks and then the ALS platform processes it using the actual safety signal path. This manually initiated test method excludes the sensor wiring to the terminal block and includes the instrument signal and data communication path from the terminal block throughout the

remainder of the instrument. As discussed in Section 3.4.1 and 3.4.2, the ALS platform architecture and communication protocols include design features to verify continued logic processing and the correctness of data transfers so either lockup or data errors are detectable failures.

Additional periodic surveillances, which are beyond this SE scope, may be required to comply with IEEE Std 603-1991 Clause 5.7. Additional periodic surveillances should be provided when the ALS platform injection point is not considered to be as close to the sensor as practical or when the ALS platform output does not extend to the actuating device. These additional periodic surveillances could include the confirmation of other continuous or manually initiated tests that overlap with the ALS platform self-diagnostics. Overlapping tests could include verification of the integrity of sensor wiring and sensor itself, or involve system-level verification of actuations.

The “ALS Platform Requirements Specification” includes a variety of proprietary specifications for power-up testing and to ensure the correct instrument configuration before indicating an operable status (see Reference 43, PR0720.3.2, PR0721.3.9, PR0722.10, and PR0723.10). The “ALS Platform Requirements Specification” includes proprietary specifications to: 1) ensure each test necessary to determine the integrity of an input or output channel has been performed before a slave board provides the channel’s data to the ALS-102 Core Logic Board, 2) perform sufficient built-in self test functionality to preclude unreported failures in the safety signal path, and 3) ensure built-in self testing does not adversely affect either the equipment’s ability to meet response time requirements or instrument outputs (see Reference 43, PR0723.11, PR0735.1, PR0735.2, and PR0735.3). The “ALS Platform Requirements Specification” notes input and output channel specific failure detection is defined in each board-specific requirement specification (References 55, 61, 67, 73, 79, 85, and 91). These board-specific specifications require non-passing self-test results to persist before a failure will be declared, so a temporary external environmental condition, such as an extreme EMI transient, will not result in nuisance failure reporting. This design feature is identified via an Intermediate Error status. During an Intermediate Error condition, the platform logic holds the data associated with the suspect channel at the most recent value before the platform logic had identified the Intermediate Error condition. The ALS platform does not report a channel as failed nor take a fail-safe action for the Intermediate Error condition. However, the Intermediate Error status is available for application-specific action, if needed. The “ALS Platform Requirements Specification” also includes functional requirements for calibration, diagnostics, maintenance, and test features that support field calibration without board removal and in a manner that does not affect other

channels or features that are not undergoing calibration activities (see Reference 43, Section 10). The “ALS Platform Specification” includes proprietary specifications governing the ALS platform’s detection of single-event upsets to FPGA logic (Reference 44, Section 2.8.1) or any SRAM used within an FPGA (Reference 44, Section 3.3.7.8). The “ALS Platform Specification” identifies the RAB communication protocol’s capability to confirm correct operation of the safety signal data path and also identifies the platform’s behavior in response to detected failures (Reference 44, Section 5.3).

The ALS platform provides serial data channels to make the operational status of an ALS platform-based system, including diagnostic results, available to plant personnel (see Reference 32, Sections 2.2.1.3 and 2.3.2). As discussed in Section 3.7, the ALS-102 Core Logic Board’s TxB1 and TxB2 communication channels provide the capability of continuous unidirectional serial data communications. These communication channels may continuously provide non-invasive built-in self test results to plant personnel. Section 3.7 also discusses the TAB connection to the Maintenance Workstation, which requires the equipment to be in an inoperable status (i.e., bypassed). In addition to providing access to the continuously running non-invasive built-in self test results, plant personnel may use the TAB to perform invasive self-tests or other maintenance activities that provide additional equipment performance information. The “ALS Platform Specification” describes maintenance capabilities that support periodic surveillance testing, analog channel calibration, set point modification and general system diagnostics (Reference 44, Section 6).

The “ALS Topical Report” provides a high level description of the ALS platform approach to diagnostics and fault indications, and this description includes a generic depiction of the verification approach for the safety signal path within an ALS platform-based instrument (see Reference 32, Section 3.1 and its Figure 3.1-1). The “ALS Topical Report” states some of the test capabilities, such as from a field Input to an ALS input board and from an ALS output board to a field output, are determined by the specific application and interfacing equipment (e.g., sensor or actuator, respectively) (see Reference 32, Section 3.1.1.2). The “ALS Topical Report” also states when failures are detected, their effects are mitigated and managed in accordance with application specifications, and acknowledges some application-specific diagnostics may also be required (see Reference 32, Sections 3.1.1.2 and 3.1.2). The “ALS Topical Report” further states application-specific surveillance testing requirements are determined during application development and technical specification changes are application-specific, and therefore, outside of the scope of the “ALS Topical Report” (see Reference 32, Sections 3.2 and 12.1.1).

The NRC staff reviewed the “ALS Topical Report,” “ALS Platform Requirements Specification,” “ALS Platform Specification” and individual standardized circuit board specifications to evaluate the diagnostic, self-test and manually initiated test and calibration capabilities provided in the ALS platform. However, the NRC staff review could neither evaluate whether the test and calibration approach duplicates, as closely as practicable, performance of the safety function nor whether the combination of channel specific testing, standardized platform testing, and licensee specific surveillance requirements provides overlapping testing, because these considerations are application-specific. Likewise, the NRC staff review could not address application-specific considerations necessary to confirm channel independence is preserved,

system integrity is maintained, and the single-failure criterion continues to be met during testing, because these considerations are in part dependent on the application-specific functionality and channel, division, and voting logic arrangement. These limitations are consistent with the "ALS Topical Report" scope, which states specific system-level failure modes, methods of detection, and system responses are expected to be documented as application-specific and notes an Application Design Specification will be provided to provide the DI&C-ISG-06 information

content for the topics of "System Integrity" and "Test & Calibration" (Reference 32, Sections 12.1.6 and 12.7).

Despite these limitations the NRC staff determined the ALS platform supports meeting the applicable provisions of IEEE Std 603-1991, Clause 5.7, RG 1.22, and RG 1.118. This determination is based on the NRC staff's review of the information provided in the "ALS Topical Report," "ALS Platform Requirements Specification," "ALS Platform Specification," and individual standardized circuit board specifications, because the design features, as described, provide the following capabilities: 1) test and calibration while retaining the equipment's ability to accomplish its safety function, 2) support of compensatory actions, such as tripping or bypassing individual functions per channel, when technical specification limiting conditions for operation are not met, and 3) continuous indication of these compensatory actions in the control room.

In consideration of the preceding limitations, the NRC staff determined plant-specific action items are required. For each safety function, plant-specific actions should demonstrate the application-specific use of ALS platform diagnostic, self test, and manually initiated test and calibration features are sufficient to verify the operational integrity of all logic components (i.e., all relays and contacts, trip units, solid state logic elements, etc.) of a logic circuit, from as close to the sensor as practicable up to but not including the actuated device, with sufficient overlap.

When a ALS platform built-in self test feature is the justification for eliminating an existing surveillances or performing a less frequent surveillance, then the applicant or licensee should demonstrate how the ALS platform built-in self test features test the components and safety functions and further demonstrate the built-in self testing provides equivalent assurance to the surveillances performed on the equipment being replaced.

Plant-specific actions should also confirm the plant's surveillance procedures will verify the built-in self tests results and ensure these tests continue to operate, as referenced by surveillance requirements provided in the plant's technical specifications and as applicable.

Plant-specific actions should also confirm the plant's installation does not exhibit unjustified Intermediate Errors without reported failures that could adversely affect a safety function.

Plant-specific actions should demonstrate the application-specific diagnostic, self test, and manually initiated test and calibration features identified within the plant's maintenance and surveillance procedures will not adversely affect channel independence, system integrity, or the system's ability to meet the single-failure criterion during testing, as permitted by the plant's

administrative controls and in consideration of the functionality per channel and the overall channel, division, and voting logic arrangement of the system.

Plant-specific actions should demonstrate the relationship between the application-specific diagnostic, self test, and manually initiated test and calibration features provided by the ALS

platform and the conformance to the NRC staff positions in RGs 1.22 and 1.118 (see Section 4.2, Item 9).

3.5 Failure Mode and Effects Analysis

RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," describes a method acceptable to the NRC staff for meeting the NRC's regulations as they apply to the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems. RG 1.53's endorses IEEE Std 379-2000, and IEEE Std 379-2000, Clause 5.5 identifies Failure Mode and Effects Analysis (FMEA) as a method to address common-cause failures when performing analysis to demonstrate the single-failure criterion has been met. Although no specific regulatory guidance on the format, complexity or conclusions of the FMEA exists, the FMEA should identify potential failure modes within a system to determine the effects of these failures on the system. The expectation is each potential failure mode should be identified, and its effects should be determined. The FMEA should demonstrate single-failures, including those with the potential to cause a nonsafety system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot also adversely affect the associated protection functions.

The "ALS Topical Report" limits the scope of its FMEA to an FMEA that is individually applicable to each standardized circuit board, and this scope does not represent a system to which the potential effects of failures can be analyzed. Therefore, in lieu of providing a system-level analysis, the ALS platform FMEA documentation forms a portion of a board's hardware design specification. This ALS platform documentation is identified with the ALS platform document prefix of "6002" and the FMEA document suffix of "xxx12" in each board-specific docketed information table under Section 3.1.4.

Table 3.5-1 groups the ALS platform FMEA documentation into one table, and these documents contain the results of the FMEA for each board. Within these documents, the manufacturer described the set of board-level analyses performed to identify each board's functions and the failure paths associated with these functions. After postulating hardware failures to the board, the manufacturer also performed and described a board-level FMEA to document whether ALS design features, including built-in self-test, would detect the hardware failure, whether the failure would affect the operability of the board's functions, and whether either the factory board-level acceptance testing or release testing would detect the hardware failure.

Table 3.5-1 Docketed ALS Platform FMEA and Reliability Information

Document ID	Title	Reference
6002-30212	ALS-302 FPA, FMEA, and Reliability Analysis	62
6002-31112	ALS-311 FPA, FMEA, and Reliability Analysis	68
6002-32112	ALS-321 FPA, FMEA, and Reliability Analysis	74

6002-40212	ALS-402 FPA, FMEA, and Reliability Analysis	80
6002-42112	ALS-421 FPA, FMEA, and Reliability Analysis	86
6002-60112	ALS-601 FPA, FMEA, and Reliability Analysis	92
6002-10212	ALS-102 FPA, FMEA, and Reliability Analysis	56

The “ALS Topical Report” establishes each application-specific ALS platform-based system will have a system-level FMEA, because the set of individual board-level analyses is not equivalent to a system-level analysis. The “ALS Topical Report” further states determination of the reliability of an ALS platform-based safety system requires an application-specific system-level FMEA. As described, the combination of the ALS platform board-specific FMEAs and the system-level FMEA are required to demonstrate there are neither any undetectable failures nor cascading failures that can contribute to a violation of the single failure criterion. Each ALS platform board-specific FMEA provides analyses of potential hardware or programming failure modes applicable to the board level component, and as such, applicants and licensees may use this information to support an application-specific system-level FMEA (see Reference 32, Sections 7.1 and 12.1.1). These limitations are consistent with the “ALS Topical Report” scope, which identifies application-specific FMEA document(s) that will address the topic of “FMEA” to meet the information content identified in DI&C-ISG-06 Section D.9.4.2.1.1 (see Reference 32, Section 12.7).

Furthermore, the “ALS Platform Specification” is consistent with the reliance upon a system-level FMEA, because it emphasizes the potential to continue to perform all designed functions when redundancy is designed into the system. The “ALS Platform Specification” also states the overall system response to failures and the classification of failures for a system will be application-specific and addressed when designing the application-specific system (Reference 44, Section 2.3.1).

The NRC staff reviewed the FMEA provided in the documents identified in Table 3.5-1 in consideration of the limited scope of the ALS platform FMEA as described within the “ALS Topical Report” and the reliance upon an application-specific system functionality and architecture as described within the “ALS Platform Specification.” These documents identify each component failure that affects the principle functions of the board and may not be detected and annunciated by ALS platform self-diagnostic features.

The NRC staff determined the manufacturer has performed a FMEA to support future evaluations against the single-failure criterion for ALS platform-based systems, because the FMEAs identify board functions and the failure paths associated with these functions, postulate hardware failures, analyze the delectability of hardware failures, and further analyze the effect of hardware failures on the continued operability of the board and its functions. This staff determination is further based on the ability to design an application-specific ALS platform-based system with sufficient diversity in redundant components to ensure the continued performance of safety functions as discussed in Section 3.9.

In consideration of the preceding limitations, the NRC staff determined plant-specific action items are required. Plant-specific actions should include a system-level FMEA to demonstrate the application-specific use of the ALS platform identifies each potential failure mode and

determines the effects of each. The FMEA should demonstrate single-failures, including those with the potential to cause a nonsafety system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions (see Section 4.2, Item 10).

3.6 Reliability and Availability Analysis

IEEE Std 603-1991 Clause 4.9 requires the identification of the methods to determine the reliability of the safety system design is appropriate for each such design, and the identification of the methods to verify reliability goals imposed on the system design have been met. However, as discussed within RG 1.152, Criteria for Use of Computers In Safety Systems of Nuclear Power Plants," and DI&C-ISG-06, the NRC's acceptance of the reliability of digital I&C systems is based on deterministic criteria for both hardware and programming, and the NRC does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for reliability of digital computers used in safety systems. Nevertheless, in Clause 5.15, IEEE Std 603-1991 further requires performance of an appropriate design analysis to confirm reliability goals have been achieved for each system with an established quantitative or qualitative reliability goal. IEEE Std 603-1991 Clause 6.7 requires the safety system shall remain capable of accomplishing its safety function while continuing to meet the single-failure criterion when sense and command features are in maintenance bypass. Similarly, IEEE Std 603-1991 Clause 7.5 requires the remaining redundant portions should provide acceptable reliability when one portion of a redundant safety system's execute features is placed into a maintenance bypass condition. DI&C-ISG-06 states the reliability and availability analysis should justify the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed with further consideration of the effect of possible failures and the design features provided to prevent or limit their effects.

Although the "ALS Platform Requirements Specification" includes a reliability specification for Mean Time Between Failures (MTBF) for individual ALS platform standardized circuit boards to be calculated using MIL-HDBK-217F (see Reference 43, PR1101), the manufacturer supported the performance of its reliability predictions by an independent second party who used data and a failure rate prediction tool from the Reliability Information Analysis Center, 217PLUS™. The manufacturer describes the use of the tool in each document identified in Table 3.5-1. The manufacturer states this tool applies similar methods to MIL-HDBK-217F but with modern data and failure rate models. The manufacturer also states experience using 217PLUS™ has shown its predictions eliminate calculation conservatism and are closer to field experience data. The reliability analysis estimates the failure rate for a standardized circuit board based on the failure data associated with its installed components, and the analysis assumes continuous board operation. The manufacturer based its ALS platform reliability predictions on an environment setting within the 217PLUS™, which the manufacturer selected to most closely match the expected operating environment for the ALS platform. Each board's reliability analysis provides quantitative predictions of Failures per Million operating Hours (FPMH) and MTBF at a specified temperature, which is representative of the nominal operating environmental temperature. Additionally, each board's analysis predicts the temperature effects on FPMH in fixed increments up to a more severe temperature, which corresponds to the maximum

specified operating temperature. The ALS platform analysis uses a conservative assumption that any failure on the board results in failure of the module. Section 4.3.2 of each Table 3.5-1 reference describes the application of the 217PLUS™ to the ALS platform. The "ALS Topical Report" states each ALS platform standardized circuit board will have a MTBF calculation documented in the board's hardware design specification to support an application-specific analysis to demonstrate the overall reliability and availability goals are met (see Reference 32, Sections 7.2 and 12.1.16). Each Table 3.5-1 reference is considered part of the board's hardware design specification because each reference provides the calculated MTBF values for its ALS platform board in Sections 2.0 and 5.4. At the maximum temperature evaluated , the lowest predicted MTBF (i.e., least reliable) of the standardized circuit boards is greater than the specified MTBF for an ALS platform standardized circuit board (i.e., sufficiently reliable to meet the specification).

The NRC staff reviewed the reliability analysis summary, approach, and results provided in the Table 3.5-1 references and confirmed these analyses identify the method to predict the reliability of each board for installed hardware component failures. The reliability analyses clarify modeling assumptions and expectations associated with the predicted FPMHs and MTBFs along with their use in modeling the expected reliability of ALS-based systems. The NRC staff agrees use of the 217PLUS™ represents a state-of-the-practice appropriate for the ALS platform. The NRC staff could not determine full compliance to IEEE Std 603-1991 Clauses 4.9, 5.15, 6.7 and 7.5, because these requirements are based on system-level reliability, which are established on a plant-specific and application-specific basis, and the analysis provided may not conform to the methods by which the applicant or licensee determines the reliability of its safety systems.

Reliability models applicable to traditional executable software need not be applied to the ALS platform, because the ALS platform limits its FPGA designs to exclude embedding of processing and executable software. Nevertheless, failure modes and the potential for failures other than those associated with hardware reliability of components, which would include faults introduced earlier in the life cycle, should be considered and at least qualitatively addressed by applicants and licensees. As discussed in Section 3.11.2.3.2, for example, the design and development of the ALS platform's FPGAs rely on software based tools, which could affect the reliability of the platform. To address this consideration, the "ALS Diversity Analysis" includes a qualitative discussion of potential sources of faults introduced earlier in the life-cycle and identifies methods for use throughout the life-cycle of an ALS platform-based project to address sources of potential unreliability (See Reference 47). ALS platform methods address the development of its FPGA logic programs, including the reliance upon software-based tools, design specification and implementation activities, IV&V activities, and configuration management activities.

In consideration of the preceding limitations, the NRC staff determined plant-specific actions are required. Plant-specific actions should include a deterministic system-level evaluation to determine the degree of redundancy, diversity, testability, and quality provided in an ALS platform-based safety system is commensurate with the safety functions that must be performed. This plant-specific action should consider the effect of possible failures, system-level design features provided to prevent or limit the failures' effects, and any application-specific inclusion of a maintenance bypass to support plant operations. As a plant-specific

action, the applicant or licensee should confirm its reliability analysis method accommodates the ALS platform reliability method or the ALS platform method provides it an equivalent level of assurance. Plant-specific actions should also confirm a resultant ALS platform-based system continues to meet any applicable reliability goals that the plant has established for the system (see Section 4.2, Item 11).

3.7 Digital Data Communication Independence and Isolation

The NRC staff positions within DI&C-ISG-04 establish a means to ensure independence among redundant safety channels while permitting some degree of interconnection and shared resources among independent channels. DI&C-ISG-04 is based on 1) the 10 CFR 50.55a(h) inclusion of IEEE Std 603-1991, and 2) the endorsement of IEEE Std 7-4.3.2-2003 within RG 1.152. IEEE Std 603-1991 requires, among other things, independence among redundant safety channels and redundant safety systems to be independent of one another. RG 1.152 endorses IEEE Std 7-4.3.2-2003 as acceptable for meeting the NRC's regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants. Clause 5.6 of IEEE Std 7-4.3.2-2003 addresses digital communication independence for safety systems.

The following subsections evaluate the ability of the ALS platform to meet safety system digital data communication evaluation criteria. The "ALS Topical Report" (Reference 32) identifies three methods that support safety system digital data communication to differing degrees and these methods are:

1) ALS-102 Core Logic Board – two transmit-only interfaces (TxB1 and TxB2);
2) Test ALS Bus (TAB) – one bidirectional (transmit and receive) interface; and,
3) ALS-601 Communication Board – eight unidirectional (transmit-only or receive-only) interfaces.

The following subsections contain the NRC staff's evaluation of each available method against the NRC staff positions and points within DI&C-ISG-04 with further consideration that the "ALS Topical Report" scope does not propose to meet all staff positions and points via ALS platform components. For example, the ALS platform components do not include the qualified isolation devices required between Class 1E and Non-Class 1E equipment, and the "ALS Topical Report" scope does not include use of the ALS platform within command prioritization applications. The exclusions to staff positions and points are documented in the corresponding evaluations.

3.7.1 ALS Platform Digital Data Communications

The DI&C-ISG-04 evaluation criteria for safety-safety interdivisional communications are the same as applies to safety-nonsafety communications. Nevertheless, the "ALS Topical Report" targets its methods for digital data communication to different types of communications between safety and nonsafety equipment and among independent safety channels. The ALS-102 Core Logic Board and the Test ALS Bus (TAB) methods target communication with nonsafety equipment while the ALS-601 Communication Board targets interdivisional communication among redundant safety channels. The following subsections first provide an overview of these

methods and then evaluate each method against applicable staff positions and points within DI&C-ISG-04.

3.7.1.1 With Nonsafety Equipment

The ALS-102 Core Logic Board method targets transmit-only communication to computing, display, and recording devices while the Test ALS Bus (TAB) method targets bidirectional communication with a maintenance workstation. The “ALS Topical Report” establishes the interfacing equipment may be nonsafety. Therefore, the NRC staff evaluated these interfaces as safety-nonsafety because communication with nonsafety equipment establishes more conservative criteria.

3.7.1.1.1 Via TxB1 and TxB2 on the ALS-102 Core Logic Board

The ALS-102 Core Logic Board provides two transmit-only interfaces, which are referred to as TxB1 and TxB2. The FPGA device on the ALS-102 Core Logic Board will include the logic that performs safety functions and the logic that supports communication via TxB1 and TxB2. Use of the ALS platform requires application specifications for each system that enables either TxB1 or TxB2 because the programming of the ALS-102 Core Logic Board’s FPGA and the digital data communication content and format for TxB1 or TxB2 are application-specific.

3.7.1.1.2 Via TAB and Instrument Backplane with Each Circuit Board

Each ALS standardized circuit board shares a bidirectional interface over the instrument backplane, which is referred to as the Test ALS Bus (TAB). The FPGA device on each ALS standardized circuit board will include the logic that performs safety functions and the logic that supports communication via the TAB. Available TAB interactions with each standardized circuit board are predefined except for the ALS-102 Core Logic Board, because only the ALS-102 Core Logic Board requires application-specific logic programming. Use of the ALS platform requires application specifications for the ALS-102 Core Logic Board’s FPGA to identify its application-specific TAB interactions.

3.7.1.2 Among Safety Divisions or with Safety Equipment

The ALS-601 Communication Board provides eight unidirectional interfaces that can be independently configured as transmit-only or receive-only. The FPGA device on the ALS-601 Communication Board will include separate logic resources to independently support the communication through each interface. The “ALS Topical Report” scope describes application of the ALS-601 Communication Board for interdivisional communications as being limited to a communication processor for sharing (i.e., transmitting and receiving) individual channel trip votes among redundant safety channels to support a coincidence voting application. In this application the ALS-601 Communication Board provides vital communication to support the safety signal path, but its logic does not implement safety functions. Use of the ALS platform for a coincidence voting application also requires an ALS-102 Core Logic Board to perform coincidence voting safety functions, which would be contained in the board’s application-specific FPGA logic. Such use of the ALS platform also requires application specifications for the ALS-102 Core Logic Board’s FPGA to identify the digital data communication content and

format for each enabled interface on the ALS-601 Communication Board, because the functionality of these interfaces is application-specific. The “ALS Topical Report” establishes the interfacing equipment may be either intradivisional or interdivisional. Therefore, the NRC staff evaluated these interfaces as interdivisional, because interdivisional communication establishes more conservative criteria.

3.7.2 Staff Guidance in Digital I&C-ISG-04

DI&C-ISG-04 contains three staff positions to address communication issues, which are: 1) Interdivisional Communications, 2) Command Prioritization, and 3) Multidivisional Control and Display Stations. The “ALS Topical Report” contains the manufacturer’s assessment of conformance to these points (see Reference 32, Sections 5 and 12.3).

Some of the points under the DI&C-ISG-04 staff positions are implementation-specific and worded primarily with consideration of microprocessor-based systems. Still other points are application-specific and cannot be fully evaluated within the scope of the “ALS Topical Report.” Regardless, the following subsections provide an evaluation of each ALS platform communication method against the applicable points for that position. These evaluations address implementation-specific points in consideration of the ALS platform’s FPGA-based logic processing to determine the degree that the platform’s approach provides equivalent assurance that the digital data communications do not adversely affect the operability of safety functions. For application-specific points, appropriate plant-specific action items are provided (see Section 4.2, Items 12, 13, 14, 15, and 16).

3.7.2.1 Staff Position 1, Points 1 through 20 – Interdivisional Communications

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

3.7.2.1.1 Point 1

Point 1 establishes accomplishment of a safety channel's safety function should not depend on information or resources outside of the safety division while recognizing performance of voting logic requires the receipt of inputs from multiple safety divisions.

The TxB1 and TxB2 interfaces on the ALS-102 Core Logic Board meet Point 1 because both are transmit-only interfaces. Therefore, neither of these interfaces can receive inputs from outside of the safety division and no dependency on data from these interfaces can be established.

The TAB interface supports meeting Point 1 because the ALS platform contains design features and provisions to establish and indicate the equipment has been bypassed when this interface is active, whereby the bypassed equipment would no longer be relied upon to perform its safety function. Furthermore, the “ALS Topical Report” describes an additional application-specific

provision that allows the installation of a physical hardware disconnection of this interface when it is used with either a nonsafety or multidivisional maintenance workstation. This additional provision would not be necessary to meet Point 1 when this interface is used with a safety maintenance workstation that is contained within the same division and the safety maintenance workstation is independent of resources outside of the safety division.

The ALS-601 Communication Board interfaces support meeting Point 1 because the "ALS Topical Report" limits its intended use to vote sharing among multiple safety divisions when an ALS-601 communication interface is configured to receive. In coincidence voting applications, the separate ALS-102 Core Logic Boards in each trip channel and in each coincidence voter should have application-specific FPGA logic specifications to identify the digital data communication content and format that govern the interdivisional communications. When an application uses the ALS-601 Communication Board for interdivisional communications, its companion ALS-102 Core Logic Board's application specifications should demonstrate Point 1 is met.

The NRC staff determined the ALS platform components support meeting Point 1 because the components can be arranged to preclude dependence on information or resources outside of the safety division. The NRC staff further determined plant-specific actions are necessary to ensure the ALS platform components are applied to produce safety equipment that is independent of information and resources outside of its safety division because each plant application defines the signal connections, data exchanges and safety functions of the equipment (see Section 4.2, Items 13 and 14).

3.7.2.1.2 Point 2

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

The TxB1 and TxB2 are transmit-only interfaces. The ALS-102 Core Logic Board has been developed as safety-related and the FPGA logic on this board is application-specific. The TxB1 and TxB2 interfaces on the ALS-102 Core Logic Board support meeting Point 2 when the application-specific ALS-102 Core Logic Board FPGA logic is developed as safety-related and when qualified safety-related isolation devices are used.

The TAB interface supports meeting Point 2 under the following conditions:

- When the application requires a qualified physical hardware disconnection (e.g., a Class 1E switch, disconnection of cable, etc.) of the TAB during system operability; and,

- When qualified safety-related isolation (i.e., a Class 1E isolating device that is part of the safety-related system) is used to isolate nonsafety or multidivisional maintenance workstations.

These two conditions are sufficient, because all ALS standardized circuit boards have been developed as safety-related, and part of their standardized functionality establishes and indicates the equipment has been bypassed when the TAB interface is active.

The TAB interface also supports meeting Point 2 without either employing a hardware disconnection of the TAB from the maintenance workstation or including isolation devices between the equipment and the maintenance workstation when the application uses a safety-related maintenance workstation that is contained within the same division. This provision is acceptable, because all division components will have been developed as safety-related, and further because the ALS platform standardized functionality includes provisions to indicate a division has been bypassed while its TAB interface remains active.

The ALS-601 Communication Board interfaces support meeting Point 2 when qualified safety-related isolation devices are used for interdivisional or safety-nonsafety communications, because the ALS-601 Communication Board has been developed as safety-related.

The NRC staff determined the ALS platform components support meeting Point 2 because the ALS platform uses internal safety resources to protect safety functions from being adversely influenced by resources, signals and information that originate from outside a safety division. The NRC staff further determined plant-specific actions are necessary to ensure the ALS platform components are applied to prevent adverse influence by resources, signals and information that originate from outside any specific safety division by confirming installation of the safety-related qualified devices for interdivisional and safety-nonsafety interfaces, and confirming the standardized bypass detection and indication logic has been applied. This determination is based on the plant-specific application defines the signal connections, interdivisional interfaces, safety-nonsafety interfaces, and safety functions associated with each safety division (see Section 4.2, Items 1, 12, 13, and 14).

3.7.2.1.3 Point 3

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

The “ALS Topical Report” states the ALS platform design is kept as simple as possible and its uses will include only functions related to the safety functions (see Reference 32, Table 5.4-1,

DI&C-ISG-04 Item 3). Through this approach the “ALS Topical Report” commits to only use TxB1 and TxB2 on the ALS-102 Core Logic Board, the TAB, and the ALS-601 Communication Board to support or enhance a safety function. The “ALS Topical Report” does not provide a definition for “simple” nor justify the level of system/programming complexity with or without inclusion of the communication functions, because its scope is limited to platform components.

Regardless, application specifications could include and justify digital data communication to support or enhance the performance of a safety function, such as: 1) sending data to a nonsafety plant process computer or transient event recorder, which is supported by TxB1 and TxB2, 2) bidirectional exchanges with a maintenance workstation, which is supported by the TAB, and 3) interdivisional communication for vote sharing, which is supported by and the ALS-601 Communication Board. The ALS platform supports these types of digital data communication, which may be required and justified by individual application specifications.

Each ALS standardized circuit board and its FPGA programming are developed in accordance with a common documented set of processes to govern their specification, implementation, V&V, and testing. These processes have been developed to meet requirements for functional reliability and design requirements for computers used in the safety systems of nuclear power plants. When FPGA programming implements individual specifications, the ALS platform programming process generates individual logic circuits for each specification. The logical behavior of the resulting circuits is autonomous and the functions performed by one logic circuit do not take resources away from any other logic circuit. This behavior differs from microprocessor-based programming where memory and processor resources are shared among individually developed software programs. Therefore, the NRC staff determined the addition of communication functions should not significantly increase the likelihood of program specification or implementation errors when the same high quality process is applied for all FPGA programming requirements included within the ALS platform because FPGA programming results in autonomous logic circuits and generation of specification or programming errors primarily results from process quality rather than the function being specified and programmed. Nevertheless, conformance to portions of Point 3 are plant-specific because the required safety functions to be enhanced or supported by communication features and data are application-specific and programmed into the ALS-102 Core Logic Board's FPGA based on application specifications and development efforts.

The safety FPGA on the ALS-102 Core Logic Board supports safety functions and the TxB1 and TxB2 interfaces. These interfaces target safety-nonsafety communications that are application-specific. The TxB1 and TxB2 interfaces on the ALS-102 Core Logic Board meet Point 3 with respect to receiving communication from outside a safety division, because both are transmit-only interfaces that do not require handshaking. Therefore, neither can be used to receive inputs from outside of the safety division. FPGA logic resources that support this interface do not take resources away from logic circuits that perform safety functions, and inclusion of TxB1 and TxB2 on the ALS-102 Core Logic Board allows this interface to be serviced without impacting the safety signal path provided via the RAB. Nevertheless, a plant-specific action is necessary to ensure application specifications adequately justify the use of the TxB1 and TxB2 to meet Point 3's exclusion of nonsafety functions within safety components regarding any

significant increase in errors that could result from increased complexity of the ALS-102 Core Logic Board' programming.

The safety FPGA on each standardized circuit board supports safety functions and the TAB interface, and this interface supports bidirectional safety-nonsafety communication that is application-specific and requires request/response handshaking. The TAB interface supports meeting Point 3 with respect to receiving communication from outside a safety division, because

the ALS platform includes provisions for a physical hardware disconnection. Standardized functionality indicates equipment has been bypassed while this interface remains active. This standardized functionality has been developed as safety-related. FPGA logic resources that support this interface do not take resources away from logic circuits that perform safety functions, and inclusion of the TAB on each standardized circuit board allows this interface to be serviced without impacting the safety signal path provided via the RAB. Nevertheless, a plant-specific action is necessary to ensure application specifications adequately justify the use of the TAB to meet Point 3's exclusion of nonsafety functions within safety components regarding any significant increase in errors that could result from increased complexity of the standardized circuit boards' programming.

Uses of the ALS-601 Communication Board do not impact its programming complexity, rather these uses impact the programming of the application-specific FPGA on the ALS-102 Core Logic Board. The ALS-601 Communication Board interfaces support meeting Point 3 because the "ALS Topical Report" limits the use of its data receivers to interdivisional vote sharing. This application of the ALS-601 Communication Board provides vital communication paths that directly support a safety function to perform coincidence voting. Nevertheless, a plant-specific review is necessary to ensure application specifications adequately justify the use of the ALS-601 Communication Board interfaces to meet Point 3's exclusion of nonsafety functions within safety components regarding any significant increase in errors that could result from increased complexity of the ALS-102 Core Logic Board's programming.

The NRC staff determined the ALS platform communication components support meeting Point 3 because the communication has been generally described in support or enhancement of the performance of the safety function. The NRC staff further determined plant-specific actions are necessary to ensure application specifications adequately justify each use of these interfaces regarding their support or enhancement of application-specific safety functions. Plant-specific actions should also demonstrate the inclusion of any functionality that does not support or enhance a safety function will not add complexity that significantly increases the likelihood of program specification or implementation errors (see Section 4.2, Items 1, 12, 13, 14 and 21).

3.7.2.1.4 Point 4

Point 4 establishes communication processes to support interdivisional communications (i.e., the transfer of data and any associated handshaking between a safety function processor and another channel or nonsafety equipment) should be carried out by a safety-related communications processor that is separate from the processor that executes the safety function,

so communications errors and malfunctions will not interfere with the successful execution of safety functions. Point 4 provides amplifying information that describes an acceptable implementation method, and this method uses shared memory resource, such as dual-ported random access memory (RAM). Point 4 further identifies demonstration of safety function determinism with respect to the data exchange between the safety processor and the communication processor. Demonstration of safety function determinism should show the safety function will: 1) be performed within the timeframe established in the safety analysis, and 2) complete successfully without data from the communication process, including either a

complete lack of access or any delays in obtaining access to a resource shared between the safety processor and the communication processor.

