March 3, 2017

Jack Rosentel
Program Technical Licensing Manager
Lockheed Martin Nuclear Systems and Solutions
459 Kennedy Drive
Archbald, PA 18403

SUBJECT: FINAL SAFETY EVALUATION OF NuPAC_ED610000-47-P, REVISION-, "GENERIC QUALIFICATION OF THE NuPAC PLATFORM FOR SAFETY-RELATED APPLICATIONS (NONPROPRIETARY)" (TAC NO. ME7900)

Dear Mr. Rosentel:

By letter dated June 28, 2011 (Agencywide Documents Access and Management System (ADAMS) Accession No.ML11201A323), Lockheed Martin Nuclear Systems and Solutions (LMNSS) submitted the topical report (TR) NuPAC_ED610000-47-P, Revision-, "Generic Qualification of the NuPAC Platform for Safety-related Applications (Proprietary)." The original submittal was supplemented by over 50 submittals that are detailed in the reference section of the attached safety evaluation (SE).

By letter dated December 8, 2016 (ADAMS Accession No. ML16161A015), a U.S. Nuclear Regulatory Commission (NRC) draft SE was provided for your review and comment. By letter dated December 14, 2016 (ADAMS Accession No. ML16363A173), LMNSS provided comments on the NRC draft SE. The comments provided by LMNSS were related to the identification of proprietary information in the draft SE, clarifications, and accuracy. The NRC staff's disposition of the LMNSS comments on the draft SE is documented in the final SE enclosed with this letter.

The NRC staff has found that NuPAC_ED610000-47-P, Revision- is acceptable for referencing in licensing applications for nuclear power plants to the extent specified and under the limitations delineated in the TR and in the enclosed final SE. The final SE defines the basis for our acceptance of the TR.

Our acceptance applies only to material provided in the subject TR. We do not intend to repeat our review of the acceptable material described in the TR. When the TR appears as a reference in licensing action request, our review will ensure that the material presented applies to the specific plant involved. Requests for licensing actions that deviate from this TR will be subject to a plant-specific review in accordance with applicable review standards.

In accordance with the guidance provided on the NRC website, we request that LMNSS publish an approved proprietary and non-proprietary versions of TR NuPAC_ED610000-47-P, Revision- within three months of receipt of this letter. The approved versions shall incorporate this letter and the enclosed final SE after the title page.

LMNSS provided a completely revised topical report after the NRC staff requests for additional information (RAIs) were issued and answered. Providing the RAIs in the –A version of the topical report would not add any value. Thus, the NuPAC –A topical report does not need to include the RAIs and answers from the original version in the final –A version.

If future changes to the NRC's regulatory requirements affect the acceptability of this TR, LMNSS will be expected to revise the TR appropriately or justify its continued applicability for subsequent referencing. Licensees referencing this TR would be expected to justify its continued applicability or evaluate their plant using the revised TR.

Sincerely,

/RA/

Kevin Hsueh, Chief
Licensing Processes Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 780

Enclosure:
Final Safety Evaluation (Non-proprietary)

SUBJECT: FINAL SAFETY EVALUATION OF NuPAC_ED610000-47-P, REVISION-, "GENERIC QUALIFICATION OF THE NuPAC PLATFORM FOR SAFETY-RELATED APPLICATIONS (NONPROPRIETARY)" (TAC NO. ME7900) DATED: MARCH 3, 2017

DISTRIBUTION:

PUBLIC	KHsueh	RidsNrrDeEvib	RidsNrrDpr	MWaters
NCarte	RidsNrrDlr	RidsNrrDlrRarb	RidsNrrLADHarrison	RidsNroOd
RidsNrrDeEmcb	JZhao	RidsACRS_MailCTR	RidsResOd	RidsNrrDe
RidsOgcMailCenter	RidsNrrDprPlpb			

ADAMS Accession Nos.: ML16165A401; *via e-mail

OFFICE	NRR/DPR/PLPB	NRR/DPR/PLPB*	NRR/DE/EICB	NRR/DPR/PLPB
NAME	JHolonich	DHarrison*	MWaters	KHsueh
DATE	12/29/2016	01/26/2017	02/09/2017	03/03/2017

OFFICIAL RECORD COPY

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION
LOCKHEED MARTIN NUCLEAR SYSTEM AND SOLUTIONS,
NUPAC ED610000-47-P, REVISION - "GENERIC QUALIFICATION OF THE NUPAC PLATFORM FOR SAFETY-RELATED APPLICATIONS," TOPICAL REPORT
(TAC NO. ME7900)

1.0 INTRODUCTION

By letter dated June 28, 2011 (Ref. 1.), Lockheed Martin Nuclear Systems and Solutions (Lockheed Martin) submitted a topical report (TR), NuPAC_ED610000-47-P, Revision -, "Generic Qualification of the [Nuclear Protection and Control (NuPAC)] Platform for Safety-related Applications (Proprietary)" (Ref. 1.a.) which proposes to use a Field Programmable Gate Array (FPGA) based instrumentation and control (I&C) platform to implement safety systems in nuclear power plants. Subsequently Lockheed Martin supplemented the application with additional information (Refs. 2-53). The TR is for a generic platform, not a plant-specific implementation.

The NuPAC development effort is a joint collaboration between Lockheed Martin Global, Inc. and State Nuclear Power Automation System (SNPAS) Engineering Company. As a topical report for US submittal, Lockheed Martin maintained the technical and licensing leadership for NuPAC. Lockheed Martin staff and SNPAS staff jointly developed system requirements, hardware design, and test procedures for the NuPAC platform. Lockheed Martin maintained overall responsibility and ownership for the work products submitted to NRC for review. For example, all docketed information were specifically required to have Lockheed Martin personnel as author or Appendix B/NQA-1 independent reviewer, without exception.

The NuPAC platform is intended to be used in safety-related applications in nuclear power plants (NPPs) in the United States (US). It is designed to be installed as original equipment for new NPP facilities, and to replace existing analog and CPU-based instrumentation and control (I&C) systems currently used in US NPP applications.

The NuPAC platform is functionally and physically similar to commercially available programmable logic controllers (PLCs). Its platform capabilities include input processing, customizable logic solving, and output processing. The NuPAC platform offers modularity and scalability, similar to a PLC, via the configuration of chassis installed logic solving modules. The platform features a modular decentralized (distributed) Field Programmable Gate Array (FPGA)-based architecture.

As discussed in this SE, the NRC staff determined the NuPAC platform is acceptable for use in safety-related I&C systems. The standardized circuit boards, design features, and production processes for the generic NuPAC platform support the applicable regulatory requirements for use within plant safety-related I&C systems, subject to the plant-specific limitations and conditions delineated in Section 4.1, and resolution of the open items in Section 4.2 of the SE.

Section 2.0 of this safety evaluation (SE) identifies the applicable regulatory bases and corresponding guidance and regulatory acceptance criteria against which the NRC staff evaluated the TR submittals. Section 3.0 starts with a description of the NuPAC platform and subsequently provides the technical evaluation of the TR submittals. Section 4.0 provides the limitations and conditions that apply to the use of the NuPAC 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.

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 acceptance criteria 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, establish the review process for digital I&C (DI&C) systems, which the NRC staff applied in this evaluation.

The suitability of a 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 platform's verification, validation, and qualification efforts. Because this equipment is intended for use in safety systems the NuPAC TR 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 NuPAC TR 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 SRP 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, regulations from 10 CFR Part 50, and regulatory guides (RGs), applicable to I&C systems and relevant to the general review of the suitability of a DI&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 TR presents elements of hardware and board-level FPGA programming that constitute the NuPAC 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 the NuPAC TR scope excludes 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 NuPAC 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 review of a full system design. Plant-specific action items have been established to identify criteria that should be addressed (see Section 4.1). In part, this criteria is provided to facilitate establishing full compliance with the design criteria and regulations identified in SRP Chapter 7, Table 7-1. In addition to the plant-specific action items identified in Section 4.1, site-specific licensees are responsible for addressing any new or changed design criteria in the platform and applicable regulations.

The cyber security aspects of a digital safety system in a nuclear power plant must meet the requirements in 10 CFR 73.54. The components and processes described in the NuPAC topical report were not evaluated against the criteria in 10 CFR 73.54.

2.1 Applicable regulations and guidance

The following regulations and guidance are applicable to the TR:

10 CFR 50.48	"Fire Protection."
10 CFR 50.49	"Environmental qualification of electric equipment important to safety for nuclear power plants." Subpart (c) defines a mild environment.
10 CFR Part 50, Appendix B	"Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."
10 CFR Part 50, Appendix S,	"Earthquake Engineering Criteria for Nuclear Power Plants."
10 CFR 50.54(jj) and 10 CFR 50.55(i)	Requires that structures, systems, and components subject to the codes and standards in 10 CFR 50.55a 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)	Requires compliance to the 1991 version of IEEE Standard 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 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 (GDC), when evaluating the TR for use in safety systems, as follows:

GDC 1 "Quality Standards and Records"

Addressed because Evaluation is against Appendix B: Generic Letter 84-01, "NRC use of the terms, "Important to Safety" and "Safety Related"," states:

> "pursuant to our regulations, nuclear power plant permittees or licensees are responsible for developing and implementing quality assurance programs for plant design and construction or for plant operation which meet the more general requirements of General Design Criterion for plant

equipment "important to safety," and the more prescriptive requirements of Appendix B to 10 CFR part 50 for "safety-related" plant equipment."

Therefore, GDC 1 contains the general requirements for quality assurance program for "important to safety" equipment. Appendix B contains the more prescriptive requirements for "safety-related" plant equipment. The NuPAC equipment is considered safety-related.

GDC 2 "Design Bases for Protection against Natural Phenomena"

GDC 4 "Environmental and Dynamic Effects Design Bases"

GDC 13 "Instrumentation and Control"

Not Applicable: This criterion contain functional requirements for all I&C equipment; therefore it is not applicable to a generic platform TR. Environmental criteria are addressed under GDC 2, 4, and 22.

GDC 20 "Protection System Functions"

Not Applicable: This criterion contain functional requirements for protection systems; therefore it is not applicable to a generic platform TR. Environmental criteria are addressed under GDC 2, 4, and 22.

GDC 21 "Protection System Reliability and Testability"

GDC 22 "Protection System Independence"

GDC 23 "Protection System Failure Modes"

GDC 29 "Protection against Anticipated Operational Occurrences"

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

RG 1.22 "Periodic Testing of Protection System Actuation Functions," Rev 0.

Not Applicable: This RG contains application specific functional criteria that cannot be addressed by a generic platform TR.

RG 1.53 "Application of the Single-Failure Criterion to Safety Systems," Rev. 2.

RG 1.75 "Criteria for Independence of Electric Safety Systems," Rev. 3.

RG 1.89 "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," Rev. 1.

Not Applicable: This RG is applicable to harsh environments, and the NuPAC equipment is only qualified to mild environments. RG 1.209 is applicable for I&C equipment in mild environments.

RG 1.100 “Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants,” Revision 3.

RG 1.105 “Setpoints for Safety-Related Instrumentation,” Revision 3. Additional guidance on the establishment of instrument setpoints can be found in Regulatory Information Summary (RIS) 2006-0017, “NRC Staff Position on the Requirements of 10 CFR 50.36, "Technical Specifications," Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels” (ADAMS accession number ML051810077).

RG 1.152 “Criteria for Use of Computers In Safety Systems of Nuclear Power Plants,” Revision 3.

RG 1.168 “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 2.

RG 1.169 “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 1.

RG 1.170 "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1.

RG 1.171 “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1.

RG 1.172 "Software Requirements Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants," Revision 1.

RG 1.173 "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1.

RG 1.180 “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Revision 1.

RG 1.209 “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants.”

DI&C-ISG-04 “Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc),” Revision 1.

The NRC staff also considered applicable portions of the branch’s technical positions (BTPs) and other 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."

Not Applicable: The NuPAC TR specifically excludes Electrical Isolation Devices from the scope of the TR.

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 7-21 "Guidance on Digital Computer Real-Time Performance"

3.0 TECHNICAL EVALUATION

The following subsections identify and describe the NuPAC platform's 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 NuPAC platform, including the components and architecture. Each of the remaining subsections provides a specific technical evaluation against the applicable regulatory evaluation criteria.

The evaluation subsections below generally consists of four types of information (often in four separate paragraphs): (1) Description of topical area, (2) Summary of the applicable regulatory criteria, (3) Summary of the information docketed to address the topical area, and (4) Evaluation of the docketed information against the applicable criteria.

3.1 Platform Description

The scope of coverage of the NuPAC TR is the design basis and the design of:

- The hardware components including:
    - the chassis, all necessary wiring, interconnections, and its cooling (i.e., fans)
    - the backplane (mid-plane)
    - the Rear Transition Module,
    - The Generic Logic Module (GLM), including:
        - the family of six input/output (I/O) mezzanine cards
        - the logic mezzanine, containing the Core and Application-Specific FPGAs
        - the carrier card
        - GLM power distribution and power auctioneering.
- The Core Programmable Logic (PL) on the logic mezzanine including:
    - Basic board support and I/O management
    - Built-in test (BIT) of GLM hardware and non-application-specific functionality
    - Configuration memory; maintenance and configuration protected memory Intra-chassis point-to-point, one-way data communications framework (across the backplane)

- Inter-chassis and interdivisional point-to-point, one-way data communications

The NuPAC platform design replaces the main operating loop of a typical microprocessor-based platform by making use of dedicated independent state machines. The use of dedicated independent state machines results in a distributed architecture that improves processing throughput.

The architecture of the NuPAC platform is centered about a configurable electronic module called the Generic Logic Module (GLM). The GLM is a circuit card assembly consisting of a Carrier Card, a Logic Mezzanine, and up to eight I/O mezzanines. Each GLM provides the capability to accomplish I/O processing, customizable control logic, diagnostics, and data communication. The GLMs are front-loaded and interface to a backplane (more accurately a mid-plane) within the chassis.

The Carrier Card interfaces up to eight I/O mezzanines to the Logic Mezzanine. The eight I/O mezzanine slots provide the flexibility to mix and match a variety of I/O functions on a single GLM. The I/O mezzanines read and write field input and output signals, including serial communication signals. The I/O mezzanines interface to the Logic Mezzanine via the Carrier Card. There are six variants of I/O mezzanines, which include:

1) Analog Input Mezzanine
2) Discrete/Pulse Input Mezzanine
3) Temperature Input Mezzanine
4) RS-422/485 Mezzanine
5) Analog Output Mezzanine
6) Solid State Relay (SSR) Mezzanine.

The Logic Mezzanine provides a logic solving capability implemented using two FPGAs. The Logic Mezzanine hosts a non-configurable FPGA and a configurable FPGA. The non-configurable FPGA, known as the Core FPGA or Core PLD, is utilized for general infrastructure-like logic. The Core PLD is reusable logic which does not change from plant application to plant application. The configurable FPGA, known as the Application Specific FPGA or Application Specific PLD (ASPLD), is utilized for implementing plant-specific designs capable of executing plant-specific logic and algorithms.

The chassis also supports Rear Transition Modules (RTMs), which plug into the back (rear) of the chassis in slot locations that match the front-loaded GLMs. The RTMs and GLMs are interconnected through connectors on the backplane. The RTM interfaces field input and output signals, including serial communication signals, to the GLM by busing those signals from card-top connectors on the RTM through the corresponding backplane connector, to the GLM carrier card, and on to the GLM I/O mezzanines.

Up to 18 GLM/RTM pairs may be installed within a single chassis. Scalability is realized by cascading multiple GLMs together within a chassis, with additional scalability realized by cascading multiple chassis of GLMs together. Modularity and scalability permit functional arrangements (both I/O and logic solving).

The hardware components covered by this TR are:

Part Number	Description
610100	Chassis
610120	Rear Transition Module (RTM)
610310	Carrier Card, Generic Logic Module (GLM)
610320	Logic Mezzanine, GLM
610330	Analog Input Mezzanine, GLM
610340	Discrete/Pulse Input Mezzanine, GLM
610350	Temperature Input Mezzanine, GLM
610360	RS-422/485 Mezzanine, GLM
610370	Analog Output Mezzanine, GLM
610380	SSR Mezzanine, GLM
610400	Core FPGA Logic

3.1.1 Platform Quality Assurance Program

All nuclear activities are subject to the policies and procedures described in the Lockheed Martin Energy Quality Systems Manual for Commercial Nuclear Programs and the "NuPAC Quality Assurance Plan" (Refs. 37.a. & 41.a.). From February 8 through February 12, 2016, the NRC staff performed a regulatory audit of the Trinity Road, Texas, facilities of Lockheed Martin (ADAMS Accession No. ML16069A237). The audit was conducted to support the NRC staff evaluation of the NuPAC TR. The NRC audit team reviewed Lockheed Martin's policies and procedures to verify compliance with Criterion II, "Quality Assurance Program," of Appendix B to 10 CFR Part 50. In addition, the NRC audit team reviewed a sample of the quality assurance (QA) program implementation in the development of the NuPAC platform. In addition to reviewing the "NuPAC Quality Assurance Plan" (Refs. 37.a. & 41.a.), and its respective second tier procedures addressing 10 CFR Part 50 Appendix B's 18 Criteria, the NRC staff verified implementation of the QA program by reviewing a sample of the following documents: software design verification, software control changes, configuration management procedure, software safety plan, software development plan, corrective action procedure, stakeholder requirements definition, component test design, integration test plan, problem change request, and software tool evaluation plan. The sample of completed documentation included evaluation of management reviews, drawings, determination of technical evaluations, and selection of methods of acceptance of test results.

Based on the materials reviewed and audited, the NRC staff concluded that the activities were performed in accordance with the regulatory requirements of Criterion II, "Quality Assurance Program," of Appendix B to 10 CFR Part 50.