As discussed in Point 3, the ALS platform specifies, implements, verifies and validates, and tests the communications and safety functions using safety-related processes. The resultant FPGA device contains communication logic circuits that are separate and unique from other safety function logic circuits. The FPGA on the ALS-102 Core Logic Board supports application-specific safety functions and the TxB1 and TxB2 interfaces, and similarly the FPGA on each standardized circuit board supports application-specific safety functions and the TAB interface. Within the ALS platform architecture, only the ALS-601 Communication Board is dedicated to communication processing and supports bidirectional communication with either safety or nonsafety equipment. Regardless, the ALS-601 Communication Board's FPGA also supports the TAB interface.

The ALS platform proposes an alternative method to shared memory between distinct processing devices. This alternative method does not provide communication processors and safety processors that reside in physically distinct processing devices using a separate shared memory resource. Instead, this alternative method provides communication processing logic that is separate from safety processing logic but resides in a common physical device, the FPGA on each standardized circuit board. In lieu of a separate shared memory resource, this alternative method uses the ALS platform development processes to create buffers within each FPGA device that provide access priority to safety logic functions in order to ensure a deterministic completion of each safety function.

As discussed in Point 3, all of the ALS platform logic circuits have been developed as safety-related, which meets Point 4's guidance that safety function processors, communications processors, the data exchange memory resource, supporting circuits, and programming be developed as safety-related. The "ALS Topical Report" states the communication logic circuits do not interact with the safety function logic circuits within an FPGA device. Instead, the communication logic circuits non-intrusively monitor the safety function logic circuits so a failure of the communication logic processing cannot adversely affect the performance of the safety function processing (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 4, and Section 5.3.2).

The NRC staff determined the ALS platform alternative method, which produces:
1) communication processing logic circuits that are separate from safety processing logic circuits but reside in a common physical FPGA device and 2) communication buffers that give access priority to safety logic functions within each device, is an acceptable alternative to the implementation method provided in Point 4, because the alternative method supports a deterministic completion of each safety function without adverse affect from the communication processing. The NRC staff also determined the ALS platform standardized circuit boards support meeting Point 4 using this alternative method, because each has been developed as safety-related and can be used to ensure deterministic behavior of safety functions. The NRC staff further determined plant-specific actions are necessary to ensure: 1) application specifications document the safety analysis that applies to its safety function determinism and 2) the application-specific implementation, V&V, and testing efforts demonstrate these safety functions will be performed within the established safety design bases timeframes, including any

lack of access or delays related to the communication activities (see Section 4.2, Items 1, 8, 12, 13 and 14).

3.7.2.1.5 Point 5

Point 5 establishes 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 and failure of the system to meet the limiting cycle time should be detected and initiate an alarm.

As discussed in Point 4, the ALS platform provides an alternative approach to shared memory access, wherein communication logic circuits non-intrusively monitor safety function logic circuits and communication activities cannot delay or otherwise adversely affect the performance of the safety functions. Additionally, the "ALS Topical Report" states the failures of the system to meet timing requirements will activate an alarm so corrective actions can be taken (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 5).

The ALS platform addresses application-specific response times during each application-specific development, which should provide an application specification for the ALS-102 Core Logic Board that includes response time specifications. The ALS platform architecture and its standardized circuit boards provide features to ensure determinism by establishing expected response time performance variances. Although the platform communication architecture does not implement a shared memory resource, the application-specific ALS-102 Core Logic Board logic should meet Point 5 with respect to cycle-time performance, because the ALS-102 Core Logic Board determines the cycle-time for TxB1, TxB2, and ALS-601 Communication Board communications.

The NRC staff determined the ALS platform communication components support meeting Point 5 because the ALS platform supports detection and alarm logic in response to a system's failure to meet its application-specific limiting cycle time. The NRC staff further determined plant-specific actions are necessary to ensure application specifications meet Point 5 with respect to detection of and initiation of an alarm for cycle time performance in excess of the limiting cycle time (see Section 4.2, Items 1, 7, 12, 13 and 14).

3.7.2.1.6 Point 6

Point 6 establishes a safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

As discussed in Point 4, the ALS platform provides an FPGA approach that implements communication logic circuits that non-intrusively monitor safety function logic circuits so communication activities cannot delay or otherwise adversely affect the performance of the safety functions. Additionally, the "ALS Topical Report" states communication functions do not perform communication handshaking and do not accept any interrupts from any communication devices (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 6).

The TxB1 and TxB2 interfaces on the ALS-102 Core Logic Board meet Point 6 because the communication logic circuits that provide this transmit-only protocol do not include handshaking and do not interrupt safety function logic circuits within the ALS-102 Core Logic Board's FPGA device.

The TAB interface meets Point 6, because the communication logic circuits that provide this bidirectional protocol neither handshake with nor interrupt the safety function logic circuits within each FPGA device.

The ALS-601 Communication Board meets Point 6 because the communication logic circuits that it provides do not include handshaking or interrupts. Furthermore, the communication activities of ALS-601 Communication Board do not handshake or interrupt the safety functions performed by the ALS-102 Core Logic Board.

The NRC staff determined the ALS platform communication components meet Point 6 because safety function logic circuits perform no communication handshaking and do not accept interrupts.

3.7.2.1.7 Point 7

Point 7 establishes only predefined data sets should be used by the receiving system. Point 7 provides amplifying information that states unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements and data from unrecognized messages must not be used within the safety logic executed by the safety function processor. The pre-specified design requirements should establish the message format, such that each message has the same field structure and sequence, including message identification, status information, data bits, etc. in the same locations. The pre-specified design requirements should establish the message protocol that ensures deterministic system behavior by including every datum in every transmit cycle without regard to whether it has changed since the previous transmission.

As discussed in Point 4, the ALS platform provides an FPGA approach that implements communication logic circuits that are separate and independent from safety function logic circuits without regard to whether the circuits reside in the same FPGA device. Section 3.1.4.6,

describes two digital data communication protocols, Byte Mode and Packet Mode, and for each communication protocol all ALS data is sent each transmission cycle without regard to whether it has changed since the previous transmission. Additionally, the "ALS Topical Report" states a receiving ALS instrument will validate the data and will only accept and use data that conforms to a pre-defined communication protocol and message format (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 7).

Point 7 does not directly apply to the TxB1 and TxB2 interfaces on the ALS-102 Core Logic Board, because these interfaces provide a transmit-only protocol. Therefore, TxB1 and TxB2 cannot be used by an ALS platform-based safety instrument to receive data. Nevertheless, the NRC staff recognizes Point 7 could indirectly apply. The ALS-102 Core Logic Board's application-specific FPGA be programmed in such a way that allows a receiving safety system

to meet Point 7. The “ALS Topical Report” scope does not include application-specific message definitions or identify specific safety system-to-safety system interfaces. Therefore as applicable, plant-specific actions are necessary to ensure the application specification for the ALS-102 Core Logic Board’s FPGA requires pre-defined messages in accordance with Point 7 when either TxB1 or TxB2 provides data to another safety system.

TAB interface supports meeting Point 7. However, not all of Point 7 applies to the TAB interface. The ALS platform includes features to indicate an ALS platform-based instrument is bypassed whenever communication over this interface has been connected. The ALS platform derives this indication from monitoring a switch contact associated with the physical connection of the maintenance workstation and the detection of TAB activity. Nevertheless, the ALS-102 Core Logic Board’s application-specific FPGA may need to be programmed to meet application-specific maintenance activities in addition to standardized activities that are accounted for by pre-defined TAB messages for each standardized circuit board. Therefore, plant-specific actions are necessary to ensure the application specification for the ALS-102 Core Logic Board’s FPGA provides any application-specific pre-defined messages necessary to meet Point 7.

The ALS-601 Communication Board supports meeting Point 7. However, the ALS-102 Core Logic Board’s application-specific FPGA must be programmed to meet application-specific messaging needs when these interfaces are used. Therefore, plant-specific actions are necessary to ensure the application specification for the ALS-102 Core Logic Board’s FPGA provides pre-defined messages and a transmission cycle to meet Point 7 when the ALS-601 Communication Board interface is used.

The NRC staff determined the ALS platform communication components support meeting Point 7 because the ALS platform supports application-specific message formats, protocols, and transmission cycles that conform to Point 7. The NRC staff further determined plant-specific actions are necessary to ensure application specifications adequately define all message formats, protocols and transmission cycles (as applicable) to each use of these interfaces (see Section 4.2, Items 1, 12, 13, and 14).

3.7.2.1.8 Point 8

Point 8 establishes 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.

As discussed in Point 4, the ALS platform provides an FPGA approach that implements communication logic circuits that are separate and independent from safety function logic circuits without regard to whether the circuits reside in the same FPGA device. Therefore, the NRC staff determined transmit-only communications cannot adversely affect a safety function regardless of its location. As such, the NRC staff determined Point 8 does not apply to the TxB1 and TxB2 interfaces of the ALS-102 Core Logic Board, but does apply to the TAB interface and the ALS 601 Communication Board interfaces.

As discussed in Point 7, the ALS platform supports bidirectional communication between safety and nonsafety division via the TAB interface on all standardized circuit boards. However, activation of the TAB interface places an ALS platform-based instrument into bypass where it is no longer relied upon to perform its safety function (see Reference 32, Table 5.4-1, DI&C-ISG-04, Item 8). The ALS platform also supports bidirectional communication among redundant safety divisions via the ALS 601 Communication Board, and the intended application of this board does not extend to bidirectional communication between safety and nonsafety divisions. Taken together, the TAB and the ALS-601 Communication Board support bidirectional communication among redundant safety divisions and between safety and nonsafety divisions. However, the "ALS Topical Report" scope neither includes the application-specific system-to-system communication architecture nor the application-specific messages to support this architecture. Therefore, a plant-specific action is necessary to ensure the application specification for the ALS-102 Core Logic Board's FPGA demonstrates the data exchanges associated with these interfaces meet Point 8.

The NRC staff determined the ALS platform communication components support meeting Point 8 because the ALS platform supports an application-specific communication architecture for data exchanges that conforms to Point 8. The NRC staff further determined plant-specific actions should verify Point 8 is met by ensuring application specifications define: 1) the administrative controls and design features that govern use of the TAB interface for data exchanges between safety and nonsafety divisions, and 2) use of the ALS 601 Communication Board to exchange data among redundant safety divisions (see Section 4.2, Items 1, 13, and 14).

3.7.2.1.9 Point 9

Point 9 establishes incoming message data should be placed in fixed and predetermined locations of communication processor shared memory and function processor memory, which both contain memory locations dedicated to store incoming message data. These memory locations should segregate input data from output data, such as through placement into

separate memory devices or in separate pre-specified physical areas of a single memory device.

As discussed in Point 4, the FPGA-based ALS platform provides an alternative method to shared memory between distinct processing devices. This alternative method does not provide communication processors and safety processors that reside in physically distinct processing devices using a separate shared memory resource. Instead, this alternative method provides communication processing logic circuits that are separate from safety processing logic circuits but resides in a common physical device, the FPGA on each standardized circuit board. In lieu of a separate shared memory resource, this alternative method uses the ALS platform development processes to create buffers that provide dedicated pre-specified physical areas within each FPGA to store incoming message data and to segregate input data from output data (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 9).

The NRC staff determined the ALS platform alternative method to that associated with Point 4 is an acceptable alternative to the guidance in Point 9 because the ALS platform alternative

method provides separate buffers within each FPGA device to store and segregate message data. As such, the NRC staff determined the ALS platform meets the intent of Point 9, as applicable FPGA technology.

3.7.2.1.10 Point 10

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

The "ALS Topical Report" summarizes the ALS platform approach to meet DI&C-ISG-04 Branch Position 1, Point 10 (see Reference 32, Table 5.4-1, Item 10). The summary states the installed safety FPGA logic programs can only be modified using special tools available to the manufacturer, unavailable to licensees, and only upon board removal. Nevertheless, certain parameters, such as setpoints, can be adjusted by licensees during plant operation when either

the equipment is bypassed or its safety function is no longer required to be operable based on the current operating mode and conditions. Either a qualified safety or a nonsafety maintenance workstation will be used to perform the allowable operational adjustments. Regardless, communication with the maintenance workstation will be activated by a key lock switch that will initiate alarms at the ALS chassis and in the control room. These adjustments will be performed in accordance with plant operating procedures that govern the parameter's adjustment, including any that establish the minimum number of redundant safety channels that must remain operable for the current operating mode and conditions.

Once an ALS platform-based instrument has been programmed and delivered to a nuclear power plant as an application-specific system, none of the available digital data communication interfaces supports alteration of the FPGA logic circuits or configuration settings that have been set to fixed values in order to meet application specifications. Therefore, the NRC staff determined the safety division FPGA logic (i.e., programs) is protected from alteration at all times.

The ALS platform provides options to support different maintenance workstation configurations. However, the “ALS Topical Report” scope does not include the maintenance workstation. The two options that the ALS platform supports are 1) a safety qualified maintenance workstation integral to each safety equipment channel/division, and 2) an external nonsafety maintenance workstation not integral to any safety equipment channel/division (see Reference 32, Section 5.3.3 and Figure 5.3-1). The ALS platform does not support a multidivisional maintenance workstation that is simultaneously connected to more than one safety channel/division, because the maintenance activities require use of the TAB interface, and the TAB is a point-to-point connection that does not support simultaneous communication with multiple divisions (see Reference 32, Section 5.4.1.1).

Only the TAB interface can be used to operationally adjust addressable constants, setpoints, or parameters. The ALS platform supports inclusion of a physical disconnection, such as a key lock switch, to physically interrupt the TAB interface communication signal path between the maintenance workstation and the safety channel/division. Additionally, the ALS platform provides design features (monitoring and indication capabilities) to alert operators when a safety channel/division is bypassed. These design features independently detect the key lock switch position, detect TAB interface activity, and provide associated local and remote alarm indications. These alarm indications can be used to identify when a maintenance workstation is connected, so operators can consider the affected channel to be inoperable. Based on this evaluation, the NRC staff determined the program can be protected against inadvertent adjustment to addressable constants, setpoints, or parameters. Regardless, the methods to connect/disconnect the TAB communication signal path between the maintenance workstation and a safety channel/division and to initiate an alarm for a connected condition to operators is application-specific. Therefore, to meet Point 10, a plant-specific action is necessary to ensure application specifications include methods to interrupt the TAB communication signal path between the maintenance workstation and the safety channel/division and to initiate an alarm for the condition of a connected maintenance workstation. This plant-specific action should also ensure these methods have been implemented.

As discussed in Point 4 and Point 9, the NRC staff determined the ALS platform alternative method, which produces 1) communication processing logic circuits that are separate from safety processing logic circuits but resides in a common physical FPGA device and 2) communication buffers that give access priority to safety logic functions within each device, is an acceptable alternative to the implementation methods provided in Point 4, which identifies an interposing communication processor and shared-memory resource to exchange incoming and outgoing messages with a safety function processor and Point 9, which identifies fixed, predetermined, and segregated locations for incoming and outgoing data exchanges within a shared memory.

Point 10 does not apply when maintenance workstations have been developed to meet safety-related equipment criteria and an individual maintenance workstation is associated with each safety division, because the applicability of DI&C-ISG-04 is limited to communication interfaces between independent safety channels/divisions and between safety and nonsafety equipment. Nevertheless, the ALS platform: 1) supports inclusion of a physical disconnection that interrupts the communication signal path from the maintenance workstation to individual safety

channels/divisions; 2) provides an acceptable alternative method to the interface implementation discussed in Points 4 and 9; 3) provides features to ensure a safety channel/division is identified as inoperable whenever a maintenance workstation is connected; and 4) does not support simultaneous use of a multidivisional maintenance workstation with redundant safety channels/divisions.

The NRC staff determined the ALS platform supports meeting Point 10, because the ALS platform's maintenance communication architecture can be configured to conform to Point 10. The NRC staff determined Point 10's provisions to physically restrict making changes to only one redundant safety division at a time are met by the design of the TAB interface, which does not support simultaneous connection of redundant safety divisions to a multidivisional maintenance workstation. The NRC staff further determined plant-specific actions should verify whether application specifications identify administrative controls and include additional design features (i.e., a safety-qualified hardware switch and detection and indication of bypass) to govern use of the TAB interface for data exchanges with a nonsafety maintenance workstation, if applicable (see Section 4.2, Items 1 and 13).

3.7.2.1.11 Point 11

Point 11 establishes 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 out-of-service. These provisions should prevent the progress of a safety function processor through its instruction sequence from being affected by any message from outside its division. As an example, there should be no possibility that interdivisional communication messages could direct a safety function processor to execute a subroutine or branch to a new instruction sequence.

The ALS platform does not contain conventional software instructions with either subroutines or branches. Instead, the ALS platform contains configured hardware logic circuits that are

contained in the FPGA. As discussed in Point 10, once an ALS platform-based instrument has been programmed and delivered to a nuclear power plant as an application-specific system, none of the available digital data communication interfaces supports alteration of the configured FPGA logic circuits. Information or messages received through TAB Interface or the ALS-601 Communication Board cannot be used to control the execution of the safety division application program (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 11). As further discussed in Point 10, the ALS platform provides design features (monitoring and indication capabilities) to alert operators when a safety channel/division is bypassed and these design features are intended to detect and indicate when the interface that supports the maintenance workstation is either enabled or active.

The NRC staff determined the ALS platform's provisions for interdivisional communication meet Point 11, because these provisions explicitly preclude any ability to change the safety division logic circuits, which is the FPGA equivalent to conventional processor software. Furthermore, the NRC staff determined available ALS platform features can be used to ensure an ALS platform-based instrument has been bypassed or is otherwise out-of-service when maintenance workstation activities are active. The NRC staff further determined plant-specific actions should

verify whether application specifications include these additional design features (i.e., a qualified hardware switch and detection and indication of bypass) to govern use of the TAB interface, as applicable to application-specific safety functions (see Section 4.2, Items 1 and 13).

3.7.2.1.12 Point 12

Point 12 establishes faults associated with interdivisional communications should not adversely affect the performance of required safety functions in any way. Point 12 also provides examples of communication faults for consideration, as applicable.

As discussed in Point 4, the ALS platform provides an FPGA approach that implements communication logic circuits that are separate and independent from safety function logic circuits without regard to whether the circuits reside in the same FPGA device. The ALS platform communication protocol and implementation, checks, detects and annunciates communication failures. The ALS-102 Core Logic Board's application-specific FPGA must be programmed to meet application-specific communications and to maintain the status of the communications needed to ensure performance of required safety functions (see Reference 32, Table 5.4-1, DI&C-ISG-04, Item 12).

The TxB1 and TxB2 interfaces on the ALS-102 Core Logic Board meet Point 12, because these interfaces provide a transmit-only protocol and the interfaces are supported by communication logic circuits that are separate from the safety function logic circuits.

The TAB interface on each standardized circuit board supports meeting Point 12, because these interfaces are only intended to be enabled when a safety channel/divisions is not being relied upon to perform its safety functions. As discussed in Point 10, the ALS platform provides design features (monitoring and indication capabilities) to alert operators when a safety channel/division is bypassed and these design features are intended to detect and indicate

when the interface that supports the maintenance workstation is either enabled or active. Plant-specific actions should verify whether application specifications identify administrative controls and include additional design features (i.e., a safety-qualified hardware switch and detection and indication of bypass) to govern use of the TAB interface with a nonsafety maintenance workstation, if applicable.

The ALS-601 Communication Board supports meeting Point 12 for vital communications. Nevertheless, the ALS-102 Core Logic Board's application-specific FPGA must be programmed to meet application-specific safety functions when these interfaces are vital communications and relied upon to perform a safety function. The number of redundant safety channels/divisions and the overall communication architecture are also application-specific. Therefore, a plant-specific action is necessary to ensure the application specification for the ALS-102 Core Logic Board's FPGA and the overall communication architecture are sufficient to ensure interdivisional vital communication failures do not adversely affect the performance of required safety functions. Application-specific equipment specifications should identify the number of redundant safety channels/divisions, the overall communication architecture, and any fail-safe actions taken in response to interdivisional communication failures to ensure a safety function will be performed when required to do so.

The ALS-601 Communication Board also supports meeting Point 12 for non-vital communications with a multidivisional display and control station (see Reference 32, Sections 5.4.1 and 5.4.1.1). Nevertheless, plant-specific actions should verify the application specifications include administrative controls and additional design features (i.e., a safety-qualified hardware switch and detection and indication of bypass) to govern this use of the interface.

The NRC staff determined the ALS platform communication components support meeting Point 12 because the ALS platform supports an application-specific communication architecture to respond to communication faults without adversely affecting the performance of required safety functions. The NRC staff further determined plant-specific actions should verify Point 12 is met by ensuring application specifications define: 1) the administrative controls and design features that govern use of the TAB interface for data exchanges between safety and nonsafety divisions, 2) the number of redundant safety channels/divisions, the overall communication architecture, and responses to communication failures that govern use of the ALS-601 Communication Board for vital communications to ensure application-specific safety functions will be performed, and 3) the administrative controls and design features that govern use of the ALS-601 Communication Board for use with a multidivisional display and control station, if applicable (see Section 4.2, Items 1, 13 and 14).

3.7.2.1.13 Point 13

Point 13 establishes vital interdivisional communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions to ensure received messages are correct and are correctly understood. The effectiveness of these provisions should be demonstrated and verified by testing. Point 13 further establishes vital interdivisional

communications should include provisions to handle corrupt, invalid, untimely or otherwise questionable data. Any error detection or error correction processing should not adversely affect the operation of the safety function processor.

As discussed in Point 4, the ALS platform provides an FPGA approach that implements communication logic circuits that are separate and independent from safety function logic circuits, so communication processing logic circuits that perform error detection will not adversely affect the operation of safety function logic circuits. The ALS platform implements only point-to-point UART communication protocols and these protocols include error detection logic circuits to ensure received messages are correct and are correctly understood. However, the protocol does not include error-correcting coding. Furthermore, the “ALS Topical Report” only describes vital interdivisional communications as being supported by the ALS-601 Communication Board. Therefore, evaluation against Point 13 is only performed for the interfaces provided on the ALS-601 Communication Board (see Reference 32, Table 5.4-1, DI&C-ISG-04 Items 12, 13, and 14).

ALS platform communication protocol validates messages and detected failures, including both bit and byte serial transfer overruns and underruns. Methods to detect data corruption during transmission include the use of parity bits and/or cyclical redundancy check (CRC) message checksums. The protocol includes a feature for encoding messages and this feature ensures

the originator of any received message is correct. Use of this feature applies to messaging protocols that include the CRC checksum, is directly supported by the ALS platform's restriction to use of a point-to-point communication architecture for all interdivisional communications, and will result in the complete rejection of a message originating from an unexpected source. The transmit interval for messages is fixed, so the ALS platform communication protocol supports detection of untimely messages (too early or too late). The communications logic circuits detect and handle communication errors. As discussed in Point 4, the ALS platform communication protocol and implementation, checks, detects and annunciates communication failures. However, the ALS-102 Core Logic Board's application-specific FPGA must be programmed to meet application-specific communications and to maintain the status of the communications needed to ensure performance of any required safety function that depends on vital interdivisional communications. The effectiveness of these provisions was verified by testing and documented as part of equipment qualification. Qualification testing of the ALS platform continuously exercised the ALS-601 communications at its maximum communication baud rate configuration. This testing included both synchronous loopback testing through a 10 meter cable and asynchronous testing with independent test equipment (see Reference 51, Section 3.2.1.5).

The NRC staff determined the ALS-601 Communication Board supports meeting Point 13 for vital interdivisional communications, because the ALS platform communication protocol includes error detection and handling provisions that have been demonstrated during equipment qualification testing. The NRC staff further determined plant-specific actions should verify Point 13 is met by ensuring application specifications define the protocol configuration, messages transmit interval, and the responses to communication failures that govern use of the

ALS-601 Communication Board for vital communications to ensure the integrity of application-specific safety functions are preserved (see Section 4.2, Items 1 and 14).

3.7.2.1.14 Point 14

Point 14 establishes vital interdivisional communications should be point-to-point over a dedicated medium without intervening nodes between the transmitter and the receiver. Point 14 further establishes alternative methods, if proposed, should be justified and demonstrated as providing equivalent reliability.

As discussed in Point 13, the ALS platform only implements point-to-point UART communication protocols and these protocols require a dedicated medium. Furthermore, the "ALS Topical Report" only describes vital interdivisional communications as being supported by the ALS-601 Communication Board. Therefore, evaluation against Point 14 is only performed for the interfaces provided on the ALS-601 Communication Board (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 14).

The NRC staff determined the provisions for vital interdivisional communication meet Point 14 because only point-to-point communications over a dedicated medium is proposed for and supported by the ALS platform. The NRC staff further determined plant-specific actions should verify Point 14 remains met by ensuring application specifications define a point-to-point

communication architecture that excludes intervening nodes between any transmitter-receiver pair used for vital interdivisional communications (see Section 4.2, Items 1 and 14).

3.7.2.1.15 Point 15

Point 15 establishes vital interdivisional communications for safety functions provide a fixed dataset at regular intervals whether data values in the set have changed or not. This fixed dataset should reflect the equipment state in support of equipment safety functions.

As discussed in Point 13, the ALS platform UART communication protocols support transmission of a pre-defined fixed dataset at prescribed intervals (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 15). As discussed within Section 3.1.4.7, the content and format of the digital data communications are to be included in application specifications for each system that uses a digital data communication channel. Furthermore, the “ALS Topical Report” only describes vital interdivisional communications as being supported by the ALS-601 Communication Board. Therefore, evaluation against Point 15 is only performed for the interfaces provided on the ALS-601 Communication Board.

The NRC staff determined the provisions for vital interdivisional communication support meeting Point 15 because the protocol can be used to transmit pre-defined fixed dataset at prescribed intervals and without regard to the data values. The NRC staff further determined plant-specific actions should verify Point 15 is met by ensuring application specifications identify the datasets required for vital communications for safety functions and identify the fixed transmission interval

for these datasets in such a way that the values are transmitted without regard to whether any value has changed (see Section 4.2, Items 1 and 14).

3.7.2.1.16 Point 16

Point 16 establishes network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol.

Point 16 is application-specific, because meeting Point 16 is dependent upon the safety functions of the application and the installed communication architecture. Nevertheless, as discussed in Point 13, the ALS platform UART communication protocols support transmission of a pre-defined fixed dataset at prescribed intervals using a point-to-point architecture, which further supports detection of untimely messages that occur too early, too late, or not at all (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 16). The ALS platform communication protocols do not support network connectivity. As discussed within Section 3.1.4.7, the content and format of the digital data communications are to be included in application specifications for each system that uses a digital data communication channel. Furthermore, the “ALS Topical Report” only describes vital interdivisional communications as being supported by the ALS-601 Communication Board. Therefore, evaluation against Point 16 is only performed for the interfaces provided on the ALS-601 Communication Board.

The NRC staff determined the provisions for vital interdivisional communication support meeting Point 16 because the protocol can be used to ensure the connectivity, liveness, and real-time properties of vital communication processes. The NRC staff further determined plant-specific

actions should verify Point 16 is met by ensuring application specifications identify provisions to detect untimely messages and provide indication of this type of communication failure to operators when it occurs (see Section 4.2, Items 1 and 14).

3.7.2.1.17 Point 17

Point 17 establishes the medium used for vital interdivisional communications should be qualified for the anticipated normal and post-accident environments associated with its installation.

Point 17 is dependent upon the plant installation and the safety application because meeting Point 17 is dependent upon the environmental conditions of the installation within which the application-specific safety functions are required to remain available. Although the ALS platform supports both copper and fiber-optic mediums, the “ALS Topical Report” scope excludes the medium used for interdivisional communication and identifies this to be application-specific (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 17). Nevertheless, ALS platform equipment qualification establishes an envelope for equipment performance using copper (see Reference 50, Figure 3-2). Furthermore, the “ALS Topical Report” only describes vital interdivisional communications as being supported by the ALS-601 Communication Board. Therefore, evaluation against Point 17 is only performed for the interfaces provided on the

ALS-601 Communication Board, even though the medium equally applies to other ALS platform communications interfaces.

Based on this evaluation, the NRC staff determined the ALS platform supports meeting Point 17 because the ALS platform was qualified for use in a mild environment, the ALS platform supports copper and fiber-optic mediums, and both copper and fiber-optic mediums that have been qualified for a mild environment are available and in-use at nuclear power plants. The NRC staff further determined plant-specific actions should verify Point 17 is met by ensuring the application-specific medium has been qualified for the normal and post-accident environments associated with its installation when the application-specific safety functions are required to be available. A plant-specific action is necessary to ensure the ALS platform equipment qualification envelope bounds the environmental conditions for the plant-specific installation (see Section 4.2, Item 14).

3.7.2.1.18 Point 18

Point 18 establishes provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complexity.

Point 18 is dependent upon the plant safety application because the plant’s application establishes potential hazards, and plant-specific needs establish the required performance, the needed functionality, and the interdivisional communication architecture to support the needed functionality. As discussed within Section 3.1.4.7, application specifications for each use of a digital data communication channel must be analyzed and designed to meet plant and system hazard and performance specifications. This analysis will occur as part of the application-specific development process. This analysis will assess unneeded functionality and complexity

to ensure no hazards or performance deficits are produced from the inclusion of unneeded functionality or increases in complexity that result from including these functions (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 18).

The ALS platform integrity characteristics to address response time and determinism are discussed within Sections 3.4.1and 3.4.2, respectively. The ALS platform characteristics for diagnostics and self-test capabilities and failure mode and effects analysis are discussed within Sections 3.4.3 and 3.5. These characteristics, as evaluated, support a plant-specific hazards analysis and a plant-specific performance analysis.

Based on the evaluations in Sections 3.4.1, 3.4.2, 3.4.3, and 3.5, the NRC staff determined the ALS platform supports meeting Point 18, because the ALS platform supports the performance of plant-specific hazard and performance analyses in consideration of an application's specified functionality and inherent level of complexity. The NRC staff further determined plant-specific actions should verify Point 18 is met by ensuring an application-specific analysis has been performed to assess unneeded functionality and complexity. The results of this analysis should demonstrate any resultant hazards or performance deficits have been addressed (see Section 4.2, Items 1, 12, 13 and 14).

3.7.2.1.19 Point 19

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

Point 19 is dependent upon the plant safety application, because the plant's application establishes the minimum communications throughput threshold for each vital interdivisional communication link and node required to reliably meet each application-specific safety function's limiting performance requirement. As discussed within Section 3.1.4.7, application specifications for the ALS 102 Core Logic Board must be analyzed, designed, and configured to meet each plant performance requirement, including those dependent on any digital data communication channel. This analysis will occur as part of the application-specific development process. This analysis will result in specified transmission rates and message transmission intervals to meet all plant performance requirements. Application-specific V&V as well as factory and system acceptance testing will demonstrate the plant-specific performance requirements have been met (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 19).

As discussed in Points 14 and 15, the ALS platform communication architecture is point-to-point over a dedicated medium, and the UART communication protocols support transmission of a pre-defined fixed dataset at prescribed intervals. Additionally, the clock circuit, from which the communication transmission rate is derived, can be monitored for the correct frequency. These platform characteristics produce a consistent and predictable communication load, which

simplifies the analysis and testing to demonstrate adequate communication throughput. The communication protocols and architecture can be applied to eliminate widely varying or excessive communication loads like those that could result from using either a shared medium or communications that are not point-to-point. Furthermore, the ALS platform integrity characteristics to address response time and determinism are discussed within Sections 3.4.1 and 3.4.2, respectively, and these characteristics, as evaluated, also simplify the plant-specific analysis and testing to demonstrate adequate communication throughput.

The NRC staff determined the ALS platform supports meeting Point 19, because the ALS platform supports the specification, V&V, and testing of data communication capacities and throughput thresholds required for proper performance of plant-specific safety functions. The NRC staff further determined plant-specific actions should verify Point 19 is met by ensuring an application-specific analysis has been performed to specify transmission rates and intervals that will meet all plant performance requirements. These plant-specific actions should document the expected communication loading and address any variations to demonstrate the adequacy of the transmission rates and intervals will remain above the minimum threshold required for proper safety function performance. These plant-specific actions should also ensure application-specific V&V and factory and system acceptance testing confirm all plant-specific performance requirements dependent on digital data communications are met (see Section 4.2, Items 1, 7, 8, 12, 14, and 23).

3.7.2.1.20 Point 20

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

Point 20 is dependent upon the plant safety application, because the plant's application establishes the safety system response time requirement. As discussed within Section 3.1.4.7, application specifications for each use of a digital data communication channel must be analyzed and designed to meet plant response time performance specifications. This analysis, and related response time calculations, will occur as part of the application-specific development process. These application-specific response time calculations will document a design basis data error rate and its relationship to the application-specific digital data communications configuration and use (see Reference 32, Table 5.4-1, DI&C-ISG-04 Item 20). The design basis data error rates applied in application-specific response time calculations will be demonstrated as equally or more conservative than the corresponding data error rates observed during design and qualification testing. The test equipment was designed to declare a test failure [ ] consecutive unsuccessful transmissions occurred (see Reference 51, Section 3.2.1.5). Although the communication protocol allows for a maximum number of consecutive unsuccessful transmissions before identifying a failure, the qualification testing bounded potential intermittent serial communications delays, which could impact response time, to a maximum based on the transmission intervals and an allowance for a maximum number of consecutive errors without declaring a failure. Future safety system response time calculations should consider the potential delay when determining the design basis error rate that has been observed in qualification testing, and further consider the impact of potential additional delays

based the maximum number consecutive unsuccessful transmissions that the application allows before declaring a failure.

The ALS platform integrity characteristics to address response time and determinism are discussed within Sections 3.4.1and 3.4.2, respectively. These characteristics, as evaluated, support plant-specific safety system response time calculations to demonstrate adequate performance when data error rates remain within the qualified design basis.

The NRC staff determined the ALS platform supports meeting Point 20, because the ALS platform supports the specification, V&V, and testing of response time performance in the consideration of design basis data error rates. The NRC staff further determined plant-specific actions should verify Point 20 is met by ensuring application-specific response time calculations have been performed that: 1) document applicable design basis data error rates, 2) demonstrate each safety function's response time requirement dependent on digital data communications is met in the presence of the applicable design basis data error rate, and 3) demonstrate each design basis error rate is equally or more conservative than the

corresponding data error rate that was observed during design and qualification testing (see Section 4.2, Items 7, 12, and 14).

3.7.2.2 Staff Position 2 – Command Prioritization

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

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

The ALS platform neither includes a priority module within its standardized circuit board set nor includes priority module-type functionality within any of its standardized circuit boards. Therefore, no ALS platform component has been developed or tested to meet DI&C-ISG-04 Staff Position 2 Command Prioritization in order to serve as a priority module (see Reference 32, Section 5.4.1, Table 5.4-2's discussions of nonsafety stations controlling the operation of safety-related equipment and of safety-related stations controlling the operation of equipment in another safety-related division). The "ALS Topical Report" states Points 1 through 10 under Staff Position 2 Command Prioritization would be demonstrated on an application-

specific basis during the development of an ALS platform-based safety system when command prioritization is specified for use (see Reference 32, Section 12.3).

The NRC staff determined the “ALS Topical Report” has not requested an evaluation of the ALS platform against Staff Position 2, Command Prioritization. Therefore, this SE neither includes an evaluation nor reaches any conclusion regarding suitability of ALS platform components for use as a priority module. The NRC staff further determined plant-specific actions should either confirm the ALS platform-based safety system does not specify use of command prioritization or demonstrate Points 1 through 10 under Staff Position 2, Command Prioritization, are met when command prioritization is specified for use (see Section 4.2, Items 1 and 15).

3.7.2.3 Staff Position 3 – Multidivisional Control and Display Stations

DI&C-ISG-04 Staff Position 3, Multidivisional Control and Display Stations, establishes guidance governing operator workstations used for the control of plant equipment in more than one safety

division and for display of information from sources in more than one safety division. This guidance also applies to workstations to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

The “ALS Topical Report” scope excludes the control and display stations (see Reference 32, Section 1.2). Furthermore, as discussed under Section 3.7.2.2, the ALS platform does not include a priority module or explicit priority logic functionality. Therefore, the ALS platform does not include either consideration of either nonsafety stations controlling the operation of safety-related equipment or safety-related stations controlling the operation of equipment in another safety-related division (see Reference 32, Section 5.4.1).

The NRC staff determined the “ALS Topical Report” has not requested an evaluation of the ALS platform against Staff Position 3, Multidivisional Control and Display Stations, beyond that already evaluated against Staff Position 1, Interdivisional Communications. Therefore, this SE neither includes an evaluation nor reaches any conclusion regarding suitability of either a Qualified Display System or ALS Service Unit as a multidivisional control or multidivisional display station. The NRC staff further determined plant-specific actions should either confirm the ALS platform-based safety system does not specify use of either a multidivisional control or a multidivisional display station or demonstrate Staff Position 3, Multidivisional Control and Display Stations, is met when either a multidivisional control or a multidivisional display station is specified for use (see Section 4.2, Items 1 and 16).

3.8 Secure Development and Operational Environment

RG 1.152, Revision 3, describes a method that the NRC considers acceptable to comply with the regulatory criteria to promote high functional reliability, design quality, and establish secure development and operational environments for the use of digital computers in safety-related systems at nuclear power plants. The guidance for secure development and operational environments states potential vulnerabilities should be addressed in each phase of the digital safety system life-cycle. The overall guidance provides the basis for physical and logical access

controls to be established throughout the digital system development process to address the susceptibility of a digital safety system to inadvertent access and modification.

The SE of the secure development and operational environment within this section represents that which the manufacturer has characterized as meeting the “intent” of RG 1.152, Revision 3, “Criteria for use of Computers in Safety Systems of Nuclear Power Plants” (see Reference 32, Section 8.2) for the ALS platform. This SE takes into consideration several factors.

First, RG 1.152 provides guidance for the top-down development of a plant-specific system to licensees for license amendment requests, design certifications, and combined operating licenses. In contrast, the ALS platform scope does not provide a plant-specific system and its manufacturer is neither a licensee nor applicant for a license. Furthermore, RG 1.152 does not endorse a bottoms-up life-cycle approach that is dictated by a specific manufacturer’s platform or its design features.

Second, RG 1.152 directs much of its guidance toward traditional microprocessor-based systems with separately developed and installed operational software, where some software may be modified and maintained by nuclear plant personnel over the equipment’s life-cycle. In contrast, the ALS platform neither includes microprocessors nor separately developed and installed operational software, and the manufacturer has proposed to be the sole maintainer of its FPGA logic programming.

Third, RG 1.152 provides guidance that the safety system design features intended to ensure reliable operation should be validated as part of the overall system requirements. RG 1.152 provides further guidance that safety system design features maintaining a secure operational environment should be addressed by the execution of system integration testing, system qualification testing, and system factory acceptance testing. This testing includes all connectivity to other systems, including external systems. In contrast, the platform's development and test scope is limited to life-cycle phases (1) through (5), as identified within Regulatory Position 2 of RG 1.152, for seven standardized circuit boards. Therefore, RG 1.152’s system validation and testing scope is beyond the scope of this SE.

The “ALS Security Plan” identifies safety system vulnerabilities within the development environment and presents its assessment for the platform. The security assessment identifies two vulnerabilities affecting a safety system design: 1) inadvertent access or modification to the safety system design, and 2) vulnerabilities within the design to adverse influence of connected systems. Additional assessments describe the basis for design features to ensure reliable operation of the system. The “ALS Security Plan” describes design features (i.e., “Core Diversity”) to address the potential for the installed operating environment to adversely influence reliability (e.g., single-event upset, etc.) (see Reference 39, Appendix A, Section A.2).

The “ALS Security Plan” also identifies potential security concerns and vulnerabilities applicable to the conceptual, requirements, design, implementation and testing life-cycle phases. The “ALS Security Plan” provides the measures to mitigate these vulnerabilities and prevent the introduction of undocumented or unwanted code. Mitigation approaches address potential vulnerabilities to both internal and external threats that could challenge the confidentiality or

integrity of the design. Mitigation approaches also address potential vulnerabilities to both accidental and malicious threats that could otherwise challenge the confidentiality or integrity of the design. The “ALS Security Plan” addresses both physical and logical security control of the development environment and design products (see Reference 39, Appendix A, Section A.3).

The “ALS Topical Report” addresses RG 1.152, Revision 3 (draft), and provides a description of the secure development activities performed for the development of the ALS platform. The manufacturer’s secure development environment process addresses the V&V activities to detect and prevent the use of unintended code, and the control and monitoring of access to the development environment (see Reference 32, Section 12.6). These measures, along with the design review and configuration management activities detailed in other ALS procedures and plans, provide protection against the introduction of unintended functionality into the platform.

The “FPGA Development Procedure” includes design reviews to verify the incorporation of all specified functionality. These design reviews also provide a means to identify the inclusion of unspecified functionality (see References 31, Section 7.4.11).

The “ALS Platform FPGA VV Test Plan” addresses the activities that the manufacturer implements to prevent the incorporation of unintended code. The V&V team performs a combination of design traceability, functional testing, code coverage analysis, code reviews, and synthesis reviews to verify no unintended functionality exists within the design (see References 31, Section 5.2.1).

The “ALS Topical Report” and the “ALS Security Plan” address access control of the ALS development environment and life-cycle security. These documents discuss secure development environment activities performed during the Planning, Development, Manufacturing and System Test life-cycle phases of a project, although manufacturing a plant-specific application and its system test remain outside the scope of the “ALS Topical Report.” Nevertheless, the manufacturer developed the ALS platform using an isolated and controlled network called the Isolated Development Infrastructure (IDI). FPGA programs and other related configuration controlled FPGA design artifacts, including NVM configuration files, are developed, controlled, and maintained within the IDI. The manufacturer also implements monitoring and tracking of activities performed within the IDI (see References 31, Section 8.2, and Reference 47).

During the November 2012 audit at the Scottsdale, Arizona facility, the NRC staff confirmed the manufacturer had implemented secure development environment activities and configuration control activities (see Reference 127).

The “ALS Security Plan“ states application-specific system design and test files may be developed outside of the IDI, but that associated FPGA and related design files, and NVM files, are developed and controlled using the IDI. This SE is based on continued applicability of the “ALS Security Plan” or an equivalent. Therefore, applicants and licensees referencing this SE should ensure the secure development environment for future efforts, including plant-specific application developments, continues to meet the regulatory evaluation criteria of RG 1.152 (see Section 4.2, Item 17).

Without a specific operational environment to assess, the NRC staff cannot reach a determination on a plant-specific ALS-based system's ability to withstand undesirable behavior of connected systems and preclude inadvertent access. However, the ALS platform does include design attributes and features that a licensee could apply and credit to demonstrate protection against undesirable behavior of connected systems and the prevention of inadvertent access (see Section 3.7.2 and Section 4.2, Items 12, 13, and 14). Nevertheless, the final determination on protection against undesirable behavior from connected systems and inadvertent access in the operational environment is a plant-specific activity (see Section 4.2, Item 18).

Based on the NRC staff's review of the information provided by the manufacturer and the results of the audit, the NRC staff determined the manufacturer established a secure development environment for the ALS platform that is consistent with the regulatory positions found in RG 1.152, Revision 3. Therefore, the NRC staff concludes the ALS platform has been designed with provisions for physical and logical access controls to ensure high functional reliability and to provide mitigation against the introduction of undocumented or unwanted code. The NRC staff also identified two plant-specific actions necessary to demonstrate the RG 1.152 regulatory evaluation criteria are met for application developments and operations. The NRC staff further determined the ALS platform contains design attributes and features that licensees could apply and credit to demonstrate protection against undesirable behavior of connected systems and the prevention of inadvertent access when addressing the operational environment.

3.9 Diversity and Defense-in-Depth

This section describes and evaluates the methods available to build diversity into the ALS platform component designs. It also describes and evaluates the designs and principles of operation of ALS platform-based systems. However, this evaluation provides limited safety conclusions because the demonstration of adequate diversity and defense-in-depth (D3) requires the context of a specific nuclear power plant's overall D3 analysis to address mitigation of plant-specific vulnerabilities. Therefore, this evaluation is limited to specific manufacturer claims regarding the built-in diversity of the ALS platform and its principles of operation, while considering ALS platform design and process attributes that either preclude or limit certain types of common-cause failures (CCFs).

The regulation at 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. Clause 5.1 of IEEE Std 603-1991 requires, in part, "safety systems shall perform all safety functions required for a design basis event in the presence of any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures." The regulation at 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS)," requires, in part, various diverse methods of responding to an ATWS. 10 CFR Part 50, Appendix A, GDC 21, "Protection System Reliability and Testability," requires, in part, "no single failure results in the loss of the protection system." GDC 22, "Protection System Independence," requires, in part, "the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions ..not result in loss of the protection function ... Design techniques, such as functional

diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function." GDC 24, "Separation of Protection and Control Systems," requires, in part, "interconnection of the protection and control systems shall be limited so as to assure safety is not significantly impaired." GDC 29, "Protection Against Anticipated Operational Occurrences," requires, in part, defense against anticipated operational transients "to assure an extremely high probability of accomplishing ... safety functions."

RG 1.53, "Application of the Single-Failure Criterion to Safety Systems", clarifies the application of the single-failure criterion (GDC 21) and endorses IEEE Std 379-2000, "IEEE Standard

Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems." Clause 5.5 of IEEE Std 379-2000 identifies D3 as a technique for addressing CCF, and Clause 6.1 identifies logic failures as a type of failure to be considered when applying the single-failure criterion.

The NRC staff Requirements Memorandum on SECY 93-087 dated July 21, 1993, describes the NRC position on D3 requirements to compensate for common-cause programming failures. This requires an applicant or licensee assess the D3 of the proposed I&C system, and if a postulated common-cause 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.

Guidance on the evaluation of D3 is provided in SRP BTP 7-19. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 31, 1994, summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses. Additional guidance on acceptable methods for implementing D3 in digital I&C system designs is contained in "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues," June 5, 2009.

NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," dated February, 2010, builds upon NUREG/CR-6303 and provides guidance to the NRC staff and nuclear industry for use after an applicant or licensee has performed a D3 assessment per NUREG/CR-6303 and determined some diversity in a safety system is needed to mitigate the consequences of potential CCFs identified through a prior evaluation of safety system design features. NUREG/CR-7007 evaluates the characteristics and efficacy of three diversity strategies (A thru C) to present a technical basis for acceptable mitigating strategies to resolve D3 assessment findings and conform to NRC regulations. NUREG/CR-7007 also identifies a fourth diversity strategy (D). However, no technical basis for Strategy D is provided.

The "ALS Topical Report" identifies intended applications of the ALS platform in various diversity configurations to support different nuclear power plant systems, including a digital reactor trip system (RTS) and the engineered safety features actuation system (ESFAS) (see Reference 32, Appendices A). In the context of D3, a reactor protection system (RPS) consists of the RTS and the ESFAS. Therefore, the identified regulatory criteria apply. Furthermore, BTP 7-19 and DI&C-ISG-02 apply to the ALS platform component designs and principles of operation, because the platform is digital and based on programmable devices. Regardless, a

platform cannot be confirmed to meet all of the NRC staff positions within either BTP 7-19 or DI&C-ISG-02.

BTP 7-19's D3 evaluation should demonstrate plant vulnerabilities to CCFs have been adequately addressed in the context of an overall suite of I&C systems. Furthermore, the four-point position within BTP 7-19 was developed in recognition that programming design errors are credible sources of CCFs that apply to nuclear power plants that incorporate digital protection systems, which includes RTS and ESFAS. BTP 7-19 in part provides guidance to evaluate the applicant's or licensee's D3 assessment, including the design of manual controls and displays to ensure conformance with the NRC positions on D3. BTP 7-19 Point 1 states:

> "The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed."

The "ALS Topical Report" does not propose a specific I&C system for a specific plant application, and a platform manufacturer is neither a licensee nor an applicant for a permit, design certification, or license. Therefore, this SE cannot determine the adequacy of the ALS platform against BTP 7-19 Point 1.

Although the entirety of BTP 7-19 cannot be evaluated for a platform, the NRC staff's evaluation of the "ALS Topical Report" addresses BTP 7-19 Point 3, albeit in a partial and generalized way. BTP 7-19 Point 3 states:

> "If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

Any equipment that results from this assessment, which is independent from the primary means to provide a safety function and implements the diverse means, is commonly referred to as a diverse actuation system. These diverse actuation systems are in addition to the ATWS systems required by 10 CFR 50.62, because existence of a diverse actuation system is predicated on a digital I&C system that is vulnerable to common-cause programming failures, while the ATWS requirements are founded on a different principle, which is independent of any implementation technology, including digital.

DI&C-ISG-02 provides acceptable methods for implementing D3 in digital I&C system designs and clarifies the criteria the NRC staff would use to evaluate whether a digital system design is consistent with D3 guidance. However, DI&C-ISG-02 cannot be directly applied to a platform for reasons similar to BTP 7-19. The DI&C-ISG-02 Issue 1, "Adequate Diversity," and Issue 2, "Manual Operator Actions," in part, state the applicant or licensee should perform a D3 analysis to demonstrate vulnerabilities to CCFs are adequately addressed. Although a platform

manufacturer is neither a licensee nor applicant, the ALS platform is a digital system based on programmable devices. Therefore, an applicant or licensee should consider whether programming errors remain credible sources of CCFs for its application, and if so, further consider DI&C-ISG-02 based on the applicant's or licensee's application-specific use.

DI&C-ISG-02 Issue 5, "Common-Cause Failure (CCF) Applicability," identifies a demonstration of sufficient diversity within the protection system is the first of two methods by which CCFs

within channels can be considered addressed. Regardless, the determination of sufficient diversity should be evaluated on a case-by-case basis in consideration of design and process attributes that preclude or limit certain types of CCFs. The second method is 100 percent testing, wherein testing may be performed on sufficiently simple systems, such that every possible combination of inputs, internal and external initial states, and every signal path is tested, so the system is fully tested and found to produce only correct responses.

DI&C-ISG-02 Issue 7, "Single Failure," in part clarifies postulated digital system CCFs should not be assumed to be a single random failure in design basis evaluations because digital system CCFs are not classified as single failures. Consequently, best-estimate techniques can be employed in performing analyses to evaluate the effect of digital system CCFs coincident with design basis events. This treatment of single failures is applied when evaluating the DI&C-ISG-02 issues of "Adequate Diversity" and "Manual Operator Actions," and BTP 7-19 Point 3's guidance on diverse actuation systems.

Although the entirety of DI&C-ISG-02 cannot be evaluated for a platform, the NRC staff's evaluation of the ALS Topical Report addresses the DI&C-ISG-02 issues of "Adequate Diversity" and "Manual Operator Actions," which state, in part, the following:

> "… When an independent and diverse method is needed as backup to an automated system used to accomplish a required safety function, the backup function can be accomplished via either an automated system, or manual operator actions performed in the main control room. The preferred independent and diverse backup method is generally an automated system. The use of automation for protective actions is considered to provide a high-level of licensing certainty.
>
> If automation is used as the backup, it should be provided by equipment that is not affected by the postulated RPS CCF … "

Like BTP 7-19 Point 3, the DI&C-ISG-02 issues of "Adequate Diversity" and "Manual Operator Actions," refer to other potential diverse actuation systems that are exclusive of ATWS functionality.

When manual operator actions provide the backup, these actions should use independent and diverse equipment that is not affected by the postulated RPS CCF. Consistent with the requirements of IEEE Std 603-1991, Clause 6.2, "Manual Control," and applicable BTP 7-19 guidance, the "point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs" and "To achieve system-level actuation at the lowest possible level in the safety system architecture, the controls may be

connected either to discrete hardwired components or to simple (e.g., component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic."

Although a platform manufacturer is not an applicant or licensee and the platform implements no specific safety function, the ALS platform manufacturer claims the generic design concepts,

which include built-in diversity and complete testing of common blocks that do not employ built-in diversity, can be configured by plant-specific applications, so the safety analysis required by BTP 7-19 is not normally necessary (see Reference 32, Section 2.1). However, the platform manufacturer later clarifies certain platform design attributes, which have been specifically constructed to mitigate the likelihood of software common cause failures, provide a foundation that licensees may use in their D3 analysis to construct reliable safety systems. These design attributes are intended to justify the elimination of a diverse actuation system (i.e., support meeting BTP 7-19 Point 3 and DI&C-ISG-02 Issues 1 and 2) for some plant-applications. The platform manufacturer claims the ALS platform supports meeting the guidance contained in DI&C-ISG-02 Issue 1, "Adequate Diversity." This claim is based on available ALS platform attributes and its principles of operation, which can be configured to provide built-in diversity within its component designs in ways that mitigate the likelihood of programming common cause failures (see Reference 32, Sections 9 and 12.5). The platform manufacturer does not claim use of the platform necessarily eliminates either an applicant's or licensee's need for any diverse actuation system (i.e., automatically meets BTP 7-19 Point 3 and DI&C-ISG-02 Issues 1 and 2), or an applicant's or licensee's need to perform a best estimate safety analysis (BTP 7-19 Point 2 and DI&C-ISG-02 Issue 7). The "ALS Topical Report" supports its claims by describing the options available to provide built-in diversity (see Reference 32, Section 9; and Reference 47, Section 2) and an assessment of ALS platform diversity against the elements of diversity originally described in NUREG/CR-6303, which have since been supplemented by NUREG/CR-7007 (see Reference 47, Section 3).

The NRC staff reviewed the content of Section 9 of the "ALS Topical Report" and the "ALS Diversity Analysis" to evaluate manufacturer claims regarding the ability of ALS platform design and process attributes to either preclude or limit certain types of CCFs. Section 9 of the "ALS Topical Report" identifies two design attributes, which are claimed to mitigate the likelihood of common-cause programming failures as sources that could disable a safety function. The "ALS Topical Report" refers to these two attributes as: 1) Core Diversity and 2) Embedded Design Diversity. Core Diversity generates two redundant logic implementations for placement within each FPGA for each standardized circuit board. The two redundant logic implementations (Core 1 and Core 2) use the same hardware descriptive language files per standardized circuit board. However, each logic implementation is produced using different synthesis directives (see Reference 47, Section 2.2 for details of Core Diversity). All ALS platform applications will contain Core Diversity. However, Embedded Design Diversity provides an optional addition to Core Diversity. Embedded Design Diversity requires the production of two versions of hardware descriptive language files for each standardized circuit board, [

] When using Embedded Design Diversity, the application must define the configuration and arrangement of the systems that use each set of FPGA design variants . For example, the configuration and arrangement of an individual channel, train, or electrical separation group may include an instrument chassis that uses one-and-only-one set of design variants or may include two instrument chasses where each chassis uses one-and-only-one design variant. The "ALS Topical Report" Appendices A thru C provide representative examples to illustrate how various ALS platform-based systems could be configured and arranged among redundant channels, trains or electrical separation groups.

Although Section 9 of the "ALS Topical Report" provides an overview of the approaches available to provide built-in diversity, the "ALS Diversity Analysis" provides an assessment of ALS platform diversity options against the diversity attributes identified in NUREG/CR-6303. The NRC staff reviewed the ALS platform approach and compared it against the diversity strategies documented in NUREG/CR-7007. From this review, the NRC staff determined the ALS platform approach, while having some similarities with strategies A and C, does not map directly to any of the documented strategies, A thru C. Instead, the NRC staff determined the ALS platform approach, as proposed and described, is consistent with the fourth strategy, Strategy D, because the ALS platform approach is characterized by use of the same technology (e.g., the same platform and logic device) for the diverse components being compared. In a Strategy D classification, the principal feature characterizing the strategy is basic components (e.g., hardware parts, software blocks, system architectural structure, etc.) of diverse systems are the same. The ALS platform approach differs from Strategy D in that different "software blocks" (i.e. FPGA programs) can exist when Embedded Design Diversity is used in both the primary and diverse actuation system, so one set of FPGA design variants could perform the primary safety function while the alternative set of design variants could provide the diverse actuation.

Based on the "ALS Diversity Analysis" (see Reference 47, Section 3), Table 3.9-1 provides a summary of the NRC staff's evaluation of each of the seven NUREG/CR-7007 baseline diversity strategies as applicable to the approaches to provide built-in diversity within ALS platform-based systems. The baseline diversity strategies are: 1) Design, 2) Equipment Manufacturer, 3) Logic Processing Equipment, 4) Functional, 5) Life-Cycle, 6) Logic, and 7) Signal. Unlike the "ALS Diversity Analysis," credit for unique aspects provided by Core Diversity and Embedded Design Diversity are addressed under only one of the seven NUREG/CR-7007 baseline diversity strategies because the baseline strategies are intended to be unique from one another to preclude double-counting. Credit for the Core Diversity as a diversity strategy is given under Logic Diversity. A small credit attributable to the Embedded Design Diversity is also given under Logic Diversity with the remaining majority of the credit being given under Life-Cycle Diversity.

Table 3.9-1 Evaluation of NUREG/CR-7007's Baseline Diversity Strategies

NUREG/CR-7007 Diversity Strategy	**Summary of Staff Evaluation**
1) Design	The ALS platform equipment is designed using a single FPGA manufacturer's technology on standardized circuit boards within a defined

"ALS Diversity Analysis" "Design Diversity" (see Reference 47, Section 3.2.1)	instrumentation architecture and framework. The processes to produce all designs are common. There is no technology-driven difference in the underlying design structure or its constituent components to produce differences in susceptibility to CCF sources with respect to diversity in the equipment's overall design. Although the use of Embedded Design Diversity provides some mitigation against common lower-level design implementation errors, this feature is credited under Logic and Life Cycle Diversity. The NRC staff determined the ALS platform approach does not significantly contribute to diversity of two equipment designs that meet the same or similar requirements (NUREG/CR-7007, Section 2.2.3.1).
2) Equipment Manufacturer "ALS Diversity Analysis" "Equipment Diversity" (see Reference 47, Section 3.2.2)	The ALS platform equipment is designed by a single manufacturer to produce fundamentally similar designs. There is no difference in the underlying equipment manufacturer or processes to produce differences in susceptibility to CCF sources with respect to equipment manufacturing processes. Although the use of Core Diversity provides some mitigation against tool synthesis errors that are part of the FPGA programming process, this feature is credited under Logic Diversity. Although the equipment can be configured to implement different versions of the same design with respect to FPGA programming when Embedded Design Diversity is applied, this capability is credited under Life-Cycle Diversity. The NRC staff determined the ALS platform approach falls on the lower end of effectiveness in mitigating equipment manufacturer related CCFs, and lies somewhere near "different versions of the same design" (see NUREG/CR-7007, Section 2.2.3.2).
3) Logic Processing Equipment Not addressed in "ALS Diversity Analysis," because it was under the general equipment diversity attribute within NUREG/CR-6303 and the ALS platform does not provide for this aspect of equipment diversity.	The ALS platform equipment is designed using a single FPGA manufacturer's technology using common ALS platform top-level requirements and specifications, including the bus communication architecture. The impact of process and the resultant products does not produce differences in susceptibility to CCF sources with respect to diversity in the logic processing equipment. The NRC staff determined the ALS platform approach does not contribute to logic processing equipment diversity (see NUREG/CR-7007, Section 2.2.3.3). The ALS platform approach does not produce architectural differences for logic processing to address sources of systematic errors that may arise during the design and implementation of systems. This determination can be made irrespective of the examples provided in NUREG/CR-7007, which are focused on microprocessor-based architectures, because the ALS platform and its processes do not produce dissimilar mechanisms that will lead to different execution profiles as described for the Logic Processing Equipment diversity strategy.

4) Functional “ALS Diversity Analysis” “Functional Diversity” (see Reference 47, Section 3.2.3)	The ALS platform equipment supports implementation of the functional diversity strategy. However, any functional diversity provided by an ALS platform-based system would be based on application specifications. The NRC staff determined the ALS platform can support overall instrumentation architectures that include functional diversity that implements “different underlying mechanisms,” “different purpose, function, control logic, or actuation means,” and/or “different response time scales” (see NUREG/CR-7007, Section 2.2.3.4). The NRC staff also determined the ALS platform itself does not provide functional diversity, because functional diversity requires specification of different functions, which is application-specific and is not provided at the platform level. Therefore, this SE for the “ALS Topical Report” cannot make a determination regarding the adequacy of application-specific functional diversity.
5) Life-Cycle “ALS Diversity Analysis” “Human Diversity” (see Reference 47, Section 3.2.4)	The ALS platform development approach uses independent teams between design and test, diverse tools between design and test, and has the option to implement designs developed by independent teams (when the Embedded Design Diversity is applied). [ ] The NRC staff determined the ALS platform provides life-cycle diversity that produces differences in susceptibility to CCF sources with respect to personnel cognition and resultant human actions, [ ]. Additional diversity is provided by the use of different tools between the implementation and test teams. When Embedded Design Diversity is applied, the ALS platform also provides “different design and development teams.” Nevertheless, this SE for the “ALS Topical Report” cannot make an overall determination regarding the adequacy of application-specific life-cycle diversity, because the choice to require Embedded Design Diversity is application-specific.
6) Logic “ALS Diversity Analysis” “Software Diversity” (see Reference 47,	The ALS platform equipment includes a Core Diversity and an Embedded Design Diversity strategy that produces logic diversity. The ALS platform equipment supports further implementation of the logic diversity strategy. However, the overall logic diversity provided by an ALS platform-based system to include different algorithms requires application specifications to identify the different algorithms to produce further logic diversity.

Section 3.2.6)	The NRC staff determined the ALS platform provides some logic diversity and supports further logic diversity, because 1) the ALS platform provides Core Diversity that produces fundamentally different logic arrangements with corresponding differences in timing although the logic is derived from the same requirements, specifications, and code implementation, and 2) Embedded Design Diversity can produce additional differences in how a given algorithm is implemented even though both implementations are based on the same top-level requirements (see NUREG/CR-7007, Section 2.2.3.6). Nevertheless, this SE for the "ALS Topical Report" cannot make an overall determination regarding the adequacy of application-specific logic diversity, because the choice to require Embedded Design Diversity or alternative algorithm requirement specifications is application-specific and is not provided at the platform level.
7) Signal "ALS Diversity Analysis" "Signal Diversity" (see Reference 47, Section 3.2.5)	The ALS platform equipment supports implementation of the signal diversity strategy. However, any signal diversity provided by an ALS platform-based system would be based on application specifications. The NRC staff determined the ALS platform can support overall instrumentation architectures that include signal diversity implementing "different reactor or process parameters sensed by different physical effects," "different reactor or process parameters sensed by the same physical effect," and/or "the same reactor or process parameter sensed by a different redundant set of similar sensors" (see NUREG/CR-7007, Section 2.2.3.7). The NRC staff also determined the ALS platform itself does not provide signal diversity, because signal diversity requires specification of different signal inputs, which is application-specific and is not provided at the platform level. Therefore, this SE for the "ALS Topical Report" cannot make a determination regarding the adequacy of application-specific signal diversity.

To summarize Table 3.9-1 the ALS platform's diversity strategies in comparison to NUREG/CR-7007, the ALS platform provides a baseline of life-cycle diversity and logic diversity. However, the degree to which these approaches will be implemented depends on plant-specific vulnerabilities and resulting requirements and specifications. Furthermore, the ALS platform provides support for function diversity and signal diversity, both of which are application-specific and are not provided at the platform level (see Reference 47, Section 3.2.3 and 3.2.5). In contrast, the ALS platform approach does not address design, equipment manufacturer, or logic processing equipment diversity strategies.

In each NUREG/CR-7007 evaluation of industry approaches to diversity (Strategies A thru C), which have been evaluated to establish a technical basis for sufficient diversity, each is cited as having a reliance on function, life-cycle, logic, and signal diversity (see NUREG/CR-7007, Page xv):

For Strategy A – "… This choice of technology inherently contributes notable equipment manufacturer, processing equipment, *functional*, *life-cycle*, and *logic* diversities. Intentional application of *life-cycle* and equipment manufacturer diversities is included in the baseline, while the traditional use of *functional* and *signal* diversities is also adopted. …"

For Strategy B – "… This choice of technology inherently contributes some measure of equipment manufacturer, processing equipment, *functional*, *life-cycle*, and *logic* diversities. Intentional application of *life-cycle* and equipment manufacturer diversities is included in the baseline, while the traditional use of *functional* and *signal* diversities is also adopted. …"

For Strategy C – "…This choice of technology inherently contributes some limited degree of equipment manufacturer, *life-cycle*, and *logic* diversities. Intentional application of equipment manufacturer, logic processing equipment, *life-cycle*, and *logic* diversities is included in the baseline, while the traditional use of *functional* and *signal* diversities is also adopted. …"

BTP 7-19 notes functional diversity and signal diversity are considered to be particularly effective. These forms of diversity are not explicitly included within the ALS platform. However nothing in the "ALS Topical Report" or this SE precludes a plant from specifying either functional or signal diversity. Similarly, nothing precludes a plant from specifying other equipment in addition to the ALS platform-based systems to provide diversity beyond the ALS platform, such as design, equipment manufacturer, and logic processing equipment diversities. Nevertheless, the scope of this SE is limited to the diversity provided within the ALS platform. Given this limitation, the NRC staff has framed its assessment of ALS platform diversity similar to the preceding NUREG/CR-7007 extracts, as follows:

ALS Platform without Embedded Design Diversity – This approach inherently contributes little to no degree of design, equipment manufacturer, or logic processing equipment diversities. This approach inherently contributes some limited degree of *life-cycle* and *logic* diversities. This approach also supports the implementation of *functional* and *signal* diversities and a further increase in *logic* diversity. However, corresponding diversity requirements must be included within application specifications to achieve the increase.

ALS Platform with Embedded Design Diversity – This approach inherently contributes little to no degree of design, equipment manufacturer, or logic processing equipment diversities. The inclusion and configuration of Embedded Design Diversity is beyond the minimum platform scope, and if required, Embedded Design Diversity must be identified within application specifications. When included through specification, this approach inherently contributes some measure of *life-cycle* and *logic* diversities. This approach also supports the implementation of *functional* and *signal* diversities and a further increase in *logic* diversity. However, corresponding diversity requirements must be included within application specifications to achieve such an increase.

The platform manufacturer described ways that its design techniques and processes provide levels of defense against latent programming errors, some of which may result from the use of [ ] (see Reference 47, Section 3.3). In addition to the activities performed for the "ALS Topical Report," the platform manufacturer committed to perform a formal mathematical proof that the output of the synthesis and place & route of the FPGA logic equals the source code. This formal equivalency verification would use an independent tool to verify the synthesis and place & route transformations. The NRC staff reviewed the manufacturer's layer of defense analysis and agrees the techniques and processes, which the manufacturer has performed and to which the manufacturer has committed, provide mitigation against latent programming errors. Although the degree of mitigation provided through these techniques and processes is qualitative, the NRC staff agrees the methods and processes can be used as in future D3 analysis whenever the applicant or licensee specifies the techniques and processes for its application. The NRC staff also determined the baseline ALS platform approach to FPGA logic, which excludes the use of a microprocessor or software instructions, addresses a portion of the failure trajectory concerns discussed within NUREG/CR-7007.
Commercially supplied non-developmental FPGA intellectual property (IP) is identified for potential use in ALS platform FPGA designs (see Reference 47, Section 2.3.3) wherein certain FPGA design elements are characterized as "Simple IP," including, but not limited to, standard arithmetic operators (e.g., adder, multiplier, etc.) and standard logical operators (e.g., counters, decoders, multiplexers, etc.). Although the ALS platform prohibits use of FPGA design elements characterized as "Complex IP" (e.g., serial interfaces, bus interfaces and microprocessor cores, etc.) to support the determination that sufficient diversity has been implemented, the use of "Simple IP" may be common between boards, instruments, and design teams. Nevertheless, the use of "Simple IP," for which a commercial FPGA tool vendor is the design organization, represents a possible source of common-cause programming errors. In part, the ALS platform relies on wide use of "Simple IP" and testing as layers of defense to justify its use.