3.2 Hardware Development Process

The hardware development process should conform to IEEE Std 603-1991, as required in 10 CFR 50.55a(h). IEEE Std 603-1991 Clause 5.3 requires components and modules be of a quality that is 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 quality assurance program.

The development of the NuPAC platform (including both hardware components and PL) addressed both functional/performance and environmental criteria. The evaluation of the qualification of the NuPAC equipment, against the environmental criteria, is documented in Section 3.5 of this SE.

Most testing included NuPAC hardware; therefore, most testing is designed, in part, to confirm hardware functionality. There was some simulation testing (i.e., testing of software, but not on the target hardware) and corresponding integrated hardware/software testing that confirmed software functionality and confirmed proper functioning of software tools; this simulation testing is addressed in Section 3.4.1.4 of this SE.

Prior to qualification testing, the NuPAC platform components underwent a series of acceptance tests. Acceptance test procedures were developed for each level of assembly, which includes the Carrier Card, Logic Mezzanine, individual I/O mezzanines, GLM, RTM, and chassis. These procedures were representative of the procedures used for acceptance testing during production.

Design Verification Test (DVT) procedures were developed to perform the testing of the GLM and chassis as individual assemblies to ensure compliance to functional requirements. As applicable, functional requirements that can be verified at this level were tested.

Functional requirements that were not tested at the GLM or chassis level were tested as part of the equipment qualification of the Test Specimen Configuration (TSC) DVT. DVT utilizes simulated inputs as required by the TSC to verify performance. The overall verification philosophy proves that the communication capabilities, the I/O capabilities, response time, and all other interface connections to external circuitry are operating in accordance with the specifications. The NRC staff evaluation summarized above concluded that the Lockheed Martin hardware development process complied with IEEE Std 603-1991.

3.3 Software Architecture

See Section 3.4.3.2, “Software Architecture Description,” below.

3.4 Software Development Process

There are several development processes one could consider (e.g., platform developer, application developer, and the nuclear power plant licensee); however, for the NuPAC TR, only the processes for the Core PL (i.e., by the platform developer) are addressed.

The software development process describes the life-cycle of the development of the software (known as Programmable Logic (PL) within Lockheed Martin) to be used by and/or in support of the DI&C system. It is important that this be a disciplined process where the necessary system performance is well defined and the management aspects of the system development project demonstrate that a high quality product is the result of a deliberate, careful and high-quality development process.

Parallel to the development process, a verification and validation program should be implemented to monitor, evaluate, and document the development process. Verification is defined as the process of determining whether the products of a given phase of the

development cycle fulfill the criteria established during the previous phase. Validation is defined as the test and evaluation of the integrated computer system to ensure compliance with the functional, performance, and interface criteria. Combined, verification and validation is the process of determining whether the criteria for a system or component are adequate, the products of each development phase fulfill (i.e., implements) the criteria imposed by the previous phase, and the system or component complies with specified criteria. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.

3.4.1 Software Planning Documentation

This subsection addresses acceptance criteria for planning activities. The acceptance criteria address specific software development planning activities and products (i.e., plans). These plans, provide the NRC staff with additional criteria for reviewing the process implementation and products of subsequent life cycle activities.

3.4.1.1 Software Management Plan (SMP)

The software management plan is the basic governing document for the entire development effort. Project oversight, control, reporting, review, and assessment are all carried out within the scope of the SMP. The SMP is directed at the project management personnel, and therefore emphasizes the management aspects of the development effort.

SRP BTP 7-14, in Section B.3.1.1, provides acceptance criteria for a software management plan. This section references RG 1.173; the current version of RG 1.173 endorses IEEE Std 1074-2006, “IEEE Standard for Developing Software Life Cycle Processes,” and Clause A.1.2.7, “Plan Project Management,” contains an acceptable approach to software project management.

The SMP for the NuPAC Core PL is summarized in Section 5.0 of the NuPAC TR and further described in the “NuPAC Programmable Logic Development Plan,” (Ref. 46.a.) and the “NuPAC Project Management Plan (PMP),” (Ref. 43.d.). This planning documentation was compared with the criteria identified above and it was determined that it is consistent with SRP acceptance criteria and is therefore acceptable.

3.4.1.2 Software Development Plan (SDP)

The SDP provides necessary information on the technical aspects of the development project that are required by the development team in order to carry out the project. The SDP should emphasize the technical aspects of the development effort, and should be directed at the technical personnel. The SDP should clearly state which tasks are a part of each life cycle activity, and state the task inputs and outputs.

The acceptance criteria for a SDP are contained in SRP, BTP 7-14, Section B.3.1.2, which states that RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” endorses IEEE Std 1074, “IEEE Standard for Developing Software Life Cycle Processes,” subject to exceptions listed, as providing an approach acceptable to the staff, for meeting the regulatory requirements and guidance as they apply to development processes for safety system software.

The NuPAC Core PL SDP is summarized in Section 5.0 of the TR and further described in the "NuPAC Programmable Logic Development Plan [PLDP]" (Ref. 46.a.). The PLDP mainly addresses Section A.3, "Development Section of activity groups," of IEEE Std 1074-2006. The software development plan documentation is consistent with the SRP acceptance criteria and is acceptable.

3.4.1.3 Software Quality Assurance Plan (SQAP)

Quality assurance (QA) is a planned and systematic pattern of all actions necessary to provide adequate confidence that the item or product conforms to requirements. Software quality assurance (SQA) is the portion of general quality assurance that applies to a software product. The SQA plan (SQAP) describes how the quality of the software will be assured by the development organization. In general, a high quality system is achieved by having both: (1) a high quality development process which minimizes the productions of errors, and (2) a high quality verification and validation processes which maximizes the elimination of errors produced. The SQAP overarches both: (1) the Software Development Plan (SDP), and (2) the Software Verification and Validation Plan (SVVP).

Quality assurance is required by 10 CFR Part 50, Appendix B. The SQAP must be implemented under an NRC approved QA program. The plan should identify which QA procedures are applicable to specific software development processes, and identify particular methods chosen to implement QA procedures. The acceptance criteria for a SQAP are contained in the SRP, BTP 7-14, Section B.3.1.3, and in RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations;" Clause 5.3 of IEEE Std 7-4.3.2, "Quality," provides applicable guidance.

The NuPAC Core PL SQAP is described in the "NuPAC Quality Assurance Plan" (Refs. 37.a. & 41.a.) This document summarizes how the eighteen criteria of Appendix B are addressed and references the applicable policies and procedures for each (including the development and V&V plans).

The NRC staff evaluated the SQAP and found that it address all software that is resident on the NuPAC platform. The SQAP includes instructions for the development, modification, and acceptance of the PL, and is therefore acceptable.

3.4.1.4 Software Integration Plan (SIntP)

For a microprocessor based systems, software integration consists of three major phases: integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product. During the first phase, the various object modules are combined to produce executable programs. These programs are then loaded in the second phase into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems and instrumentation. The final phase consists of testing the results. For FPGA based systems, the terminology is different, but conceptually, the steps are the same.

The acceptance criteria for a software integration plan are contained in the SRP, BTP 7-14, Section B.3.1.4, “Software Integration Plan.” This section states that RG 1.173, endorses IEEE Std 1074, and that within that standard, Clause A.1.2.8, “Plan Integration,” contains an acceptable approach relating to planning for software (code) integration. Clause A.1.2.8 states that the integration methods should be documented. The integration plan should also include the tools, techniques, and methodologies to perform the software (code) integrations.

The SIntP is described in the “NuPAC Programmable Logic Verification Procedure - Core PLCI,” (Ref. 45.c.). This plan describes that after PL is developed, and before it is integrated with the target hardware, there are two levels of simulation testing (Register-Transfer Level (RTL) source code & Gate level simulations - executed to test the design after the synthesis and place-and-route operations to check the design for potential timing issues as the design is transferred from RTL into a gate level netlist). The Netlist testing is done in part to confirm the preservation of functionality after the software tools have converted the source code to a placed and routed FPGA netlist. After simulation testing, the placed and routed design is loaded onto the target FPGA, and the integrated assembly (FPGA & Code) is tested using some of the same simulation test vectors to ensure there is a one for one correspondence between simulated and actual behavior. This testing also provides confirmation that both the simulation software tools and the software loading tools operated properly.

The SIntP was reviewed and the NRC staff found it to be consistent with the SRP acceptance criteria for SIntP. Furthermore, the integration of the PL with the FPGA, and the subsequent testing followed industry accepted best practices.

3.4.1.5 Software Installation Plan (SInstP)

Software installation is the process of installing the finished software products in the production environment. The Software Installation Plan will describe the general procedures for installing the software product. For any particular installation, modifications, or additions may be required to account for local conditions.

The SInstP is a plant-specific plan and therefore not applicable to the generic review of the NuPAC TR. A SInstP should be developed for a plant specific application.

3.4.1.6 Software Maintenance Plan (SMaintP)

Software maintenance is the process of correcting faults in the software product that led to failures during operation. There is a related activity, sometimes termed “enhancement,” which is the process of adding functionality to a software product. Enhancement of a reactor protection system should repeat all of the development steps.

The SMaintP is a plant-specific plan and therefore not applicable to the generic review of the NuPAC TR. A SMaintP should be developed for a plant specific application.

3.4.1.7 Software Training (STrngP)

The training plan will describe the procedures that will be used to train the operators of the software system. In this case, reactor operators will need to be trained in use of the protection

system software. It is also possible that training will be required for managers and for maintenance personnel.

The STrngP is a plant-specific plan and therefore not applicable to the generic review NuPAC TR.

3.4.1.8 Software Operations Plan (SOP)

The Software Operation Plan is separate from operating manuals and maintenance manuals provided by the system suppliers. Those documents describe detailed procedures, whereas the SOP describes resource organization, responsibilities, policies, and general procedures. For example, the SOP may say that the system administrator will ensure that databases are backed up daily. An operation or maintenance manual will describe how to do a backup.

The SOP is a plant-specific plan and therefore not applicable to the generic review of NuPAC TR.

3.4.1.9 Software Safety Plan (SSP)

The Software Safety Plan (SSP) is used for safety critical applications, such as reactor protection systems, to make sure that system safety concerns are properly considered during the software development.

The acceptance criteria for a software safety plan are contained in SRP, BTP 7-14, Section B.3.1.9, "Software Safety Plan." This section states that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.1.5 "Software Safety Plan," and Section 4.1.5 "Software Safety Plan," contain guidance on Software Safety Plans. Further guidance on safety analysis activities can be found in RG 1.173, Section C.3, "Software Safety Analyses."

The SSP is described in the "NuPAC Platform Safety Project Plan," (Ref. 19.c.). The corner stone of safety during the platform stage of development is the NuPAC Hazard tracking system. The information located in the hazard tracking system is summarized in the form of a NuPAC Hazard Log. The hazard tracking system takes the general form of a comprehensive failure modes and effects analysis (FMEA) with respect to safety.

In accordance with the SSP, Lockheed Martin reviewed the NuPAC platform architecture and functionality with the understanding that it will support development of future safety systems. The principal activities outlined by the SSP are designed to uncover any NuPAC design features or functions that are incompatible with future safety system operation or objectives. Failure modes were reviewed for any potential contribution to future hazards and for inclusion in future Safety System FMEA.

The staff evaluated the "NuPAC Platform Safety Project Plan" (Ref. 19.c.) using the acceptance criteria identified above and found it to be acceptable. Although the SSP does not follow the outline for a SSP given in NUREG/CR-6101 (ADAMS Accession No. ML072750055), it does contain the appropriate material for the NuPAC platform TR.

3.4.1.10 Software V&V Plan (SVVP)

Verification is the process that examines the products of each life cycle phase for compliance with the requirements and products of the previous phase. Validation is the process that compares the final software product with the original system requirements and established standards. The combination of verification and validation (V&V) processes generally includes both inspections and tests of intermediate and final products of the development effort.

The acceptance criteria for software verification and validation plans are contained in SRP, BTP 7-14, Section B.3.1.10, "Software Verification and Validation Plan," and Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities." These sections state that RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems Of Nuclear Power Plants," endorses IEEE Std 1012, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to verification and validation of safety system software, subject to the exceptions listed in these Regulatory Positions. Section B.3.2.2 states that further guidance can be found in RG 1.152, and NUREG/CR-6101 (ADAMS Accession No. ML072750055), Sections 3.1.4 and 4.1.4.

The SVVP is described in the "NuPAC FPL [Field Programmable Logic] Verification and Validation Plan" (Ref. 24.a.).

Lockheed adapted IEEE-1012 Std 1012-2004 into a set of standards & criteria into its SVVP, that was appropriate for the generic platform. The NuPAC project is a generic platform development project and not an end user application development project, which is the assumption of IEEE Std 1012. The staff compared the SVVP to IEEE Std 1012-2004 and found the SVVP is consistent with the activities described in IEEE Std 1012-2004 to the extent practical for a generic platform, and is therefore acceptable.

3.4.1.11 Software Configuration Management Plan (SCMP)

Configuration management provides the methods and tools to identify and control the system and programming throughout its development and use. Activities include: (1) the identification and establishment of baselines, (2) the review, approval, and control of changes, (3) the tracking and reporting of such changes, (4) the audits and reviews of the evolving products, and (5) the control of interface documentation. Configuration management is the means through which the integrity and traceability of the system are recorded, communicated, and controlled during development.

The acceptance criteria for a software configuration management plan is contained in SRP, BTP 7-14, Section B.3.1.11, "Software Configuration Management Plan," and Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities." These sections state that both RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" which endorses IEEE Std 1074, contains a clause on, "Plan Configuration Management," and RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 828, "IEEE Standard for Configuration Management Plans," provides an acceptable approach for planning configuration management. BTP 7-14, Section B.3.1.11 further states that additional guidance can be found in IEEE Std 7-4.3.2-2003, "IEEE Standard

Criteria for Digital Computers in Safety Systems on Nuclear Power Generating Stations," Clause 5.3.5, "Software Configuration Management," and in Clause 5.4.1.3, "Establish Configuration Management Controls." NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.1.3 "Software Configuration Management Plan," and Section 4.1.3, also titled, "Software Configuration Management Plan," also contain guidance.

The SCMP is described in the "NuPAC Configuration and Data Management Plan" (Ref. 43.e.). Some of the criteria in the guidance identified above is addressed by other plans (e.g., SVVP, SMP, & SQAP). The SCMP relies on internal processes and procedures to implement the plan. The staff compared the SCMP to the criteria identified above and found the plan appropriately addresses the criteria applicable to a generic platform and is therefore acceptable. Although the SCMP is not organized as described in IEEE Std 828-2005 (which is allowed by IEEE Std 828-2005), it does address the appropriate criteria identified above (including IEEE STD 828-2005), for both hardware and software configuration items, by referencing Lockheed Martin internal processes.

3.4.1.12 Software Test Plan (STP)

The purpose for the software test plan is to prescribe the scope, approach, resources, and schedule of the testing activities; to identify the items being tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with the plan. The Software Test Plan should cover all testing done on the software, including unit testing and integration testing.

The acceptance criteria for a software test plan are contained in SRP, BTP 7-14, Section B.3.1.12, "Software Test Plan," and in Section B.3.2.4, "Acceptance Criteria for Testing Activities." These sections state that both RG 1.170, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 829, "IEEE Standard for Software Test Documentation," and RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 1008, "IEEE Standard for Software Unit Testing," identify acceptable methods to satisfy software unit testing criteria.

Part of the STP is described in the "NuPAC FPL Verification and Validation Plan" (Ref. 24.a.), and the other part is described in the "NuPAC Master Test Plan (MTP)" (Ref. 22.a). The "NuPAC FPL Verification and Validation Plan," identifies the design verification testing that is needed while the MTP describes the overall integration and testing of the TSC system. The TSC is needed, in part, for integrated system verification tests, but mostly it is needed for equipment qualification testing. These test plans do not include the manufacturing testing that is performed on all manufactured/assembled units, or application-specific integration and testing.

The staff compared the test plans to the criteria identified above and found the plans to provide a comprehensive integration and testing strategy; therefore, the STP plan is acceptable.

3.4.2 Software Implementation Documentation

This subsection addresses staff evaluation of the implementation activities; the NRC staff assessed whether the plans were followed by the developer. The acceptance criteria are provided by the developer and evaluated by the NRC staff in its acceptance of the plans.

3.4.2.1 Safety Analyses (SA)

The central element of the SA is the hazard analysis, which was used to systematically identify and evaluate hazards, both real and potential, for elimination or control. RIL-1101 (ADAMS Accession No. ML14237A359), provides the following hazard definition: A hazard, in general, is defined as "potential for harm." In RIL-1101, the scope of "harm" is limited to the loss of a safety function in a nuclear power plant.

The acceptance criteria for a safety analysis are contained in SRP, BTP 7-14, Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." This section states that the Software Safety Plan (SSP) describes the safety analysis (SA) implementation tasks that are to be performed. The acceptance criterion for SSP implementation is that the tasks in the SSP have been completed. The SA shows that the safety analysis activities have been successfully accomplished for each life cycle activity group and that the proposed digital system is safe. In particular, the SA shows that the system safety criteria have been adequately addressed for each activity group; that no hazards have been introduced; that the software criteria, design elements, and code elements that can affect safety have been identified; and that all other software criteria, design, and code elements should not adversely affect safety.

The documentation of the implementation of the SSP is located in four places (a database and three reports): (1) a [ ] database (DB) hazard tracking system, (2) "NuPAC Plan (Concept) Phase Safety Report" (Ref. 52.a.), (3) "NuPAC Requirements Phase Safety Report" (Ref. 52.b.), and (4) "Programmable Logic Failure Modes and Effects Analysis PL (FMEA) Report" (Ref. 51.a.). The [ ] DB was examined early in the project, during an audit (ADAMS Accession No. ML15334A410). The three reports were subsequently docketed and evaluated as described below.