Under the ALS Topical Report scope, the ALS platform manufacturer has not performed the formal mathematical proof that the output of synthesis and place & route of the FPGA logic equals the source code. Although the ALS platform approach qualitatively discusses sources of common-cause programming errors and provides layers of defense against sources of common-cause programming errors, it falls short of providing an analysis that conclusively demonstrates the combination of different tools (design versus test), different personnel (design and test) and different design variants [ ] either eliminates all potential sources of common-cause programming errors or quantifies all remaining sources of common-cause programming errors to facilitate systematic mitigation of any resulting plant vulnerabilities.

Programming the FPGA requires [ ] the ALS-102 Core Logic Board FPGA devices are required to be application-specific. Post-programming testing efforts of the application-specific system are necessary to demonstrate the as-built ALS-102 Core Logic Board FPGA devices meet DI&C-ISG-02 Issue 5, "Common-Cause Failure (CCF) Applicability." However, these efforts do not fall under the ALS Topical Report scope.

The application-specific board configurations and application-specific logic within the ALS-102 Core Logic Board FPGA devices are beyond the “ALS Topical Report” scope, and this application-specific information, in part, defines equipment fail-safe behavior in response to detectable failures. Fail-safe equipment behavior is one method of providing internal design features to mitigate vulnerabilities to potential common-cause programming errors. However, appropriate use of these design features is based on application-level specifications. Furthermore, the “ALS Topical Report” has not included an analysis that demonstrates the coverage provided through continuous self-test functionality overlaps the entire safety function path for all future application-specific systems. Assuming the appropriate continuous self-test functionality is included by specification, a subsequent analysis could demonstrate sufficient V&V of continuous self testing has been performed and the set of continuous-self tests covers the entirety of each application-specific safety function path. This analysis could demonstrate the continued ability to perform the safety function when no faults have been annunciated, because the continuous self-tests themselves would have been developed based on unique and independent requirements from the application-specific safety functions and result in individual FPGA logic circuits that are separate from the FPGA safety function logic circuits. Regardless, such an approach still requires operators to periodically perform appropriate surveillance tests, which would need to be included within each plant’s technical specification, to verify the continuous self-test functions remain operable.

For D3 analysis, the “ALS Topical Report” includes application-specific licensee obligations within its matrix that maps DI&C-ISG-06 information requirements between topical report documentation and license amendment requests. Specifically, “Utility D3 Analysis” is identified under the “LAR” column to provide to address DI&C-ISG-06 D.6.2 information requirements. An applicant or licensee D3 analysis is required to evaluate compliance against BTP 7-19. This provision for a “Utility D3 Analysis” is consistent with the referenced precedent for the Wolf Creek MSFIS application of the initial ALS platform, which provided a D3 assessment (see Reference 3).

Wolf Creek’s D3 assessment did not address BTP 7-19 more broadly because of the limited scope of the MSFIS modification. Instead, the assessment limited its determination to the programmable portion of the ALS platform when reaching its conclusion of sufficient diversity, such that CCFs of the programming are adequately addressed for Wolf Creek’s MSFIS application. Therefore, the MSFIS ALS-based design meets the intent of the DI&C-ISG-02 Issue 5, “Common-Cause Failure (CCF) Applicability,” Staff Position 1. The NRC staff’s SE report for Wolf Creek’s MSFIS evaluated these diversity claims and concluded the ALS platform development process provided sufficient diversity within the programmable portion of the ALS platform, such that CCFs of programming are adequately addressed. This staff conclusion is based on the following: 1) a fundamental difference between an FPGA logic implementation and a microprocessor-based implementation, 2) an ability to directly confirm the resultant diversity from development process output products, 3) prior precedent, which approved equivalent diverse microprocessors with diverse operating software, and 4) the simplicity of the MSFIS (it is only a valve actuation system and is not a full trip or actuation system) (see Reference 2, Enclosure 2, Section 3.3.3).

When addressing IEEE Std 603-1991, Clause 6.2, Manual Control, the “ALS Topical Report” describes use of the ALS-302 Digital Input Board to implement manual actuations, including system-level actuations (see Reference 32, Section 12.1.18). This description states “Manual control applies as an application-specific system-level requirement, and is a function of the architecture of the system being replaced.” Regardless, use of the ALS platform with an ALS-302 Digital Input Board to implement manual actuations may be inconsistent with BTP 7-19 in consideration of DI&C-ISG-02 Issue 1, “Adequate Diversity,” and Issue 2, “Manual Operator Actions,” because 1) this type of configuration would not necessarily inject the manual control connection to the safety equipment at a point downstream of the plant's digital I&C safety system outputs, and 2) the NRC staff cannot determine whether the application will use independent and diverse equipment that is unaffected by the postulated common-cause failure for an RPS application. Implementation of manual actuations with the ALS-302 Digital Input Board requires use of ALS-302 board logic configured to meet application-specific needs, application-specific communications over the RAB, and application-specific logic within the ALS-102 Core Logic Board. Depending on the application, an implementation of manual actuations may also require further application-specific use of the RAB for communication with an output board. BTP 7-19 guidance states for system-level actuation at the lowest possible level in the safety system architecture, the controls may be connected either to discrete hardwired components or to simple (e.g., component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.

In recognition of BTP 7-19’s guidance to inject the manual control connection to the safety equipment at a point downstream of the plant's digital I&C safety system outputs, the NRC staff’s SE report for Wolf Creek’s MSFIS took into consideration that the manual valve control signals came directly from the operator control panel and provided only open or close signals for the valves. Both the signals provided by the operator control panel to the MSFIS and provided by the MSFIS to the valves are binary (on/off) signals rather than more complex digital data. This architectural arrangement of the system and its signal communications, in part, supported the NRC staff judgment that the MSFIS exhibited a low level of complexity. However, alternative architectural arrangements of ALS platform-based systems and the signal communications are possible, including use of an ALS-601 Communications Board to receive manual commands that are more complex digital data. Therefore, the NRC staff determined an evaluation against this BTP 7-19 guidance cannot be performed at the platform level.

Consistent with DI&C-ISG-02 Issue 7, “Single Failure,” the NRC staff’s SE report for Wolf Creek’s MSFIS does not consider remaining non-programmable portions of each board (e.g., analog portions, etc.), which do not have diversity because these portions are not subject to common-cause software or programming error. Diversity is not required for the non-programmable portions of each board, because design deficiencies and manufacturing errors are specifically exempted from consideration when conducting the single-failure analysis by IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," Clause 5.5, "Common-cause failures" (see Reference 2, Enclosure 2, Section 3.3.3).

The NRC staff's SE of D3 for the Wolf Creek's MSFIS concludes by stating any future uses of the ALS platform that are more complex than the MSFIS, such as for a system receiving sensor signals and making trip or actuation determinations, may require additional design diversity, and any future determination of adequate diversity based on meeting DI&C-ISG-02 Issue 5, "Common-Cause Failure (CCF) Applicability," Staff Position 1 will be based on the application-specific use of the ALS platform. Therefore, an application-specific D3 Assessment should be provided for each future use of the ALS platform.

Based on this evaluation, the NRC staff determined the ALS platform development and test approach provides logic and life-cycle diversity within the programmed FPGA functions. The NRC staff also determined the ALS platform's optional "Embedded Design Diversity" increases built-in diversity beyond that established for Wolf Creek's MSFIS. The NRC staff further determined the ALS platform supports application-specific functional diversity and signal diversity, which would result in additional logic diversity. Consistent with NUREG/CR-6303, NUREG/CR-7007, and the Wolf Creek MSFIS SE, the NRC staff determined licensees can use these diversity attributes in future system applications of the ALS platform for plant-specific evaluations to determine whether CCFs can be eliminated from consideration, because in the absence of 100 percent testing, elimination of CCFs from consideration is allowed by BTP 7-19 and DI&C-ISG-02 when sufficient diversity has been demonstrated by an applicant or licensee. The NRC staff has not determined platform concepts alone are sufficient to generically eliminate the need for either a diverse actuation system or a best estimate safety analysis, in part, because of the reliance on application specifications and manufacturer's commitments. Therefore, an applicant's or licensee's D3 analyses should be performed, when applicable. This D3 analysis should explicitly identify whether and how the ALS platform's "Embedded Design Diversity" is specified to be applied, identify any additional diversity strategies that the applicant or licensee includes in its design basis for ALS platform-based equipment, identify the specified use of any platform features (e.g., continuous self-tests, fail-safe behavior, surveillances, etc.) that provide mitigations against CCFs, and identify any other equipment that is diverse from the ALS platform that supports continued availability of a safety function. The applicant's or licensee's D3 analysis should either 1) demonstrate adequate diversity exists to mitigate plant vulnerabilities without the need for a diverse actuation system, or 2) determine the need for a diverse actuation system to provide adequate mitigation against plant vulnerabilities. Consistent with this determination, the NRC staff has created a plant-specific action item (see Section 4.2, Item 19), because important diversity strategies depend on the application specifications and the plant's overall I&C system architectures. This approach is consistent with both the BTP 7-19 and DI&C-ISG-02 guidance for an applicant or licensee to assess the D3 of the proposed I&C system to demonstrate plant vulnerabilities to common-cause failures have been adequately addressed. The NRC staff has also determined this plant-specific action is consistent with the "ALS Topical Report" mapping for the information covered under DI&C-ISG-06 D.6.2 to provide a "Utility D3 Analysis," and the functional and signal diversity dependency on the application as described within the "ALS Diversity Analysis." The NRC staff determined this plant-specific action is also consistent with the manufacturer's statements for compliance to IEEE Std 603-1991, Clause 6.2, "Manual Control", which states "Manual control applies as an application-specific system-level requirement, and is a function of the architecture of the system being replaced" (see Reference 32, Section 12.1.18).

3.10 Compliance to IEEE Std 603-1991

Equipment based on ALS platform components is intended for use in safety systems and other safety-related applications. Therefore, the platform topical report was evaluated against its ability to support the application-specific system provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." The NRC staff's evaluation is based on the guidance contained in SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," which provides acceptance criteria for this standard. This NRC staff evaluation also addresses the RG 1.153, "Criteria for Safety Systems," endorsement of IEEE Std 603-1991.

The following subsections contain the NRC staff's evaluation of the ALS platform against the clauses of IEEE Std 603-1991 with further consideration that the "ALS Topical Report" scope does not propose to meet all clauses via its components. For example, the ALS platform components do not address Clause 4.9, because an ALS-based safety system requires an application-specific reliability analysis and a system level Failure Modes and Effects Analyses (FMEA), which are application and system specific. For this case and similar ones, the following subsections evaluate the clause with a limited scope instead of providing a SE of the ALS platform against the full clause. Because the NRC staff evaluation is largely limited to a determination regarding whether the ALS platform supports meeting the various clauses of IEEE Std 603-1991, a single general plant-specific action item has been created to address full compliance to each IEEE Std 603-1991 clause, which applies to each plant-specific and application-specific use of the ALS platform (see Section 4.2, Item 20).

3.10.1 IEEE Std 603-1991 Section 4 – Safety System Designation

Section 4 of IEEE Std 603-1991 states a specific basis shall be established and documented for the design of each safety system of the nuclear power generating station. The individual clauses under Section 4 require identification and documentation of specific design basis information, which is characterized by the following:

- Clause 4.1 Design basis events of the generating station, including initial conditions and allowable limits for each
- Clause 4.2 Safety functions and corresponding protective actions for execute features for each design basis event
- Clause 4.3 Permissive conditions for each operating bypass capability
- Clause 4.4 Variables monitored to control and to ensure protective actions
- Clause 4.5 Minimum criteria for manual initiation of protective actions for execute features
- Clause 4.6 Minimum number and location of sensors for variables with special dependence
- Clause 4.7 Range of transient and steady state motive power, control power and environmental conditions
- Clause 4.8 Conditions with the potential to degrade safety system performance for which provisions are provided to retain safety functions

Clause 4.9 Methods appropriate for each safety system design, which are to be used to determine the reliability of the safety system design and any reliability goals imposed on it.
Clause 4.10 Critical points in time after the onset of a design basis event
Clause 4.11 Equipment protective provisions that prevent the safety systems from accomplishing safety functions
Clause 4.12 Any other special design basis such as diversity, interlocks, regulatory agency criteria, etc.

SRP Chapter 7, Appendix 7.1-C, Section 4, "Safety System Designation" provides acceptance criteria for these requirements.

The determination and documentation of the design basis for a safety system is an application-specific activity dependent on the plant design, and the "ALS Topical Report" acknowledges this (see Reference 32, Section 12.1.1). Therefore, the NRC staff did not evaluate of the ALS platform components against the regulatory requirements of Section 4 and instead performed a limited evaluation of the ALS platform's ability to support plant-specific and application-specific evaluations against Section 4 design basis information. This evaluation was limited to Section 4 design basis information that the platform directly supports.

Table 3.10-1 provides a cross-reference between clauses of IEEE Std 603-1991 Section 4 to sections within this SE. Each SE section identified in Table 3.10-1 contain corresponding plant-specific action items to demonstrate the plant and application-specific design basis for a safety system has been bounded within the scope of this SE. If the plant or application-specific design basis for a safety system has not been adequately bounded then additional evaluations should be performed as further plant-specific actions.

Table 3.10-1 Cross-reference of IEEE Std 603-1991 Section 4 and SE Sections

IEEE Std 603-1991 Section 4	**SE Section**
Clause 4.7	Section 3.3, Equipment Qualification
Clause 4.9	Section 3.6, Reliability and Availability Analysis
Clause 4.12	Section 3.9, Diversity and Defense-in-Depth

3.10.2 IEEE Std 603-1991 Section 5 – Safety System Criteria

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

3.10.2.1 IEEE Std 603-1991 Clause 5.1 – Single-Failure Criterion

Clause 5.1 of IEEE Std 603-1991 requires safety systems be able to perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. SRP Chapter 7, Appendix 7.1-C, Section 5.1, "Single Failure Criterion," provides acceptance criteria for the single failure criterion. In addition, RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," endorses IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," as providing an acceptable method for meeting this requirement.

As described in the "ALS Topical Report," the manufacturer has indicated applicants and licensees will implement a configuration of redundant and independent ALS platform components to meet the single failure criterion for any ALS platform-based safety system (see Reference 32, Section 12.1.2). Consequently, evaluation for full conformance against this portion of the acceptance criteria remains for the plant-specific review.

The NRC staff evaluation of the capabilities and characteristics of the ALS platform that are relevant to the Single-Failure Criterion are documented in Section 3.4.3, Self-Diagnostics, Test and Calibration Capabilities, and Section 3.5, Failure Mode and Effects Analysis. The Section 3.4.3 evaluation identifies plant-specific actions to demonstrate the application-specific use of ALS platform diagnostic, self test, and manually initiated test and calibration features are sufficient to verify the operational integrity of safety functions in a manner that supports meeting the Single-Failure Criterion. The Section 3.5 evaluation describes the board-level approach to identify Failure Modes and Effects in support of plant-specific and application-specific activities to be performed at the system level and should include an assessment of the complete system design. Section 3.5 also includes plant-specific actions to perform a system-level FMEA to demonstrate: 1) the application-specific use of the ALS platform identifies each potential failure mode and determines the effects of each; and 2) single-failures, including those with the potential to cause a nonsafety system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions.

3.10.2.2 IEEE Std 603-1991 Clause 5.2 – Completion of Protective Action

Clause 5.2 of IEEE Std 603-1991 states the safety systems shall be designed so, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion, and deliberate operator action shall be required to return the safety systems to normal. SRP Chapter 7, Appendix 7.1-C, Section 5.2, "Completion of Protective Action," provides acceptance criteria for this requirement.

The "ALS Topical Report" states the requirement to complete a protective action requires verification on an application-specific basis (see Reference 32, Section 12.1.3). Consequently,

evaluation for full conformance against this portion of the acceptance criteria remains for a plant-specific review.

Determination that protective actions of the execute features of a safety system continues to completion after initiation and requires a deliberate operator action thereafter to restore to normal are plant-specific and application-specific activities, and the topical report scope does not include specific applications to implement execute features for a specific safety system. Therefore, the evaluation against the requirements of IEEE Std 603-1991 Clause 5.2 is not addressed by this SE. Application-specific logic must be specified and programmed into the ALS-102 Core Logic Board and should be verified by plant-specific and application-specific activities.

3.10.2.3 IEEE Std 603-1991 Clause 5.3 – Quality

Clause 5.3 of IEEE Std 603-1991 states the components and modules within the safety system must be of a quality consistent with minimum maintenance requirements and low failure rates, and safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program. SRP Chapter 7, Appendix 7.1-C, Section 5.3, “Quality,” provides acceptance criteria for the quality requirement. This acceptance criteria states the QA provisions of 10 CFR Part 50, Appendix B, apply to a safety system.

GDC 1 states structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A QA program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

The regulation at 10 CFR 50.55a(a)(1), “Quality Standards,” requires that “structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.”

CSI developed the ALS platform, which consists of standardized circuit boards and FPGA programs, for use in nuclear power plants rather than dedicating pre-existing commercially available products. These development activities were performed following CSI’s quality assurance program (see Reference 27), and the quality assurance program had been subjected to a licensee audit for its effectiveness in implementing an acceptable ALS-based system in conformance with 10 CFR Part 50, Appendix B, and 10 CFR Part 21 for nuclear industry safety-related work. A licensee, Wolf Creek Nuclear Operating Corporation, accepted CSI’s ALS-based MSFIS, which established CSI as an Appendix B supplier to the Wolf Creek. Westinghouse later conducted a separate supplier audit to evaluate the effectiveness and proper implementation of an acceptable quality assurance program for the supply of I&C

hardware and engineering design services in support of nuclear safety-related work as it applies to 10 CFR Part 50, Appendix B, and 10 CFR Part 21 for the nuclear industry. The Westinghouse audit addressed changes to the quality assurance program since Wolf Creek's licensee audit and evaluated the supporting engineering processes to produce the ALS platform (see Reference 32, Sections 10 and 12.1.4). Pacific Gas & Electric subsequently performed a licensee audit of CSI to support its application of the ALS platform for Diablo Canyon.

During the ALS platform development, CSI began transitioning its quality assurance program to comport with the "Westinghouse Quality Management System." The change from the "9000-00311 Electronics Development Procedure" (Reference 28) and the "9000-00313 FPGA Development Procedure" (Reference 30) to the respective "NA 4.50 Electronics Development Procedure" (Reference 29) and "NA 4.51 FPGA Development Procedure" (Reference 31) provides an example of this transition. During the NRC staff's audit of the ALS platform, the NRC staff discussed this transition and documented the discussion in the "ALS Platform Audit Summary Report" (Reference 127). On February 15, 2013, CSI finalized the replacement of its QA Program Manual with the "Westinghouse Quality Management System" (see Reference 32, Section 10). From February 15, 2013 forward, CSI is committed to perform all ALS platform work in accordance with the "Westinghouse Quality Management System." Separate from this SE and by letter dated February 24, 2011, NRC staff concluded Revision 6 to the "Westinghouse Quality Management System" continues to meet the requirements of Appendix B to 10 CFR Part 50 and is therefore acceptable (see Reference 4). Although the transition to the "Westinghouse Quality Management System" completed after the majority of the ALS platform development had finished, 10 CFR Part 50, Appendix B, does not prohibit changes to quality assurance programs that continue to fulfill the regulatory requirements, and holds licensees responsible for vendor quality. Licensees typically use audits, which are distinct from NRC staff regulatory audits, to fulfill this responsibility.

Sections 3.2.2 and 3.2.3 of this SE provide the NRC staff 's evaluation of the manufacturer's development processes, wherein the NRC staff determined the ALS platform's hardware and FPGA logic program components have been designed and developed with a sufficiently high quality process and in a manner suitable for use in safety-related applications at nuclear power plants. Additionally, subsections below 3.11.2.3 of this SE provide additional NRC staff evaluations that address aspects of IEEE Std 7-4.3.2-2003, Clause 5.3, Quality, as applicable to the ALS platform's development and FPGA logic programs.

Based on the NRC staff's prior determination for CSI in support of the Wolf Creek MSFIS, the NRC staff's assessment that "Westinghouse Quality Management System" meets the requirements of Appendix B to 10 CFR Part 50, prior licensee audits, and the regulatory requirement that licensees remain responsible for vendor quality through performance of licensee audits for the ALS platform-based systems, the NRC staff concludes ALS platform components should be treated as basic components produced by an Appendix B supplier. The NRC staff determined conformance with IEEE Std 603-1991 Clause 5.3 remains an application-specific activity that should take into consideration the applicant's or licensee's Appendix B program and the activities of "inspection, installation, pre-operational testing, operation, and maintenance," because these activities are outside the "ALS Topical Report" scope and would occur at a licensed facility.

3.10.2.4 IEEE Std 603-1991 Clause 5.4 – Equipment Qualification

Clause 5.4 of IEEE Std 603-1991 states safety system equipment must be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate it will be capable of meeting the performance requirements as specified in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.4, "Equipment Qualification" provides acceptance criteria for IEEE Std 603-1991 Clause 5.4. This acceptance criteria states an applicant or licensee should confirm the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. This clause of IEEE Std 603-1991 also states qualification of Class 1E equipment be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980, "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations." RG 1.209 endorses and provides guidance for compliance with IEEE Std 323-2003 for qualification of safety-related computer-based I&C systems installed in mild environment locations.

The NRC staff evaluation of the ALS platform equipment qualification is documented in Section 3.3, Equipment Qualification. The Section 3.3 evaluation identifies plant-specific actions to demonstrate ALS platform performance, as bounded by its equipment qualification, meets the requirements of the plant-specific installation environment for the plant-specific and application-specific safety functions in accordance with the "ALS Topical Report" (see Reference 32, Section 12.1.5).

The NRC staff evaluation provided in Section 3.3 determined the ALS platform equipment qualification provided a type test and supporting analyses to establish documented platform safety functions, a range of installation conditions, and installation limitations for the ALS platform that are suitable for reference by applicants and licensees and conform to RG 1.209's endorsement of IEEE Std 323-2003 for qualification of safety-related computer-based I&C systems installed in mild environment locations. The NRC staff further determined the ALS platform equipment qualification meets IEEE Std 603-1991, Clause 5.4, for the plant-specific use of the seven standardized printed circuit cards, backplane, and chassis, which are included within the ALS platform scope, after a referencing applicant or licensee adequately addresses the plant-specific actions associated with confirming the application and installation have been bounded by the ALS platform equipment qualification, including each boundary/interface condition, installation limitation, and related application guidance.

3.10.2.5 IEEE Std 603-1991 Clause 5.5 – System Integrity

Clause 5.5 of IEEE Std 603-1991 states each safety system design must remain capable of accomplishing its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," provides acceptance criteria for system integrity. This guidance on acceptance criteria states the NRC staff should confirm tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady state conditions of both the energy supply and the environment. Furthermore, the NRC staff should

confirm tests show if the system does fail, it fails in a safe state. Also, the NRC staff should verify any failures detected by self-diagnostics specified to place a protective function into a safe state. Finally, confirmation that system real-time performance is adequate to ensure completion of protective action within critical time frames is identified as a special concern for digital computer-based systems.

The “ALS Topical Report” states application-specific system level requirements are necessary to define a safe state and the conditions required to enter a fail-safe state. As described in the “ALS Topical Report,” the manufacturer has indicated applicants and licensees will identify specific system level failure modes, methods of detection, and system responses and document these characteristics in an application-specific FMEA (see Reference 32, Section 12.1.6).

Therefore, the determination of system integrity is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address integrity characteristics to support fulfillment of this requirement by a system design based on the platform. The platform’s evaluation against this requirement is limited to consideration of the integrity demonstrated by the platform and its features to allow a safe state to be reached in the presence of failures, because the “ALS Topical Report” does not address a specific application or establish a definitive safety system design. Although the evaluation indicates the suitability of the platform to contribute to meeting this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.5.

As discussed in Section 3.3 of this SE, the ALS platform underwent equipment type testing to demonstrate qualification for installation in mild environment locations in nuclear power plants. Upon an applicant’s or licensee’s demonstration that the equipment’s boundary/interface conditions, installations limitations and application guidance, as discussed in Section 3.3 and delineated in Section 4.2 of this SE, have been addressed, the ALS platform qualification program provides reasonable assurance that safety systems based on the ALS platform will be capable of performing safety functions over the full range of environmental stressors defined by the qualification envelope for the ALS platform.

As described in Section 3.5 of this SE, the manufacturer performed a failure modes and effects analysis (FMEA) for each of the seven ALS platform standardized circuit boards. The NRC staff reviewed the FMEAs (References 56, 62, 68, 74, 80, 86, and 92) to confirm the platform design features provide capabilities that allow construction of a safety system with the ability to fail in a safe state. Nevertheless, an assessment of the application specifications for a full system design is necessary to demonstrate fulfillment of the requirement to fail in a safe state, when applicable.

The evaluation of response time and deterministic performance is discussed in Sections 3.4.1 and 3.4.2 of this SE. The ALS platform demonstrates credible response time characteristics and supports definition and demonstration of minimum and maximum response time performance to meet safety system performance and determinism requirements. Therefore, the ALS platform’s response time and determinism meet the criteria of this clause at the platform level and are suitable to support safety applications. The actual response times for particular safety functions are application-specific, and acceptable performance depends on the overall

system design, architecture and required plant safety functions. Therefore, a plant-specific action item is identified to confirm suitability of the response time characteristics of the ALS platform for a particular safety function implementation and to demonstrate acceptable relevant response times. Consequently, evaluation for full conformance against this portion of the acceptance criteria remains for a plant-specific review.

Based on the review items discussed above, the NRC staff concludes the integrity characteristics (e.g., response time, deterministic performance, failure detection and response, fault tolerance, environmental withstand) of the ALS platform, when appropriately implemented for a plant-specific application, are suitable for safety applications at nuclear power plants and meet Clause 5.5 at the platform level.

3.10.2.6 IEEE Std 603-1991 Clause 5.6 – Independence

Clause 5.6 of IEEE Std 603-1991 requires in part independence between: (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence" provides acceptance criteria for system integrity. The acceptance criteria state three aspects of independence: (1) physical independence, (2) electrical independence, and (3) communications independence, should be addressed for each of the previously listed cases. Guidance for evaluation of physical and electrical independence is provided in RG 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems," which endorses IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the use of separate power sources. Transmission of signals between independent channels should be through isolation devices.

SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence," provides additional acceptance criteria for communications independence. Section 5.6 states where data communication exists between different portions of a safety system, the analysis should confirm a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and if a digital computer system used in a safety system is connected to a digital computer system used in a nonsafety system, a logical or software malfunction of the nonsafety system must not be able to affect the functions of the safety system.

SRP Chapter 7, BTP 7-11, "Guidance on Application and Qualification of Isolation Devices," provides guidelines for reviewing the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and non-safety systems.

The "ALS Topical Report" states specific redundancy needed for an ALS-based system is intended to be defined at the system level during the actual plant implementation (see Reference 32, Section 12.1.7). Therefore, the determination of independence is an application-specific activity that requires an assessment of a full system design. A platform-level

assessment can only address independence characteristics to support fulfillment of this requirement by a system design based on the platform. The platform's evaluation against this requirement is limited to consideration of the digital communications evaluated in Section 3.7 of this SE, because the "ALS Topical Report" does not address a specific application or establish a definitive safety system design. Although the evaluation indicates the suitability of the platform to contribute to meeting this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.6.

Although the ALS platform supports the use of unique components within different redundant portions of a safety system, application-specific activities should assess the full system design to ensure different redundant portions of a safety system do not rely on a common component. This assessment should provide reasonable assurance that the safety system will retain the capability to accomplish the safety function due to the loss or failure of any common component.

Although the ALS platform supports an installation that physically separates redundant portions of safety equipment from one another and that physically separates the safety system from other equipment, application-specific activities should assess the full system design and installation to ensure adequate separation and physical barriers exist between different redundant portions of a safety system and between the safety system and other equipment. This assessment should provide reasonable assurance that the safety system will retain the capability to accomplish the safety function in the presence of any single-failure and in the presence of each design basis event, including its environmental affects.

Although the ALS platform supports an installation that provides separate and independent electrical power sources to redundant portions of safety equipment, application-specific activities should assess the full system design and power distribution architecture to ensure independent electrical power sources are provided to redundant portions of safety equipment. This assessment should provide reasonable assurance that the safety system will retain the capability to accomplish the safety function in the presence of any single loss of an electrical power source.

The isolation provided on ALS platform circuit boards is limited to that which is required for electromagnetic compatibility and circuit reliability. However, the board level provisions are not intended to ensure sufficient isolation exists between the ALS platform-based Class 1E equipment and Non-1E equipment. The "ALS Topical Report" scope excludes explicit identification of the method to ensure sufficient isolation exists between the ALS platform-based Class 1E equipment and Non-1E equipment. The "ALS Topical Report" states the

demonstration that this isolation criterion is met will be performed as part of a plant-specific application and qualified isolation devices will be used when required by the application (see Reference 32, Sections 2.5.7, 5, and 12.1.7.3). As such, a plant-specific action item results from this exclusion (see Section 4.2, Item 21).

The NRC staff determined conformance with IEEE Std 603-1991 Clause 5.6 remains an application-specific activity that should take into consideration the full system design, any use of a shared component, the equipment's installation, and the power distribution architecture. When considering the use of a shared component or the power distribution architecture, the

application-specific activities of the full system design should take into further consideration the digital communications evaluation in Section 3.7 of this SE and the requirement to include isolation devices, because the isolation device requirement has been excluded from the "ALS Topical Report" scope.

3.10.2.6.1 IEEE Std 603-1991 Clause 5.6.1 – Independence between Redundant Portions of a Safety System

The "ALS Topical Report" states specific redundancy needed for an ALS system is intended to be defined at the system level during the actual plant implementation to accomplish the safety function during and following any design basis event requiring that safety function. As described in the "ALS Topical Report," the manufacturer has indicated applicants and licensees will establish requirements for any communications between otherwise redundant portions of a safety system, any use of common components among redundant portions of a safety system, the maintenance of physical separation between redundant portions of safety systems and between safety system and other equipment, and the maintenance of electrical independence between redundant portions of a safety system (see Reference 32, Sections 12.1.7 and 12.1.7.1).

Based on the use described for the ALS platform and the design features provided by its standardized circuit boards, the NRC staff determined the ALS platform supports the use of unique components within different redundant portions of a safety system, so a safety system can be constructed with independent and physically separate redundant portions capable of accomplishing the safety function during plant-specific design basis events that require that safety function.

3.10.2.6.2 IEEE Std 603-1991 Clause 5.6.2 – Independence between Safety Systems and Effects of Design Basis Event

The "ALS Topical Report" states the ALS platform is intended for installation in a mild environment (see Reference 32, Sections 4 and 12.1.7.2). Section 50.49(c) of 10 CFR Part 50 defines a mild environment as one "that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences." The ALS platform was qualified to establish the bounding envelope for its installed operating environment, and this equipment qualification is discussed and evaluated in Section 3.3 of this SE.

Based on the installation of ALS platform equipment in a mild environment that is bounded by the equipment qualification discussed and evaluated in Section 3.3 of this SE, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.6.2.

3.10.2.6.3 IEEE Std 603-1991 Clause 5.6.3 – Independence between Safety Systems and Other Systems

Evaluation of this Clause requires identification of credible failures in and consequential actions by other systems as documented in the applicant's or licensee's plant-specific design basis. The ALS platform provides digital communication design features to support independence

between an ALS-based safety system and other interfacing systems, which are discussed and evaluated in Section 3.7 of this SE. The ALS platform also supports classification of interconnected equipment. However, demonstration that adequately qualified isolation devices have been used where required should be performed as part of the plant-specific application of the ALS platform. Therefore, no additional staff determinations are appropriate for the ALS platform to address IEEE Std 603-1991 Clause 5.6.3.

3.10.2.7 IEEE Std 603-1991 Clause 5.7 – Capability for Test and Calibration

The "ALS Topical Report" does not address a specific application or establish a definitive safety system design. Determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements (e.g., accuracy, response time, etc.) that apply. The establishment of the types of surveillance necessary for the safety system to ensure detection of identifiable single failures only revealed through testing is also an application-specific activity. For these reasons, this SE is limited to consideration of the means provided within the platform to enable testing and calibration for a redundant portion of a safety system (i.e., a channel). Section 3.4.3 of this SE discusses the ALS platform's ability to support meeting IEEE Std 603-1991 Clause 5.7, and identifies plant-specific actions to ensure IEEE Std 603-1991 Clause 5.7 will be met.

3.10.2.8 IEEE Std 603-1991 Clause 5.8 – Information Displays

The following four subclauses of Clause 5.8 of IEEE Std 603-1991 apply to Information Displays associated with safety systems.

3.10.2.8.1 IEEE Std 603-1991 Clause 5.8.1 – Displays for Manually Controlled Actions

Clause 5.8.1 of IEEE Std 603-1991 requires unambiguous display instrumentation to be part of safety systems and to minimize the possibility of operator confusion wherever manually controlled actions are required for a safety system to accomplish its safety function and no automatic control is provided.

The "ALS Topical Report" states display instrumentation provided for manually controlled safety actions is an application-specific system level requirement and the ALS platform does not include display instrumentation for manually controlled actions. The "ALS Topical Report" then goes on to discuss the ALS platform standardized circuit board capabilities to receive manual demand signals, perform the required safety actions, and drive analog or digital displays associated with the manually controlled action (see Reference 32, Section 12.1.9.1).

The NRC staff's review of the design features provided by ALS platform standardized circuit boards is addressed in Section 3.1 of this SE.

Although the ALS platform does not include display instrumentation or directly display information beyond discrete front panel status indicators, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.8.1. This determination is based on the use described for the ALS platform and the design features provided by its standardized circuit boards. Nevertheless, a plant-specific action is necessary when the ALS platform supports use

of display instrumentation that is provided to support manually controlled safety actions necessary to accomplish a safety function for which no automatic control is provided. This plant-specific action should ensure the supporting ALS components and display instrumentation will be functional during plant conditions under which manual actions may be necessary.

3.10.2.8.2 IEEE Std 603-1991 Clause 5.8.2 – System Status Indication

Clause 5.8.2 of IEEE Std 603-1991 requires unambiguous display instrumentation, which need not be part of the safety system, to minimize the possibility of operator confusion and to provide accurate, complete, and timely information pertinent to a safety system's status, including indication and identification of protective actions.

The "ALS Topical Report" states display instrumentation provided for safety systems' status is an application-specific system level requirement and the ALS platform does not include remote display instrumentation for safety systems' status. The "ALS Topical Report" then goes on to discuss the ALS platform standardized circuit board capabilities to perform the protective actions and provide status both locally via discrete front panel indicators and remotely to display instrumentation (see Reference 32, Section 12.1.9.2).

The NRC staff's review of each ALS platform standardized circuit board's design features is addressed in Section 3.1 of this SE.

Although the ALS platform does not include display instrumentation or directly display information beyond discrete front panel status indicators, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.8.2. This determination is based on the use described for the ALS platform and the design features provided by its standardized circuit boards. Nevertheless, a plant-specific action is necessary when the ALS platform supports use of display instrumentation to provide indication and identification of protective actions as part of a safety system's status. This plant-specific action should ensure the supporting ALS components and the display instrumentation provide unambiguous, accurate, complete and timely status of safety system protective actions.

3.10.2.8.3 IEEE Std 603-1991 Clause 5.8.3 – Indication of Bypasses

Clause 5.8.3 of IEEE Std 603-1991 requires display instrumentation in the control room, which need not be part of the safety system, continue to indicate whether the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperable (excluding an operating bypass) for each affected safety group. Indicated bypasses are required to be automatically actuated if the bypass or inoperable condition will occur more frequently than once a year and when the affected system is required to be operable. The control room shall provide the capability to manually activate the bypass indication.

The "ALS Topical Report" states display instrumentation provided for safety systems' status is an application-specific system level requirement and the ALS platform does not include remote display instrumentation for safety systems' status. The "ALS Topical Report" then goes on to discuss the ALS platform standardized circuit board capabilities to provide indication of bypass for plant and application-specific protective actions and provide indication of bypass both locally

via discrete front panel indicators and remotely to display instrumentation. The ALS platform supports the automatic actuation of the bypass or inoperable condition of a safety group when the maintenance workstation 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 (see Reference 32, Section 12.1.9.3). The "ALS Topical Report" describes the ALS platform's maintenance features, which address the behavior of bypass and inoperable status indications (see Reference 32, Section 3).

The NRC staff's review of the design features provided by ALS platform standardized circuit boards is addressed in Section 3.1 of this SE. The NRC staff reviewed the features and intended operation in support of safety system bypass and inoperable status indications for conformance with the guidance of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

Although the ALS platform does not include display instrumentation or directly display information beyond discrete front panel status indicators, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.8.3. This determination is based on the use described for the ALS platform and the design features provided by its standardized circuit boards. Nevertheless, a plant-specific action is necessary when the ALS platform supports use of display instrumentation to provide indication of bypassed or inoperable protective actions. This plant-specific action should ensure the supporting ALS components and the display instrumentation automatically actuate the bypass indication for bypassed or inoperable conditions, when required, and provide the capability to manually activate the bypass indication from within the control room.

3.10.2.8.4 IEEE Std 603-1991 Clause 5.8.4 – Location

Clause 5.8.4 of IEEE Std 603-1991 requires information displays be located accessible to the operator and be visible from the location of the controls used to effect manually controlled protective actions.

The "ALS Topical Report" states location of displays is an application-specific system level requirement and the ALS platform does not include remote display instrumentation (see Reference 32, Section 12.1.9.4). The "ALS Topical Report" also discusses the ALS platform standardized circuit board capabilities to locally monitor protective action states via discrete front panel indicators and initiate manually controlled protective actions via front panel toggle switches.

The NRC staff's review of the design features provided by ALS platform standardized circuit boards is address in Section 3.1 of this SE.

The NRC staff agrees evaluation of this clause is plant-specific and application-specific. Therefore, no NRC staff determinations are appropriate for the ALS platform to address IEEE Std 603-1991 Clause 5.8.4. A plant-specific action is necessary to ensure 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 an ALS-based system.

3.10.2.9 IEEE Std 603-1991 Clause 5.9 – Control of Access

Clause 5.9 of IEEE Std 603-1991 requires the capability to administratively control access to safety system equipment via supporting provisions within the safety systems and/or the generating station design.

The “ALS Topical Report” does not address a specific application or establish a definitive safety system design and acknowledges the location of safety related equipment within the generating station is a plant-specific implementation issue. Nevertheless, the “ALS Topical Report” describes provisions intended for any ALS-based safety system. The “ALS Topical Report” states physical access to the ALS platform equipment can be controlled via locked cabinet doors that generate an alarm if opened (see Reference 32, Section 12.1.10). Although the ALS platform excludes the cabinet from its scope, the “ALS Topical Report” describes a typical cabinet installation (see Reference 32, Sections 1.2 and 2.6.1). The typical cabinet 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 Maintenance Workstation. Furthermore, access to modify the ALS platform FPGA logic is not available to the applicant or licensee and all changes to the FPGA logic are to be performed by CSI within its secure development environment and under the Westinghouse quality assurance program.

The NRC staff’s review of the design features provided by ALS platform standardized circuit boards is addressed in Section 3.1 of this SE. These design features support administrative controls of the access to an ALS-based safety system through mechanical key locks and alarms that are automatically generated when the equipment is accessed.

The “ALS Topical Report” does not address a specific application or establish a definitive safety system design. Additionally, the location of safety related equipment within the generating station is a plant-specific implementation issue. However, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.9. This determination is based on the use described for the ALS platform and the design features provided by its standardized circuit boards. A plant-specific action is still necessary when the ALS platform is solely relied upon to meet to IEEE Std 603-1991 Clause 5.9 administrative controls. For safety system equipment, this plant-specific action should ensure the application system V&V activities demonstrate the implementation of integral key locks on cabinet door handles, and alarms upon cabinet access via the cabinet door or upon any digital data communication access such as by the Maintenance Workstation.

3.10.2.10 IEEE Std 603-1991 Clause 5.10 – Repair

Clause 5.10 of IEEE Std 603-1991 requires safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

The “ALS Topical Report” describes the continuously performed ALS platform diagnostics and application diagnostics, which are designed to facilitate timely recognition and identification of malfunctioning equipment. However, the “ALS Topical Report” does not address a specific application or its application diagnostics. Therefore, the scope of the “ALS Topical Report” is limited to the troubleshooting and replacement of the standardized circuit boards at the board level only (sees Reference 32, Section 12.1.11). The “ALS Topical Report” also describes board features to remove and reinstall boards into the chassis without requiring the removal of power (see Reference 32, Sections 2.5.5, and 2.9), which directly supports timely repair.

The NRC staff’s review of the design features provided by ALS platform standardized circuit boards and their instrument chassis is addressed in Section 3.1 of this SE. The NRC staff’s review of the ALS platform self-diagnostics, test, and calibration capabilities is addressed in Section 3.4.3 of this SE.

Because the “ALS Topical Report” does not address a specific application or its application diagnostics, this SE does not assess the report against the regulatory positions contained in RG 1.22, “Periodic Testing of Protection Actuation Functions,” or RG 1.118, “Periodic Testing of Electric Power and Protection Systems.” Furthermore, because the ALS platform FMEA informs an application-specific system level FMEA, this SE address failures detected by hardware, software, and surveillance testing to ensure the board-level FMEAs are consistent with the assumed failure detection of an application-specific single-failure analysis and FMEA.

Although the “ALS Topical Report” does not address a specific application or establish a definitive safety system design, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.10. This determination is based on the use described for the ALS platform and the design features provided by its standardized circuit boards. Nevertheless, a plant-specific action is necessary to ensure IEEE Std 603-1991 Clause 5.10 is met. This plant-specific action item should address applicable provisions of RG 1.22 and RG 1.118 and ensure the failures detected by hardware, FPGA logic, and surveillance testing are consistent with the assumed failure detection of the application’s single-failure analysis and FMEA.

3.10.2.11 IEEE Std 603-1991 Clause 5.11 – Identification

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

The “ALS Topical Report” states when the ALS platform is used in instrumentation retrofits, the safety group identification, which uses cabinet name plates and color-coded wiring, will not change from the existing approach in the plant. An ALS platform cabinet will include unique cabinet/division identifying nameplates on each cabinet’s exterior as required by generating station procedures. Within the cabinet, each ALS chassis is labeled with a unique identification and each installed ALS board provides a unique identification, including the board type, via its front panel plate (see Reference 32, Section 12.1.12). The “ALS Platform Requirements

Specification" includes identification requirements for ALS platform components (see Reference 43, PR0440 and PR0590).

Because the "ALS Topical Report" states plant-specific labeling requirements are specified by the applicant or licensee, this SE does not include a full evaluation against IEEE Std 603-1991 Clause 5.11.

Although the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Clause 5.11, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.11. This determination is based on the use described for the ALS platform, the identification features provided by its standardized circuit boards, and the ability for the ALS platform to accommodate plant-specific labeling requirements. Nevertheless, a plant-specific action is necessary to ensure IEEE Std 603-1991 Clause 5.11 is met.

3.10.2.12 IEEE Std 603-1991 Clause 5.12 – Auxiliary Features

Clause 5.12 of IEEE Std 603-1991 requires auxiliary supporting features, which are systems or components that provide services (such as cooling, lubrication, and energy supply) required for the safety systems to accomplish their safety functions, to meet all requirements of the standard. Clause 5.12 of IEEE Std 603-1991 also requires other auxiliary features that are not required for safety functions but are part of a safety system by association to be designed to

meet the criteria necessary to ensure these components, equipment, and systems do not degrade the safety systems below an acceptable level.

The "ALS Topical Report" does not address a specific application or establish a definitive safety system design for the ALS platform to provide an auxiliary supporting feature or some other auxiliary feature that is part of the safety system by association (see Reference 32, Section 12.1.13).

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

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

3.10.2.13 IEEE Std 603-1991 Clause 5.13 – Multi-Unit Stations

Clause 5.13 of IEEE Std 603-1991 permits the sharing of structures, systems, and components between units at multi-unit generating stations provided that the ability to simultaneously perform safety functions in all units is not impaired. Clause 5.13 of IEEE Std 603-1991 also provides guidance on the sharing of electrical power between units and application of the single failure criterion to shared systems.

The "ALS Topical Report" states the applicability of this clause will be evaluated on a plant-specific basis (see Reference 32, Section 12.1.14).

The NRC staff agrees evaluation of this clause is plant-specific and application-specific. Therefore, no staff determinations are appropriate for the ALS platform to address IEEE Std 603-1991 Clause 5.13. Nevertheless, a plant-specific action is necessary to ensure Clause 5.13 is met whenever an ALS-based system or an ALS platform component is shared between units at multi-unit generating station.

3.10.2.14 IEEE Std 603-1991 Clause 5.14 – Human Factors Considerations

Clause 5.13 of IEEE Std 603-1991 requires human factors considerations at the initial stages and throughout the design process to assure any functions allocated in whole or in part to

human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals.

The "ALS Topical Report" describes human factors considerations which were applied initially throughout the ALS platform development process. The "ALS Topical Report" states the ALS platform design considerations indicate compliance with relevant human factors guidance (see Reference 32, Sections 2.9 and 12.1.15).

The "ALS Topical Report" does not address a specific application or establish a definitive safety system. Furthermore, safety system design goals are established on a plant and application-specific basis. As such, no specific safety functions have been allocated in whole or in part to human operator(s) and maintainer(s) at a specific generating station.

The NRC staff's review of the design features provided by ALS platform standardized circuit boards and their instrument chassis is addressed in Section 3.1 of this SE. The NRC staff's review of the ALS platform self-diagnostics and test and calibration capabilities is addressed in Section 3.4.3 of this SE.

Although the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Clause 5.14, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.14. This determination is based on the use described for the ALS platform and the evaluation of the platform's design features. Nevertheless, a plant-specific action is necessary to ensure IEEE Std 603-1991 Clause 5.14 is met based on the application of the ALS platform and an evaluation of any functions allocated in whole or in part to human operator(s) and maintainer(s) to assure these functions can be successfully accomplished to meet safety system design

goals. This evaluation should be consistent with the applicant's or licensee's commitments documented in Chapter 18 of the plant's safety analysis report, as updated (UFSAR).

3.10.2.15 IEEE Std 603-1991 Clause 5.15 – Reliability

Clause 5.15 of IEEE Std 603-1991 requires appropriate analysis of system designs to confirm any established reliability goals, either quantitative or qualitative, have been met.

The NRC staff's evaluation of reliability establishes the applicant or licensee should justify the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. Furthermore, for computer systems this analysis should address both hardware and software reliability, as applicable.

The "ALS Topical Report" relies on the individual board documents in Table 3.5-1 to provide the information for each individual standardized circuit board reliability calculation. Each board's reliability analysis includes individual hardware component failures and excludes consideration of software failures because the FPGA-based ALS platform standardized circuit boards do not contain traditional software. The "ALS Topical Report" describes these reliability calculations as providing a Mean Time Between Failure (MTBF) prediction with the goal of not requiring

surveillance tests at an interval more frequent than once every 92 days and with the objective of allowing a licensee to pursue a Technical Specification change for less frequent surveillances after some period of an ALS-based system's operation that successfully demonstrates its sufficiently low failure rate (see Reference 32, Sections 7 and 12.1.16). The "ALS Platform Requirements Specification" includes a calculated reliability specification of MTBF for individual standardized circuit boards (see Reference 43, PR1101).

The "ALS Topical Report" does not provide specific configuration details for any application to establish a definitive safety system configuration. Furthermore, safety system reliability goals are established on a plant-specific and application-specific basis. As described in the reliability analyses, the predicted MTBF for a safety function depends on the application-specific logic and the number and arrangement of ALS components, which includes its standardized circuit boards and other peripherals. Because the application-specific logic development and the number and arrangement of ALS components will be plant and application-specific, the reliability of a plant safety function cannot be predicted based solely on the ALS standardized circuit board reliability analyses. Nevertheless, the reliability analyses of the standardized circuit boards support reliability predictions of ALS-based safety systems.

The NRC staff's review of ALS platform reliability is addressed Section 3.6 of this SE. This review identifies a plant-specific action item.

The NRC staff determined the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Clause 5.15. However, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 5.15 based on the standardized circuit board reliability predictions and the adequate closure of the plant-specific action item identified in Section 3.6 of this SE.

3.10.3 IEEE Std 603-1991 Section 6 – Sense and Command Features - Functional and Design Requirements

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

3.10.3.1 IEEE Std 603-1991 Clause 6.1 – Automatic Control

Clause 6.1 of IEEE Std 603-1991 requires for each design basis event, all protective actions should automatically initiate without operator action, except as justified in Clause 4.5 of IEEE Std 603-1991. SRP Chapter 7, Appendix 7.1-C, Section 6.1, "Automatic Controls," provides

acceptance criteria for Clause 6.1. The acceptance criterion states the automatic initiation should be precise and reliable, and the evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. Section 6.1 also states SRP BTP 7-12 discusses considerations for the review of the process for establishing instrument setpoints. In part, these acceptance criteria contribute to the demonstration that a safety system meets Appendix A to 10 CFR Part 50, GDC 13, “Instrumentation and Control,” and RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” when applicable.

The “ALS Topical Report” does not address a specific application or establish a definitive safety system, which is necessary to define the extent that setpoints, margins, errors, and response times are factored into a plant’s safety analysis or associated with IEEE Std 603-1991 Clause 4.5 (see Reference 32, Sections 2.8 and 12.1.17). Per SRP Chapter 7, Appendix 7.1-C, Section 6.1, applicant or licensee analyses should confirm the safety system has been qualified to demonstrate performance requirements are met.

The NRC staff’s review of the design features provided by ALS platform standardized circuit boards and their instrument chassis is addressed in Section 3.1 of this SE. The NRC staff’s review of the ALS platform’s response time characteristics is addressed Sections 3.4.1 and 3.4.2.1 of this SE. The NRC staff’s review of self-diagnostics and test and calibration capabilities provided by the ALS platform is addressed in Section 3.4.3 of this SE. The NRC staff’s review of ALS platform reliability is addressed Section 3.6 of this SE. The NRC staff’s review of the approaches to build diversity into an ALS-based system is addressed in Section 3.9 of this SE.

The NRC staff's evaluation of precision of the safety system with regard to the degree that setpoints, margins, errors, and response times are factored into the analysis is addressed in Section 3.10.3.8 of this SE, which discusses setpoints.

Although the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Clause 6.1, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 6.1. This determination is based on the platform design features, deterministic performance characteristics, reliability calculations, methods to build-in diversity, and adequate closure of the associated plant-specific action items. Nevertheless, a plant-specific action is necessary when the ALS platform provides safety system sense and command features that include automatic control. This plant-specific action should ensure Clause 6.1 is met, and this action should include applicant or licensee analyses to confirm the safety system has been qualified to demonstrate specified performance requirements have been met.

3.10.3.2 IEEE Std 603-1991 Clause 6.2 – Manual Control

Clause 6.2 of IEEE Std 603-1991 contains three subclauses related to the availability of manual controls in the control room. Clause 6.2.1 requires the control room provide a means to manually initiate protective actions at the division level of automatically initiated protective actions, such that the number of discrete operator manipulations and operated equipment is

minimized while the independence between redundant portions of a safety system per IEEE Std 603-1991 Clause 5.6.1 is preserved. Clause 6.2.2 requires the control room provide a means to manually initiate the protective actions that were not selected for automatic control along with the associated information displays. Clause 6.2.3 requires the control room provide a means to perform manual actions necessary to maintain safe conditions after the protective actions are completed along with the associated information displays in sufficient quantities and locations to support surveillance and action by the number of available qualified operators.

SRP Chapter 7, Appendix 7.1 C, Section 6.2, "Manual Control," provides acceptance criteria for IEEE Std 603-1991 Clause 6.2. This acceptance criteria states features for manual initiation of protective action should conform to RG 1.62, "Manual Initiation of Protection Action," and should be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary.

The "ALS Topical Report" does not address a specific application, establish a definitive safety system, or locate manual controls and displays within a plant-specific control room. The "ALS Topical Report" scope also excludes information displays. The "ALS Topical Report" states manual control applies as an application specific system level requirement, which may also be a function of the architecture of any system being replaced by an ALS-based system. Nevertheless, the ALS platform has been qualified for use in a mild environment that is consistent with installation in a control room, and the ALS platform standardized circuit boards provide features that support the implementation of manual controls and connectivity to information displays (see Reference 32, Section 12.1.18).

RG 1.62 includes BTP 7-19 Point 4, which applies to the set of displays and controls located in the main control room to provide manual system-level actuation of critical safety functions and

for monitoring of parameters that support safety functions. BTP 7-19 states these displays and controls should be independent and diverse from any digital protection system with common-cause failure vulnerabilities that could disable a safety function. As such, safety equipment manual controls should be connected downstream of the plant's digital I&C safety system outputs where these manual control connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. These manual controls may be connected either to discrete hardwired components or to simple, dedicated, and diverse digital equipment that performs the coordinated actuation logic. RG 1.62 allows a single safety-related means of manual initiation of protective actions to meet BTP 7-19 Point 4 system-level actuation of critical safety functions and IEEE Std 603-1991 Clause 6.2 division level actuation of automatically initiated protective actions. In accordance with DI&C-ISG-02's modification to BTP 7-19 Point 4, where the displays and controls provide backup capabilities, the displays and controls should also be able to function downstream of the lowest-level software-based components subject to the same common-cause failure that necessitated the diverse backup system.

The NRC staff's review of the design features provided by ALS platform standardized circuit boards and their instrument chassis is addressed in Section 3.1 of this SE. The NRC staff's

review of the approaches to build diversity into an ALS-based system is addressed in Section 3.9 of this SE.

Although the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Clause 6.2, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 6.2. This determination is based on the platform design features and methods to build-in diversity. Nevertheless, a plant-specific action is necessary when the ALS platform provides safety system sense and command features that include manual control. This plant-specific action should ensure Clause 6.2 is met and also addresses RG 1.62 and BTP 7-19 Point 4.

3.10.3.3 IEEE Std 603-1991 Clause 6.3 – Interaction Between the Sense and Command Features and Other Systems

Clause 6.3 of IEEE Std 603-1991 contains two subclauses related to the diversity and defense-in-depth of protective actions. Clause 6.3.1 of IEEE Std 603-1991 contains a requirement to mitigate the consequences of a credible event (and its direct and indirect consequences) that is an initiator of a nonsafety system action resulting in a condition requiring protective action while concurrently preventing the protective actions from being performed by the channels designated as providing principal protection against the resulting condition. Two alternatives to fulfill the requirement are specified. The first alternative is channels not subject to failure from the same single credible event shall be provided to limit the consequences of this event to a value specified by the design basis using either one or a combination of both of the following options: 1) provide alternate channels that sense a set of different variables from the principal channels, 2) provide alternate channels that use equipment different from that of the principal channel to sense the same variable. The second alternative is equipment not subject to failure from the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design basis, where this equipment is not considered a part of the safety system. Clause 6.3.2 of IEEE Std 603-1991 requires and identifies three provisions that will

allow Clause 6.3.1 to remain met during the maintenance bypass of a channel. These provisions are: 1) reducing the required coincidence, 2) defeating the nonsafety system signals taken from the redundant channels, or 3) initiating a protective action from the bypassed channel.

The “ALS Topical Report” states ALS platform has the capability to be configured in a manner that meets IEEE Std 603-1991 Clause 6.3. However, the “ALS Topical Report” does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. As such, the “ALS Topical Report” also states conformance to IEEE Std 603-1991 Clause 6.3 will be addressed during a plant-specific implementation (see Reference 32, Section 12.1.19).

Within the first alternative provided in Clause 6.3.1, the specified differences between the alternate channels and the principal channels correspond to diversity attributes discussed in Section 3.9 of this SE. The second alternative would provide an automatic diverse backup system, as discussed in DI&C-ISG-02, to provide the diverse means discussed in BTP 7-19

Point 3. The NRC staff’s review of the approaches to build diversity into an ALS-based system is addressed in Section 3.9 of this SE. The NRC staff’s review of the design features provided by ALS platform standardized circuit boards and their instrument chassis is addressed in Section 3.1 of this SE.

Although the “ALS Topical Report” cannot fully address IEEE Std 603-1991 Clause 6.3, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 6.3 through the implementation of either principal channels, alternate channels, or a diverse backup system. This determination is based on the built-in diversity options, platform design features to implement coincidence logic, and maintenance features to either bypass or trip channels. Nevertheless, a plant-specific action is necessary when the ALS platform provides sense and command features for principal protection against the resulting condition of a nonsafety system action that has been caused by a single credible event, including its direct and indirect consequences. This plant-specific action should ensure Clause 6.3 is met and also address DI&C-ISG-02 and BTP 7-19 Point 3, as applicable.

3.10.3.4 IEEE Std 603-1991 Clause 6.4 – Derivation of System Inputs

Clause 6.4 of IEEE Std 603-1991 requires, to the extent practical, sense and command feature inputs be derived from signals that are direct measures of the desired variables as specified in the design basis.

The “ALS Topical Report” states the applicability of this clause will be evaluated on a plant-specific basis, because it applies as a system level and application specific requirement. As described in the “ALS Topical Report,” the manufacturer has indicated the ALS platform directly supports a plant’s existing methods for direct measurement of the desired variables, as specified in the plant’s design basis, so no changes to plant transmitters or sensors will be required (see Reference 32, Section 12.1.20).

The NRC staff agrees evaluation of this clause is plant-specific and application-specific. Therefore, no staff determinations are appropriate for the ALS platform to address IEEE Std 603-1991 Clause 6.4. A plant-specific action is necessary to ensure Clause 6.4 is met.

3.10.3.5 IEEE Std 603-1991 Clause 6.5 – Capability for Testing and Calibration

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

The "ALS Topical Report" states the applicability of this clause will be evaluated on a plant-specific basis. As described in the "ALS Topical Report," the manufacturer has indicated the ALS platform directly supports a plant's existing methods to perform cross-checking between

redundant safety system channel sensors or between sensor channels that bear a known relationship to each other. The manufacturer has indicated the ALS platform will support cross-checking through its design features, which will provide sufficiently precise readouts for the sensors (see Reference 32, Section 12.1.21).

The NRC staff's review of the design features provided by ALS platform standardized circuit boards is addressed in Section 3.1 of this SE. The NRC staff's review of self-diagnostics and test and calibration capabilities provided by the ALS platform is addressed in Section 3.4.3 of this SE.

BTP 7-17 discusses issues that should be considered in sensor check and surveillance test provisions where digital computer I&C systems are involved. In particular, when automatic test features, which would include any automatic sensor cross-check, is credited with performing a surveillance test function, then provisions should be made to confirm the continued execution of the automatic tests during plant operations. Additionally, the safety classification and quality of the hardware and software performing periodic tests should be equivalent to that of the tested system, and the design should maintain channel independence, maintain system integrity, and meet the single-failure criterion during testing.

Although the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Clause 6.5, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 6.5. This determination is based on the following factors.

- Platform design features support implementation of application-specific diagnostic logic and confirmation of continued execution via the Maintenance Workstation.
- The classification and quality of the hardware and FPGA logic performing diagnostic functions, as part of the tested system, are equivalent to the classification and quality of safety function hardware and FPGA logic.

- The proposed instrumentation architecture supports meeting channel independence, system integrity, the single-failure criterion, and use of a qualified display system as the Maintenance Workstation during test and calibration activities.

Nevertheless, the NRC staff agrees evaluation of this clause is plant-specific and application-specific. A plant-specific action is necessary to ensure Clause 6.5 is met in further consideration of applicable portions of BTP 7-17, RG 1.118, and RG 1.47.

3.10.3.6 IEEE Std 603-1991 Clause 6.6 – Operating Bypasses

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

The “ALS Topical Report” states the applicability of this clause will be evaluated on a plant-specific basis, because it applies as a system level and application specific requirement. As described in the “ALS Topical Report,” the manufacturer has indicated the ALS platform directly supports implementation of operating bypasses within the application-specific logic of the ALS-102 Core Logic Board. The manufacturer has indicated the application-specific logic for the operating bypass will meet IEEE Std 603-1991 Clause 6.6 through automatic actions that neither require operator intervention nor confirmation (see Reference 32, Section 12.1.22).

The NRC staff’s review of the design features provided by ALS platform standardized circuit boards is addressed in Section 3.1 of this SE. The NRC staff’s review of ALS platform response time characteristics is addressed Sections 3.4.1 and 3.4.2.1 of this SE. The NRC staff’s review of self-diagnostics and test and calibration capabilities provided by the ALS platform is addressed in Section 3.4.3 of this SE.

Although the “ALS Topical Report” cannot fully address IEEE Std 603-1991 Clause 6.6, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 6.6. This determination is based on the platform design features to implement application-specific logic. Furthermore, the NRC staff also agrees evaluation of this clause is plant-specific and application-specific. Therefore, no broader staff determination is appropriate for the ALS platform to address IEEE Std 603-1991 Clause 6.6. A plant-specific action is necessary to ensure Clause 6.6 is met.

3.10.3.7 IEEE Std 603-1991 Clause 6.7 – Maintenance Bypass

Clause 6.7 of IEEE Std 603-1991 requires a safety system retain its ability to accomplish its safety function while sense and command features equipment is in maintenance bypass, and during the maintenance bypass both the single-failure criterion of Clause 5.1 and the diversity and defense-in-depth of protective actions of Clause 6.3 shall continue to be met. An exception

to continuing to meet Clauses 5.1 and 6.3 is provided for one-out-of-two portions of the sense and command features when one portion is rendered inoperable, provided that acceptable reliability of equipment operation has been demonstrated to show removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability.

The “ALS Topical Report” states the applicability of this clause will be evaluated on a plant-specific basis, because it applies as a system level and application specific requirement that depends on the number of redundant safety channels. As described in the “ALS Topical Report,” the manufacturer has indicated the ALS platform directly supports implementation of maintenance bypasses in accordance with plant technical specifications (see Reference 32, Section 12.1.23).

The NRC staff’s review of the design features provided by ALS platform standardized circuit boards is addressed in Section 3.1 of this SE. The NRC staff’s review of self-diagnostics and test and calibration capabilities provided by the ALS platform is addressed in Section 3.4.3 of this SE.

Although the “ALS Topical Report” cannot fully address IEEE Std 603-1991 Clause 6.7, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 6.7. This determination is based on the platform design features to implement multiple redundant safety channels/divisions while maintaining independence between them and the ability perform a maintenance bypass on an individual safety channel/division. Nevertheless, evaluation of this clause requires review of plant and application-specific technical specification content. Therefore, the NRC staff also agrees evaluation of this clause is plant-specific and application-specific. As such, no broader staff determination is appropriate for the ALS platform to address IEEE Std 603-1991 Clause 6.7. A plant-specific action is necessary to ensure Clause 6.7 is met.

3.10.3.8 IEEE Std 603-1991 Clause 6.8 – Setpoints

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

The “ALS Topical Report” does not address a specific application or establish a definitive safety system, which is necessary to demonstrate the adequacy of setpoints associated with IEEE Std 603-1991 Clause 4.4. Nevertheless, the manufacturer has indicated protection system setpoints will be calculated in accordance with a well-established methodology that accounts for all measurement and signal processing inaccuracies, as well as time and temperature effects

(see Reference 32, Section 12.1.7). Per SRP Chapter 7, Appendix 7.1-C, Section 6.8, an applicant's or licensee's analyses should confirm an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system. The applicant's or licensee's analyses should also confirm an adequate margin remains between setpoints and safety limits, such that the system initiates protective actions before safety limits are exceeded. RG 1.105, Revision 3, "Instrument Setpoints for Safety Systems," and SRP BTP 7-12 provides guidance on the establishment of instrument setpoints.

The "ALS Topical Report" mapping of DI&C-ISG-06 to provide information related to setpoint methodology identifies an application-specific design specification will be provided as part of a referencing application or license amendment request. The mapping of DI&C-ISG-06 to provide information related to setpoint methodology also identifies the 6002-00011, "ALS Platform Specification" (Reference 44), which describes the operational concept for calibration and calibration check, but does not provide board-specific accuracy specifications or otherwise establish an applicant or licensee setpoint methodology.

Although the "ALS Topical Report" scope excludes the process of establishing instrument setpoints, it does describe the operational concept by which an automatic control would be implemented using the platform and provides a high level description of ALS system accuracy. The "ALS Topical Report" does not provide board level accuracy calculations, accuracy requirements in terms of plant process variables, or the supporting statistical basis for board-level accuracy error terms in support of a plant-specific setpoint methodology or an application-specific setpoint calculation. As described in the "ALS Topical Report," the manufacturer has indicated the ALS board accuracy supports a safety system accuracy that is the same or better than the system being replaced, so the setpoints will not change and a plant's operating margin will be preserved (see Reference 32, Sections 2.8 and 12.1.17).

The "ALS Topical Report" further states the determination of actual setpoints will be made on a plant-specific basis, and the accuracy and response time performance of the plant-specific application of the ALS platform will become part of the plant's setpoint methodology program, which will follow current setpoint guidance and requirements (see Reference 32, Section 12.1.24).

The NRC staff's review of the design features provided by ALS platform standardized circuit boards is addressed in Section 3.1 of this SE. The NRC staff's review of self-diagnostics and test and calibration capabilities provided by the ALS platform is addressed in Section 3.4.3 of this SE.

Although the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Clause 6.8, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Clause 6.8. This determination is based on the platform's deterministic processing characteristics, equipment accuracy specifications, plant-specific and application-specific logic within the ALS-102 Core Logic Board, and equipment calibration and test operational concepts. Nevertheless, evaluation of this clause requires review of an applicant's or licensee's plant-specific setpoint methodology and application-specific instrument error terms. Therefore, the NRC staff also agrees evaluation of this clause is plant-specific and application-specific. As such, no broader staff determination

is appropriate for the ALS platform to address IEEE Std 603-1991 Clause 6.8. A plant-specific action is necessary to ensure Clause 6.8 is met, and this should include applicant or licensee analyses to provide information related to the applicant's or licensee's setpoint methodology, calculations, and technical basis for associated ALS platform error terms in consideration of RG 1.105, "Setpoints for Safety-Related Instrumentation," and SRP BTP 7-12.

3.10.4 IEEE Std 603-1991 Section 7 – Execute Features - Functional and Design Requirements"

Section 7 of IEEE Std 603-1991 contains five clauses that only apply to execute features of safety systems. In addition to the preceding evaluation of the ALS platform against the requirements in Section 5 of IEEE Std 603-1991, the NRC staff evaluated the ALS platform against requirements of Section 7. Execute features are the electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of

the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling. The following evaluations against the requirements of IEEE Std 603-1991 Section 7 are limited to capabilities and characteristics of the ALS platform relevant to meet each requirement.

The five clauses in Section 7 of IEEE Std 603-1991 that apply to the execute features of safety systems are:

- Clause 7.1 Automatic Control requires the capability to receive and act upon automatic control signals from sense and command features consistent with Clause 4.4 of the design basis.
- Clause 7.2 Manual Control requires that any inclusion of manual control within an actuated component in the execute features shall not defeat the requirements of Clauses 5.1 and 6.2. Clause 7.2 also requires the capability to receive and act upon manual control signals from sense and command features consistent with the design basis.
- Clause 7.3 Completion of Protective Action requires the design of execute features to ensure a once initiated protective action follows through to completion. However, this does not preclude the use of equipment protective devices identified in clause 4.11 or provisions for deliberate operator interventions. Also this clause requires a separate, deliberate operator action to return execute features to normal and precludes the reset of the sense and command features to automatically return execute features to normal.
- Clause 7.4 Operating Bypass requires any operating bypass of execute features to comply with requirements identical to the provisions for the sense and command features.
- Clause 7.5 Maintenance Bypass requires any maintenance bypass of execute features to comply with requirements similar to the provisions for the sense and command features.