The Concept Phase Safety Report provides the results of the concept phase safety analysis results in the form of NuPAC concept phase postulated hazards. This report is a historical document and the issues originally identified in it can be obtained in their most current form by reviewing the hazard tracking system located in the [ ] DB.

The Requirements Phase Safety Report provides the results of the requirements phase safety analysis results in the form of NuPAC requirements phase postulated hazards. This report is a historical document and the issues originally identified in it can be obtained in their most current form by reviewing the hazard tracking system located in the [ ] DB.

The PL FMEA (Ref. 51.a) was generated using the "NuPAC Programmable Logic Development Specification - Core PLCI" (PLDS, Ref. 46.b.), as the governing input document. The PLDS defines the Core FPGA internal architecture and functionality. The PLDS describes how each PL function has been allocated to one or more elements or sub elements within the Core FPGA.

The PL FMEA captures the effect on the GLM / NuPAC system should the internal functional elements within the Core FPGA be subjected to failures.

Based on the audit examination of the [ ] DB, and a comparison of the three documents identified above, the staff concluded that Lockheed Martin followed the SSP, met the applicable regulatory criteria, and therefore adequately documented the implementation of the SSP.

3.4.2.2 V&V Analysis and Reports

SRP Chapter 7 BTP 7-14 Section B.3.2.2 contains SRP acceptance criteria and references to applicable guidance:

> RG 1.168, endorses IEEE Std 1012, "IEEE Standard for Software Versification and Validation," as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to verification and validation of safety system software, subject to the exceptions listed.
>
> RG 1.168, also endorses IEEE Std 1028, "IEEE Standard for Software Reviews and Audits," as providing an approach acceptable to the staff for carrying out software reviews, inspections, walkthroughs and audits, subject to the exceptions listed.
>
> RG 1.152, endorses IEEE Std 7-4.3.2-2003 which contains Clause 5.3.3, "Verification and Validation," and Clause 5.3.4, "Independent V&V (IV&V) requirements," describing guidance on V&V.

The SVVP describes the V&V implementation tasks that are to be carried out. The acceptance criterion for software V&V implementation is that the tasks in the SVVP have been completed.

The V&V activities associated with the two most recent software versions were used as the basis for the NuPAC V&V evaluation. Version 1.3.1 was established and thoroughly evaluated by IV&V. All issues identified in Version 1.3.1 were intended to be resolved in Version 1.3.2; however, as documented in the final V&V report for Version 1.3.2 (Ref. 47.a.), not all issues were resolved. These will need to be resolved as documented in generic open item No. 5 in Section 4.2 of the SE. Version 1.3.1 V&V reports were used during the audits, and individual issues identified were entered into the corrective action program.

The NuPAC IV&V team, led by Lockheed Martin, consisted of Lockheed Martin staff, SNPAS staff, and two experienced US-based, independent subcontractors. Lockheed Martin staff and SNPAS staff performed the documentation review and system test portions of the IV&V effort. However, the simulation verification testing and the code inspection efforts were performed by the independent subcontractors without the participation of SNPAS.

Version 1.3.2 V&V reports (Ref. 53.a. through e.) were evaluated as part of this SE; these five activity summary reports followed the SVVP (or justified deviations), meet the applicable acceptance criteria listed above, and are therefore acceptable. The five activity summary reports (for Version 1.3.2) are summarized in the "NuPAC Baseline 1.3.2 V&V Final Report" (Ref. 47.a.) The acquisition and planning activity V&V reports were only produced for Version 1.3.1, and were found to be acceptable during the audits.

3.4.2.3 Configuration Management Activities

SRP Chapter 7, BTP 7-14, Section B.3.3, contains SRP acceptance criteria and references to applicable guidance. RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” endorses IEEE Std 1042, “IEEE Guide to Software Configuration Management,” subject to specific provisions identified in the RG, as providing guidance that is acceptable for carrying out software configuration management.

The Configuration Management (CM) self-assessment (NuPAC_CDM610000-001, Rev. -, “Internal CM Audit Record”) was reviewed during an audit which found that the self-assessment activities for the CM organization are documented in accordance with Section 5.1.2 of the Configuration Management Plan (CMP).

The CM self-assessment and the associated implementing processes and procedures were examined during an audit and found to appropriately implement the CMP.

3.4.2.4 Testing Activities

Thorough software testing consists of testing the smallest testable units, and then integrating those units into larger testable units, and testing that integrated unit. This process is repeated until the system is tested after installation.

SRP Chapter 7, BTP 7-14, Section B.3.4, contains SRP acceptance criteria and references to applicable guidance:

> RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," with a few noted exceptions, identifies an acceptable method for addressing computer system qualification testing.
>
> RG 1.168, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” specifically the sections on Regression Analysis and Testing and Test Evaluation, contain guidance related to testing activities.
>
> RG 1.170, “Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” endorses IEEE Std 829, “IEEE Standard for Software Test Documentation,” with a few noted exceptions, identifies an acceptable method for addressing test documentation.
>
> RG 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 1008, “IEEE Standard for Software Unit Testing,” with a few noted exception, identifies an acceptable method for addressing software unit testing. It is understood that RG 1.171 applies to all testing before integrated system testing.

The module test procedures and associated test results were examined as part of the V&V audit, and were found to be implemented appropriately. The system level testing (i.e., of the TSC) was reviewed as part of the qualification testing, and is evaluated in Section 3.5.

3.4.3 Software Design Outputs

This subsection describes the evaluation of whether the software has each of the characteristics important to safety system software.

3.4.3.1 Software Requirements Specification (SRS)

The Software Requirements Specification (SRS) documents the results of the requirements phase activities by the design team and documents the aspects of the safety system that are to be addressed in the software design.

The acceptance criteria for an SRS is contained in SRP, BTP 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements Specification." This sections states that RG 1.172, "Software Requirements Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 830, "IEEE Recommended Practice for Software Requirements Specifications," and that standard describes an acceptable approach for preparing software requirements specifications for safety system software. Section B.3.3.1 also states that additional guidance can be found in NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.2.1 "Software Requirements Specification," and Section 4.1, also titled, "Software Requirements Specifications."

The "NuPAC Programmable Logic Requirement Specifications – Core PLCI" (Ref. 46.d.) is the SRS for the Core PL. The purpose of the Programmable Logic Requirement Specification (PLRS), of the Core Programmable Logic Configuration Item (PLCI), is to define requirements allocated from the GLM Configuration Item (CI) Specification to the Core PLCI.

The SRS was written after a conceptual NuPAC system design was established. In this respect, the SRS is not consistent with the intent established in the guidance documents identified above; however, given the context within which it was developed, it meets the rest of the criteria above.

3.4.3.2 Software Architecture Description

The acceptance criteria for the software architecture description are contained in SRP, BTP 7-14 Section B.3.3.2, "Design Activities - Software Architecture Description." This section states that the Software Architecture Description should describe all of the functional and software development process characteristics listed, and that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.

The "NuPAC Programmable Logic Development Specifications – Core PLCI" (Ref. 46.b.) decomposes the Core Programmable Logic Configuration Item (PLCI) functional requirements into an architecture description and a design description. Section 3.0, "Description of the NuPAC Digital Safety I&C Platform," of the NuPAC TR shows the various hardware devices and

the ways in which they are connected. In addition, it shows a typical safety system architecture. Furthermore, Section 3.3, “Programmable Logic Architecture,” provides a high level overview of the software architecture, which is described in detail in Section 2.0, “Architecture Description,” of the NuPAC Programmable Logic Development Specifications.

The material identified in the previous paragraph was reviewed by the staff and found to contain sufficient descriptions, at the platform level, to meet the criteria identified in the first paragraph above.

3.4.3.3 Software Design Specification (SDS)

The acceptance criteria for the Software Design Specification are contained in SRP, BTP 7-14, Section B.3.3.3, “Design Activities - Software Design Specification.” This section states that the software design specification should accurately reflect the software requirements specification, and that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.3.2 “Software Design Specification,” and Section 4.3.2, “Software Design Specifications,” contain relevant guidance.

The “NuPAC Programmable Logic Development Specifications – Core PLCI” (Ref. 46.b.), decomposes the Core Programmable Logic Configuration Item (PLCI) functional requirements into an architecture description and a design description. Section 3.0, “Design Description,” of the Programmable Logic Development Specifications contains a description for the Core PL design.

The guidance identified above are directly applicable to traditional software systems, and abstractly applicable to state machine based PL designs. The guidance criteria identified in the first paragraph above was considered while the PL design description was read. Based on a review of the IV&V reports, the design description was found to be sufficiently descriptive for a PL designer to unambiguously interpret it, and was therefore found to be acceptable.

3.4.3.4 Thread Audit of Source Code Listings (CLs)

SRP Chapter 7, BTP 7-14, Section B.3.3.4, provide SRP acceptance criteria and references to applicable guidance.

Programmable logic (PL) development was also a joint development effort under the leadership of Lockheed Martin. The vast majority of all PL design and PL design team verification tasks were performed by either Lockheed Martin staff or subcontractors under the immediate supervision of Lockheed Martin staff. SNPAS staff performed some PL design and PL design team verification tasks under the immediate supervision of Lockheed Martin staff. All SNPAS authored work products were reviewed by Lockheed Martin senior staff prior to finalization and use on the NuPAC platform. Incorporation of any SNPAS generated PL could be incorporated into the NuPAC PL final repository only by Lockheed Martin senior staff. Lockheed Martin also used the Secure Development Environment (SDE) as the means to control accessibility and as the final repository of the developed PL. SDE write access is available only to selected Lockheed Martin employees.

The requirements tracing activities of the audits traced requirements from their source to the source code and associated test documents. Based on the thoroughness of the requirements

tracing and associated testing, additional time spent auditing the source code (as a separate activity) was deemed to be of limited benefit. The source code listing that were examined as part of the requirements and were well commented and found to contain the functional and process characteristics described in SRP Chapter 7, BTP 7-14, Section B.3.3.4; therefore the source code listings are acceptable.

3.4.3.5 System Build Documents (SBD)

The acceptance criteria for the system build documentation are contained in the SRP, BTP 7-14, Section B.3.3.5, "Integration Activities -System Build Documents." This section states that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.5.1, "System Build Documents," and Section 4.5.1, also titled, "System Build Documents," contain relevant guidance.

The NuPAC TR addresses an application framework, that is, it consists of a set of components and a methodology to use those components to construct an application system. System Build Documents are related to an application system, not to platform components; therefore, the NuPAC TR did not address this area. The production of acceptable system build documents are Plant-Specific Action Item No. 5.

3.5 Environmental Equipment Qualification

The purpose of environmental equipment qualification is to demonstrate the equipment would be able to operate within the specified environment. This includes normal operations and worst case conditions expected during abnormal operations and accident conditions where the equipment is expected to perform its safety function. Lockheed Martin described its environmental qualification of the NuPAC FPGA-based logic platform in Section 6 and Appendix A of its TR (Ref. 49.a.). The NRC staff evaluated docketed documentation of the qualification of the NuPAC platform for performing its safety functions during normal and abnormal operations including the environments expected during the occurrence of natural phenomena such as earthquakes.

This evaluation is divided into four sections: Sections 3.5.1 and 3.5.2 describe the regulations and regulatory guidance applicable to environmental qualification and highlights criteria used in the evaluation, Section 3.5.3 provides the technical review against the applicable criteria, and Section 3.5.4 lists the conclusions by area evaluated. Section 4.1 describes plant-specific action items, and Section 4.2 describes generic open items.

This evaluation is a generic evaluation of the NuPAC platform against the regulations, regulatory guidance, and standards. It is not plant-specific. As part of the NRC staff review, this SE includes a list of plant-specific action items in Section 4.1 that need to be addressed.

3.5.1 Regulations and Regulatory Basis

The regulatory criteria applicable to the environmental qualification of safety-related instrumentation and control (I&C) equipment are: 10 CFR Part 50, Appendix A, GDC 2, GDC 4, and GDC 22; 10 CFR 50.55(a)(h), 10 CFR 50.48, 10 CFR 50.49(c), and 10 CFR Part 50, Appendix S.

3.5.1.1 10 CFR Part 50, Appendix A, GDC 2

GDC 2 requires a design basis for structures, systems, and components (SSCs) important to safety (ITS) such that SSCs ITS can maintain their safety function during the occurrence of natural phenomena.

This design basis considers the most severe natural phenomena at the site, combinations of normal and accident conditions during the natural phenomena, and the importance of safety functions.

Seismic events can directly affect I&C equipment by initiating vibratory ground motions to structures and equipment within cabinets. Other natural phenomena can indirectly affect I&C equipment by leading to loss of ventilation in cabinets containing the equipment.

3.5.1.2 10 CFR Part 50, Appendix A, GDC 4

GDC 4 requires SSCs ITS be designed to function within environments that include normal operation, maintenance, and testing. It requires them to function during postulated accidents, including loss of coolant accidents. It also requires SSCs ITS be protected from dynamic effects such as missiles or discharging fluids resulting from equipment failures within the plant and from events occurring outside.

The NuPAC platform operates within a cabinet in a mild environment (a mild environment is defined in 10 CFR 50.49(c), as described below). The NuPAC platform would need to function during normal operation, maintenance, testing, and during postulated accidents.

3.5.1.3 10 CFR Part 50, Appendix A, GDC 22

GDC 22 requires a protection system be designed to maintain its safety function if a redundant portion of the system is affected by natural phenomena or is affected by the dynamic effects of normal operation, maintenance, testing, or accident conditions. Alternatively, GDC 22 allows for a protection system to be demonstrated acceptable based on some other defined basis.

The TSC reviewed in this SE is a two-chassis system representing one division.

3.5.1.4 10 CFR 50.55a(h)

10 CFR 50.55a(h) requires protection systems in plants with construction permits issued between January 1, 1971, and May 13, 1999, to meet the requirements in IEEE Std 603-1991 with correction sheet dated January 30, 1995, or meet the requirements in IEEE Std 279. For those plants with construction permits before January 1, 1971, protection systems must be consistent with the licensing basis or meet the requirements in IEEE Std 603-1991 and the correction sheet.

The environmental equipment qualification evaluation in this SE is in accordance with IEEE 603-1991 requirements.

3.5.1.5 10 CFR 50.48

10 CFR 50.48 includes fire protection requirements. Adhering to fire protection requirements minimizes the likelihood that equipment is exposed to smoke. RG 1.209 includes smoke exposure as an environmental stressor and describes reducing the possibility of smoke exposure and enhancing smoke tolerance of equipment. Because smoke exposure is an environmental stressor, adherence to fire protection requirements is important to environmental qualification of SSCs ITS.

Smoke tolerance is evaluated as part of atmospheric qualification in Section 3.5.3.3 of this SE.

3.5.1.6 10 CFR 50.49(c)

10 CFR 50.49(c) defines a mild environment as, "…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."

The NuPAC platform operates in a mild environment and the evaluation in this SE pertains to its operation in this mild environment. (See the atmospheric evaluation in Section 3.5.3.3.)

3.5.1.7 10 CFR Part 50, Appendix S

Appendix S elaborates on GDC 2 for seismic events by providing the criteria for SSCs ITS to withstand the effects of earthquakes. It includes the operating basis earthquake (OBE) ground motion, and the safe shutdown earthquake (SSE) ground motion in its list of definitions.

Those SSCs that must withstand the effects of the SSE are those necessary to assure: (i) the integrity of the reactor coolant pressure boundary, (ii) the capability to shut down the reactor and maintain it in a safe-shutdown condition, or (iii) the capability to prevent or mitigate the consequence of accidents that could result in offsite exposures comparable to those in 10 CFR 50.34(a)(1). Furthermore, the required safety functions of SSCs must be assured during and after the SSE through design, testing, or qualification methods.

Appendix S specifies for SSCs subjected to the OBE in combination with normal operating loads, that all SSCs necessary for continued operation without undue risk to the health and safety of the public must remain functional and within applicable stress, strain, and deformation limits. This requirement can be satisfied without performing explicit response or design analyses when the OBE is at one-third or less of the SSE; otherwise, analysis and design must be performed to demonstrate the requirement is met.

3.5.2 Regulatory Guidance

The regulatory guidance applicable to environmental qualification of I&C equipment in mild environments includes RG 1.209, RG 1.152, RG 1.100, and RG 1.180.

3.5.2.1 RG 1.209

RG 1.209 provides guidance for the environmental qualification of safety-related computer-based I&C systems that operate in mild environments. As stated in RG 1.209, "…qualification is a validation of design to demonstrate that a safety-related computer-based

I&C system is capable of performing its safety function under the specified environmental and operational stresses." In addition, RG 1.209 states that IEEE 323-2003 is appropriate for satisfying the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants subject to certain enhancements and exceptions. These enhancements and exceptions are summarized below:

- Type testing is the preferred method of environmental qualification.
- Qualification testing should be performed with the I&C system functioning, with software and diagnostics that are representative of those used in actual operation, while the system is subjected to the specified environmental service conditions, including abnormal operational occurrences. In addition, testing should exercise portions necessary to accomplish the safety-related function or those portions whose failure could impair the safety-related function.
- Standards and guidance applicable to testing for electromagnetic interference/radio frequency interference (EMI/RFI) and surge voltages are, Revision 1 of RG 1.180, Revision 1 of Electric Power Research Institute (EPRI) Topical Report 102323, and those references noted in IEEE Std 323-2003, Section 6.3.1.7.
- NRC takes exception to IEEE Std 323-2003, Section 7.1 and states, "The evidence of qualification in a mild environment should be consistent with the guidance given in Section 7.2…."

RG 1.209 provides additional guidance with regard to IEEE Std 323-2003 stating, "…the design-basis accident element of type testing for qualification does not apply to computer-based I&C systems in mild environments."