For each of these clauses, the "ALS Topical Report" states the associated requirements apply on an application-specific basis (see Reference 32, Sections 12.1.25 through 12.1.29).

Furthermore, the set of examples of ALS platform applications do not implement actuated equipment associated with execute features of safety systems and instead primarily address sense and command features of safety systems (see see Reference 32, Appendices A through C). As such, the NRC staff agrees no review of the ALS platform against Section 7 of IEEE Std 603-1991 is necessary. Nevertheless, the NRC staff's review of Section 5 and Section 6, as noted in the Table 3.10-2, provides an adequate evaluation of the ALS platform's potential use within execute features.

Table 3.10-2 Cross-reference of IEEE Std 603-1991 Section 7 and SE Sections

IEEE Std 603-1991 Section 7	**SE Section**
Clause 7.1	Section 3.10.3.1, IEEE Std 603-1991 Clause 6.1 – Automatic Control
Clause 7.2	Section 3.10.3.2, IEEE Std 603-1991 Clause 6.2 – Manual Control
Clause 7.3	Section 3.10.2.2, IEEE Std 603-1991 Clause 5.2 – Completion of Protective Action
Clause 7.4	Section 3.10.3.6, IEEE Std 603-1991 Clause 6.6 – Operating Bypasses
Clause 7.5	Section 3.10.3.7, IEEE Std 603-1991 Clause 6.7 – Maintenance Bypass

The NRC staff determined the NRC staff evaluations identified in Table 3.10-2 are sufficient based on the following three points: 1) the IEEE Std 603-1991 requirements for these clauses, which are applicable to the execute features, do not materially differ from those identified as general requirements or applicable to the sense and command features, 2) the associated design features and capabilities of the ALS platform do not change based on their use to fulfill either sense and command features or execute features, and 3) conformance to each of these clauses requires plant-specific action. Therefore, a separate review of the ALS platform against these clauses would be redundant, provides no additional benefit, and is therefore unnecessary.

Although the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Section 7, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Section 7. This determination is based on the platform design features to implement application-specific logic on the ALS-102 Core Logic Board, to implement multiple redundant safety channels/divisions while maintaining independence between them, and to implement and indicate compliant bypasses on an individual safety channel/division. Nevertheless, evaluation of this clause requires plant-specific action. Therefore, the NRC staff also agrees evaluation of this clause is plant-specific and application-specific. As such, no broader staff determination is appropriate for the ALS platform to address IEEE Std 603-1991 Section 7. A plant-specific action is necessary to ensure Section 7 is met for ALS platform applications of a safety system execute feature.

3.10.5 IEEE Std 603-1991 Section 8 – Power Source Requirements

Section 8 of IEEE Std 603-1991 contains three clauses related to power sources for safety systems. Clause 8.1 requires any portion of the Class 1E power system required to provide

electrical power to the safety system shall be considered part of the safety systems and shall be governed by the criteria of IEEE Std 603-1991. Clause 8.2 requires non-electrical power sources (e.g., control-air, bottled-gas, hydraulic accumulator, etc.) required to provide motive power to safety system components shall be considered part of the safety systems and shall provide power consistent with the requirements of IEEE Std 603-1991. Clause 8.3 requires safety systems retain their ability to accomplish their safety functions while power sources are in maintenance bypass similar to the maintenance bypass provisions for the sense and command features and execute features.

When addressing IEEE Std 603-1991 Section 8, the "ALS Topical Report" states each ALS-based safety system cabinet will contain two qualified, independent power supplies, where each power supply will be capable of independently providing full-power for an ALS chassis if one of its power supplies fails or is removed from service (see Reference 32, Section 12.1.30).

This redundant power supply approach addresses the local power supplies within an instrument cabinet in support of the single-failure criterion. However, these power supplies have been excluded from the ALS platform scope (see Reference 32, Section 1.2) and are not considered part of overall Class 1E power system. The set of examples of ALS platform applications does include a Load Shedder and Emergency Load Sequencer (LSELS), which would be considered part of the overall Class 1E electrical power system (see Reference 32, Appendix B). In contrast, no platform application is identified which would be part of a non-electrical power system.

The NRC staff agrees no review of the ALS platform against Section 8 of IEEE Std 603-1991 is necessary. Nevertheless, the NRC staff's review of Sections 4, 5, and 6, as noted in the Table 3.10-3, provides an adequate evaluation of the ALS platform's potential use within the overall Class 1E electrical power system.

Table 3.10-3 Cross-reference of IEEE Std 603-1991 Section 8 and SE Sections

IEEE Std 603-1991 Section 8	**SE Section**
Clause 8.1	Section 3.10.1, IEEE Std 603-1991 Section 4 – Safety System Designation, and Section 3.10.2, IEEE Std 603-1991 Section 5 – Safety System Criteria
Clause 8.3	Section 3.10.3.7, IEEE Std 603-1991 Clause 6.7 – Maintenance Bypass

The NRC staff determined the NRC staff evaluations identified in Table 3.10-3 are sufficient based on the following three points: 1) the IEEE Std 603-1991 requirements for these clauses, which are applicable to power sources, do not materially differ from those identified as general requirements or applicable to the sense and command features, 2) the associated design features and capabilities of the ALS platform do not change based on their use to fulfill either sense and command features or power source features, and 3) conformance to these clauses requires a plant-specific action. Therefore, a separate review of the ALS platform against these clauses would be redundant, provides no additional benefit, and is therefore unnecessary.

Although the "ALS Topical Report" cannot fully address IEEE Std 603-1991 Section 8, the NRC staff determined the ALS platform supports meeting IEEE Std 603-1991 Section 8. This

determination is based on the platform design features to implement application-specific logic on the ALS-102 Core Logic Board, to implement multiple redundant safety channels/divisions while maintaining independence between them, and to perform a maintenance bypass on an individual safety channel/division. Nevertheless, evaluation of this clause requires plant-specific action. Therefore, the NRC staff also agrees evaluation of this clause is plant-specific and application-specific. As such, no broader staff determination is appropriate for the ALS platform to address IEEE Std 603-1991 Section 8. A plant-specific action is necessary to ensure Section 8 is met for ALS platform applications of a safety system power source feature.

3.11 Conformance with IEEE Std 7-4.3.2-2003

Equipment based on ALS platform components is intended for use in safety systems and other safety-related applications. Therefore, the platform topical report was evaluated against its ability to support the application-specific system provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." RG 1.152, "IEEE Standard Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," states conformance with the requirements of IEEE Std 7 4.3.2-2003 is a method that the NRC staff has deemed acceptable for meeting the Commission's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. The NRC staff's evaluation is based on the guidance contained in SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," which provides acceptance criteria for this standard. Furthermore, the NRC staff considered applicable precedent established by prior staff determinations, which considered the applicability and tailoring of IEEE Std 7-4.3.2-2003 in order to apply it to an FPGA-based development, within the Wolf Creek MSFIS SE (see Reference 2).

With the consideration that the "ALS Topical Report" scope does not propose to meet all clauses of IEEE Std 7-4.3.2-2003 via its components–similar to the clauses IEEE Std 603-1991–the NRC staff's evaluation of each clause has a limited scope that does not provide a SE of the ALS platform against the full clause. With the additional consideration that not all provisions of the microprocessor-based software standard are directly applicable to an FPGA-based platform, the following subsections necessarily tailor the applicability of each IEEE Std 7-4.3.2-2003 clause similar to the Wolf Creek MSFIS SE.

Because the NRC staff evaluation is largely limited to the determination of the degree that the ALS platform and its FPGA development processes support meeting the various clauses of IEEE Std 7-4.3.2-2003, as applicable to an FPGA-based platform, a single general plant-specific action item has been created to address full compliance to each IEEE Std 7-4.3.2-2003 clause, which applies to each plant-specific and application-specific use of the ALS platform (see Section 4.2, Item 22).

3.11.1 IEEE Std 7-4.3.2-2003 Section 4 – Safety System Design Basis

Section 4 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Section 4 of IEEE Std 603 are necessary.

The “ALS Topical Report” states an ALS-based safety system replacement will not change the design basis from that which applies to the system being replaced (see Reference 32, Section 12.2.1).

The NRC staff’s review of the ALS platform against the requirements found in Section 4 of IEEE Std 603-1991 is addressed in Section 3.10.1 of this SE.

3.11.2 IEEE Std 7-4.3.2-2003 Section 5 – Safety System Criteria

Section 5 of IEEE Std 7-4.3.2-2003 contains fifteen clauses that apply to all safety system functions and features. Some of the clauses in Section 5 of IEEE Std 603-1991 are supplemented by IEEE Std 7-4.3.2-2003 to address technology specific issues related to the use of digital computers in safety systems. The following evaluations against IEEE Std 7-4.3.2-2003 Section 5 are limited to capabilities and characteristics of the ALS platform relevant to meet each requirement.

3.11.2.1 IEEE Std 7-4.3.2-2003 Clause 5.1 – Single-Failure Criterion

Clause 5.1 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Clause 5.1 of IEEE Std 603 are necessary.

The “ALS Topical Report” states an ALS-based safety system supports an application-specific design that will meet the single-failure criterion of Clause 5.1 of IEEE Std 603-1991 (see Reference 32, Section 12.2.2).

The NRC staff’s review of the ALS platform against the requirements found in Clause 5.1 of IEEE Std 603-1991 is addressed in Section 3.10.2.1 of this SE.

3.11.2.2 IEEE Std 7-4.3.2-2003 Clause 5.2 – Completion of Protective Action

Clause 5.2 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Clause 5.2 of IEEE Std 603 are necessary.

The “ALS Topical Report” states an ALS-based safety system supports an application-specific design that will meet the completion of protective action requirements of Clause 5.2 of IEEE Std 603-1991 (see Reference 32, Section 12.2.3).

The NRC staff’s review of the ALS platform against the requirements found in Clause 5.2 of IEEE Std 603-1991 is addressed in Section 3.10.2.2 of this SE.

3.11.2.3 IEEE Std 7-4.3.2-2003 Clause 5.3 – Quality

Clause 5.3 of IEEE Std 7-4.3.2-2003 states hardware quality is addressed in IEEE Std 603-1991, and software quality is addressed in IEEE/EIA Standard 12207.0-1996 and supporting standards. Clause 5.3 further requires the digital computer development process include the development activities for both computer hardware and software, the integration of the hardware and software, and the integration of the computer with the safety system.

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

The “ALS Topical Report” describes CS Innovations quality assurance program comply with 10 CFR Part 50, Appendix B and also describes the ALS platform life-cycle management process (see Reference 32, Sections 6, 10, and 12.2.4).

The Wolf Creek MSFIS SE acknowledged CS Innovations had established a QA program based on 10 CFR Part 50, Appendix B, and was designated a 10 CFR Part 50, Appendix B, supplier by Wolf Creek. For the Wolf Creek MSFIS SE, the NRC staff reviewed the development and review processes for hardware development, for the life-cycle development of the programmable aspects of the FPGA, and for IEEE Std 603-1991, Clause 5.3, Quality requirements (see Reference 2, Enclosure 2, Section 3.3.6.2.3).

For the ALS platform, the manufacturer has maintained a QA program based on 10 CFR Part 50, Appendix B and its QA program has since been subjected to further staff, supplier, and licensee audit activities. Section 3.10.2.3 of this SE provides the NRC staff evaluation for quality against IEEE Std 603-1991, Clause 5.3. The next six subsections of this SE address the six subclauses of IEEE Std 7-4.3.2-2003, Clause 5.3, which identify activities beyond the requirements of IEEE Std 603-1991 necessary to meet quality criterion for a digital computer-based system, including its software.

3.11.2.3.1 IEEE Std 7-4.3.2-2003 Clause 5.3.1 – Software Development

Clause 5.3.1 of IEEE Std 7-4.3.2-2003 states computer software shall be developed, modified, or accepted in accordance with an approved software quality assurance (QA) plan consistent with the requirements of IEEE/EIA 12207.0-1996. Clause 5.3.1 further states the software QA plan shall address all software resident on the computer at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics), and provides reference guidance for developing software QA plans.

The “ALS Topical Report” states the ALS platform has no resident software at run time and describes its overall approach to providing an Appendix B compliant QA program (see Reference 32, Sections 12.2.5 and 10). The manufacturer docketed its “Quality Assurance Manual” (Reference 27) and “ALS Quality Assurance Plan” (Reference 34) to address quality assurance aspects of the ALS platform’s FPGA programming. Since that time and as discussed in Section 3.10.2.3 of this SE, the manufacturer has transitioned to the “Westinghouse Quality Management System.” Separate from this SE, NRC staff and a licensee audited the “Quality Assurance Manual.” Also separate from this SE, NRC staff concluded Revision 6 to the “Westinghouse Quality Management System” continues to meet the requirements of Appendix B to 10 CFR Part 50 and is therefore acceptable (see Reference 4).

Based on the continuity of the “Quality Assurance Plan” and manufacturer’s position as an Appendix B supplier throughout the ALS platform development, the NRC staff concludes all FPGA programming resident in the ALS platform has or should be developed, modified, and

accepted in accordance with a quality assurance plan that is appropriate for the FPGA technology and for use in safety-related systems of nuclear power plants.

3.11.2.3.1.1 IEEE Std 7-4.3.2-2003 Clause 5.3.1.1 – Software Quality Metrics

Clause 5.3.1.1 of IEEE Std 7-4.3.2-2003 states the use of software quality metrics shall be considered throughout the software life-cycle to assess whether software quality requirements are being met. Clause 5.3.1.1 also identifies life-cycle phase characteristics that should be considered when software quality metrics are used, and states the basis for the selected metrics should be included in the software documentation.

The “ALS Topical Report” states the ALS platform is FPGA-based and does not use software in a traditional sense. Nevertheless, the ALS platform development life-cycle includes consideration of methods to assess satisfactory implementation of FPGA programming quality (see Reference 32, Sections 12.2.6 and 6). Although the “ALS Topical Report” does not identify specific FPGA programming quality metrics to identify explicit measurement indicators or the basis for the selected metrics, the “ALS V&V Plan” does address correctness and completeness of requirements during the requirements phase, compliance with requirements as part of the design phase, compliance with design as part of the implementation phase, and functional compliance with requirements as part of the test and integration phase. Because the “ALS Topical Report” scope excludes a specific system design and its subsequent installation and use, the “ALS V&V Plan” addresses on-site functional compliance with requirements as part of the installation and checkout phase and performance history as part of the operation and maintenance phase (see Reference 36, Section 4).

During the life-cycle activities of the ALS platform development, the manufacturer documented error reports and maintained and tracked associated records and corrective actions for the ALS platform, as a whole, without unique treatment of error reports for FPGA programming, as documented in the “ALS Platform Audit Summary Report” (see Reference 127, Sections 4 and 5).

The NRC staff determined the manufacturer did not establish or use specific FPGA program quality metrics. Therefore, software quality metrics, as defined in IEEE Std 7-4.3.2-2003, Clause 5.3.1.1, were not applied for the ALS platform FPGA program development efforts. Therefore, the NRC staff further concludes the manufacturer does not intend to use quality inferences from FPGA program quality metric measurements to demonstrate the quality requirements of 10 CFR Appendix B have been met. The NRC staff’s evaluation of quality, which is addressed in Sections 3.10.2.3 and 3.11.2.3 of this SE, does not include software quality metrics.

3.11.2.3.2 IEEE Std 7-4.3.2-2003 Clause 5.3.2 – Software Tools

Clause 5.3.2 of IEEE Std 7-4.3.2-2003 states software tools to support software development processes and V&V processes shall be controlled under configuration management. Clause 5.3.2 also identifies two methods whereby software tools may be confirmed as suitable for use, where one or both methods shall be used. These confirmation methods are identified as: a) a test tool validation program to provide confidence that the necessary features of the

software tool function as required, and b) use of the software tool so defects not detected by the software tool will be detected by V&V activities. Additionally, Clause 5.3.2 allows for the use of operating experience to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.

The design and development of the ALS platform's FPGAs rely on several commercially available software-based tools, which the ALS platform applicant has placed under its configuration management program for control and maintenance. These software-based tools are subjected to an assessment and tool qualification to ensure each tool is capable of performing its design or verification functions in accordance with 6002-00030, "ALS Design Tools" (Reference 46). The software tools have not been developed as safety-related products. Therefore, the manufacturer performs a tool assessment and qualification to ensure adequate quality and the suitability for each software-based tool's intended use in a design development activity. "ALS Design Tools" identifies how the V&V assessments are performed on tool outputs to verify a tool correctly performed its functions. The tool outputs for each design development activity are also subject to project configuration management. To provide additional confidence in suitability for intended use, "ALS Design Tools" also discusses the ALS manufacturer's experience with the software-based tools along with broader industry use. Furthermore, following each in-process V&V activity, which includes the tool output assessments, V&V testing is performed on the programmed FPGA to confirm correct device operation, and this testing represents a verification of the final software-based tool's output. The "ALS Topical Report" states the tool assessment and qualification process meets the intent of IEEE Std 7-4.3.2, Section 5.3.2 "Software Tools" (see Reference 32, Section 12.2.7).

The NRC staff confirmed the "ALS Platform Configuration Status Accounting" (Reference 40) identifies the 3rd party software tools as configuration items by name and version. The NRC staff reviewed the "ALS V&V Plan" and "ALS Platform FPGA V&V Test Plan" (References 36 and 45) and confirmed processes include activities to verify 3rd party software tool versions and review tool outputs to ensure tools perform as expected for the intended use in the design activity. Additionally, as described in the "ALS V&V Plan" and "ALS Diversity Analysis" (Reference 47), IV&V activities use test and analysis tools that are different than those used in design activities. This approach provides tool diversity as mitigation against the introduction of an undetected program flaw through either a tool error or incorrect tool operation. The NRC staff also reviewed "ALS Design Tools," which describes tool assessment and qualification and identifies the ALS platform software-based design tools (see Reference 46). "ALS Design Tools" identifies each manufacturer's tool along with the process that each supports. "ALS Design Tools" also provides rationale for the manufacturer's confidence in each tool.

Although the commercially available software tools are not qualified as safety-related due to the lack of full V&V information for the tools and their development, the NRC staff concludes the tool assessment and qualification described within "ALS Design Tools" meets IEEE Std 7-4.3.2-2003, Clause 5.3.2, because the ALS platform manufacturer controls software tools under configuration management, the ALS platform manufacturer has implemented a tool validation program to provide confidence that the necessary features of software tools function as required, the ALS platform manufacturer has incorporated methods to detect defects by the

software tool within its design and V&V activities, and the ALS platform manufacturer has provided additional confidence in the suitability of tools through operating experience, as applicable to the platform's development.

3.11.2.3.3 IEEE Std 7-4.3.2-2003 Clause 5.3.3 – Verification and Validation

Clause 5.3.3 of IEEE Std 7-4.3.2-2003 adopts the terminology of process, activity, and task from IEEE Std 1012-1998, in which software V&V processes are subdivided into activities, which are further subdivided into tasks. Clause 5.3.3 also states the V&V processes shall address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the nuclear power plant. The V&V activities and tasks shall include system testing of the final integrated hardware, software, firmware, and interfaces. Clause 5.3.3 requires the software V&V effort to be performed in accordance with IEEE Std 1012-1998, where the V&V requirements for the highest integrity level apply to systems developed using IEEE Std 7-4.3.2-2003.

RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, endorses IEEE Std 1012-1998 with exceptions to describe a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the V&V of safety system software.

The "ALS Topical Report" states the V&V process is an integral part of each ALS platform life-cycle (see Reference 32, Sections 12.2.8 and 6). In accordance with the "ALS Management Plan" (Reference 33), the "ALS V&V Plan" (Reference 36) defines the techniques, procedures, and methodologies that provide IV&V for ALS projects to meet the requirements defined by IEEE Std 1012-1998 for a Software Verification and Validation Plan. The "ALS V&V Plan" also provides a mapping of IEEE Std 1012-1998 V&V activities and tasks to ALS project efforts (see Reference 36, Table 2-1). Additionally, the "ALS Platform FPGA V&V Test Plan" (Reference 45) defines the techniques, procedures, and methodologies that provide IV&V of ALS platform FPGA logic programs.

"ALS V&V Plan" excludes criticality analysis from its IEEE Std 1012-1998 IV&V tasks, because all FPGA program components are specified to be developed at the highest integrity level (4), which applies to safety systems in accordance with RG 1.168. Without a higher integrity level, the performance of a criticality analysis cannot result in additional IEEE Std 1012-1998 tasks. The purpose of criticality analysis on program components is to determine whether additional IEEE Std 1012-1998 IV&V tasks, which are associated with a higher integrity level, should apply based on the criticality of a program component or the program component's use in combination with another of a higher integrity level. The NRC staff agrees criticality analyses are unnecessary when all program components are subjected to the set of IV&V tasks of the highest integrity level (4), which is the case for all ALS platform FPGA program components. This determination is based on the same set of IEEE Std 1012-1998 IV&V tasks, which correspond to the highest integrity level (4), having already been applied to all ALS platform FPGA program components. Therefore, a criticality analysis cannot result in additional IV&V tasks for the platform.

Certain IEEE Std 1012-1998 tasks are excluded from this NRC staff evaluation, because the IV&V tasks are beyond the "ALS Topical Report" scope. One IEEE Std 1012-1998 task, hazard analysis, cannot be fulfilled within the ALS platform scope, because the task is project-specific. Other tasks cannot be fulfilled within the ALS platform topical report scope, because the task is not performed on a platform component, such as plant-specific risk analysis, system integration test, system acceptance test, installation, operation, maintenance and training tasks. In these and similar cases, the "ALS V&V Plan" defers IEEE Std 1012-1998 tasks to an applicant's or licensee's use of the ALS platform.

Section 3.2.3 of this SE describes the ALS platform V&V activities applicable to FPGA logic programs reviewed by the NRC staff. The NRC staff confirmed the manufacturer performed V&V program tasks throughout the life-cycle development of the ALS platform and in accordance with RG 1.168's endorsement of IEEE Std 1012-1998, as applicable to standard FPGA logic programs of the platform. The NRC staff confirmed the "ALS V&V Plan" addresses the integrity level 4 activities and tasks within IEEE Std 1012-1998, as provided by RG 1.168 for safety systems. The NRC staff also confirmed the processes covered within the V&V plans address the ALS platform hardware, FPGA logic programs, and the integration onto each standardized circuit board. Although the equipment qualification activities included a representative integration of a single chassis, this activity was performed by the design team rather than the V&V team. Therefore, the NRC staff determined it does not meet the IEEE Std 1012-1998 V&V tasks of independent system integration test or system acceptance test, which apply to the final integrated set of ALS platform hardware, FPGA logic programs, and interfaces to meet a plant-specific application.

Given the scope of the "ALS Topical Report," the NRC staff determined the manufacturer performed V&V appropriate for the ALS platform standardized circuit boards and their intended use within a safety-related system in a nuclear power plant. This platform SE against IEEE Std 7-4.3.2-2003 Clause 5.3.3 excludes the V&V tasks deferred to plant-specific applications that reference this SE and provides an appropriate plant-specific action to address the deferrals. Applicants and licensees referencing this SE should demonstrate it has fulfilled the IEEE Std 1012-1998 tasks that have been deferred, as identified in the "ALS V&V Plan" (see Reference 36, Section 2.2 and Table 2-1). Applicants and licensees referencing this SE should ensure appropriate activities are included in its project-specific V&V plan and the performance of each activity is acceptably independent. The project-specific V&V plan should identify any alternative method(s) to IEEE Std 1012-1998 for any IV&V task and demonstrate the alternative method(s) provides equivalent assurance (see Section 4.2, Item 23).

Based on the NRC staff's evaluation of the ALS platform's V&V tasks, its confirmation against the criteria applicable to the seven standardized circuit boards and associated FPGA programs, and fulfillment of the plant-specific action, the NRC staff concludes the ALS platform V&V activities and tasks meet the criteria of IEEE Std 7-4.3.2-2003 Clause 5.3.3, as applicable to the platform's development.

3.11.2.3.4 IEEE Std 7-4.3.2-2003 Clause 5.3.4 – Independent V&V (IV&V) Requirements

Clause 5.3.4 of IEEE Std 7-4.3.2-2003 defines the levels of independence required for the V&V effort covered by Clause 5.3.3 in terms of technical independence, managerial independence, and financial independence. Clause 5.3.4 requires the individuals or groups that verify and validate the development activities and tests exclude original design developers but possess appropriate technical competence. Clause 5.3.4 also requires an organization that is separate from the development and program management organizations be vested with the oversight of IV&V activities, and this IV&V effort include selection of the following three items: 1) the segments of the software and system to be analyzed and tested, 2) the V&V techniques to be used, and 3) the technical issues and problems upon which to act. Lastly, Clause 5.3.4 requires the IV&V effort to be allocated resources that are independent of the development resources.

RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, endorses IEEE Std 1012-1998 with exceptions to describe a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to IV&V. Specifically, RG 1.168 states the method described in IEEE Std 1012-1998 in Clause 7.4.1 and Annex C is acceptable for performing IV&V. Clause 7.4.1 of IEEE Std 1012-1998 addresses the organization of the V&V effort where Annex C addresses the degree of IV&V technical, managerial, and financial independence from development. For nuclear power plant safety systems, RG 1.168 provides guidance to apply IEEE Std 1012-1998 Annex C "Classical IV&V" from development for each IV&V task, because RG 1.168 states nuclear power plant safety system programming should be assigned an integrity level 4 or equivalent. RG 1.168 goes on to state "the extent of independence between the organization responsible for design and the organization responsible for verification and checking of the design must be verified by the applicant or licensee to meet the NRC's requirements contained in Appendix B."

The "ALS Topical Report" states the ALS platform V&V process meets V&V technical, managerial, and financial independence from development (see Reference 32, Section 12.2.9). The "ALS Management Plan" discusses and depicts the project's organization and shows the project's IV&V team is managed independently from both the development team and the quality assurance team (see Reference 33, Section 3.1). The "ALS Management Plan" also discusses required training for specific job functions along with associated training records (see Reference 33, Section 4.1.4). The "ALS V&V Plan" similarly defines the IV&V organization in terms of technical, managerial, and financial independence from development, provides a more detailed explanation of each independence characteristic, and describes the IV&V teams interface through configuration management and anomaly reporting to the development effort. The "ALS V&V Plan" states the IV&V organization fulfills the role of "Classical IV&V" as defined within IEEE Std 1012-1998 to ensure the V&V process is not compromised by schedule or resource demands placed on the design process (see Reference 36, Section 3.1).

The NRC staff reviewed and evaluated the ALS platform documentation governing the independence of V&V from development and audited the independence characteristics. Through these activities, NRC staff confirmed the ALS platform V&V, as discussed in Section 3.11.2.3.3 of this SE, was technically, managerially, and financially independent from

the design and development activities. The NRC staff also confirmed the ALS platform V&V responsibilities included defining the portions of the FPGA program and ALS platform to analyze and test, establishing the V&V techniques to apply, and deciding upon the technical issues and problems upon which to act. Additionally, the NRC staff confirmed personnel not involved in the design development and possessing appropriate technical competence performed the V&V activities, and the V&V resources were independent from the development resources.

Based on the NRC staff's evaluation of the ALS platform's V&V independence and confirmation of the independence criteria, the NRC staff concludes the ALS platform V&V activities meet the criteria of IEEE Std 7-4.3.2-2003 Clause 5.3.4, as applicable to the platform's development.

3.11.2.3.5 IEEE Std 7-4.3.2-2003 Clause 5.3.5 – Software Configuration Management

Clause 5.3.5 of IEEE Std 7-4.3.2-2003 requires software configuration management to be performed in accordance with IEEE Std 1042-1987. Clause 5.3.5 also lists nine activities required to be addressed by software configuration management. These activities specify items that must be identified and controlled, address the control of software design changes, software documentation, software applicant development activities, and the retrieval of qualification information for software designs and code, and also include software configuration audits and status accounting. Clause 5.3.5 requires the software configuration management plan to describe the division of responsibility whenever some of its activities are performed or controlled by other quality assurance activities. Clause 5.3.5 also requires software baselines to be established at appropriate points in the software life-cycle process to synchronize engineering and documentation activities, and requires approved changes to the baseline. Clause 5.3.5 further requires unique identification of each software configuration item and revision and/or date time stamps for each configuration item. Lastly, Clause 5.3.5 requires formal documentation and approval of changes to software/firmware consistent with the software configuration management plan. This documentation is required to include the reason for the change, identification of the affected software/firmware, and the impact of the change on the system.

RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 1042-1987, subject to additional provisions, to describe a method acceptable to the NRC staff for carrying out software configuration management plans produced under the auspices of IEEE Std 828-1990, because IEEE Std 1042-1987 is a tutorial guide that explains how to comply with IEEE Std 828-1990.

The "ALS Topical Report" states configuration management for the ALS platform is addressed in the quality assurance plan and performed throughout the life-cycle (see Reference 32, Sections 12.2.10). The "ALS Management Plan" (Reference 33) includes references to both the "ALS QA Plan" (Reference 34) and the "ALS Configuration Management Plan" (Reference 35) and states the "ALS Configuration Management Plan" defines the change control mechanisms for the ALS platform (see Reference 33, Section 4.3.1). The "ALS Management Plan" describes the project deliverables within the "ALS Topical Report" scope and states a detailed list of all project deliverables is defined in Configuration Status Accounting documents where there will

be a Configuration Status Accounting document per ALS board type along with a platform Configuration Status Accounting document (see Reference 33, Section 2.1.4).

For this ALS platform SE, the 6002-xxx50, “ALS-xxx Configuration Status Accounting” documents (References 57, 63, 69, 75, 81, 87,and 93) identify configuration controlled items for each ALS board, and the 6002-00007, “ALS Platform Status Accounting” document (Reference 40) identifies configuration controlled items for the platform. Each ALS board’s 6002-xxx81, “Configuration Management Summary Report” (References 58, 64, 70, 76, 82, 88, and 94) provides a summary of established configuration controlled project milestone baselines, identifies the board’s primary configuration items, identifies, explains the corresponding “Configuration Status Accounting” documentation, and identifies any unresolved developmental product defects that are part of the ALS project scope. The 6002-00400, “ALS Platform Configuration Management Summary Report” (Reference 53) similarly provides an overall summary for the entire ALS platform. This overall summary states no developmental product defect that is part of the ALS project scope remains unresolved.

The “ALS Management Plan” states the Configuration Manager is responsible for creating and executing the “ALS Configuration Management Plan” (see Reference 33, Section 3.2). The Configuration Manager is part of the ALS Project Team reporting to the Scottsdale Operations Director (see Reference 33, Figure 3-1 and Table 3-1). The “ALS Configuration Management Plan” (Reference 35) states it is based on the guidance provided in IEEE Std 828-1998, the “Westinghouse Quality Management System,” “WEC 23.20-Westinghouse Nuclear Automation / CS Innovations Interface Agreement,” and the “ALS Management Plan” (Reference 33). The “ALS Configuration Management Plan” states all configuration management activities shall be conducted in accordance with the “Westinghouse Quality Management System,” “WEC 23.20-Westinghouse Nuclear Automation / CS Innovations Interface Agreement,” and the “ALS Management Plan.” Although the “ALS Configuration Management Plan” is governed by the “Quality Management System,” it does not identify a division of responsibilities that assigns configuration management activities to directly report to quality assurance personnel. The “ALS QA Plan” identifies the quality assurance activities as verifying adherence to documented development processes and controls—which includes configuration management through established review points and audits—to ensure the processes and controls are effective, and to evaluate the set of development products for completeness and correctness, but the “ALS QA Plan” does not establish quality assurance personnel perform the configuration management activities (see Reference 34, Sections 3 and 6).

The “ALS Configuration Management Plan” identifies the configuration items to be placed under configuration management, provides configuration management process and control requirements, identifies individual responsibilities for the change process, and defines the baselining process. The “ALS Configuration Management Plan” also includes requirements for identification of documentation, tools, hardware, FPGA logic programs, and standardized circuit board non-volatile memory configuration and includes provisions for releasing, archiving and retrieving configuration items. Furthermore, the configuration management processes address issue reporting, tracking and corrective action as they affect configuration items. Lastly, the configuration management processes and controls are subject to quality assurance activities to

ensure the effectiveness of configuration management activities along with the completeness and correctness of the specified configuration items.

The “ALS Configuration Management Plan” does not include subcontracted programming efforts. It treats the programmed, configured and delivered ALS platform components as hardware end items that cannot be modified by licensees. The ALS platform does not involve licensee or subcontracted programming when developing application-specific FPGA programming or non-volatile memory configurations. Therefore, only the single configuration management program that is described within the “ALS Configuration Management Plan” applies to the “ALS Topical Report” scope.

The NRC staff reviewed and evaluated the ALS platform documentation governing configuration management activities and audited these activities, as applied to the ALS platform and its FPGA programs. Through these efforts, the NRC staff confirmed applicable ALS platform configuration management activities have been identified and are controlled. ALS platform configuration management activities that NRC staff reviewed exclude user, operating, and maintenance documentation, because these activities are not within the “ALS Topical Report” scope. The NRC staff reviews exclude subvendor logic development activities, because the ALS platform manufacturer is the developer of all FPGA programs. The NRC staff confirmed the ALS platform configuration management activities address the control of FPGA program design changes, FPGA program documentation and development activities, and the retrieval of qualification information for FPGA program designs and code. Additionally, the NRC staff confirmed that configuration management activities include configuration audits and status accounting.