RG 1.209 refers to Section 5.4.1 of IEEE Std 7-4.3.2-2003, which provides criteria for equipment qualification of computer-based safety systems and includes testing under environment stress with the full range of safety-related software functioning. RG 1.209 describes Annex F.2.3 to IEEE 7-4.3.2-2003 with regard to response probability and common cause failure probability stating, "Addressing qualification requirements for safety-related computer-based I&C systems is one method of ensuring that the probability of common-cause failure attributable to environmental stressors is reduced to an acceptable level."

RG 1.209 describes the susceptibility of metal oxide semiconductor (MOS) technology to ionizing radiation doses, and indicates that commercial MOS technologies are very susceptible to ionizing radiation doses and have hardness levels of about 10 gray (Gy) (10 Gy is equivalent to 1 kilorad (krad)) for commercial-off-the-shelf circuits to about 10^5 Gy (10^4 krad) for radiation-hardened circuits.

RG 1.209 includes smoke exposure from an electrical fire as an environmental stressor and describes reducing the possibility of smoke exposure and enhancing smoke tolerance. It indicates that the most effective approach to address smoke susceptibility is to reduce the likelihood of smoke exposure by rigorously adhering to the fire protection requirements in 10 CFR Part 50.48 or other individual plant license commitments. It also describes reducing equipment susceptibility to smoke exposure through design choices and construction practices such as chip packaging and conformal coatings.

3.5.2.2 RG 1.152

RG 1.152 provides guidance for designing digital systems for use in safety systems at nuclear power plants such that these systems have high functional reliability. As described in Regulatory Position 1, IEEE Std 7-4.3.2-2003 is endorsed with respect to designing systems for high functional reliability; the NRC does not endorse Annexes B through F of IEEE Std 7-4.3.2-2003.

Clause 5.4 of IEEE Std 7-4.3.2-2003 is applicable to the environmental qualification of digital systems. Clause 5.4.1 specifies qualification testing with the computer functioning with software and diagnostics that are representative of those used in actual operation. It further specifies that all portions of the computer necessary to accomplish the safety functions, or those portions whose operation or failure could impair the safety functions, be exercised during testing. This clause is relevant to the environmental qualification review because as stated in Section 6.1.1 of the TR (Ref. 49.a.), Lockheed Martin performed environmental qualification testing of the NuPAC platform using a TSC emulating an RTS. The TSC represented one division of a redundant, four-division system. Clause 5.4.2 of IEEE Std 7-4.3.2-2003 describes the process for qualifying computers that were not specifically designed for nuclear power plant applications. Because the NuPAC platform was specifically designed for nuclear power plant applications, this clause is not applicable to this review.

3.5.2.3 RG 1.100

RG 1.100 provides guidance for the seismic qualification of both electrical and active mechanical equipment. Because the NuPAC platform is being reviewed in this SE and not active mechanical equipment, only the portions of RG 1.100 relevant to electrical equipment are described here. RG 1.100 endorses IEEE Std 344-2004 for seismic qualification of electrical equipment subject to certain provisions. Provisions relevant to this review are summarized below:

- Seismic qualification by testing, analysis, or combined analysis and testing are acceptable methods for seismic qualification of electrical equipment.
- The frequency range for testing should be consistent with the required response spectra (RRS) of the specific plant equipment and should not be restricted to values up through 33 hertz (Hz). While one-third octave spacing is used for low frequency excitation, for high-frequency sensitive equipment, one-sixth octave spacing should be used extending up to the frequency of interest shown in the RRS.
- For certain hard-rock-based plants, the site-specific spectra may exceed the certified design spectra in the high-frequency range (20 Hz and above). The use of prior testing results should be justified by demonstrating that the frequency content of the power spectral density (PSD) of the test waveform is sufficient in accordance with Annex B to IEEE Std 344-2004.
- New seismic qualification tests for plants with high-frequency ground motion should demonstrate the adequacy of the frequency content and the stationarity of the frequency content for the input waveforms. Annex B to IEEE Std 344-2004 provides acceptable guidelines on frequency content and stationarity.

RG 1.100 clarifies for certain hard-rock-based plants along the east coast of the United States that the site-specific spectra may exceed the certified design spectra in the high frequency

range (20 Hz and above). It also states that when licensees plan new seismic qualification tests for equipment in such plants, the formulation of the test input waveforms should properly consider this high-frequency excitation.

The design of certain electrical equipment has evolved to use DI&C components over analog components; however, as stated in RG 1.100, some solid-state relays and microprocessor-based components may be sensitive to earthquake excitations. Therefore, as indicted in RG 1.100, the NRC staff considers the use of test experience data from older electrical components to be inappropriate and unacceptable for seismic qualification of the new generation of electrical components.

RG 1.100 contains additional guidance with regard to experience data (i.e., earthquake experience data and test experience data) to address the major change between the 1987 version of IEEE Std 344 and the 2004 version. Because Lockheed Martin did not rely on experience data, the guidance in RG 1.100 related to experience is not described further in this evaluation.

3.5.2.4 RG 1.180

RG 1.180 provides guidance on acceptable methods for complying with NRC regulations on design, installation, and testing of safety-related I&C systems with regard to EMI, RFI, and power surges. RG 1.180 states that EMI, RFI, and power surges are environmental conditions that can affect the performance of safety-related equipment. It identifies acceptable suites of test methods from International Electrotechnical Commission (IEC) 61000, which is an international commercial standard and MIL-STD-461E, which is a military (MIL) standard (STD). Additionally, it identifies IEEE C62.41-1991 and IEEE C62.45-1992 regarding power surge withstand capability (SWC) testing. The testing practices from the commercial and military standards address electromagnetic emissions, EMI/RFI susceptibility, and SWC as part of an overall effort within a nuclear power plant to ensure electromagnetic compatibility (EMC) of equipment.

RG 1.180 endorses operating envelopes corresponding to IEC 61000 and MIL-STD-461E test methods. It states that operating envelopes were tailored from MIL-STD-461E test limits to represent the characteristic electromagnetic environment in key locations at nuclear power plants. Also, RG 1.180 states that the application of MIL-STD-461E test methods is tailored for the intended function of the equipment and the characteristic environment. It further clarifies this by stating, which tests are applied and what levels are used depend on the function to be performed and the location of operation.

RG 1.180 includes the details of the NRC staff's guidance within a series of regulatory positions.

- Regulatory Position 1 provides general information relevant to the application of standards for testing, and within Table 1, summarizes Regulatory Positions 2 through 6 relative to EMC and applicable industry and military standards.
- Regulatory Position 2 endorses IEEE Std 1050-1996 with one exception to Clause 4.3.7.4 involving radiative coupling. This regulatory position explains that radiative coupling is a far-field effect and that field strength falls off as 1/r (r is the distance from the source of radiation).

- Regulatory Position 3 applies to emissions testing. It endorses certain EMI/RFI emissions test methods from IEC 61000 and MIL-STD-461E and describes operating envelopes for these tests. It also identifies the baseline test program and provides for alternative test programs under certain conditions.
- Regulatory Position 4 applies to susceptibility testing. It endorses certain EMI/RFI susceptibility test methods from IEC 61000 and MIL-STD-461E and describes operating envelopes for these tests.
- Regulatory Position 5 applies to SWC testing. It endorses certain surge test waveforms and test methods from IEC 61000-4 and certain surge test waveforms from IEEE 62.41-1991 and test methods from IEEE 62.45-1992.
- Regulatory Position 6 addresses EMI/RFI emissions and susceptibility testing at frequencies above 1 GHz. It states that MIL-STD-461E contains applicable test methods and criteria for testing above 1 GHz (i.e., tests RE102 and RS103); whereas, IEC 61000-3 and 4 do not.
- Regulatory Position 7 lists a minimum level of documentation to be included for qualification of equipment.

3.5.3 Technical Evaluation

Environmental qualification is a validation that equipment can perform its safety functions during normal operation, maintenance, and testing, as well as during equipment failures and during the occurrence of natural phenomena such as earthquakes and tornadoes. This section is separated into the major areas of environmental qualification to include descriptions of the test system and operability and prudency testing as well as qualification for atmospheric, radiation, EMI/RFI, and seismic, and the associated NRC staff evaluation.

3.5.3.1 Test System

IEEE Std 7-4.3.2-2003, Clause 5.4.1, requires testing with all portions necessary to accomplish the safety function or portions whose failure could impair the safety function. Lockheed Martin describes the TSC in Section 6.1.1 of the TR (Ref. 49.a.). The TSC represents one division of a redundant system. As shown in Section 3.1.2 and discussed in Section 6.1.1 of the TR (Ref. 49.a.), each division consists of reactor trip detect logic in one chassis and coincidence (or voter) logic in a second chassis. In addition, Lockheed Martin developed an Automated Test System (ATS) to generate the analog and digital signals needed for testing. Note, however, Section 3.1.1 of the TR (Ref. 49.a.) describes five elements that are not part of the qualification:

1. Power supplies (external power source and cabinet-level).
2. Application-specific (plant-specific) PL; note, however, that the ASPLD/FPGA is included as a hardware component.
3. Class 1E/non-Class 1E isolation.
4. Data communications outside of NuPAC (safety and non-safety).
5. Safety-related display.

The qualification of the cabinet-level power supplies is Generic Open Item No. 3.

In addition, plant specific applications should address the five elements, which are plant-specific, that were not included in the qualification of the NuPAC platform. In regard to element number one, power supplies, applications using the NuPAC platform should address

power quality related to power sources external to the NuPAC platform. This is a plant-specific action item.

NRC Staff Evaluation

The NRC staff reviewed Sections 3 and 6 of the TR (Ref. 49.a.). The NRC staff performed this evaluation in accordance with the regulatory criteria in GDC 2 and 4, the guidance in RG 1.152, and the normative criteria in IEEE Std 7-4.3.2-2003.

Lockheed Martin's TSC represents one division of a redundant system. It consisted of two chassis, each containing 18 GLMs. Section 6.1.1 of the TR (Ref. 49.a.) states that the TSC contained at least one of each type of NuPAC platform hardware component listed in Section 3.1.4 of the TR (Ref. 49.a.). In order to perform testing, Lockheed Martin used an ATS, which provided inputs to the TSC and monitored outputs. Because the TSC formed the primary elements of the NuPAC system and contained at least one of each type of hardware component being qualified, the NRC staff finds that Lockheed Martin performed testing consistent with Clause 5.4.1 of IEEE Std 7-4.3.2-2003 which requires testing with all portions necessary to accomplish the safety function or portions whose failure could impair the safety function.

3.5.3.2 Operability and Prudency Testing

Clause 6.2.5 of IEEE Std 323-2003 requires specifying criteria (i.e., acceptance criteria) to demonstrate equipment can perform its safety function. In addition, Clause 7.2f of IEEE Std 323-2003 requires test documentation to include an identification of acceptance criteria and performance results.

Section 5.3 of EPRI TR-107330 specifies operability test requirements and acceptance criteria. Lockheed Martin specifies acceptance criteria for its operability tests in Section 13 of the "NuPAC System Operability Test Procedure" (Ref. 46.e.) on test record data sheets. In addition, Addendum I to the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.) shows operability test criteria and baseline test results recorded against the criteria. Lockheed Martin describes the baseline test results in Section 8.1 of the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.) and states that (i) accuracy measurements met the required tolerance; (ii) discrete inputs and outputs and failover operability test results showed acceptable performance; and (iii) for communication operability, pulse shapes were measured and found to be within tolerance. However, Lockheed Martin identified some issues related to response time measurements and addressed these issues in Section 2.2.1 of the "NuPAC Equipment Qualification (EQ) Summary Report" (Ref. 48.a.). Section 2.2.1 states that Lockheed Martin included the sampling rate of 1.67 msec when evaluating response time measurements against baseline values and modified some response time limits. Modifications were made to the response time limits for Temperature 1 and 5 and Valve Positions 1a, 2a, and 3a (see Table 2-3 of the "NuPAC Equipment Qualification (EQ) Summary Report" (Ref. 48.a.)).

Section 5.3 of EPRI TR-107330 specifies the items to include in operability tests. However, Lockheed Martin excluded some of them and provided its basis in Section 4.1.8 of the "NuPAC System Operability Test Procedure" (Ref. 46.e.). The items excluded along with Lockheed Martin's bases for excluding them are listed below:

1. Coprocessor Operability: This item is not applicable because the NuPAC platform does not include coprocessors (see Section 4.1.8.1 of the "NuPAC System Operability Test Procedure" (Ref. 46.e.)).
2. Timer Tests: Section 4.1.8.2 of the "NuPAC System Operability Test Procedure" (Ref. 46.e.) states that the intent of the timer test (i.e., verifying the accuracy of timer functions) is continuously being tested during normal operation and therefore a separate operability test is not required. Timer functions, when implemented in the ASPL, would be based off the primary system clock with an accuracy of [

   ]. Section 5.3G of EPRI TR-107330 requires timer variation to be no greater than ±1 percent. [

   ]
3. Test of Failure to Complete Scan Detection: Section 4.1.8.3 of the "NuPAC System Operability Test Procedure" (Ref. 46.e.) states that the NuPAC platform goes through a complete Power On Self-Test (POST) during every startup of each GLM within the system. The GLM will not go into RUN mode if any conditions do not pass POST checks. Section 5.3H of EPRI TR-107330 allows power up testing to be used to establish operability in lieu of any special test setups.
4. Power Interruption Test: This item is not applicable because the current qualification of the NuPAC platform does not include power supplies (see Section 4.1.8.4 of the "NuPAC System Operability Test Procedure" (Ref. 46.e.)).

Section 5.4 of EPRI TR-107330 specifies prudency test requirements and acceptance criteria. Lockheed Martin specifies acceptance criteria for its prudency testing in Section 13 of the "NuPAC System Prudency Test Procedure" (Ref. 46.f.) on test record data sheets. In addition, Addendum II to the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.) shows prudency test criteria and baseline test results recorded against the criteria. Lockheed Martin describes the baseline test results in Section 8.2 of the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.) and states that acceptance criteria were met for Burst of Events response time testing; however, one accuracy measurement was out of specification due to an incorrect Configuration Data Base setting. This setting was corrected for subsequent prudency tests. In addition, Lockheed Martin states that response time measurements were within tolerance when it added the [ ] sampling rate to its acceptance criteria with the exception of two measurements that were faster than expected.

NRC Staff Evaluation

The NRC staff reviewed the "NuPAC System Operability Test Procedure" (Ref. 46.e.), the "NuPAC System Prudency Test Procedure" (Ref. 46.f.), and the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.). The NRC staff performed this evaluation in accordance with the regulatory criteria in GDC 2 and 4, the guidance in RG 1.209, and the normative criteria in IEEE Std 323-2003 and EPRI TR-107330.

The NRC staff finds that Lockheed Martin's operability tests and acceptance criteria are consistent with the normative criteria of IEEE Std 323-2003 and Section 5.3 of EPRI TR-107330. Section 4.1.8 of the "NuPAC System Operability Test Procedure" (Ref. 46.e.) describes operability test items Lockheed Martin excluded and its bases for excluding them from the qualification. The NRC staff finds the bases are acceptable because the requirements for

the test item were addressed outside of operability testing or the test item was not applicable because power supplies were not part of the qualification.

The NRC staff finds that Lockheed Martin prudency tests and acceptance criteria are consistent with the normative criteria of IEEE Std 323-2003 and Section 5.4 of EPRI TR-107330. Section 4.1.1 of the "NuPAC System Prudency Test Procedure" (Ref. 46.f.) describes the prudency tests Lockheed Martin conducted. These tests include burst of events, failure of serial port receiver, serial port noise, and fault simulation which are specified in Section 5.4 of EPRI TR-107330.

The NRC staff finds that Lockheed Martin adequately performed baseline operability and prudency testing. Lockheed Martin shows its operability tests met its acceptance criteria in Addendum I to the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.) and Table 2-3 of the "NuPAC Equipment Qualification (EQ) Summary Report" (Ref. 48.a.). Lockheed Martin shows its prudency tests met its acceptance criteria in Addendum II to the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.). Although two response time measurements were not within tolerance during baseline testing, they were faster than expected and subsequent results in Addendum V to the to the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.) showed them within tolerance.

3.5.3.3 Atmospheric

Lockheed Martin initially performed environmental qualification testing on January 26, 2015, at [ ]. An anomaly occurred during testing while ramping up to high temperature and high humidity (see Section 8.1 of the "NuPAC Environmental Test Report" (Ref. 47.b.)). Lockheed Martin states in Section 3.4 of the "NuPAC Environmental Test Report" (Ref. 47.b.) that testing was resumed [ ] following resolution of the anomaly and modification to the "NuPAC System Environmental Test Procedure" (Ref. 37.b.) to define ramp-up rates during the initial transition to high temperature and high humidity.

GDC 4 requires SSCs ITS be protected from dynamic effects such as missiles or discharging fluids resulting from equipment failures within the plant and from events occurring outside. As described in Sections 5.0 and 5.1.1 of Appendix A to the TR (Ref. 49.a.), the NuPAC platform is designed to fit within a cabinet and be operated in a mild environment. Therefore, licensees should verify that the NuPAC platform is located in a mild environment and that the location of the NuPAC platform would preclude it from being subjected to dynamic effects such as missiles, discharging fluids, or pipe whipping resulting from other equipment failures or natural phenomena this is Plant-Specific Action Item No. 7.(a).