The NRC staff also confirmed the manufacturer had established and documented specific FPGA program baselines within the development life-cycle. However, throughout its review during the ALS platform development, the NRC staff has also observed documentation activities have not always been fully and accurately synchronized to the current engineering activities at the time of a baseline. Nevertheless, the NRC staff determined changes to any configuration controlled item and the established baseline requires a formal organizational approval that includes the reason for change. The NRC staff also determined the manufacturer’s processes include an assessment of the impact of the change and regression testing. The NRC staff confirmed unique identification exists for each configuration item along with revision and date information.

Based on the NRC staff’s evaluation of configuration management documentation and the confirmation of applicable configuration management activities, the NRC staff concludes the ALS platform FPGA configuration management activities meet the applicable criteria of IEEE Std 7-4.3.2-2003 Clause 5.3.5.

3.11.2.3.6 IEEE Std 7-4.3.2-2003 Clause 5.3.6 – Software Project Risk Management

Clause 5.3.6 of IEEE Std 7-4.3.2-2003 requires risk management to be performed at all levels of a digital system project to provide adequate coverage for each potential problem area. Software project risk management should ensure technical, schedule, or resource-related risks

do not compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety related functions. Clause 5.3.6 also lists seven high-level steps that should be included in risk management.

The “ALS Topical Report” states risk management for the ALS platform is a part of the software development plan, is documented in the “ALS Management Plan,” and is part of the ALS platform life-cycle (see Reference 32, Section 12.2.11). In addition to the “ALS Management Plan” that applies to the ALS platform, the mapping of DI&C-ISG-06 to provide information for software project risk management identifies an “Application Management Plan” to fully address the topic (see Reference 32, Section 12.7, Table 12.7-1, Entries 1.24 and 3.8). The “ALS Management Plan” states the manufacturing schedule is established based on the risk at the time NRC approval dates are estimated. Status reports are distributed periodically that include risks. The “ALS Management Plan” describes Project Management risk at a high level consistent with but without specific identification of the IEEE Std 7-4.3.2-2003 Clause 5.3.6 list of steps that should be included in software project risk management (see Reference 33, Sections 2.1.6, 4.3.5, and 4.4).

As discussed in Section 3.1, the ALS platform is FPGA-based and does not contain executable software. Instead, the ALS platform contains devices that are programmable (FPGAs and NVMs). The characteristics of the ALS platform necessitate an appropriate tailoring of IEEE 7-4.3.2, "Software Risk Management" for applicability to the platform, and this tailoring includes licensee-specific risk management activities, because an “Application Management Plan” is required by each applicant or licensee referencing this SE.

The "ALS Quality Assurance Plan" states risks are managed and discussed during regular project meetings and maintained by the ALS Project Manager (see Reference 34, Section 14). The “ALS V&V Plan” similarly contains provisions for management of FPGA development risks, including reports during regular project meetings. The “ALS V&V Plan” includes the use of diverse tools to reduce the risk of undetected flaws introduced by the tools (see Reference 36, Sections 3.5.5 and 3.6). The “ALS V&V Plan” also addresses the risk of using tools that have not been formally validated by restricting the ALS Test Equipment’s (ATE) use to informal testing only, which is not credited as part of IV&V within the requirement traceability matrices (see Reference 36, Section 3.6.4). Rather than use the ATE, credited IV&V board testing relies on ALS Board Test System (ABTS), which was developed by the IV&V team and validated (see Reference 36, Section 3.6.3).

Risk mitigating activities are defined within the plans and procedures that govern the ALS platform design and development. The “ALS Management Plan” introduces prototyping, which is a method of risk mitigation (see Reference 33, Section 3.3, Table 3-2). Consistent with the “ALS Management Plan,” the “Electronics Development Procedure” (Reference 29) identifies

prototypes, along with circuit simulations, as part of the ALS platform development process, which provides risk mitigation. Similarly, the “FPGA Development Procedure” (Reference 31) identifies HDL simulation, which also provides risk mitigation.

The “Electronics Development Procedure” specifies the creation of a design history binder as a container to archive analyses, changes, review comments, and reports as they are produced

during the development process. The “Electronics Development Procedure” also identifies design reviews for both prototypes and candidate product releases. Except for early prototypes, first article production is performed using the same processes as production builds to mitigate production process risks. Information from the formal reviews, prototype testing, and first article testing may identify corrective actions, which would be tracked and supports informed project management of risk.

Similarly, the “FPGA Development Procedure” specifies design specification reviews for both prototype and candidate product releases. Within the steps associated with the FPGA development, tool outputs are reviewed for warnings or errors. The “FPGA Development Procedure” also specifies preliminary and final design reviews for each FPGA design, which must be complete before formal release testing/simulation is performed. The “FPGA Development Procedure" Release Review evaluates the design to determine if it can become a formal baseline release, which would then trigger future tracking of all proposed changes and their implementation through use of Engineering Change Notices (ECNs). Information from the formal reviews and testing/simulation may identify corrective actions, which would be tracked and supports informed project management of risk.

Although the “ALS Topical Report” cannot fully address IEEE Std 7-4.3.2-2003 Clause 5.3.6, the NRC staff determined the ALS platform supports meeting IEEE Std 7-4.3.2-2003 Clause 5.3.6. This determination is based on the inclusion of specified reviews and testing within the “Electronics Development Procedure" and the “FPGA Development Procedure,” the meetings to regularly address risk within "ALS Quality Assurance Plan," and the risk mitigation techniques described within the “ALS V&V Plan.” Nevertheless, a plant-specific action is necessary when the ALS platform is used for a safety system. This plant-specific action should ensure Clause 5.3.6 is met and this should include an applicant or licensee analysis that confirms the “Application Management Plan” adequately addresses the list of steps identified within IEEE Std 7-4.3.2-2003 Clause 5.3.6.

3.11.2.4 IEEE Std 7-4.3.2-2003 Clause 5.4 – Equipment Qualification

Clause 5.4 of IEEE Std 7-4.3.2-2003 contains two subclauses necessary to qualify digital computers for use in safety systems. These subclauses are in addition to the equipment qualification criteria provided in IEEE Std 603.

3.11.2.4.1 IEEE Std 7-4.3.2-2003 Clause 5.4.1 – Computer System Testing

Clause 5.4.1 of IEEE Std 7-4.3.2-2003 requires computer system qualification testing to be performed with the computer functioning with software and diagnostics that are representative

of those used in actual operation. Clause 5.4.1 also requires all portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, to be exercised during testing. This testing is required to demonstrate performance requirements related to safety functions have been met.

As discussed in Section 3.1, the ALS platform is FPGA-based and does not contain executable software. Therefore, there is no ALS platform software to run during system testing.

Additionally, each standardized circuit board's NVM and the ALS-102 Core Logic Board's FPGA requires application-specific programming in order to represent the final operational configuration. Nevertheless, the ALS platform's FPGAs are programmed in a manner similar to a conventional microprocessor-based software program development, which provides similar versatility and potential weaknesses. Because of these similarities, the NRC staff determined that to meet IEEE Std 7-4.3.2-2003 Clause 5.4.1—qualification testing needs to include type-testing with FPGA and NVM programming representative of an operational configuration.

The manufacturer performed equipment qualification testing using the type testing approach, which used a representative set of FPGA logic on each standardized circuit board. The qualification testing demonstrated ALS platform performance for a range of normal and anticipated worst case mild environment conditions and established limitations and conditions for use of the ALS platform. The limitations and conditions include plant-specific actions to ensure an applicant's or licensee's installation environment has been sufficiently bounded by equipment qualification tests, and the acceptance criteria used during the ALS platform type testing is sufficient to identify portions of the ALS platform that could operate or fail in a way that would impair a plant-specific safety system's safety function. One conclusion of the "ALS EQ Summary Report" is "Plant specific applications shall reconcile differences between the qualified and installed configurations in order to extend the EMC, environmental, and seismic qualifications for specific applications" (see Reference 32, Section 12.2.12.1, and Reference 51, Sections 7.2 and 8).

To support the extension of platform equipment qualification to plant-specific applications, the manufacturer produced the "ALS Platform Qualification Evaluation" (Reference 52). The "ALS Platform Qualification Evaluation" addresses the potential for gaps between ALS platform capabilities and those that may be considered satisfactorily qualified through representative type test because the ALS platform has capabilities for a variety of configurations and options, but the type test only provides a representative configuration. The "ALS Platform Qualification Evaluation" also identifies exclusions, constraints on ALS platform interfaces, restrictions on use, and plant-specific evaluations which applications should address for it to be considered covered by the equipment qualification tests.

To support the extension of equipment qualification for future FPGA logic modifications and the application-specific ALS-102 FPGA logic, the manufacturer produced the "ALS FPGA Qualification Evaluation" (Reference 99). The "ALS FPGA Qualification Evaluation" addresses the evaluation of differences between the FPGA logic used during the representative type test, which was an early version of a single development team, and the FPGA logic of the second development team and final FPGA logic versions because the ALS platform may be

programmed with one of two FPGA logic designs. Additionally, changes to the FPGA versions have occurred since equipment qualification, and similar future changes should be anticipated, requiring evaluation of differences. The ALS platform's "FPGA Development Procedure" makes direct reference to the "ALS FPGA Qualification Evaluation" when specifying the evaluation of new or revised FPGA logic for potential impacts on the extension of prior equipment qualification tests (see Reference 31, Section 7.8).

The NRC staff reviewed the equipment qualification tests and confirmed this testing included a notional safety system application on the ALS-102 board and exercised diagnostics representative of those intended for actual operations. For the equipment qualification type testing, the manufacturer specifically identified ALS platform functions considered necessary to accomplish safety functions, monitored the EUT for diagnostic failures, and performed baseline tests to confirm continued operability of ALS platform functions identified as necessary to accomplish safety functions. The NRC staff also reviewed the "ALS Platform Qualification Evaluation" and "ALS FPGA Qualification Evaluation."

Section 3.3 of this SE addresses the equipment qualification of the ALS platform and identifies plant-specific actions associated with extending the equipment qualifications for specific applications.

Based on the NRC staff evaluation documented in Section 3.3 of this SE, fulfillment of its associated plant-specific actions, and confirmation that type tested components exercised diagnostics representative of those intended for actual operations, the NRC staff concludes the ALS platform system supports the construction of a safety system to meet the criteria of IEEE Std 7-4.3.2-2003 Clause 5.4.1.

3.11.2.4.2 IEEE Std 7-4.3.2-2003 Clause 5.4.2 – Qualification of Existing Commercial Computers

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

The ALS platform manufacturer dedicated some commercial suppliers as a service under its Appendix B program (e.g., for the manufacture of bare printed circuit boards, etc.). Regardless, as discussed in Sections 3.1 and 3.10.2.3 of this SE, the ALS platform was developed under a 10 CFR Part 50, Appendix B, program specifically for the nuclear power industry and is, therefore, not considered commercial grade digital equipment. This requirement is therefore not applicable to the review of the ALS platform.

3.11.2.5 IEEE Std 7-4.3.2-2003 Clause 5.5 – System Integrity

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

3.11.2.5.1 IEEE Std 7-4.3.2-2003 Clause 5.5.1 – Design for Computer Integrity

Clause 5.5.1 of IEEE Std 7-4.3.2-2003 requires the computer to be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential

for defeating the safety function. Clause 5.5.1 further requires the ability to place the safety system in its preferred failure mode in the presence of a computer failure. Lastly, Clause 5.5.1 requires the retention of the safety system's ability to perform its safety functions when a computer system restart operation occurs.

The manufacturer designed the ALS platform to handle anticipated external and internal conditions, and the ALS platform contains design features and capabilities to ensure a safety system maintains full integrity when subjected to these conditions. The manufacturer described its modes and states for the ALS platform, classification of failures and the effect on of failures on the system. The manufacturer also described digital communication design that contains provisions to address conditions with the potential to defeat a safety function (see Reference 32, Section 12.2.13.1). The NRC staff reviewed these descriptions along with supporting requirement and specification documents.

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

Although ALS platform scope does not provide a specific safety system with a preferred failure mode, the NRC staff determined the ALS 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 ALS platform contains provisions to enter a fail-safe state defined by the plant-specific configuration and to force a channel's output to a defined state using the maintenance workstation. The ALS platform also supports plant-specific safety system configurations that provide redundancy, so no single failure has the potential to defeat the safety function. The ALS 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 ALS-102 board allows the further establishment of conditions for entry into a fail-safe state that is conservative with respect to a system's safety function. To further address external conditions, the ALS platform hardware and representative FPGA logic has been subjected to the equipment qualification discussed in Section 3.3 of this SE.

The NRC staff confirmed the manufacturer's processes incorporated requirements and specifications for computer integrity features, including identification of internal and external conditions, fail-safe states and support for redundancy, which have been traced through requirements and to IV&V activities.

Based on the NRC staff determinations and confirmations in this section, the NRC staff concludes the ALS platform system supports the construction of a safety system to meet the criteria of IEEE Std 7-4.3.2-2003 Clause 5.5.1 because the ALS platform contains design

features and capabilities to ensure a safety system can maintain its full integrity when subjected to the internal and external conditions, including the environmental envelope established by the "ALS Topical Report" scope.

3.11.2.5.2 IEEE Std 7-4.3.2-2003 Clause 5.5.2 – Design for Test and Calibration

With the exclusion of an appropriate bypass of one redundant channel being in place, Clause 5.5.2 of IEEE Std 7-4.3.2-2003 prohibits test and calibration functions from creating any adverse affect on the ability of the computer to perform its safety function. Clause 5.5.2 also requires verification that test and calibration functions do not affect computer functions that were not included in a calibration change. When sole verification of test and calibration data is provided on a separate computer, Clause 5.5.2 requires V&V, configuration management, and QA for test and calibration functions of the separate computer. Likewise, Clause 5.5.2 requires V&V, configuration management, and QA when the test and calibration function is built into the safety system computer. In other words, the only case where V&V, configuration management, and QA for test and calibration functions would not be required would be when these functions reside on a separate computer and do not provide the sole verification of test and calibration data for the safety system computer.

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

For each standardized circuit board, test and calibrations features are discussed in the specifications for that board. The ALS platform incorporates test and calibration features to provide a means to bypass channels during surveillance testing, setpoint changes, and calibration. The ALS platform also incorporates features to provide a means to force a channel's output to a defined state. Furthermore, the ALS platform allows a maintenance workstation to access configuration data, which includes setpoint and calibration data, when a channel is bypassed. Sections 3.2 through 3.6 of the "ALS Topical Report" discuss the capabilities of test and calibration for an overall system. The manufacturer designed these test and calibration functions so the functions do not impede the safety functions of a system.

Furthermore, the manufacturer incorporated test and calibration functions within the initial product specifications and subsequently developed the associated FPGA programming following its safety-related development process (see Reference 32, Sections 3 and 12.2.13.2). The manufacturer also included the test and calibration functions within its type testing of the ALS platform standardized circuit boards during equipment qualification. Section 3.3 of this SE provides the NRC staff's evaluation of the ALS platform equipment qualification.

Unlike microprocessor-based computer systems, to which Clause 5.5.2 of IEEE Std 7-4.3.2-2003 typically applies, the ALS platform does not contain executable software that uses shared processing resources (e.g., processor, processing registers, cache memory, etc.). Instead, an ALS 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 ALS platform, test and calibration function logic neither uses the safety signal path's Reliable ALS Bus nor competes with safety function logic for FPGA logic resources.

The NRC staff confirmed the manufacturer's processes incorporated requirements and specifications for test and calibration functions, which have been traced through requirements and to IV&V activities. The NRC staff also confirmed the test and calibration functions were present during equipment qualification testing.

The NRC staff determined the ALS platform test and calibration will not impede the safety function of an ALS-based safety system, because the self-diagnostic functions do not compete with safety functions for the safety signal path or FPGA programming resources, the platform provides features to limit test and calibration functions to bypassed or inoperable channels, and equipment qualification activities verified continued operability of the ALS platform's safety functions and safety signal path for FPGA logic that included test and calibration functions. The NRC staff confirmed the manufacturer included specifications for test and calibration functions. The NRC staff also confirmed the manufacturer followed the same design, development, and IV&V processes for test and calibration functions as for all other ALS platform functions. Based on these NRC staff determinations and confirmations, the NRC staff concludes the ALS platform meets the applicable criterion in IEEE Std 7-4.3.2-2003 Clause 5.5.2. Nevertheless, any licensee who relies on a separate computer for the sole verification of test and calibration data should ensure adequate V&V, configuration management, and QA for the test and calibration functions of the separate computer.

3.11.2.5.3 IEEE Std 7-4.3.2-2003 Clause 5.5.3 – Fault detection and Self-diagnostics

Clause 5.5.3 of IEEE Std 7-4.3.2-2003 provides reliability requirements for a safety system to determine the need and scope of self-diagnostics. Clause 5.5.3 does not require self-diagnostics for systems in which failures can be detected by alternative means in a timely manner. When self-diagnostics are built into the safety system, then Clause 5.5.3 requires these functions to be subject to the same V&V processes as the safety system functions. If reliability requirements warrant self-diagnostics, then Clause 5.5.3 requires computer programs to incorporate functions to detect and report computer system faults and failures in a timely

manner. Clause 5.5.3 also prohibits self-diagnostic functions from adversely affecting the ability of the computer system to perform its safety function, or causing spurious actuations of the safety function. Lastly, whenever self-diagnostics are applied, clause 5.5.3 requires the system design address: 1) self-diagnostics performed during system startup, 2) self-diagnostics performed periodically while the computer system is operating, and 3) failure reporting of the self-diagnostic results.

The ALS platform incorporates self-diagnostic features to provide a means to detect and alert any failure within the ALS 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. Section 2 of the "ALS Topical Report" discusses the capabilities of fault detection and self-diagnostics for an overall system. The manufacturer designed these self-diagnostic functions so the functions do not impede the safety

functions of a system. Furthermore, the manufacturer incorporated self-diagnostic functions within the initial product specifications and subsequently developed the associated FPGA programming following its safety-related development process (see Reference 32, Section 12.2.13.3). The manufacturer also included the self-diagnostic functions within its type testing of the ALS platform standardized circuit boards during equipment qualification. Section 3.3 of this SE provides the NRC staff's evaluation the equipment qualification.

The manufacturer predicted the reliability for each standardized circuit board and analyzed the ability of self-diagnostics to detect failures. Section 3.6 of this SE provides the NRC staff's evaluation of platform reliability and availability, and Section 3.4.3 of this SE provides the NRC staff's evaluation ALS platform self-diagnostic capabilities. Regardless, the reliability and failure detection analyses are not based on a specific safety system. Therefore, the manufacturer did not establish the need and scope of the self-diagnostics based on reliability requirements of a specific safety system. Instead, the manufacturer established ALS platform requirements and specifications for reliability and self-diagnostics in general terms. As discussed within Section 3.6 of this SE, plant-specific actions are necessary to confirm the plant-specific configuration of an ALS-based safety system produces adequate safety system reliability. These plant-specific actions do not preclude detecting failures by alternative means.

Unlike microprocessor-based computer systems, to which Clause 5.5.3 of IEEE Std 7-4.3.2-2003 typically applies, the ALS platform does not contain executable software that uses shared processing resources (e.g., processor, processing registers, cache memory, etc.). Instead, an ALS 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 ALS platform, self-diagnostic function logic does not compete with safety function logic for FPGA logic resources.

The NRC staff confirmed the manufacturer's processes incorporated requirements and specifications for self-diagnostic functions, which have been traced through requirements and to IV&V activities. The NRC staff reviewed the equipment qualification to ensure this testing monitored self-diagnostics results for failures and verified self-diagnostic functions remained operable.

The NRC staff determined the ALS platform self-diagnostics will not impede the safety function of the system, because the self-diagnostic functions do not compete with safety functions for FPGA programming resources and equipment qualification demonstrated continued operability of the ALS platform's safety functions and safety signal path while the self-diagnostics were operable. The NRC staff confirmed the manufacturer included specifications for the self-diagnostic functions at power-up and periodically along with failure result reporting capabilities. The NRC staff also confirmed the manufacturer followed the same design, development, and IV&V processes for self-diagnostic functions as for all other ALS platform functions. Based on these NRC staff determinations, the NRC staff concludes the ALS platform meets the criterion in IEEE Std 7-4.3.2-2003 Clause 5.5.3 with the exception of using reliability requirements of the safety system to establish the need and scope of self-diagnostics. Nevertheless, the NRC staff further concludes that plant-specific actions provided in Section 3.6 of this SE will be sufficient

to provide equivalent assurance that the entirety of IEEE Std 7-4.3.2-2003 Clause 5.5.3 can be met for an ALS-based safety system.

3.11.2.6 IEEE Std 7-4.3.2-2003 Clause 5.6 – Independence

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

SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence" provides acceptance criteria for safety and nonsafety software and communications independence. This section points out 10 CFR Appendix A, GDC 24, "Separation of protection and control systems," states the protection systems must be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control system, leaves intact a system meeting all reliability, redundancy, and independence requirements of the protection system, and interconnection of the protection and control systems shall be limited so as to assure safety is not significantly impaired. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence" also provides acceptance criteria for nonsafety software and equipment development where barriers do not exist between safety and nonsafety software or equipment.

DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc),” Revision 1, describes methods acceptable to the NRC staff to prevent adverse interactions among safety divisions and between safety-related equipment and equipment that is not safety-related. This guidance directly addresses most of IEEE Std 7-4.3.2-2003 Clause 5.6.

Unlike microprocessor-based computer systems, to which Clause 5.6 of IEEE Std 7-4.3.2-2003 typically applies, the ALS platform does not contain executable software that uses shared processing resources (e.g., processor, processing registers, cache memory, etc.). Instead, an ALS 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. The “ALS Topical Report” scope establishes electrical isolation requirements between safety and nonsafety equipment are outside its scope. Therefore, this SE does not address meeting electrical isolation requirements beyond the creation of a plant-specific action item. The “ALS Topical Report” addresses Clause 5.6 of IEEE Std 7-4.3.2-2003 within topical report Sections 5 and 12.1.7 (see Reference 32, Section 12.2.14).

Section 3.7 of this SE addresses “ALS Topical Report” Section 5 using the guidance within DI&C-ISG-04. Section 3.10.2.6 of this SE addresses “ALS Topical Report” Section 12.1.7 for compliance to IEEE Std 603-1991 Clause 5.6, Independence. Both evaluations include plant-specific actions, because the prohibition against data communication between safety channels or between safety and nonsafety systems from inhibiting the performance of the safety function must be addressed based on each plant-specific application of the ALS platform.

Sections 3.7 and 3.10.2.6 of this SE adequately address IEEE Std 7-4.3.2-2003 Clause 5.6 with the exception of its contingency for nonsafety software functions to be developed in accordance with safety function requirements when no barrier exists. However, the manufacturer has developed all FPGA programming within the scope of the “ALS Topical Report” using the same safety-related development process without regard to whether the function is safety or nonsafety.

The NRC staff determined the ALS platform supports meeting IEEE Std 7-4.3.2-2003 Clause 5.6 based on the evaluations and fulfillment of the plant-specific action items provided within Sections 3.7 and 3.10.2.6 of this SE, and because the ALS platform design applies the same safety-related development processes to all FPGA programming, which includes programming that does not perform a safety function.

3.11.2.7 IEEE Std 7-4.3.2-2003 Clause 5.7 – Capability for Test and Calibration

Clause 5.7 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Clause 5.7 of IEEE Std 603 are necessary.

The “ALS Topical Report” states an ALS-based safety system supports an application-specific design that will meet the capability for test and calibration requirements of Clause 5.7 of IEEE Std 603-1991 (see Reference 32, Section 12.2.15).

The NRC staff’s review of the ALS platform against the requirements found in Clause 5.7 of IEEE Std 603-1991 is addressed in Section 3.10.2.7 of this SE.

3.11.2.8 IEEE Std 7-4.3.2-2003 Clause 5.8 – Information Displays

Clause 5.8 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Clause 5.8 of IEEE Std 603 are necessary.

The “ALS Topical Report” states an ALS-based safety system supports an application-specific design that will meet the information display requirements of Clause 5.8 of IEEE Std 603-1991 (see Reference 32, Section 12.2.16).

The NRC staff’s review of the ALS platform against the requirements found in Clause 5.8 of IEEE Std 603-1991 is addressed in Section 3.10.2.8 of this SE.

3.11.2.9 IEEE Std 7-4.3.2-2003 Clause 5.9 – Control of Access

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

The “ALS Topical Report” states an ALS-based safety system supports an application-specific design that will meet the control of access requirements of Clause 5.9 of IEEE Std 603-1991 (see Reference 32, Section 12.2.17).

The NRC staff’s review of the ALS platform against the requirements found in Clause 5.9 of IEEE Std 603-1991 is addressed in Section 3.10.2.9 of this SE.

3.11.2.10 IEEE Std 7-4.3.2-2003 Clause 5.10 – Repair

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

The “ALS Topical Report” states an ALS-based safety system supports an application-specific design that will meet the repair requirements of Clause 5.10 of IEEE Std 603-1991 (see Reference 32, Section 12.2.18).

The NRC staff’s review of the ALS platform against the requirements found in Clause 5.10 of IEEE Std 603-1991 is addressed in Section 3.10.2.10 of this SE.

3.11.2.11 IEEE Std 7-4.3.2-2003 Clause 5.11 – Identification

Clause 5.11 of IEEE Std 7-4.3.2-2003 provides three identification requirements specific to software systems to assure the required computer system hardware and software are installed in the appropriate system configuration. These identification requirements are: 1) firmware and software identification to assure the correct software is installed in the correct hardware component, 2) means to retrieve the identification from the firmware using software maintenance tools, and 3) IEEE Std 603 compliant physical identification of the digital computer system hardware.

SRP Chapter 7, Appendix 7.1-D, Section 5.11, "Identification" provides acceptance criteria and adds the identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation that identifies the changes made by that revision for equipment qualifications.

Unlike microprocessor-based computer systems, to which Clause 5.11 of IEEE Std 7-4.3.2-2003 typically applies, the ALS platform does not contain separate and distinct executable software that must be loaded onto a system or updated at a licensed facility. The ALS platform restricts FPGA and application-specific NVM configuration programming to the ALS platform manufacturer. Each FPGA and NVM device permanently resides on its standardized circuit board. Once the manufacturer programs a standardized circuit board’s FPGA and its NVM per application specifications, the programmed devices are subsequently treated as hardware devices and subject to the identification control activities for the

standardized circuit board upon which they permanently reside. The manufacturer's FPGA and NVM programming processes include checks to verify devices are correctly programmed (see Reference 47, Section 3.3.2 and Reference 29, Section 7.7.3). The ALS platform also contains design features that ensure each standardized circuit board has been correctly installed in its designated chassis and backplane location to form an application-specific system (see Reference 32, Sections 2.1.5.2 and 2.5.2, and Reference 43, PR0721.3.9 and PR0745.2). These attributes address the first portion of IEEE Std 7-4.3.2-2003, Clause 5.11.

The ALS platform contains features that include FPGA and NVM version identifiers, which may be viewed using maintenance equipment to confirm the configuration of the installed equipment. This information is stored in a section of the NVM device that is configured by the manufacturer and non-modifiable by the end user (see Reference 32, Section 2.1.5.2, Table 2.1-2). System and board information provides details about the configuration of an ALS system and this information includes board FPGA programming, board build information, and the board's configuration (see Reference 32, Section 2.6.3). These features address the second portion of IEEE Std 7-4.3.2-2003, Clause 5.11.

Section 3.10.2.11 of this SE addresses compliance to IEEE Std 603 general physical identification requirements for hardware, which includes digital hardware. Therefore, no further staff evaluation is required to address the third portion of IEEE Std 7-4.3.2-2003, Clause 5.11.

The NRC staff evaluated the ALS platform design features against each portion of Clause 5.11 of IEEE Std 7-4.3.2-2003 and the acceptance criteria described in SRP Chapter 7, Appendix 7.1-D, Section 5.11. Based on this evaluation, the NRC staff determined the ALS platform design features support meeting Clause 5.11 of IEEE Std 7-4.3.2-2003.

3.11.2.12 IEEE Std 7-4.3.2-2003 Clause 5.12 – Auxiliary Features

Clause 5.12 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Clause 5.12 of IEEE Std 603 are necessary.

The "ALS Topical Report" states an ALS-based safety system supports an application-specific design that will meet the auxiliary features requirements of Clause 5.12 of IEEE Std 603-1991 (see Reference 32, Section 12.2.20).

The NRC staff's review of the ALS platform against the requirements found in Clause 5.12 of IEEE Std 603-1991 is addressed in Section 3.10.2.12 of this SE.

3.11.2.13 IEEE Std 7-4.3.2-2003 Clause 5.13 – Multi-Unit Stations

Clause 5.13 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Clause 5.13 of IEEE Std 603 are necessary.

The "ALS Topical Report" states an ALS-based safety system supports an application-specific design that will meet the multi-unit station requirements of Clause 5.13 of IEEE Std 603-1991 (see Reference 32, Section 12.2.21).

The NRC staff's review of the ALS platform against the requirements found in Clause 5.13 of IEEE Std 603-1991 is addressed in Section 3.10.2.13 of this SE.

3.11.2.14 IEEE Std 7-4.3.2-2003 Clause 5.14 – Human Factors Considerations

Clause 5.14 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Clause 5.14 of IEEE Std 603 are necessary.

The "ALS Topical Report" states an ALS-based safety system supports an application-specific design that will meet the human factors requirements of Clause 5.14 of IEEE Std 603-1991 (see Reference 32, Section 12.2.22).

The NRC staff's review of the ALS platform against the requirements found in Clause 5.14 of IEEE Std 603-1991 is addressed in Section 3.11.2.14 of this SE.

3.11.2.15 IEEE Std 7-4.3.2-2003 Clause 5.15 – Reliability

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

The manufacturer treats its FPGA programs as hardware for reliability purposes. Furthermore, the manufacturer relies on the adequacy of the overall set V&V activities in conjunction with its development processes to provide sufficient reliability (see Reference 32, Section 12.2.23). The manufacturer's FPGA development procedures include regression testing of FPGA programs (see Reference 31, Sections 7.5 and 7.7) along with evaluations of any future FPGA program change to ensure the change does not adversely affect the previously established reliability through equipment qualification testing (see Reference 31, Section 7.8).

The "ALS Topical Report" cannot fully address Clause 5.15 of IEEE Std 7-4.3.2-2003, because the IEEE Std 603 reliability goals are both plant and application-specific. Nevertheless, the NRC staff evaluated the ALS platform for its ability to meet this clause.

Unlike microprocessor-based computer systems, to which Clause 5.15 of IEEE Std 7-4.3.2-2003 typically applies, the NRC staff agrees the ALS platform does not contain separate and distinct executable software. Although the ALS platform does not provide distinct and separate executable software, the manufacturer subjected the functions and circuits associated with the FPGA logic to a reliability analysis (see Section 3.6 of this SE). Furthermore, the manufacturer performed simulation testing and other IV&V activities on each FPGA program along with equipment qualification testing on a representative set of FPGA programs. During these activities, error recording and corrective actions associated with error reporting were maintained and tracked for the ALS platform, as a whole, without unique treatment of the FPGA programs, as documented in the "ALS Platform Audit Summary Report" (see Reference 127, Sections 4 and 5).

Although no field experience yet exists to record, track, or trend because the ALS platform is a new product the ALS platform contains identification features that include project-specific FPGA version and NVM configuration version identifiers in addition to the standardized circuit board hardware revision identifiers. The FPGA and NVM version identifiers may be viewed using maintenance equipment (see Section 3.11.2.11 of this SE), and the set of version identifiers support error recording, tracking, and trending for fielded equipment.

Although the "ALS Topical Report" cannot fully address Clause 5.15 of IEEE Std 7-4.3.2-2003, the NRC staff determined the ALS platform supports meeting Clause 5.15 of IEEE Std 7-4.3.2-2003. This determination is based on the platform development activities, which included reliability analyses along with error recording and tracking, and platform design features, which include FPGA, NVM, and hardware version identification. Nevertheless, evaluation of this clause requires plant-specific action. Therefore, the NRC staff also agrees evaluation of this clause is plant-specific and application-specific. As such, no broader staff determination is appropriate for the ALS platform to address Clause 5.15 of IEEE Std 7-4.3.2-2003, and a plant-specific action is necessary to ensure Clause 5.15 is met for each future ALS platform application of a safety system. Furthermore, to ensure adequate error reporting, tracking, and trending for fielded equipment, licensee purchase orders should specify 10 CFR Part 21 reporting requirements and should ensure licensee Appendix B supplier requirements for safety-related uses of the ALS platform promulgate to sub-suppliers, because the manufacturer has indicated it will act as an Appendix B supplier (see Section 3.10.2.3 of this SE).

3.11.3 IEEE Std 7-4.3.2-2003 Section 6 – Sense and Command Features - Functional and Design Requirements

Section 6 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Section 6 of IEEE Std 603 are necessary.

The "ALS Topical Report" states an ALS-based safety system supports an application-specific design that will meet the sense and command feature requirements of Section 6 of IEEE Std 603-1991 (see Reference 32, Section 12.2.24).

The NRC staff's review of the ALS platform against the requirements found in Section 6 of IEEE Std 603-1991 is addressed in Section 3.10.3 of this SE.

3.11.4 IEEE Std 7-4.3.2-2003 Section 7 – Execute Features - Functional and Design Requirements"

Section 7 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Section 7 of IEEE Std 603 are necessary.

The "ALS Topical Report" states an ALS-based safety system supports an application-specific design that will meet the execute feature requirements of Section 7 of IEEE Std 603-1991 (see Reference 32, Section 12.2.25).

The NRC staff's review of the ALS platform against the requirements found in Section 7 of IEEE Std 603-1991 is addressed in Section 3.10.4 of this SE.

3.11.5 IEEE Std 7-4.3.2-2003 Section 8 – Power Source Requirements

Section 8 of IEEE Std 7-4.3.2-2003 states no requirements beyond those found in Section 8 of IEEE Std 603 are necessary.

The "ALS Topical Report" states an ALS-based safety system supports an application-specific design that will meet the power source requirements of Section 8 of IEEE Std 603-1991 (see Reference 32, Section 12.2.26).

The NRC staff's review of the ALS platform against the requirements found in Section 8 of IEEE Std 603-1991 is addressed in Section 3.10.5 of this SE.

4.0 LIMITATIONS AND CONDITIONS

For each generic open item and plant-specific action item that applies to the applicant's or licensee's use of the ALS platform, applicants and licensees referencing this SE should demonstrate it has satisfactorily addressed the applicable items. The set of applicable items provide limitations and conditions for the ALS platform's use, as reviewed by the NRC staff and documented within this SE.

The manufacturer clarified further applicant or licensee information requirements in consideration of NUREG-0800, "U.S. Nuclear Regulatory Commission Standard Review Plan (SRP)," Chapter 7, "Instrumentation and Controls" Table 7.1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety" (see Reference 124, Item 2). Therefore, the following set of items excludes those that

depend on a specific instrumentation application, which is consistent with SRP Table7.1, the manufacturer's response, and the platform's scope.

4.1 Generic Open Items

Beyond the plant-specific action items that follow, the NRC staff identified no generic open items to be addressed by an applicant or licensee referencing this SE for installation of a safety-related system based on the ALS platform.

4.2 Plant-Specific Action Items

The following plant-specific actions should be performed by an applicant or licensee referencing this SE for a safety-related system based on the ALS platform.

1. Application-specific ALS-102 Requirements Specification(s) - An applicant or licensee referencing this SE should demonstrate it has provided application specification(s) to govern each unique ALS-102 FPGA logic program's development.

2. Application Conformance to ALS Platform Development Process - An applicant or licensee referencing this SE should demonstrate the development of its application-specific ALS-102 FPGA logic programs followed a development process equivalent to the one described and evaluated in Section 3.2.3 of this SE. When the application uses only a single FPGA design variant, this demonstration should identify the associated design variant (either “Core A” or “Core B”) and include the production and configuration control of related life-cycle development products, including those identified in Table 3.2.5-1 for that design variant, where “xxxx” represents a project specific identifier or may directly refer to “6002” if that document may be used without application-specific modification.

3. Application Conformance to “Embedded Design Diversity” Development Process - When an applicant or licensee referencing this SE specifies “Embedded Design Diversity,” the applicant or licensee should demonstrate the development of its application-specific ALS-102 FPGA logic programs followed equivalent development processes to those described and evaluated in Section 3.2.4 of this SE. This demonstration should include the production and configuration control of the related life-cycle development products, including those identified in Table 3.2.5-1 for both “Core A” and “Core B.”

4. ALS Platform Boundary/Interface Conditions and Installation Limitations - An applicant or licensee referencing this SE should address its conformance to or deviations from the manufacturer identified boundary/interface conditions and installation limitations within the “ALS Platform EQ Summary Report” (see Reference 51, Section 7). An applicant or licensee referencing this SE should identify the applicability of each condition and limitation. For each applicable condition or limitation, the applicant or licensee should either demonstrate its conformance or provide justification for any deviation. For any deviation, an applicant or licensee should demonstrate the deviation does not invalidate the ALS platform qualification in a manner adverse to the reliable performance of a safety function. Such demonstrations that deviations are justified should consider performance of supplemental testing, supplemental analysis, or both.

5. ALS Platform Application Restrictions - An applicant or licensee referencing this SE should address its adherence to the manufacturer identified application restrictions within the “ALS Application Guidance” (see Reference 41). An applicant or licensee referencing this SE should identify the applicability of each restriction. For each applicable restriction, the applicant or licensee should either demonstrate its adherence or provide justification for excluding the restriction. For any exclusion, an applicant or licensee should also demonstrate the exclusion does not invalidate the ALS platform qualification in a manner adverse to the reliable performance of a safety function. Such demonstrations should consider performance of supplemental testing, supplemental analysis, or both.

6. Demonstration of Equipment Qualification - An applicant or licensee referencing this SE should demonstrate the equipment qualification testing documented and evaluated within this SE remains valid and bounding. Otherwise, additional plant-specific equipment qualification efforts should be performed, which may include analyses and/or tests. If an applicant or licensee cannot demonstrate the “ALS Topical Report” equipment qualification remains valid and bounding, then the applicant or licensee should demonstrate plant-

specific qualification efforts are bounding. The demonstration should identify the NVM Configuration for each ALS standardized circuit board it uses and the equipment qualification that shows the circuit board's performance has been bounded for each application-specific configuration.

7. Response Time Performance - As discussed within Section 3.4.1, an applicant or licensee referencing this SE should: 1) establish application-specific design timing requirement(s) for the system; 2) perform application-specific analysis to budget the timing requirement(s) to associated components of the system architecture; 3) validate the most restrictive timing requirement for each ALS platform component used within the system architecture has been bounded by the qualified performance envelope for that ALS platform component; 4) perform verification testing that demonstrates the integrated ALS platform-based system meets each design timing requirement and performs as expected; and, 5) include appropriate technical specification surveillance requirements to confirm the equipment's digital response time characteristics, as applicable.

8. Deterministic Performance - As discussed within Section 3.4.2, an applicant or licensee referencing this SE should confirm the application specifications identify the board access sequence, frame time, and implementation of the design features to activate system alarms upon detection of a failure to meet timing requirements, so an operator can take corrective action. An applicant or licensee referencing this SE should also verify the application-specific logic does not introduce non-deterministic computation or non-deterministic digital data communications.

9. Self-Diagnostics, Test and Calibration Capabilities - As discussed within Section 3.4.3, an applicant or licensee referencing this SE should demonstrate the adequacy of the application-specific use of ALS platform diagnostic, self test, and manually initiated test and calibration features. The following should be considered:

    a. Test Coverage - The applicant or licensee should demonstrate ALS platform diagnostic, self test, and manually initiated test and calibration features are sufficient to verify the operational integrity of all logic components (i.e., all relays and contacts, trip units, solid state logic elements, etc.) of a logic circuit, from as close to the sensor as practicable up to but not including the actuated device for each safety function and with sufficient overlap.

    b. Relationship to Existing Surveillances - If a licensee proposes to use ALS platform built-in self test features to justify the elimination of existing surveillances or less frequent performance of existing surveillances, then the licensee should also demonstrate the built-in self testing provides equivalent assurance to the surveillances performed on the equipment being replaced.

    c. Reliance upon Automatic Testing - If an applicant or licensee relies upon the continued performance of diagnostic or self test features that an ALS platform-based system has been designed to automatically perform, then the surveillance procedures that the plant's technical specification references through surveillance

requirements should verify the built-in self tests results and ensure these tests continue to acceptably operate. This activity should confirm the plant's installation does not exhibit unjustified Intermediate Errors without reported failures that could adversely affect a safety function.

d. No Adverse Impact on the Reliability of Safety Functions - The applicant or licensee should demonstrate the application-specific diagnostic, self test, and manually initiated test and calibration features will not adversely affect channel independence, system integrity, or the system's ability to meet the single-failure criterion.

e. Administrative Controls to Prevent Limiting Conditions for Operation - For manual calibration or surveillance activities, the applicant or licensee should demonstrate adequate administrative controls to ensure a limiting condition for operation is not routinely entered. This demonstration should consider the functionality per channel and the overall channel, division, and voting logic arrangement of the system.

f. Conformance to RGs - The applicant or licensee should demonstrate the relationship between a) the application-specific diagnostic, self test, and manually initiated test and calibration features provided by the ALS platform and b) the conformance to the NRC staff positions in RGs 1.22 and 1.118.

10. Failure Mode and Effects Analysis - As discussed within Section 3.5, an applicant or licensee referencing this SE should perform a system-level FMEA to demonstrate the application-specific use of the ALS platform identifies each potential failure mode and determines the effects of each. The FMEA should demonstrate 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.

11. Reliability and Availability Analysis - As discussed within Section 3.6, an applicant or licensee referencing this SE should perform a deterministic system-level evaluation to determine the degree of redundancy, diversity, testability, and quality provided in an ALS platform-based safety system is commensurate with the safety functions that must be performed. An applicant or licensee should confirm a resultant ALS platform-based system meets any applicable reliability goals that the plant has established for the system. This plant-specific action should consider the effect of possible failures, system-level design features provided to prevent or limit the failures' effects, and any application-specific inclusion of a maintenance bypass to support plant operations. An applicant or licensee should demonstrate the ALS platform reliability analysis method provides an equivalent level of assurance to the applicant's or licensee's reliability analysis method.

12. Application-specific ALS-102 Digital Communications - As discussed within Section 3.7.2.1, an applicant or licensee referencing this SE and using either TxB1 or TxB2 digital data communication interface of the ALS-102 Core Logic Board should produce the application specification(s) that govern the interface and demonstrate conformance of its application to DI&C-ISG-04 staff points 2, 3, 4, 5, 7, 18, 19, and 20 under the NRC staff position for

interdivisional communications, which includes data communications between different safety divisions and data communications between a safety division and equipment that is not safety-related.

13. Application-specific TAB Communications - As discussed within Section 3.7.2.1, an applicant or licensee referencing this SE and using the TAB digital data communication interface, which is provided by each ALS platform standardized circuit board, should produce the application specification(s) that govern the interface and demonstrate conformance of its application to DI&C-ISG-04 staff points 1, 2, 3, 4, 5, 7, 8, 10, 11, 12, and 18 under the NRC staff position for interdivisional communications, which includes data communications between different safety divisions and data communications between a safety division and equipment that is not safety-related.

14. Application-specific ALS-601 Digital Communications - As discussed within Section 3.7.2.1, an applicant or licensee referencing this SE and using the ALS-601 Communication Board should produce the application specification(s) that govern each communication channel and demonstrate conformance of its application to DI&C-ISG-04 staff points 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 15, 16, 17, 18, 19, and 20 under the NRC staff position for interdivisional communications.

15. Application-specific Command Prioritization - As discussed within Section 3.7.2.2, an applicant or licensee referencing this SE and implementing command prioritization with ALS platform components should produce the application specification(s) that govern each priority module application and demonstrate conformance of each application to DI&C-ISG-04 staff points 1 through 10 under the NRC staff position for command prioritization.

16. Application-specific Multidivisional Control and Display Stations - As discussed within Section 3.7.2.3, an applicant or licensee referencing this SE and implementing multidivisional control or a multidivisional display station should produce the application specification(s) that govern each multidivisional control or multidivisional display station application and demonstrate conformance of each application to DI&C-ISG-04 Staff Position 3 for multidivisional control and display stations.

17. Secure Development Environment for Applications - As discussed within Section 3.8, an applicant or licensee referencing this SE for a safety-related plant-specific application should ensure the development environment for its plant-specific application continues to meet the applicable regulatory evaluation criteria of RG 1.152.

18. Secure Operational Environment - As discussed within Section 3.8, an applicant or licensee referencing this SE for a plant-specific application should ensure the operational environment for its safety-related plant-specific applications meets the applicable regulatory evaluation criteria of RG 1.152.

19. Demonstration of Adequate Diversity – As discussed within Section 3.9, an applicant or licensee referencing this “ALS Topical Report” SE should identify the approaches specified

to provide built-in diversity and mitigations against CCFs within its application of the ALS platform. The following should be considered:

a. Embedded Design Diversity - ALS application specifications should designate whether Embedded Design Diversity is required in addition to Core Diversity for each safety function performed by that application. When Embedded Design Diversity is required, the specifications should also identify the required arrangement of the independent designs among channels, trains and electrical separation groups.

b. Application Specific Core Diversity Comparison Checks - Specifications should identify any application-specific ALS-102 logic signals that need to be subject to the Core Diversity comparison checks.

c. Fail Safe Behavior - Specifications should identify application-specific fail-safe behavior that should result from any comparison check mismatch.

d. Additional Diversity Measures - Specifications should identify any additional diversity measures, such as functional, signal, or additional logic diversity, that are included in the safety system in the context of maintaining plant safety.

e. Extent of Built in Diversity - The applicant or licensee should describe the extent that it relies upon the techniques and processes that provide levels of defense against programming CCFs, which are described in Section 3.3 of the “ALS Diversity Analysis” (Reference 46), for its use of the ALS platform and its application-specific

   ALS-102 logic. Using this information, the licensee should demonstrate the application adequately addresses potential plant vulnerabilities to common-cause programming failures in consideration of BTP 7-19 and DI&C-ISG-02, as applicable.

f. Identification of Echelons of Defense – Applicant or licensee D3 Analysis should identify the echelon(s) of defense (i.e., control, RTS, ESFAS, and monitoring and display) within the plant that each ALS platform-based I&C function is assigned.

g. Diverse Manual Control Features - When manual controls are not provided as discrete hardwired components connected to the safety equipment at a point downstream of the plant's digital I&C safety system outputs, the applicant or licensee D3 Analysis should demonstrate simple (e.g., component function can be completely demonstrated by test), dedicated, and diverse program-based digital equipment performs any coordinated system-level actuation logic, if applicable.

20. IEEE Std 603-1991 Compliance – As discussed within Section 3.10 of this SE, although the NRC staff determined the ALS platform supports meeting various sections and clauses of IEEE Std 603-1991, an applicant or licensee referencing this SE should identify the approach taken to meet each applicable clause of IEEE Std 603-1991. The applicant or licensee should consider its plant-specific design basis because the “ALS Topical Report” scope is limited. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. Therefore, an applicant or licensee

should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std 603-1991 clause to its application-specific ALS-based safety system or component. As described within Section 3.10 of this SE, the applicant or licensee should demonstrate the plant-specific and application-specific use of the ALS platform meets the applicable IEEE Std 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

21. Demonstration of Sufficient Isolation - An applicant or licensee referencing this SE should identify all safety/nonsafety interfaces and interdivisional interfaces, and for each interface the applicant or licensee should demonstrate sufficient isolation has been provided by a qualified isolation device to meet IEEE Std 603 Clause 5.6.3.1(2), IEEE Std 384-1992, as endorsed by RG 1.75 and in accordance with BTP 7-11, and DI&C-ISG-04, as applicable. The application-specific information should identify the maximum credible voltage associated with each plant-specific use of each interface, and demonstrate each qualified isolation device applied to each interface is compatible with its maximum credible voltage and sufficient to prevent damage to the ALS platform safety-related components covered by this SE.

22. IEEE Std 7-4.3.2-2003 Compliance – As discussed within Section 3.11 of this SE, although the NRC staff determined the ALS platform supports meeting various sections and clauses of IEEE Std 7-4.3.2-2003, an applicant or licensee referencing this SE should identify the approach taken to meet each applicable clause of IEEE Std 7-4.3.2-2003. The applicant or licensee should consider its plant-specific design basis, because the “ALS Topical Report” scope is limited. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. The applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std 7-4.3.2-2003 clause to its application-specific ALS-based safety system or component. As further described within Section 3.11 of this SE, the applicant or licensee should demonstrate the plant-specific and application-specific use of the ALS platform meets the applicable IEEE Std 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.

23. IEEE Std 1012-1998 Compliance – As discussed within Section 3.11.2.3.3 of this SE, although the NRC staff determined the ALS platform IV&V processes support various sections and clauses of IEEE Std 1012-1998, an applicant or licensee referencing this SE should demonstrate it has fulfilled the tasks that have been deferred to an applicant’s or licensee’s use of the ALS platform. Some IEEE Std 1012-1998 tasks cannot be fulfilled within the ALS platform topical report scope, because the task is project-specific, such as hazard analysis and risk analysis. Other IEEE Std 1012-1998 tasks cannot be fulfilled within the ALS platform topical report scope, because the task is not performed on a platform component, such as system integration test, system acceptance test, installation, operation, and maintenance tasks. An applicant or licensee referencing this SE should ensure appropriate activities are included in its project-specific V&V plan and the performance of each activity is acceptably independent. The project-specific V&V plan should identify any

alternative method(s) to IEEE Std 1012-1998 for any IV&V task and demonstrate the alternative method(s) provides equivalent assurance.

5.0 REFERENCES

Staff Acceptance Letter

1. "Acceptance for Review of CS Innovations Advanced Logic System Topical Report," dated October 29, 2010 (Non-proprietary - ML102730833)

Precedent SE and References

2. "Wolf Creek Generating Station - Issuance of Amendment Re: Modification of the Main Steam and Feedwater Isolation System Controls (TAC No. MD4839)," dated March 31, 2009 (Non-proprietary - ML090610317)
3. Wolf Creek Nuclear Operating Corporation, "MSFIS D3 Assessment," Rev 2, dated January9, 2009 (Non-proprietary - ML090270825)
4. "Westinghouse Electric Company Quality Management System, Revision 6 (TAC No. ME5256)," dated February 24, 2011 (Non-proprietary - ML110310088)

Transmittal Letters Submitting Topical Report Information

5. "CS Innovations ALS Topical Report and Supporting Documents Submittal," dated July 29, 2010 (Non-proprietary - ML102160471)
6. "CS Innovations ALS Topical Report and Supporting Documents Submittal Follow Up of Non-proprietary Document Versions," dated August 13, 2010 (Non-proprietary - ML102570791)
7. "CS Innovations ALS Topical Report and Supporting Documents Submittal," dated February 8, 2011 (Non-proprietary - ML110410380)
8. "CS Innovations ALS Topical Report and Supporting Documents Submittal," dated February 25, 2011 (Non-proprietary - ML110600671)
9. "CS Innovations ALS Topical Report and Supporting Documents Submittal," dated March 18, 2011 (Non-proprietary - ML110810494)
10. "CS Innovations ALS Topical Report and Supporting Documents Submittal," dated March 25, 2011 (Non-proprietary - ML110900127)
11. 9200-00005, "Advanced Logic System Topical Report and Supporting Documents Submittal," dated November 11, 2011 (Non-proprietary - ML11320A047)
12. 9200-00006, "Advanced Logic System Topical Report and Supporting Documents Submittal," dated February 10, 2012 (Non-proprietary - ML12048B425)
13. 9200-00009, "Advanced Logic System Topical Report and Supporting Documents Submittal," dated April 5, 2012 (Non-proprietary - ML12097A320)
14. 9200-00010, "Advanced Logic System Topical Report and Supporting Documents Submittal," dated April 25, 2012 (Non-proprietary - ML12118A364)

15. 9200-00011, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated May 1, 2012 (Non-proprietary - ML12123A716)

16. 9200-00013, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated July 24, 2012 (Non-proprietary - ML12208A253)

17. 9200-00014, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated August 30, 2012 (Non-proprietary - ML12244A442)

18. 9200-00016, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated November 1, 2012 (Non-proprietary - ML12318A154)

19. 9200-00017, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated November 15, 2012 (Non-proprietary - ML12332A181)

20. 9200-00018, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated December 4, 2012 (Non-proprietary - ML12342A194)

21. 9200-00020, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated January 30, 2013 (Non-proprietary - ML13037A687)

22. 9200-00019, “Advanced Logic System Topical Report and Supporting Documents Submittal,” Revision 1, dated February 6, 2013 (Non-proprietary - ML13036A378)

23. 9200-00021, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated February 15, 2013 (Non-proprietary - ML13060A260)

24. 9200-00023, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated March 4, 2013 (Non-proprietary – ML13078A179)

25. 9200-00024, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated March 6, 2013 (Non-proprietary - ML13078A178)

26. 9200-00025, “Advanced Logic System Topical Report and Supporting Documents Submittal,” dated March 27, 2013 (Non-proprietary - ML13108A079)

CSI Corporate Documents

27. 9000-00000, “CSI Quality Assurance Manual,” Revision 6, dated November 11, 2011 (Proprietary - ML11320A102)

28. 9000-00311, “Electronics Development Procedure,” Revision 4, dated July 29, 2010 (Proprietary - ML102160485)

29. NA 4.50, “Electronics Development Procedure,” Revision 0, August 31, 2012 (Proprietary - ML12332A311)

30. 9000-00313, “FPGA Development Procedure,” Revision 4, September 6, 2012 (Proprietary - ML12332A315)

31. NA 4.51, “FPGA Development Procedure,” Revision 1, January 1, 2013 (Proprietary - ML13036A400)

Platform Documents

32. 6002-00301, “ALS Topical Report” Revision 4, February 2, 2013 (Proprietary - ML13060A271, Non-proprietary - ML13078A233)
33. 6002-00000, “ALS Management Plan,” Revision 7, October 2012 (Proprietary - ML12332A212, Non-proprietary - ML12332A215)
34. 6002-00001, “ALS Quality Assurance Plan,” Revision 9, October 25, 2012 (Proprietary - ML12332A249, Non-proprietary - ML12332A250)
35. 6002-00002, “ALS Configuration Management Plan,” Revision 9, February 2013 (Proprietary - ML13060A263, Non-proprietary - ML13060A262)
36. 6002-00003, “ALS V&V Plan,” Revision 8, January 2013 (Proprietary - ML13108A089), Non-proprietary - ML13108A088)
37. 6002-00004, “ALS EQ Plan,” Revision 8, December 2012 (Proprietary - ML13036A379)
38. 6002-00005, “ALS Test Plan,” Revision 4, March 1, 2013 (Proprietary – ML13078A234)
39. 6002-00006, “ALS Security Plan,” Revision 1, November 16, 2012 (Proprietary - ML13036A380)
40. 6002-00007, “ALS Platform Configuration Status Accounting,” Revision 10, March 4, 2013 (Proprietary - ML13078A235)
41. 6002-00008, “ALS Application Guidance,” Revision 4, February 2013 (Proprietary - ML13060A266)
42. 6002-00009, “ALS Platform Requirements Traceability Matrix,” Revision 3, February 11, 2013 (Proprietary - ML13060A267)
43. 6002-00010, “ALS Platform Requirements Specification,” Revision 17, January 30, 2013 (Proprietary - ML13060A268)
44. 6002-00011, “ALS Platform Specification,” Revision 13, January 30, 2013 (Proprietary - ML13060A269)
45. 6002-00018, “ALS Platform FPGA VV Test Plan,” Revision 9, February 2013 (Proprietary - ML13060A270)
46. 6002-00030, “ALS Design Tools,” Revision 9, December 13, 2012 (Proprietary - ML13036A386)
47. 6002-00031, “ALS Diversity Analysis,” Revision 2, January 2013 (Proprietary - ML13038A178)
48. 6002-00040, “ALS Terms and Abbreviations,” Revision 3, September 27, 2012 (Proprietary - ML13078A236)
49. 6002-00060, “ALS Board Manufacturing Procedures,” Revision 1, September 12, 2012 (Proprietary - ML13078A217)
50. 6002-00070, “ALS EQ Rack System Specification,” Revision 5, January 11, 2013 (Proprietary - ML13036A387)

51. 6002-00200, “ALS Platform EQ Summary Report,” (parts 1 and 2) Revision 2, January 2013 (Proprietary - ML13038A179, ML13038A180)

52. 6002-00240, “ALS Platform Qualification Evaluation,” Revision 0, January 16, 2013 (Proprietary - ML13036A391)

53. 6002-00400, “ALS Platform Configuration Management Summary Report,” Revision 3, March 2013 (Proprietary - ML13078A239)

54. 6002-00500, “ALS Platform VV Summary Report,” Revision 2, February 2013 (Proprietary - ML13060A275)

Circuit Board Documents

55. 6002-10201, “ALS-102 Requirements Specification,” Revision 3, December 17, 2012 (Proprietary - ML13036A393)

56. 6002-10212, “ALS-102 FPA, FMEA, and Reliability Analysis,” Revision 2, October 8, 2012 (Proprietary - ML12332A371)

57. 6002-10250, “ALS-102 Configuration Status Accounting,” Revision 4, February 10, 2013 (Proprietary - ML13060A278)

58. 6002-10281, “ALS-102 Configuration Management Summary Report,” Revision 6, February 2013 (Proprietary - ML13060A280)

59. 6002-10282, “ALS-102 VV Summary Report,” Revision 2, February 2013 (Proprietary - ML13060A281)

60. 6002-10294, “ABTS-102 Test Summary Report,” Revision 2, February 2013 (Proprietary - ML13060A282)

61. 6002-30201, “ALS-302 Requirements Specification,” Revision 4, December 18, 2012 (Proprietary - ML13036A394)

62. 6002-30212, “ALS-302 FPA, FMEA, and Reliability Analysis,” Revision 2, October 8, 2012 (Proprietary - ML12332A398)

63. 6002-30250, “ALS-302 Configuration Status Accounting,” Revision 5, February 10, 2013 (Proprietary - ML13060A285)

64. 6002-30281, “ALS-302 Configuration Management Summary Report,” Revision 7, February 2013 (Proprietary - ML13060A286)

65. 6002-30282, “ALS-302 VV Summary Report,” Revision 3, February 2013 (Proprietary - ML13060A287)

66. 6002-30294, “ABTS-302 Test Summary Report,” Revision 2, February 2013 (Proprietary - ML13060A288)

67. 6002-31101, “ALS-311 Requirements Specification,” Revision 3, December 18, 2012 (Proprietary - ML13036A395)

68. 6002-31112, “ALS-311 FPA, FMEA, and Reliability Analysis,” Revision 2, October 11, 2012 (Proprietary - ML12334A059)

69. 6002-31150, “ALS-311 Configuration Status Accounting,” Revision 5, February 14, 2013 (Proprietary - ML13060A291)

70. 6002-31181, “ALS-311 Configuration Management Summary Report,” Revision 7, February 2013 (Proprietary - ML13060A292)

71. 6002-31182, “ALS-311 VV Summary Report,” Revision 4, February 2013 (Proprietary - ML13060A293)

72. 6002-31194, “ABTS-311 Test Summary Report,” Revision 2, February 2013 (Proprietary - ML13060A295)

73. 6002-32101, “ALS-321 Requirements Specification,” Revision 3, December 18, 2012 (Proprietary - ML13060A296)

74. 6002-32112, “ALS-321 FPA, FMEA, and Reliability Analysis,” Revision 2, October 8, 2012 (Proprietary - ML12334A047)

75. 6002-32150, “ALS-321 Configuration Status Accounting,” Revision 5, February 11, 2013 (Proprietary - ML13060A298)

76. 6002-32181, “ALS-321 Configuration Management Summary Report,” Revision 7, February 2013 (Proprietary - ML13060A299)

77. 6002-32182, “ALS-321 VV Summary Report,” Revision 3, February 2013 (Proprietary - ML13060A300)

78. 6002-32194, “ABTS-321 Test Summary Report,” Revision 3, February 2013 (Proprietary - ML13060A301)

79. 6002-40201, “ALS-402 Requirements Specification,” Revision 2, December 18, 2012 (Proprietary - ML13036A397)

80. 6002-40212, “ALS-402 FPA, FMEA, and Reliability Analysis,” Revision 2, October 8, 2012 (Proprietary - ML12334A100)

81. 6002-40250, “ALS-402 Configuration Status Accounting,” Revision 5, February 10, 2013 (Proprietary - ML13060A304)

82. 6002-40281, “ALS-402 Configuration Management Summary Report,” Revision 6, February 2013 (Proprietary - ML13060A305)

83. 6002-40282, “ALS-402 VV Summary Report,” Revision 3, February 2013 (Proprietary - ML13060A308)

84. 6002-40294, “ABTS-402 Test Summary Report,” Revision 2, February 2013 (Proprietary - ML13060A310)

85. 6002-42101, “ALS-421 Requirements Specification,” Revision 6, December 18, 2012 (Proprietary - ML13036A398)

86. 6002-42112, “ALS-421 FPA, FMEA, and Reliability Analysis,” Revision 2, October 26, 2012 (Proprietary - ML12334A160)

87. 6002-42150, “ALS-421 Configuration Status Accounting,” Revision 3, February 11, 2013 (Proprietary - ML13060A313)

88. 6002-42181, “ALS-421 Configuration Management Summary Report,” Revision 5, February 2013 (Proprietary - ML13060A314)

89. 6002-42182, “ALS-421 VV Summary Report,” Revision 1, February 2013 (Proprietary - ML13060A315)

90. 6002-42194, “ABTS-421 Test Summary Report,” Revision 3, February 2013 (Proprietary - ML13060A316)

91. 6002-60101, “ALS-601 Requirements Specification,” Revision 4, December 18, 2012 (Proprietary - ML13036A399)

92. 6002-60112, “ALS-601 FPA, FMEA, and Reliability Analysis,” Revision 2, October 10, 2012 (Proprietary - ML12334A139)

93. 6002-60150, “ALS-601 Configuration Status Accounting,” Revision 4, February 11, 2013 (Proprietary – ML13060A319)

94. 6002-60181, “ALS-601 Configuration Management Summary Report,” Revision 5, February 2013 (Proprietary – ML13060A320)

95. 6002-60182, “ALS-601 VV Summary Report,” Revision 1, February 2013 (Proprietary – ML13060A321)

96. 6002-60194, “ABTS-601 Test Summary Report,” Revision 2, February 2013 (Proprietary – ML13060A322)

FPGA Documents

97. 6002-00016, “FPGA Core A Common Module Design Specification,” Revision 5, December 17, 2012 (Proprietary - ML13036A385)

98. 6002-00017, “ALS FPGA Core B Common Module Design Specification,” Revision 1, August 23, 2012 (Proprietary - ML12332A288)

99. 6002-00241, “ALS FPGA Qualification Evaluation,” Revision 1, January 2013 (Proprietary - ML13036A392)

100. 6002-10210, “ALS-102 Core A Requirements Traceability Matrix,” Revision 3, February 6, 2013 (Proprietary - ML13060A276)

101. 6002-10211, “ALS-102 Core B Requirements Traceability Matrix,” Revision 3, February 6, 2013 (Proprietary - ML13060A277)

102. 6002-10216, “ALS-102 VV Simulation Environment Specification,” Revision 0, August 28, 2012 (Proprietary - ML12342A198)

103. 6002-30210, “ALS-302 Core A Requirements Traceability Matrix,” Revision 6, February 6, 2013 (Proprietary - ML13060A283)

104. 6002-30211, “ALS-302 Core B Requirements Traceability Matrix,” Revision 4, February 6, 2013 (Proprietary - ML13060A284)

105.6002-30216, “ALS-302 VV Simulation Environment Specification,” Revision 3, August 2012 (Proprietary - ML12342A200)

106.6002-31110, “ALS-311 Core A Requirements Traceability Matrix,” Revision 4, February 14, 2013 (Proprietary - ML13060A289)

107.6002-31111, “ALS-311 Core B Requirements Traceability Matrix,” Revision 4, February 14, 2013 (Proprietary - ML13060A290)

108.6002-31116, “ALS-311 VV Simulation Environment Specification,” Revision 4, December 2012 (Proprietary - ML13078A240)

109.6002-32110, “ALS-321 Core A Requirements Traceability Matrix,” Revision 7, February 6, 2013 (Proprietary - ML13060A296)

110.6002-32111, “ALS-321 Core B Requirements Traceability Matrix,” Revision 5, February 6, 2013 (Proprietary - ML13060A297)

111.6002-32116, “ALS-321 VV Simulation Environment Specification,” Revision 3, October 2012 (Proprietary - ML12342A205)

112.6002-40210, “ALS-402 Core A Requirements Traceability Matrix,” Revision 4, February 6, 2013 (Proprietary - ML13060A302)

113.6002-40211, “ALS-402 Core B Requirements Traceability Matrix,” Revision 4, February 6, 2013 (Proprietary - ML13060A303)

114.6002-40216, “ALS-402 VV Simulation Environment Specification,” Revision 0, August 2012 (Proprietary - ML12342A208)

115.6002-42110, “ALS-421 Core A Requirements Traceability Matrix,” Revision 4, February 6, 2013 (Proprietary - ML13060A311)

116.6002-42111, “ALS-421 Core B Requirements Traceability Matrix,” Revision 4, February 6, 2013 (Proprietary - ML13060A312)

117.6002-42116, “ALS-421 VV Simulation Environment Specification,” Revision 3, October 2012 (Proprietary - ML12342A210)

118.6002-60110, “ALS-601 Core A Requirements Traceability Matrix,” Revision 4, February 6, 2013 (Proprietary - ML13060A317)

119.6002-60111, “ALS-601 Core B Requirements Traceability Matrix,” Revision 4, February 6, 2013 (Proprietary - ML13060A318)

120.6002-60116, “ALS-601 VV Simulation Environment Specification,” Revision 0, August 2012 (Proprietary - ML12342A212)

Requests for Additional Information and Responses

121.“Request for Additional Information, CS Innovations - Advanced Logic Systems Topical Report (TAC No. ME4454),” dated July 14, 2011 (Non-proprietary - ML111751722)

122. LTR-NRC-11-42, "Responses to Requests for Additional Information on 6002-00301, CS Innovations' Advanced Logic System Topical Report" dated August 9, 2011 (Non-proprietary - ML11234A053)

123. "Second Request for Additional Information on Topical Report 6002-00301, 'Advanced Logic System Topical Report' (TAC No. ME4454)," dated May 20, 2013 (Non-proprietary - ML13133A039)

124. LTR-NRC-13-36, "Response to Second NRC Request for Additional Information Regarding Topical Report 6002-00301, Revision 4, 'Advanced Logic System Topical Report'," dated May 31, 2013 (Non-proprietary – ML13157A003)

Audit Plan, Report, and Response

125. "Regulatory Audit Plan for October 30, 2012, through November 2, 2012, Audit of CS Innovations, LLC and Westinghouse Electric Company at the Scottsdale, Arizona and Cranberry, Pennsylvania Facilities for the Advanced Logic System Topical Report (TAC No. ME4454)" dated October 30, 2012 (Non-proprietary - ML12275A005)

126. "Regulatory Audit Report of CS Innovations/Westinghouse, November 26-30, 2012, at Scottsdale, Arizona and Warrendale, Pennsylvania Facilities for the Advanced Logic System Topical Report (TAC No. ME4454)" dated February 4, 2013 (Non-proprietary - ML12355A134)

127. "ALS Platform Audit Summary Report" dated February 4, 2013 (Proprietary- ML13016A422, Non-proprietary - ML12355A135)

128. 9200-00022, "Reply to the ALS Audit Report Observations Reference: ML12355A132)" dated February 15, 2013 (Proprietary - ML13051A271)

6.0 CONCLUSION

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

Attachment: Comment Resolution Table

Principal Contributor: Bernard Dittman

Date: September 9, 2013