Lockheed Martin shows in Table 6.2-1 of the TR (Ref. 49.a.) that the basis for its temperature and humidity qualification testing is EPRI TR-107330. In addition, Section 5.2 of Appendix A to the TR (Ref. 49.a.) describes environmental qualification testing to the normative criteria of Section 4.3.6 of EPRI TR-107330. Section 5.2 also references RG 1.209 and IEEE Std 323-2003. Section 4.3.6.3 of EPRI TR-107330 requires operation to the environmental profile in Figure 4-4. Lockheed Martin states in Section 6.2.2 of the TR (Ref. 49.a.) that the TSC was tested to the environmental profile in Figure 4-4 of EPRI TR-107330 at a maximum temperature of [ ] degrees Fahrenheit] degrees Fahrenheit (i.e., margin of [ ] degrees Fahrenheit) and maximum relative humidity of [ ] percent [ ] percent (i.e., margin of [ ] percent). Lockheed Martin shows its temperature and humidity test data in Attachment B of the [ ] Environmental Test Report (Ref. 34.a.).

Clause 6.2.3 of IEEE Std 323-2003 specifies margin be included in qualification programs to provide assurance equipment can perform under adverse service conditions. In addition, Section 6.3.3 of EPRI TR-107330 specifies margins of 5 degrees Fahrenheit and 5 percent relative humidity; it states that the margin for relative humidity may be reduced if it results in a value that is not achievable. The "NuPAC System Environmental Test Procedure" (Ref. 37.b.) includes the [ ] degrees Fahrenheit and [ ] percent relative humidity margins in Sections 7.4.1 and 7.4.5. Section 7.2.3.1 of the "NuPAC Environmental Test Report" (Ref. 47.b.) describes the [ ] degrees Fahrenheit and [ ] percent relative humidity margins at high temperature and humidity test conditions. At low temperature and humidity, Section 7.2.3.2 describes testing to [ ] degrees Fahrenheit and [ ] percent relative humidity followed by testing to [ ] percent relative humidity and [ ] degrees Fahrenheit. Lockheed Martin's testing at low temperature did not include the [ ] degrees Fahrenheit margin specified in Section 7.4.5 of the "NuPAC System Environmental Test Procedure" (Ref. 37.b.).

IEEE Std 323-2003, Clause 6.1.5.1, requires the normal and abnormal service conditions for equipment be specified. This clause requires nominal and extreme values for temperature and relative humidity be specified along with their expected durations. Lockheed Martin states in Section 6.2 of the "NuPAC Environmental Test Report" (Ref. 47.b.) that it developed temperature-humidity test criteria using EPRI TR-107330, Section 4.3.6 for guidance. Figure 6-2 of the "NuPAC Environmental Test Report" (Ref. 47.b.) is Figure 4-4 of EPRI TR-107330. This figure shows the test profile Lockheed Martin used for testing and this profile includes temperature-humidity durations and minimum ramp times. Additionally, Lockheed Martin specified an initial ramp-up rate to high temperature and humidity conditions in Section 7.4.1 of the "NuPAC System Environmental Test Procedure" (Ref. 37.b.). Figure 10-1 of the "NuPAC Environmental Test Report" (Ref. 47.b.) shows Lockheed Martin's qualification envelope:

- High Temperature and Humidity: [ ] degrees Fahrenheit ([ ] degrees Fahrenheit margin) and [ ] percent ([ ] percent margin) relative humidity
- Low Temperature and Humidity: [ ] degrees Fahrenheit ([ ] degrees Fahrenheit margin) and [ ] percent ([ ] percent margin) relative humidity

In addition, Figure 10-1 shows an initial ramp-up rate of [ ] degrees Fahrenheit per hour followed by an increase in relative humidity of [ ] percent per hour.

Section D.5.4.1 of ISG – 06 states that the system should be qualified for the most severe environment to which it may be exposed and relied upon to perform its safety function. It further states that typically the most limiting combination of temperature and humidity occurs at high values of both (i.e., high temperature and high humidity), and that unless a more limiting combination exists, testing should be performed at the upper extreme of both. Lockheed Martin performed testing at the upper extreme of temperature and relative humidity in accordance with Figure 4-4 of EPRI TR-107330. It performed operability and prudency testing at the end of the high temperature, high humidity cycle (see Section 6.2.2 of the TR (Ref. 49.a.) and Table 6-1 of the "NuPAC Environmental Test Report" (Ref. 47.b.)).

IEEE Std 323-2003, Clause 6.2.5 requires specifying criteria (i.e., acceptance criteria) to demonstrate equipment can perform its safety function. In addition, IEEE 323-2003, Clause 7.2f, requires test documentation to include an identification of acceptance criteria and performance results. Section 3.4 of the "NuPAC Environmental Test Report" (Ref. 47.b.)

describes that operability and prudency testing was performed prior to testing to the environmental test profile and at the conclusion of testing to the environmental test profile. The operability test was performed at points shown in Figure 4-4 of EPRI TR-107330. Additionally, the prudency test was performed at the conclusion of the 48 hour high temperature and high humidity test run (see Section 8.1.2 of the "NuPAC Environmental Test Report" (Ref. 47.b.)). Table 6-1 of the "NuPAC Environmental Test Report" (Ref. 47.b.) summarizes these operability and prudency test points. Lockheed Martin specifies its acceptance criteria for its operability tests in Section 13 of the "NuPAC System Operability Test Procedure" (Ref. 46.e.) and "NuPAC System Prudency Test Procedure" (Ref. 46.f.) on test record data sheets that it used during testing to record test results. Lockheed Martin summarized its environmental test results in Section 8.0 of the "NuPAC Environmental Test Report" (Ref. 47.b.). Addendums II through IX of the "NuPAC Environmental Test Report" (Ref. 47.b.) provide the operability and prudency test data and results.

Clause 7.2s of IEEE Std 323-2003 requires evaluation of anomalies including their effect on qualification. Lockheed Martin includes its discussion of anomalies encountered during testing with its discussion of test results in Section 8.0 and in Addendum X to the "NuPAC Environmental Test Report" (Ref. 47.b.).

[

] (see Section 4.2 Generic Open Item No. 2.a.).

[

] This is Plant-Specific Action Item No. 8.(b).

Additionally, Section 8.1.4 and Table 8-1 of the “NuPAC Environmental Test Report” (Ref. 47.b.) show BIT faults associated with serial communication errors. Lockheed Martin determined the Bit Error Rate (BER) was acceptable for these communication errors and documented this resolution in Table 9-2 of the “NuPAC Environmental Test Report” (Ref. 47.b.).

Section 8.1.4 of the “NuPAC Environmental Test Report” (Ref. 47.b.) describes a [

] (see Section 4.2 Generic Open Item No. 1.c). [

] This is Plant-Specific Action Item 8.(c).

Table 9-2 of the “NuPAC Environmental Test Report” (Ref. 47.b.) describes anomalies discovered during post-test data review. These anomalies are described as follows:

- [

  ]
- [

] (see Section 4.2, Generic Open Item No. 1.e.).

- [

]

- [

] (see Section 4.2, Generic Open Item No. 1.d.).

RG 1.209 includes consideration for smoke exposure from an electrical fire as an environmental stressor and describes reducing the possibility of smoke exposure and enhancing smoke tolerance. It indicates that the most effective approach to address smoke susceptibility is to reduce the likelihood of smoke exposure by rigorously adhering to the fire protection requirements in 10 CFR Part 50.48 or other individual plant license commitments. However, it also describes reducing equipment susceptibility to smoke exposure through design choices and construction practices such as chip packaging and conformal coatings. Lockheed Martin describes its use of [

]

NRC Staff Evaluation

The NRC staff reviewed Section 6.2.2 of the TR (Ref. 49.a.), Section 5.2 of Appendix A to the TR (Ref. 49.a.), the "NuPAC System Environmental Test Procedure" (Ref. 37.b.), the "NuPAC Environmental Test Report" (Ref. 47.b.), [

] included in Addendum X of the "NuPAC Environmental Test Report" (Ref. 47.b.), the NuPAC Pre-Qualification Test Procedure (Ref. 29.c.), the "NuPAC Pre-Qualification Test Report" (Ref. 29.n.), the [ ] Environmental Test Procedure (Ref. 29.g.), and the [ ] Environmental Test Report (Ref. 34.a.). The NRC staff performed this evaluation in accordance with the regulatory criteria in GDC 2 and 4, the guidance in RG 1.209, and the normative criteria in EPRI TR-107330, and IEEE Std 323-2003.

The NRC staff finds that Lockheed Martin performed operability and prudency testing at the points required during environmental testing. Lockheed Martin shows its test points in Table 6-1 of the "NuPAC Environmental Test Report" (Ref. 47.b.) and these points agree with Figure 4-4 and Table 5-1 of EPRI TR-107330.

The NRC staff finds that Lockheed Martin adequately performed operability testing. As stated in Section 3.5.3.2 of this SE, the NRC staff finds Lockheed Martin specified acceptance criteria for its operability tests consistent with its design and the normative criteria of IEEE Std 323-2003 and Section 5.3 of EPRI TR-107330. Sections 8.1.1 through 8.1.3 of the "NuPAC Environmental Test Report" (Ref. 47.b.) describe the operability tests being completed successfully (or data was verified to be within tolerance) with the exception of [

] In both cases these errors affected response time testing. The

NRC staff determined the operability testing was completed satisfactorily even though these errors occurred because they were one-time occurrences and the tests were completed successfully at other test points. Lockheed Martin shows the tests met the acceptance criteria in Addendums II, IV, VI, VII, and VIII to the "NuPAC Environmental Test Report" (Ref. 47.b.). These addendums recorded test results with acceptance criteria and the pass/fail status.

The NRC staff finds that Lockheed Martin adequately performed prudency testing. As stated in Section 3.5.3.2 of this SE, the NRC staff finds Lockheed Martin specified acceptance criteria for its prudency tests consistent with its design and the normative criteria of IEEE Std 323-2003 and Section 5.4 of EPRI TR-107330. Sections 8.1.1 through 8.1.3 of the "NuPAC Environmental Test Report" (Ref. 47.b.) describe the prudency tests being completed successfully (or data was verified to be within tolerance). In addition, Lockheed Martin shows the tests met the acceptance criteria in Addendums III, V, and IX to the Environmental Test Report (Ref. 47.b.). These addendums recorded test results with acceptance criteria and the pass/fail status.

The NRC staff finds that Lockheed Martin adequately evaluated anomalies including their effect on qualification with the following exceptions:

- [ ] (see Section 4.2, Generic Open Item No. 1.d.).
- [ ] (see Section 4.2, Generic Open Item No. 1.c.).
- [ ] (see Section 4.2, Generic Open Item No. 1.e.).

The NRC staff finds that Lockheed Martin specified a qualification envelope consistent with the environmental testing it conducted. Lockheed Martin's qualification envelope is [ ] degrees Fahrenheit ([ ] degrees Fahrenheit margin) to [ ] degrees Fahrenheit ([ ] degrees Fahrenheit margin) and [ ] percent ([ ] percent margin) to [ ] percent relative humidity. Attachment B of the [ ] Environmental Test Report (Ref. 34.a.) shows temperature and humidity test data that bounds Lockheed Martin's qualification envelope. In addition, the NRC staff finds that Lockheed Martin performed testing at the upper extremes of temperature and humidity consistent with Section D.5.4.1 of ISG – 06. Section 5.3 of Appendix A to the TR (Ref. 49.a.) requires the licensee to perform heat management calculations when mounting the NuPAC chassis into enclosures to ensure the qualification envelope is not exceeded. Licensees should verify that temperature and relative humidity conditions, including abnormal and accident conditions where the NuPAC platform is installed would not exceed the limits of atmospheric qualification testing. This verification includes heat management calculations in accordance with Section 5.3 of the Application Design Guide in Appendix A to the TR (Ref. 49.a.) and verification the initial heat up rate of [ ] degrees Fahrenheit per hour is not exceeded. This is a plant-specific action item.

3.5.3.4 Radiation

GDC 4 requires SSCs ITS be designed to function within environments that include normal operation, maintenance, and testing. RG 1.209 identifies ionizing dose radiation hardness levels of 1 krad for commercial off-the-shelf (COTS) metal oxide semiconductor (MOS) integrated circuits.

Clause 6.1.5.1 of IEEE Std 323-2003 requires the normal and abnormal service conditions for equipment be specified. This clause requires nominal and extreme values for the radiation environment be specified along with their expected durations. In addition, Clause 6.3.1.9 of IEEE Std 323-2003 states that if normal and accident radiation doses and dose rate are demonstrated to have no effect on the safety function(s) of the equipment, then radiation testing may be excluded, and the justification should be documented.

Sections 4.3.6.1 and 4.3.6.2 of EPRI TR-107330 (for normal and abnormal environments, respectively) require operation within specification for radiation exposure up to 1 krad and this exposure is consistent with radiation hardness levels for COTS MOS integrated circuits described in RG 1.209. Lockheed Martin states in Section 6.2.4 of the TR (Ref. 49.a.) that it performed radiation withstand testing in accordance with its test procedure and EPRI TR-107330 to at least 1 krad gamma radiation. Furthermore, Section 5.5 of the Application Design Guide in Appendix A to the TR (Ref. 49.a.) describes this testing to at least [ ] krad over a short period for withstand capability to a mild environment radiation exposure of [ ] krad integrated over a [ ] period. Section 1.4 of the [ ] Radiation Test Report (Ref. 29.p.) shows the laboratory test results for two card files irradiated at a gamma dose rate of [ ] rad-air/hour for [ ] minutes for a total integrated dose (TID) of [ ] krad.

IEEE 323-2003, Clause 6.2.5 requires specifying criteria (i.e., acceptance criteria) to demonstrate equipment can perform its safety function. In addition, IEEE Std 323-2003, Clause 7.2f, requires test documentation to include an identification of acceptance criteria and performance results. Although the test specimen was not energized during radiation exposure, Section 7.2 of the NuPAC Radiation Test Report (Ref. 29.o.) states that Lockheed Martin performed operability and prudency testing prior to exposure and afterwards. Lockheed Martin includes acceptance criteria for operability and prudency testing on test record data sheets that it used during testing. Lockheed Martin shows its operability and prudency test results in Addendums II through V of the NuPAC Radiation Test Report (Ref. 29.o.).

Clause 7.2s of IEEE Std 323-2003 requires an evaluation of test anomalies, including their effect on qualification. Lockheed Martin describes an intermittent fault discovered during testing following radiation exposure in Sections 8.1.3 and 8.1.5 of the NuPAC Radiation Test Report (Ref. 29.o.). Lockheed Martin states in Section 8.1.5 that through repeated radiation testing and analysis, it determined the fault was not due to radiation exposure but rather to design parameters that were too limiting or not required for certain components. Lockheed Martin provides its failure review conclusions and corrective actions in Sections 8.1.5.1 and 8.1.5.2 of the NuPAC radiation test report.

NRC Staff Evaluation

The NRC staff reviewed Section 6.2.4 of the TR (Ref. 49.a.), Section 5.5 of the Application Design Guide in Appendix A to the TR (Ref. 49.a.), the NuPAC Radiation Test Procedure

(Ref. 29.i.), the NuPAC Radiation Test Report (Ref. 29.o.), the [ ] Radiation Test Procedure (Ref. 30.g.), and the [ ] Radiation Test Report (Ref. 29.p.). The NRC staff performed this evaluation in accordance with the regulatory criteria in GDC 2 and 4, the guidance in RG 1.209, and the normative criteria in IEEE Std 323-2003 and EPRI TR-107330.

The NuPAC platform is designed to operate in a mild environment (see Section 5.0 of the Application Design Guide in Appendix A to the TR (Ref. 49.a.)). The NRC staff finds that Lockheed Martin adequately specified the radiation environment for the NuPAC platform in Section 5.5 of its Application Design Guide (Appendix A to the TR (Ref. 49.a.)). It specified withstand capability to mild environment radiation exposure of [ ] krad integrated over a [ ] period. This level is consistent with Section 4.3.6.1 and 4.3.6.2 of EPRI TR-107330, and consistent with the RG 1.209 threshold for COTS circuits using MOS technology.

The NRC staff finds that Lockheed Martin adequately evaluated an anomaly it discovered during testing. [

] (see Section 4.2, Generic Open Item No. 1.g.).

The NRC staff finds that Lockheed Martin adequately tested the NuPAC platform for radiation withstand capability. Lockheed Martin tested the NuPAC platform to at least [ ] krad of gamma radiation consistent with the environment it specified in Section 5.5 of its Application Design Guide in Appendix A to the TR (Ref. 49.a.). It showed exposure levels of at least [ ] krad in its test results included in Section 1.4 of the [ ] Radiation Test Report (Ref. 29.p.). Furthermore, it performed operability and prudency testing to demonstrate the NuPAC platform continued to perform as intended following exposure. Licensees referencing this SE should confirm that the NuPAC platform would be located in a mild environment and would be exposed to a lifetime gamma dose of not more than [ ] krad at their individual plant locations.

3.5.3.5 Electromagnetic Interference / Radio Frequency Interference

RG 1.180 identifies the use of tests from the IEC 61000 series (i.e., IEC 61000-3, 4, and 6) and MIL-STD-461E. Lockheed Martin shows in Section 6.2.5 of the TR (Ref. 49.a.) that it used MIL-STD-461E tests for radiated emissions testing and IEC 61000-4 series tests for susceptibility testing and SWC testing. It used IEC 61000-4-2 for Electrostatic Discharge (ESD) immunity testing. Lockheed Martin summarizes its test results in the NuPAC EMC Test Report (Ref. 47.c.) with laboratory test results in [ ] EMI Test Report (Ref. 50.a.). It also summarizes its EMC testing in Section 2.3.3 of its Environmental Qualification (EQ) Summary Report (Ref. 48.a.). Lockheed Martin states in Section 2.3.3 of the EQ Summary Report (Ref. 48.a.) that it performed EMC testing from September through November of 2015 at [ ]. Lockheed Martin includes its emissions, susceptibility, and SWC test procedures (i.e., NuPAC EMC Test Procedures, Ref. 37.d.), and its NuPAC ESD Test Procedure (Ref. 37.e.).

Section 3.3.2 of the NuPAC EMC Test Report (Ref. 47.c.) describes [
] (see also Section 5.1.2 of the NuPAC EMC Test Report (Ref. 47.c.)). Section 3.3.2 describes [
] (see Section 4.2, Generic Open Item No. 4.a).

IEEE Std 323-2003, Clause 6.2.5 requires specifying criteria (i.e., acceptance criteria) to demonstrate equipment can perform its safety function. In addition, IEEE Std 323-2003, Clause 7.2f, requires test documentation to include an identification of acceptance criteria and performance results. Lockheed Martin describes its testing in Section 6.2 of the NuPAC EMC Test Report (Ref. 47.c.). Section 6.2.1 describes operability and prudency testing. Section 6.2.2 describes how Lockheed Martin monitored the system under static conditions and performed abbreviated operability and prudency testing. Table 6-2 of the NuPAC EMC Test Report (Ref. 47.c.) shows each EMI/RFI test along with Lockheed Martin's demonstration of functionality. Table 7-1 of the NuPAC EMC Test Report (Ref. 47.c.) shows the test sequence. Lockheed Martin specifies acceptance criteria in Tables 3-1 and 3-2 of the NuPAC EMC Test Report (Ref. 47.c.) and includes acceptance criteria on test record data sheets that it used during testing to record test results (see Addendums I through XII of the NuPAC EMC Test Report (Ref. 47.c.)).

3.5.3.5.1 Emissions Testing

RG 1.180, Regulatory Position 3, provides guidance for EMI/RFI emissions testing. It lists MIL-STD-461E tests in Table 2 and shows their operating envelopes in Figures 3.1 through 3.4. Lockheed Martin shows in Table 2-2 of its Environmental Qualification (EQ) Summary Report (Ref. 48.a.) that it performed MIL-STD-461E radiated emissions RE101 and RE102 testing. Section 3.3.2 of the NuPAC EMC Test Report (Ref. 47.c.) states that power supplies were not part of the system qualification and that no individual power line testing was performed. Therefore, Lockheed Martin did not perform conducted emissions testing (i.e., MIL-STD-461E CE101 and CE102) because it did not qualify power supplies. Lockheed Martin should address conducted emissions in accordance with RG 1.180, Regulatory Position 3 (see Section 4.2, Generic Open Item No. 4.b.). Table 3.5.3.5-1 summarizes Lockheed Martin's emissions testing.

Table 3.5.3.5-1. Emissions Testing		
MIL-STD-461E Test	**Applicability**	**Lockheed Martin Testing**
RE101	Radiated Emissions, Magnetic Field RE101 is applicable to equipment and subsystem enclosures and interconnecting leads. Figure 3.3 of RG 1.180 specifies the operating envelope.	Criteria: Section 8.3.6 of NuPAC EMC Test Report (Ref. 47.c.) specifies emissions below the limit of Figure 8-2 (This figure corresponds to Figure 3.3 of RG 1.180). Results: Section 5.6 of the [ ] EMI Test Report (Ref. 50.a.) shows the limits in Figure 8-2 of the NuPAC EMC Test Report (Ref. 47.c.) were not exceeded for various positions on the front and rear of Chassis 1 and 2 and the interconnecting cable bundle.
RE102	Radiated Emissions, Electric Field RE102 is applicable to equipment and subsystem enclosures and interconnecting leads. Above 30 MHz, the test is performed for both horizontally and vertically polarized fields. Figures 3.4 and 6.1 of RG 1.180 specify the operating envelope.	Criteria: Section 8.4.6 of NuPAC EMC Test Report (Ref. 47.c.) specifies emissions below the limit of Figure 8-4 (This figure corresponds to Figures 3.4 and 6.1 (above 1 GHz) of RG 1.180). Results: For the antenna positions listed in Table 6-2 of the [ ] EMI Test Report (Ref. 50.a.) Section 6.6 shows the limits in Figure 8-4 of the NuPAC EMC Test Report (Ref. 47.c.) were not exceeded. Lockheed Martin provides antenna beam width calculations in Section 6.5.1 of the [ ] EMI Test Report (Ref. 50.a.) that it used to determine the number of antenna positions. In addition, Lockheed Martin provides calibration results in Section 6.6 of the [ ] EMI Test Report (Ref. 50.a.). Note that [ ] were used (see Figure 8-3, Note 2 and Section 8.4.5 of the NuPAC EMC Test Report (Ref. 47.c.)). Limitations: To fully comply with RE102, Lockheed Martin requires the following for plant-specific configurations: • [ ] • [ ] • [ ]

Lockheed Martin states in Table 2-5 of the EQ Summary Report (Ref. 48.a.) that radiated emissions tests RE101 and RE102 were compliant. [ ] (see Section 5.5.2 of the NuPAC EMC Test Report (Ref. 47.c.)). For RE102, Lockheed Martin specifies in Table 2-5 of the EQ Summary Report (Ref. 48.a.) that 12 V power supplies must be present for future qualification testing.

NRC Staff Evaluation

The NRC staff reviewed Section 6.2.5 of the TR (Ref. 49.a.), Section 2.3.3 of the EQ Summary Report (Ref. 48.a.), Sections 3.3.2, 8.3.6, and 8.4.6 of the NuPAC EMC Test Report (Ref. 47.c.), Sections 5.0 and 6.0 of the [ ] EMI Test Report (Ref. 50.a.), and Section 4.2 of the NuPAC EMC Test Procedure (Ref. 37.b.). The NRC staff performed this evaluation in accordance with the criteria in GDC 2 and 4, the guidance in RG 1.180, and the requirements in MIL-STD-461E.

The NRC staff finds that Lockheed Martin's radiated magnetic field emissions testing is compliant with MIL-STD-461E, RE101, and is consistent with the guidance in RG 1.180 for an equipment under test (EUT) configuration that does not include power supplies. Lockheed Martin states in Section 8.3.3.1 of the NuPAC EMC Test Report (Ref. 47.c.) that the TSC was supplied power from the ATS 12 VDC power supplies. These power supplies were external to the EUT. Emissions from the tested configuration may be significantly lower when compared to one that includes power supplies, and MIL-STD-461E requires the EUT to be operating in a mode which produces maximum emissions. Therefore, once Lockheed Martin identifies power supplies it should address radiated magnetic field emissions for an EUT configuration that includes power supplies and tested in an operating mode which produces maximum emissions in accordance with RG 1.180, Regulatory Position 3 (see Section 4.2, Generic Open Item No. 4.c.).

The NRC staff finds that Lockheed Martin's radiated emissions testing is compliant with MIL-STD-461E, RE102, and is consistent with the guidance in RG 1.180 for an EUT tested with [ ]. Lockheed Martin calculated antenna beam widths and shows the results of this calculation in Table 6-3 of the [ ] EMI Test Report (Ref. 50.a.). It used the beam width calculations to determine the number of antenna positions that it lists in Table 6-2 over the frequency ranges for each antenna. The NRC staff finds the number of antenna positions determined is consistent with the normative criteria of Section 5.16.3.3.c(2)(c) of MIL-STD-461E. Lockheed Martin states in Section 8.4.3.1 of the NuPAC EMC Test Report (Ref. 47.c.) that the TSC was powered by [ ]. This configuration [ ] differs from the required setup described in Section 5.16.3.3 of MIL-STD-461E. In addition, because [ ], the NRC staff finds the EUT was not configured for maximum emissions as required by Section 4.3.9 of MIL-STD-461E. Therefore, once Lockheed Martin identifies power supplies, it should address radiated electric field emissions for an EUT configuration that includes power supplies and tested in an operating mode which produces maximum emissions in accordance with RG 1.180, Regulatory Position 3 (see Section 4.2, Generic Open Item No. 4.c.).

3.5.3.5.2 Susceptibility Testing

Lockheed Martin performed EMI/RFI susceptibility testing using IEC 61000-4 test methods. RG 1.180, Regulatory Position 4 lists ten IEC susceptibility test methods in Table 7 and describes the acceptable operating envelopes in the subsections of Regulatory Position 4.

RG 1.180 specifies MIL-STD-461E test methods separately for: (i) conducted susceptibility on power leads, (ii) conducted susceptibility on interconnecting signal leads, and (iii) radiated susceptibility.

Lockheed Martin lists its susceptibility test results in Table 2-5 of the EQ Summary Report (Ref. 48.a.) and Table 11-1 of the NuPAC EMC Test Report (Ref. 47.c.). These tables show Classification A, B, or C by I/O type for each of the IEC 61000-4 tests Lockheed Martin performed.

RG 1.180, Regulatory Position 1, states that conditions at the point of installation for safety related I&C equipment should be assessed for local interference and steps should be taken to ensure that systems are not exposed to EMI/RFI levels greater than 8 dB below the specified operating envelopes. Additionally, RG 1.180 provides information on the establishment of exclusion zones through administrative controls. For establishing the size of the exclusion zone, it recommends maintaining an 8 dB difference between the susceptibility operating envelope and the allowed emissions level. Therefore licensees referencing this SE should verify their intended locations for the NuPAC platform and their administrative controls for establishing exclusion zones meet the criteria in RG 1.180, Regulatory Position 1 such that emissions in the vicinity of the NuPAC platform are within the tested susceptibility operating envelopes.

3.5.3.5.2.1 Conducted Susceptibility on Power Leads

RG 1.180, Regulatory Position 4 in Section 4.1, describes three IEC tests (IEC 61000-4-6, 4-13, and 4-16) for conducted susceptibility on power leads. It lists these tests in Table 9 and describes their operating envelopes in Section 4.1.3. RG 1.180 identifies IEC 61000-4-13 and its Class 2 operating envelope in Table 10, IEC 61000-4-16 and its Level 3 operating envelopes in Table 11, and IEC 61000-4-6 at Level 3 or 140 dBµV.

Section 3.3.2 of the NuPAC EMC Test Report (Ref. 47.c.) states that power supplies were not part of the system qualification and that no individual power line testing was performed. Therefore, Lockheed Martin did not perform conducted susceptibility testing on power leads because it did not qualify power supplies. Therefore, Lockheed Martin should address conducted susceptibility on power leads in accordance with RG 1.180, Regulatory Position 4 (see Section 4.2, Generic Open Item No. 4.d.).

3.5.3.5.2.2 Conducted Susceptibility on Interconnecting Signal Leads

RG 1.180, Regulatory Position 4 in Section 4.2, describes five tests for EMI/RFI conducted susceptibility on interconnecting signal leads. It includes IEC 61000-4-4, 4-5, 4-6, 4-12, and 4-16 in Table 13, with operating envelopes for low and medium exposure levels in Tables 15 and 16, respectively. RG 1.180 defines the operating envelopes for the susceptibility tests in Section 4.2. In addition, it states in Section 4.2 that most signal leads are expected to be subject to surge environments that correspond to low exposure levels. Table 3.5.3.5-2 summarizes Lockheed Martin's conducted susceptibility testing on signal leads. As shown in this table, Lockheed Martin tested to medium exposure levels.

Table 3.5.3.5-2. Conducted Susceptibility Testing on Interconnecting Signal Leads		
IEC Test	**Applicability**	**Lockheed Martin Testing**
61000-4-4	Electrical Fast Transient (EFT)/Burst Immunity For medium exposure, RG 1.180, Table 16 specifies a Level 4, 2 kV test voltage.	Criteria: Section 8.8.5 of NuPAC EMC Test Report (Ref. 47.c.) specifies testing to IEC 61000-4-4 at a peak output voltage of 2kV (open circuit). (IEC 61000-4-4 identifies this test level as Level 4). Test Data: [ ] Results: [ ] Limitations: [ ]
61000-4-5	Surge Immunity For medium exposure, RG 1.180, Table 16 specifies a Level 3, 2 kV open circuit test voltage and 1 kA short circuit current	Criteria: Section 8.17.5 of NuPAC EMC Test Report (Ref. 47.c.) specifies testing to IEC 61000-4-5 at a medium exposure of 2 kV open circuit voltage and 1 kA short circuit current. (IEC 61000-4-5 identifies this test level as Level 3). Test Data: [ ] Results: [ ]

Table 3.5.3.5-2. Conducted Susceptibility Testing on Interconnecting Signal Leads		
IEC Test	**Applicability**	**Lockheed Martin Testing**
		[ ] Limitations: [ ]: • [ ] • [ ] • [ ] • [ ]
61000-4-6	Radio Frequency Conducted Susceptibility For medium exposure, RG 1.180, Table 16 specifies a Level 3, 140 dBµV test voltage.	Criteria: Sections 8.13.1 and 8.13.5 of NuPAC EMC Test Report (Ref. 47.c.) specifies testing to IEC 61000-4-6 at a 140 dBµV level from 150 kHz to 80 MHz. (IEC 61000-4-6 identifies this test level as Level 3). Test Data: [ ] Results: [

Table 3.5.3.5-2. Conducted Susceptibility Testing on Interconnecting Signal Leads		
IEC Test	**Applicability**	**Lockheed Martin Testing**
		] [ ] Limitations: [ ]
61000-4-12	Oscillatory Transients (Ring Wave) Immunity For medium exposure, RG 1.180, Table 16 specifies a Level 3, 2 kV test voltage.	Criteria: Section 8.11.5 of NuPAC EMC Test Report (Ref. 47.c.) specifies testing to IEC 61000-4-12 to a medium exposure of 2 kV. Test Data: [ ] Results: [ ] Limitations: [ ]

Table 3.5.3.5-2. Conducted Susceptibility Testing on Interconnecting Signal Leads		
IEC Test	**Applicability**	**Lockheed Martin Testing**
61000-4-16	Immunity to Conducted, Common Mode Disturbances For medium exposure, RG 1.180, Table 16 specifies a Level 3 and refers to Table 11. Table 11 shows: 10-1 Vrms (15 – 150 Hz) 1 Vrms (150 – 1.5 kHz) 1 – Vrms (1.5 – 15 kHz) 10 Vrms (15 – 150 kHz)	Criteria: Section 8.10.5 of NuPAC EMC Test Report (Ref. 47.c.) specifies testing to IEC 61000-4-16. Section 15.1 of the NTS EMI Test Report (Ref. 50.a.) specifies testing from 15 Hz to 150 kHz at the RG 1.180 levels. (IEC 61000-4-16 identifies this test level as Level 3). Test Data: [ ] Results: [ ] Limitations: [ ]

NRC Staff Evaluation

The NRC staff reviewed Section 6.2.5 of the TR (Ref. 49.a.), Section 2.3.3 of the EQ Summary Report (Ref. 48.a.), Sections 8.8, 8.10, 8.11, 8.13, 8.17, and Addendums I and XII of the NuPAC EMC Test Report (Ref. 47.c.), Sections 11.0, 12.0, 13.0, 14.0, and 15.0 of the [ ] EMI Test Report (Ref. 50.a.), and Section 4.2 of the NuPAC EMC Test Procedure (Ref. 37.b.). The NRC staff performed this evaluation in accordance with the criteria in GDC 2 and 4, the guidance in RG 1.180, and the normative criteria in IEC 61000.

Lockheed Martin performed the conducted susceptibility tests on interconnecting signal leads required by RG 1.180 showing the test waveforms met the normative criteria of the IEC 61000 standards and showing test results at the levels required for medium exposure in accordance with RG 1.180. Therefore, the NRC staff finds that Lockheed Martin's conducted susceptibility testing on interconnecting signal leads is compliant with IEC 61000-4-4, 4-5, 4-6, 4-12, and 4-16, and is consistent with the guidance in RG 1.180 with the following exceptions:

- [

  ](See Section 4.2 Generic Open Item 4.e.i.).
- [

  ] (see Section 4.2, Generic Open Item No. 4.e.ii.).
- [

  ]

  [

] (see Section 4.2, Generic Open Item No. 4.f.).

- [

] (see Section 4.2, Generic Open Item No. 4.e.iii.).

The NRC staff finds that Lockheed Martin adequately specified acceptance criteria and demonstrated performance results consistent with these criteria. Lockheed Martin used an EMI signal source box to provide a stable input to the TSC during conducted susceptibility testing on interconnected signal leads. Lockheed Martin's criteria in Table 3-1 and Addendum I to the NuPAC EMC Test Report (Ref. 47.c.) are consistent with the normative criteria in Section 4.3.7 of EPRI TR-107330. In addition, Lockheed Martin shows the criteria were met for the six cables (with the exception of analog outputs where the criteria are marked "N/A"). In addition, operability and prudency testing following EMI/RFI tests confirmed the NuPAC platform continued to function. See for example Addendum XII of the NuPAC EMC Test Report (Ref. 47.c.) for operability and prudency test results at the end of all EMI/RFI testing.

The NRC staff finds that Lockheed Martin adequately evaluated anomalies including their effect on qualification. Lockheed Martin identified anomalies during testing, documented them in trouble reports along with their resolution. [

] they are identified in Section 4.2 Generic Open Item No. 1. The unresolved trouble reports are as follows:

- [

] (See Section 4.2 Generic Open Item No. 1.b.).

- [

](See Section 4.2 Generic Open Item No. 1.a.).

- [

] (See Section 4.2, Generic Open Item No. 1.h.)

3.5.3.5.2.3 Radiated Susceptibility

RG 1.180, Regulatory Position 4 in Section 4.3 identifies four tests for EMI/RFI radiated susceptibility. For radiated electric field susceptibility, Section 4.3.3 of RG 1.180 identifies IEC 61000-4-3 with an operating envelope from 26 MHz to 1 GHz at a test level of 10 V/m. For radiated magnetic field susceptibility, RG 1.180 identifies IEC 61000-4-8, 4-9, and 4-10 with the operating envelopes shown in Table 19. Table 3.5.3.5-3 summarizes Lockheed Martin's radiated susceptibility testing.

Table 3.5.3.5-3. Radiated Susceptibility Testing		
IEC Test	**Applicability**	**Lockheed Martin Testing**
61000-4-3	Radiated Susceptibility, Electric Field RG 1.180, Section 4.3.3 specifies a Level 3, 10 V/m test level from 26 MHz to 1 GHz. As stated in Section 3.5.3.5.4 of this SE the frequency range is extended to 10 GHz.	Criteria: Sections 8.12.1 and 8.12.5 of the NuPAC EMC Test Report (Ref. 47.c.) specify testing to a 10 V/m level from 26 MHz to 10 GHz. Section 7.1 of the NTS EMI Test Report (Ref. 50.a.) specifies testing to 10 V/m from 26 MHz to 10 GHz at horizontal and vertical polarizations on the four faces of the EUT. Test Data: [ ] Results: [ ] Limitations: [ ] • [ ] • [ ]
61000-4-8	Radiated Susceptibility, Magnetic Field at 50 Hz and 60 Hz	Criteria: Sections 8.5.3.1 and 8.5.5 of the NuPAC EMC Test Report (Ref. 47.c.) specify exposing each chassis one at a time to the magnetic field at a 300-second (continuous), 30-amp sweep and a 3-second,

Table 3.5.3.5-3. Radiated Susceptibility Testing		
IEC Test	**Applicability**	**Lockheed Martin Testing**
	RG 1.180, Table 19 specifies continuous pulses at 30 A/m and short duration (1 to 3 second) pulses at 300 A/m	300-amp sweep for both 50 Hz and 60 Hz. (IEC 61000-4-8 identifies these test levels as Level 4). Test Data: [ ] Results: [ ] Limitations: [ ]
61000-4-9	Radiated Susceptibility, Magnetic Field (Pulse Magnetic Field Immunity Test)	Criteria: Section 8.6.5 of the NuPAC EMC Test Report (Ref. 47.c.) specifies exposing each chassis one at a time to the magnetic field at a 300 A/m level. (IEC 61000-4-9 identifies this test level as Level 4). Test Data: [ ] Results: [ ]

Table 3.5.3.5-3. Radiated Susceptibility Testing		
IEC Test	**Applicability**	**Lockheed Martin Testing**
		[ ] Limitations: [ ]
61000-4-10	Radiated Susceptibility, Magnetic Field (Damped Oscillatory Magnetic Field Immunity Test)	Criteria: Section 8.7.5 of the NuPAC EMC Test Report (Ref. 47.c.) specifies exposing each chassis one at a time to the magnetic field at 100 kHz and 1 MHz for 2 seconds at a 30 A/m level. Additionally, Table 10-1 of the [ ] EMI Test Report (Ref. 50.a.) specifies a 40 Hz repetition rate at 100 kHz and a 400 Hz repetition rate at 1 MHz. (IEC 61000-4-10 identifies the 30 A/m test level as Level 4.) Test Data: [ ] Results: [ ] Limitations: [

Table 3.5.3.5-3. Radiated Susceptibility Testing		
IEC Test	**Applicability**	**Lockheed Martin Testing**
		]

NRC Staff Evaluation

The NRC staff reviewed Section 6.2.5 of the TR (Ref. 49.a.), Section 2.3.3 of the EQ Summary Report (Ref. 48.a.), Sections 8.5, 8.6, 8.7, 8.12, and Addendums III through VIII of the NuPAC EMC Test Report (Ref. 47.c.), Sections 7.0 through 10.0 of the [ ] EMI Test Report (Ref. 50.a.), and Section 4.2 of the NuPAC EMC Test Procedure (Ref. 37.b.). The NRC staff performed this evaluation in accordance with the criteria in GDC 2 and 4, the guidance in RG 1.180, and the normative criteria in IEC 61000.

To be fully compliant with the standards for radiated susceptibility, Lockheed Martin needs to include power supplies in its qualification because of the potential for power supplies to show susceptibility and for interactions to exist between the power supplies and other components of the EUT. Therefore, Lockheed Martin should address radiated susceptibility for an EUT configuration that includes power supplies in accordance with RG 1.180, Regulatory Position 4 (see Section 4.2, Generic Open Item No. 4.i.1.). However, Lockheed Martin performed the radiated susceptibility tests required by RG 1.180 showing the test waveforms met the normative criteria of the IEC 61000 standards and showing test results at levels required by RG 1.180. Therefore, the NRC staff finds that Lockheed Martin's radiated susceptibility testing is compliant with IEC 61000-4-3, 4-8, 4-9, and 4-10, and is consistent with the guidance in RG 1.180 for an EUT that does not include power supplies with the following exception:

- [

] (see Section 4.2 Open, Item No. 4.i.2.).

The NRC staff finds that Lockheed Martin adequately specified acceptance criteria and demonstrated performance results consistent with these criteria. Lockheed Martin performed operability and prudency testing during exposure and following exposure. The operability and prudency testing confirmed the NuPAC platform performed as intended during and following its exposure. See for example, the test results listed below and included in addendums to the NuPAC EMC Test Report (Ref. 47.c.):

- IEC 61000-4-3: Addendums VII (during) and VIII (post)
- IEC 61000-4-8: Addendums III (during) and Addendum VI (post)
- IEC 61000-4-9: Addendums IV (during) and Addendum VI (post)
- IEC 61000-4-10: Addendums V (during) and Addendum VI (post)

The NRC staff finds that Lockheed Martin adequately evaluated anomalies including their effect on qualification. Lockheed Martin identified anomalies during testing and documented them in trouble reports along with their resolution. Lockheed Martin determined the anomalies were not the result of radiated susceptibility. See for example, [

]

3.5.3.5.3 Surge Withstand Capability

RG 1.180, Regulatory Position 5 describes the IEEE C62.41-1991 SWC test methods in Table 20 and the corresponding IEC tests in Table 21 (i.e., IEC 61000-4-4, 4-5, and 4-12). It describes the waveforms for these tests in the subsections of Regulatory Position 5. Note that these three IEC test methods are also used for conducted susceptibility testing on interconnecting signal leads.

Section 3.3.2 of the NuPAC EMC Test Report (Ref. 47.c.) states that power supplies were not part of the system qualification and that no individual power line testing was performed. Therefore, Lockheed Martin did not perform SWC testing on power leads because it did not qualify power supplies. Lockheed Martin should address SWC on power leads in accordance with RG 1.180, Regulatory Position 5 (See Section 4.2 Generic Open Item No. 4.g.).

3.5.3.5.4 EMI/RFI Testing Above 1 GHz

RG 1.180, Regulatory Position 6 identifies MIL-STD-461E test RE102 for radiated emissions testing above 1 GHz and test RS103 for radiated susceptibility testing above 1 GHz. Figure 6.1 of RG 1.180 shows the operating envelope for RE102 and describes the operating envelope for RS103 as 10 V/m root mean square (rms).

Radiated emissions above 1 GHz is not evaluated separately in this SE. Instead, it is included in the radiated emissions evaluations in Section 3.5.3.5.1 of this SE.

Lockheed Martin did not perform MIL-STD-461E RS103 testing. Instead, it performed IEC 61000-4-3 radiated susceptibility testing but extended the upper limit of the frequency range to 10 GHz. The NRC staff determined this is acceptable because the more recent versions of IEC 61000-4-3 provide for testing at frequencies above 1 GHz. In addition, RG 1.180 specifies the same operating envelope of 10 V/m that is used at lower frequencies. Section 3.5.3.5.2.3 of this SE includes radiated susceptibility testing above 1 GHz.

3.5.3.5.5 Electrostatic Discharge

RG 1.180 identifies EPRI topical report TR-102323 as one method of addressing issues of EMC for safety related DI&C systems in nuclear power plants. In addition, RG 1.209 states that Revision 1 of EPRI TR-102323 is applicable to testing for EMI/RFI and surge voltages. Appendix B, Section 3.5.1 of EPRI TR-102323, Revision 1 has levels of ±8 kV for the contact discharge voltage and ±15 kV for the air discharge voltage. Lockheed Martin states in Section 8.16.5 of the NuPAC EMC Test Report (Ref. 47.c.) that it performed ESD testing in accordance with IEC 61000-4-2. It performed contact discharge testing at ±8 kV. It states in Section 8.16.5 of the NuPAC EMC Test Report (Ref. 47.c.) that it did not need to perform air-discharge testing because the test points were all accessible. In addition, Section 5 of IEC 61000-4-2 states that contact discharge is the preferred test method.

Lockheed Martin lists its test points in Table 16-2 of the [ ] EMI Test Report (Ref. 50.a.) and Tables 4-2 and 4-3 of the NuPAC ESD Test Procedure (Ref. 37.e.). It shows photographs of direct and indirect contact discharge testing at these points in Section 16.6 of the [ ] EMI Test Report (Ref. 50.a.). Lockheed Martin's indirect contact discharge testing included the use of a Vertical Coupling Plane (VCP). IEC 61000-4-2 specifies test levels in Table 1 for which the Level 4 contact discharge voltage is 8 kV. Lockheed Martin shows its contact discharge test levels of 8 kV on its data sheet included in Section 16.6 of the [ ] EMI Test Report (Ref. 50.a.). In addition, this section includes plots showing waveform characteristics that are consistent with the normative criteria of IEC 61000-4-2.

Section 4.3.8 of EPRI TR-107330 specifies the normative criteria for ESD withstand capability. It specifies conformance to EPRI TR-102323, Appendix B, Section 3.5 and requires the equipment to withstand the ESD levels without disruption in operation or damage. Lockheed Martin describes its test results and anomalies in Table 8-25 and Sections 8.16.7 and 8.16.8 of the NuPAC EMC Test Report (Ref. 47.c.). Lockheed Martin shows several BIT faults that occurred during testing in Table 8-27 of the NuPAC EMC Test Report (Ref. 47.c.). In addition, Lockheed Martin states in Section 8.16.8 of the NuPAC EMC Test Report (Ref. 47.c.) [

]. Lockheed Martin states in Section 8.16.9 of the NuPAC EMC Test Report (Ref. 47.c.) [

] Lockheed Martin concludes in Section 8.16.9 of the NuPAC EMC Test Report that the NuPAC platform did not perform as required but returned to normal operation after exposure. It also states analog inputs and discrete inputs showed no susceptibility.

NRC Staff Evaluation

The NRC staff reviewed Section 6.2.5 of the TR (Ref. 49.a.), Section 2.3.3 of the EQ Summary Report (Ref. 48.a.), Section 8.16 of the NuPAC EMC Test Report (Ref. 47.c.), Section 16 of the [ ] EMI Test Report (Ref. 50.a.), and the NuPAC ESD Test Procedure (Ref. 37.e.). The NRC staff performed this evaluation in accordance with the criteria in GDC 2 and 4, the guidance in RG 1.209 and RG 1.180, and the normative criteria in IEC 61000-4-2, EPRI TR-107330, and EPRI TR-102323, Revision 1.

The NRC staff finds that Lockheed Martin's ESD testing was consistent with the normative criteria of IEC 61000-4-2; [

]. In addition, Lockheed Martin states in Section 8.16.7 of the NuPAC EMC Test Report (Ref. 47.c.) [

] (See Section 4.2 Generic Open Item No. 4.h.).

The NRC staff finds that Lockheed Martin adequately specified acceptance criteria in Table 3-2 of the NuPAC EMC Test Report (Ref. 47.c.) and this criteria is consistent with Section 4.3.8 of EPRI TR-107330. Lockheed Martin demonstrated performance results before and after ESD testing consistent with these criteria. It shows I/O levels are within acceptable ranges before and after ESD testing in Addendum X to the NuPAC EMC Test Report (Ref. 47.c.). It includes operability and prudency test results before ESD testing in Addendum IX, and after ESD testing in Addendum XI to the NuPAC EMC Test Report (Ref. 47.c.). These test results confirmed the NuPAC platform performed as intended after exposure to the ESD levels.

The NRC staff finds that Lockheed Martin adequately evaluated anomalies including their effect on qualification. Lockheed Martin identified anomalies during testing and documented them in trouble reports along with their resolution. Lockheed Martin determined that [

] (See Section 4.2 Generic Open Item No. 1.b.). This trouble report and associated channel trips are also described in Section 3.5.3.5.2.2 of this SE.

3.5.3.5.6 Electromagnetic Compatibility Documentation

RG 1.180, Regulatory Position 7 provides guidance for EMC documentation. It includes test results (with the test procedure) as item 5 that it describes as part of a minimum level of documentation. Lockheed Martin summarized all of its testing in the NuPAC EMC Test Report (Ref. 47.c.), the NuPAC EMC Test Procedure (Ref. 37.b.), and the NuPAC ESD Test Procedure (Ref. 37.e.). Lockheed Martin provided laboratory test results in its [ ] EMI Test Report (Ref. 50.a.) which includes individual sections for each test to include the compliance standard and associated limits along with a summary of the test procedure and tabulated results. Lockheed Martin addresses any anomalies it found during the testing in the NuPAC EMC Test Report (Ref. 47.c.).

NRC Staff Evaluation

The NRC staff reviewed Section 6.2.5 of the TR (Ref. 49.a.), the NuPAC EMC Test Report (Ref. 47.c.), the [ ] EMI Test Report (Ref. 50.a.), the NuPAC EMC Test Procedure (Ref. 37.b.), and the NuPAC ESD Test Procedure (Ref. 37.e.). The NRC staff performed this evaluation in accordance with the criteria in GDC 2 and 4 and the guidance in RG 1.180.

The NRC staff finds that Lockheed Martin provided adequate documentation with regard to EMI/RFI and ESD testing of the NuPAC platform in accordance with RG 1.180, Regulatory Positon 7. Lockheed Martin provided test reports, test procedures, and laboratory reports as evidence the NuPAC platform met its specification requirements.

3.5.3.6 Seismic

RG 1.100 states that rigorous seismic qualification by analysis, testing, or combined analysis and testing, as described in Clauses 7, 8, and 9 of IEEE Std 344-2004 are acceptable for seismic qualification of electrical equipment. Lockheed Martin states in Section 3.4 of the

NuPAC Seismic Test Report (Ref. 46.h.) that it performed seismic testing of each chassis individually with the other one connected and communicating. It conducted this testing from November 16 through 18, 2015, at [
].

IEEE 344-2004, Clause 8.1.1 requires mounting equipment in a manner that simulates the intended service mounting. Lockheed Martin states in Section 3.3 of the NuPAC Seismic Test Report (Ref. 46.h.) that the TSC consisted of two chassis assemblies with each one containing 18 GLMs. One chassis consisted of Trip Detect Logic modules and the other one consisted of Coincidence/Output Logic modules. Together these two chassis form the primary elements of the NuPAC system. Each chassis was tested separately by mounting it in a rack-mount test fixture that was bolted directly to a triaxial seismic table. Lockheed Martin states in Section 5.2 of the [ ] Seismic Test Report (Ref. 38.b.) that the Equipment Under Test (EUT) was oriented on the test table such that the horizontal axes of the specimens were collinear with the horizontal axes of the table. It states in Section 8.7.1 of the NuPAC Seismic Test Report (Ref. 46.h.) that Chassis 1 was installed into the test fixture using [
] and that this exact method will be used when installing a chassis into a cabinet in future applications. Section 8.9 of the NuPAC Seismic Test Report (Ref. 46.h.) describes the same installation for Chassis 2 in the test fixture.

Section 6.3.4.3 of EPRI TR-107330 specifies that a resonance search be conducted first. IEEE Std 344-2004, Clause 8.1.4 states that exploratory vibration tests (or resonance searches) are generally not part of the seismic qualification requirements but may be performed to aid in the determination of the best test method for qualification or to determine the dynamic characteristics of the equipment. Clause 8.1.4.1 describes resonance searching performed prior to seismic qualification testing using a slowly swept low-level sinusoidal vibration. It recommends a resonance search beyond 33 Hz, for example, to 50 Hz or to the Required Response Spectrum (RRS) cutoff frequency, whichever is higher. The sweep rate should be two octaves per minute, or less. A 0.2 g peak input is the conventional input level, but it may be adjusted lower to avoid equipment damage or higher to take nonlinearities into consideration. Lockheed Martin describes in Section 8.7.2 (for Chassis 1) and Section 8.10 (for Chassis 2) of the NuPAC Seismic Test Report (Ref. 46.h.) and Section 5.5 of the [ ] Seismic Test Report (Ref. 38.b.) that it performed resonance searches using a low-level (approximately 0.2 g) single-axis sine sweep from 1 to 100 Hz in each of the three orthogonal axes at a sweep rate of 1 octave per minute.

Lockheed Martin shows its Chassis 1 resonance search results on pages B-113 through B-136, and Chassis 2 resonance search results on pages B-248 through B-271 of the [ ] Seismic Test Report (Ref. 38.b.). Resonances may be defined as transmissibility plots that have an amplitude ratio greater than 2.0 and a corresponding phase shift of at least 90 degrees. Lockheed Martin states in Section 8.7.2 (for Chassis 1) and Section 8.10 (for Chassis 2) of the NuPAC Seismic Test Report (Ref. 46.h.) that its criterion for determining a resonance was an amplification of [ ]. For this criterion, Lockheed Martin did not identify a resonance from 1 to 100 Hz. It states in Section 8.7.2 of the NuPAC Seismic Test Report (Ref. 46.h.) that the transmissibility plots did not indicate the narrow, sharp amplification typical of resonances. Note, however, Lockheed Martin did not provide phase plots which could have helped in identifying resonances.

Although Lockheed Martin did not identify any resonances, it did identify various issues in the resonance searches:

- [

  ]
- [

  ]
- [

  ]

Section 6.3.4.3 of EPRI TR-107330 specifies testing to include five tri-axial operating basis earthquakes (OBEs) followed by a tri-axial safe shutdown earthquake (SSE). IEEE Std 344-2004, Clause 8.1.5.2 states that seismic qualification tests must include OBE tests preceding the SSE. In addition, it states that the number of OBEs shall be justified for each site or shall produce the equivalent effect of five OBEs. Lockheed Martin states in Section 1.0 of the NuPAC Seismic Test Report (Ref. 46.h.) that each chassis was exposed to five OBEs followed by one SSE at 30 seconds duration with performance verified before, during, and after each event.

IEEE Std 344-2004, Clause 4.4 states that the goal of seismic simulation is to simulate the earthquake environment in a realistic manner and states that the response spectrum, time history, and power spectral density (PSD) are functions that can be used to describe the simulated seismic motion. A response spectrum is the maximum response of single degree of-freedom oscillators as a function of frequency and damping when subjected to input motion. Section 4.3.9 of EPRI TR-107330 specifies testing to the OBE and SSE levels shown in Figure 4-5 which has a frequency range from 1 to 100 Hz at 5 percent damping. In Section 9.1 of the NuPAC Seismic Test Report (Ref. 46.h.), Lockheed Martin describes its RRS as the profile shown in Figure 4-5 of a newer release (without a revision number change) to EPRI TR-107330. It states in Sections 5.7 and 5.9 of the [ ] Seismic Test Report (Ref. 38.b.) that the RRS exceeds the table limitations at some frequencies and therefore seismic simulation was performed on a best effort basis.

Section C.1.1.1.e of RG 1.100 states that the frequency range for testing should be consistent with the RRS of the specific plant equipment and that although 1/3 octave spacing is for use with low frequency excitation, for high-frequency sensitive equipment, an interval of 1/6 octave

spacing should be used extending up to the frequency of interest shown in the RRS. Lockheed Martin states in Sections 5.7 and 5.9 of the [ ] Seismic Test Report (Ref. 38.b.) [

]

IEEE Std 344-2004, Clause 6.3.2 states that any practical value of damping, such as 5 percent, may be employed in the RRS for testing, and it need not correspond to the actual equipment damping. Clause 8.6.1.3 states that damping of 5 percent is the recommended choice for testing. In addition, Section 6.3.4.4 of EPRI TR-107330 requires reporting the TRS for 0.5, 1, 2, and 3 percent damping. Section 5.2 of the [ ] Seismic Test Report (Ref. 38.b.) lists the tests and the corresponding TRS plots with damping values of [

]

IEEE Std 344-2004, Clause 8.6.1 states that the seismic simulation waveforms should: (i) produce a TRS that closely envelopes the RRS using single-frequency or multiple-frequency input, (ii) have a peak acceleration equal to or greater than the RRS zero period acceleration (ZPA), (iii) not include frequency content above the RRS ZPA asymptote, and (iv) have a duration as specified in Clause 8.6.5. IEEE 344-2004, Clause 8.6.5 states that the duration of the strong motion portion of each test should at least be equal to the strong motion portion of the original time history used to obtain the RRS, with a minimum of 15 seconds. Section 9.3.3 of the NuPAC Seismic Test Report (Ref. 46.h.) describes the period of strong motion beginning at second 6 and ending at second 25. In addition, Lockheed Martin shows its test results in Appendix B of the [ ] Seismic Test Report (Ref. 38.b.). For example, Lockheed Martin shows the TRS enveloping the RRS for the Run 8 OBE test on pages B-61 through B-63. In addition, Lockheed Martin summarizes the OBE results in Figure 9-13 of the NuPAC Seismic Test Report (Ref. 46.h.). This figure shows the TRS enveloping the RRS at all frequencies for all OBE tests on both chassis. Lockheed Martin shows the combined Chassis 1 and 2 SSE results in Figure 9-19 of the NuPAC Seismic Test Report (Ref. 46.h.). This figure shows the TRS enveloping the RRS at all frequencies above 5 Hz. IEEE 344, Clause 8.6.3.1 specifies enveloping the RRS down to [ ] Hz provided no resonances exist below [ ] Hz. Although Lockheed Martin did not identify resonances below [ ] Hz, it did not envelope the SSE RRS down to [ ] Hz.

IEEE Std 344-2004, Clause 8.6.3.1 specifies waveform stationarity and intends stationarity to exist over the strong motion portion of the test waveform. It states that stationarity can be demonstrated by showing the frequency/amplitude content of the waveform is statistically constant with time. In addition, Annex B to IEEE Std 344-2004 describes methods for showing stationarity including the use of time interval power spectral density (PSD). The PSD is the mean squared amplitude per unit frequency of a waveform. Section 9.3.3 of the NuPAC Seismic Test Report (Ref. 46.h.) states that Lockheed Martin captured one second power spectral density (PSD) “snapshots” for each chassis. It plotted them in Figures 9-20 through 9-25 of the NuPAC Seismic Test Report (Ref. 46.h.) on what it identifies as waterfall plots.

Because the data was not retained, numerical calculations to show stationarity could not be reviewed. However, visual examination of the plots shows that the PSD levels at specific frequencies are similar during the strong motion portion of the seismic test. This is an indicator of stationarity. In addition, Lockheed Martin states in Section 9.3.3 of the NuPAC Seismic Test Report (Ref. 46.h.) that the waterfall plots show the stationarity requirement has been met.

IEEE Std 344-2004, Clause 8.6.6.3 requires waveform independence in all three orthogonal directions. It states that the table time histories should have coherence values of less than 0.5 when computed with at least 12 data samples. Alternatively, it states that a correlation coefficient of absolute value less than 0.3 for all time delays may be used. Additional discussion is in Annex E of IEEE Std 344-2004. Lockheed Martin shows its coherence results in Figures 9-26 through 9-31 of the NuPAC Seismic Test Report (Ref. 46.h.). For both chassis, it shows coherence values [

]. For this one case, [

]. Lockheed Martin concludes in Section 9.3.4 of the NuPAC Seismic Test Report (Ref. 46.h.) that the coherence criteria were met for Chassis 1 and 2.

IEEE Std 323-2003, Clause 6.2.5 requires specifying criteria (i.e., acceptance criteria) to demonstrate equipment can perform its safety function. In addition, IEEE Std 323-2003, Clause 7.2f, requires test documentation to include an identification of acceptance criteria and performance results. Lockheed Martin specifies its test requirements in Section 4.0 of the NuPAC Seismic Test Report (Ref. 46.h.). In addition, it specifies operability and prudency testing before and after seismic testing in Section 6.1.1, and abbreviated operability testing (i.e., accuracy testing only) in Section 6.1.2 of the NuPAC Seismic Test Report (Ref. 46.h.). Lockheed Martin includes acceptance criteria for operability and prudency testing on test record data sheets that it used during testing to record test results (See Addendums II through XIX of the NuPAC Seismic Test Report (Ref. 46.h.)). [

]

Clause 7.2s of IEEE Std 323-2003 requires evaluation of anomalies including their effect on qualification. Lockheed Martin describes the anomalies it encountered during testing in Section 8.13 of the NuPAC Seismic Test Report (Ref. 46.h.). Lockheed Martin documented these anomalies and their resolution in the trouble reports listed in Table 10-1 of the NuPAC Seismic Test Report (Ref. 46.h.). A summary of these anomalies is as follows:

- [

]

- [

] (See Section 4.2 Generic Open Item No. 1.f.).

- [

]

- [

] This is a plant-specific action item.

Lockheed Martin concludes in Section 11.0 of the NuPAC Seismic Test Report (Ref. 46.h.) that the NuPAC platform is qualified to operate up to the seismic levels in Figures 9-32 and 9-33. Figure 9-32 shows the minimum OBE and SSE TRS levels for all test runs and both chassis against the EPRI TR-107330 Figure 4-5 RRS. Figure 9-33 shows the SSE TRS levels minus a 10 percent margin. In addition, Table 9-7 of the NuPAC Seismic Test Report (Ref. 46.h.) tabulates the qualification levels at 1/6 octave intervals.

NRC Staff Evaluation

The NRC staff reviewed Section 6.2.3 of the TR (Ref. 49.a.), Section 5.4 of Appendix A to the TR (Ref. 49.a.), the NuPAC Seismic Test Procedure (Ref. 37.c.), the NuPAC Seismic Test Report (Ref. 46.h.), the [ ] Seismic Test Procedure (Ref. 36.a.), and the [ ] Seismic Test Report (Ref. 38.b.). The NRC staff performed this evaluation in accordance with the criteria in GDC 2 and 4, the guidance in RG 1.100, and the requirements in EPRI TR-107330, IEEE Std 344-2004, and IEEE Std 323-2003.

The NRC staff finds that Lockheed Martin's resonance search results were adequate for determining that no resonances exist below [ ] Hz. The test level, frequency range, and sweep

rate were consistent with the requirements in IEEE Std 344-2004. In addition, the NRC staff determined that Lockheed Martin's criterion for determining a resonance at an amplification of [ ] is acceptable. However, the NRC staff cannot conclude that there are no resonances below 100 Hz because no phase plots were provided and the search results above 13 Hz are inconclusive. [

] However, resonance searches are not required by IEEE Std 344-2004 although they may be needed to demonstrate the requirements of Clause 8.6.3.1j have been met. Therefore, inconclusive results do not invalidate seismic qualification.

The NRC staff finds that Lockheed Martin adequately specified acceptance criteria and demonstrated performance results consistent with these criteria. Lockheed Martin performed pre-seismic and post-seismic operability and prudency testing. It performed abbreviated operability testing during seismic testing in addition to static mode data analysis. Post-seismic operability and prudency testing confirmed the NuPAC platform performed as intended following exposure to seismic levels. See for example the post-seismic operability test results in Addendum XVIII and the post-seismic prudency test results in Addendum XIX of the NuPAC Seismic Test Report (Ref. 46.h.).

The NRC staff finds that Lockheed Martin adequately evaluated anomalies including their effect on qualification with the exception of [

] (see Section 4.2 Generic Open Item No. 1.f.).

Lockheed Martin showed that its test inputs met independence and stationarity requirements for SSE test runs in accordance with IEEE Std 344-2004. Lockheed Martin's waterfall plots include time slice PSDs that are relatively constant over time. This is an acceptable qualitative demonstration of stationarity. To demonstrate waveform independence, Lockheed Martin provide plots showing coherence values are all [

]

The NRC staff finds that Lockheed Martin adequately specified its seismic qualification levels. Although the SSE TRS does not envelope the EPRI TR-107330, Figure 4-5 RRS, Lockheed Martin demonstrated the performance of the NuPAC platform to the levels shown in Figures 9-32 and 9-33 and listed in Table 9-7 of the NuPAC Seismic Test Report (Ref. 46.h.). Licensees referencing this SE should ensure the plant-specific In-Equipment Response Spectra (IERS) is enveloped by the NuPAC platform TRS qualification envelope.

3.5.4 Conclusion

This section provides the conclusions from the review subject to the limitations and conditions in Section 4.2.

The NRC staff concludes, based on the considerations discussed herein, that (1) there is reasonable assurance that the health and safety of the public will not be endangered by use of the equipment in the proposed manner, and (2) such use will be conducted in compliance with the Commission's regulations.

The NRC staff has verified that Lockheed Martin provided sufficient information and that the results of the review support the conclusions in the following subsections.

3.5.4.1 Atmospheric

The NRC staff concludes that Lockheed Martin's qualification of the NuPAC platform for atmospheric effects is in accordance with 10 CFR Part 50, GDC 2 and 4, RG 1.209, EPRI TR-107330, and IEEE Std 323-2003 for type testing. Lockheed Martin performed its testing at the extremes of temperature and relative humidity. It specified its qualification envelope, demonstrated the NuPAC platform's performance is acceptable at levels that bound the qualification envelope, and documented its testing consistent with the requirements of IEEE Std 323-2003.

3.5.4.2 Radiation

The NRC staff concludes that Lockheed Martin's qualification for radiation withstand capability is in accordance with 10 CFR Part 50, GDC 2 and 4; RG 1.209; IEEE Std 323-2003; and EPRI TR-107330. Lockheed Martin demonstrated the NuPAC platform continued to perform as intended following a radiation exposure of at least 1 krad consistent with Sections 4.3.6.1 and 4.3.6.2 of EPRI TR-107330 and consistent with the guidance in RG 1.209.

3.5.4.3 Electromagnetic Interference / Radio Frequency Interference

The NRC staff concludes that Lockheed Martin's qualification of the NuPAC platform for EMI/RFI and ESD is in accordance with 10 CFR Part 50, GDC 2 and 4, RG 1.180, IEC 61000, MIL-STD-461E, EPRI TR-107330, and EPRI TR-102323 Revision 1, for the tests it conducted in an EUT configuration without power supplies. Lockheed Martin performed radiated emissions, conducted susceptibility on interconnecting signal leads, radiated susceptibility, and ESD testing. It did not perform conducted emissions, conducted susceptibility on power leads, and SWC testing because it did not qualify power supplies. Lockheed Martin conducted operability and prudency testing and performed static mode data analysis to demonstrate the performance of the NuPAC platform before, during, and after exposure. Post EMI/RFI and ESD operability and prudency testing confirmed the NuPAC platform performed as intended following exposure.

3.5.4.4 Seismic

The NRC staff concludes that Lockheed Martin's seismic qualification of the NuPAC platform is in accordance with 10 CFR Part 50, GDC 2 and 4, RG 1.100, EPRI TR-107330, IEEE Std 323-2003, and IEEE Std 344-2004 for the qualification envelope it defined. The NuPAC

platform's TRS qualification envelope does not envelope the EPRI TR-107330 Figure 4-5 SSE RRS, but does envelope the OBE RRS. In addition, Lockheed Martin conducted operability and prudency testing and performed static mode data analysis to demonstrate the performance of the NuPAC platform before, during, and after seismic testing. Post-seismic operability and prudency testing confirmed the NuPAC platform performed as intended following exposure.

3.6 Defense-in-Depth and Diversity (D3)

Digital instrumentation and control (DI&C) systems can be vulnerable to common-cause failure (CCF) caused by software errors or software developed logic, which could defeat the redundancy achieved by hardware architecture; therefore, the NRC staff documented its position with respect to CCF in digital systems and diversity and defense-in-depth (D3). This position was documented as Item 18, II.Q, in SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," and was subsequently modified in the associated staff requirements memorandum (SRM).

There are two ways that D3 can be addressed: (1) internal diversity, and (2) alternative equipment. Generally (1), internal diversity, can be addressed by a platform by including diverse implementations within the platform family, but (2), alternative equipment, is generally addressed at the plant or application level by including diverse systems (e.g., Anticipated Transient Without Scram (ATWS) per 10 CFR 50.62). The NuPAC TR did not address this area; therefore it must be addressed as a plant-specific action item (see Plant-Specific Action Item No. 15).

3.7 Communications

Section 3.4 and Appendix D of the NuPAC TR, discusses the data communication aspects of the platform, and conformance to NRC staff guidance. The NuPAC platform supports intra-divisional and inter-divisional serial data communication. Data communication originates on a GLM and terminates at another GLM within the same division (intra-divisional) or in different division (inter-divisional). Intra-divisional serial data communication is supported through RS-422/485 I/O mezzanine on the GLM and LVDS backplane as described in Sections 3.4.2 and 3.4.4 of the NuPAC TR. Inter-divisional serial communication is supported through RS-422/485 I/O mezzanine on the GLM as described in Sections 3.4.3, 3.4.5, and 3.4.7 of the NuPAC TR.

3.7.1 Intra-division data communication

Intra-divisional data communication can be accomplished either through the RS-422 I/O mezzanine card on the GLM or through the LVDS backplane of the chassis.

For RS-422 intra-divisional communication, two GLMs located in different chassis but in the same division can talk to one another through the RS-422 circuit cards. For RS-422 data communication, isolation is provided by the I/O mezzanine transceiver devices; Figure 3.4.2.-1 of the NuPAC TR shows isolation through [ ].

For LVDS intra-divisional communication, GLMs can communicate to other GLMs in the same chassis through LVDS transmitters and receivers on the GLMs, and through the network of

[ ] communication pathways. Figure 3.4.4-4 of NuPAC TR shows the network configuration of available communication pathways. LVDS communication is designed for communication within a chassis, and not for communication outside the chassis. LVDS communication pathways are physically isolated from other chassis.

NuPAC uses RS-422 circuit cards and LVDS for intra-divisional communication, and such communication circuits are isolated from the intra-divisional communication circuits of other divisions. Since a failure of intra-divisional communication circuits in one division does not affect the intra-divisional communication circuits in other divisions, the NRC staff finds that the RS-422 and LVDS intra-divisional communication conforms the data communication independence of Clause 5.6 of IEEE Std 7-4.3.2-2003.

DI&C-ISG-04 Conformance

The GDCs, IEEE 279-1971, and IEEE 603-1991 require, among other things that redundant safety systems be independent of one another, and that protections systems be independent of control systems. Digital communication between independent systems could compromise their independence unless appropriated measure are taken to ensure their independence. DI&C-ISG-04, Rev. 1, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," established criteria to ensure independence in the presence of digital communication.

Appendix D, "DI&C ISG-04 Compliance Matrix," of the NuPAC TR, discusses conformance to select DI&C ISG-04 staff positions, and also stated which staff positions were not analyzed for the generic platform but will be addressed in a future plant-specific submittal. As a result, the NRC staff made safety determinations only for the analyzed DI&C ISG-04 staff positions, and future submittals referencing this SE should address unanalyzed staff positions through plant-specific action items which are listed in Section 4.1 of this SE.

Inter-divisional communication is supported through the RS-422 I/O mezzanine on the GLMs for point-to-point serial data communication. Staff did not review the RS-485 serial interface since NuPAC TR states, "RS-485 interface will be addressed in a future revision."

3.7.1.1 DI&C-ISG-04, Section 1 – Interdivisional Communications

Interdivisional communications includes transmission of data and information among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. It does not include communications within a single division. Interdivisional communications may be bidirectional or unidirectional.

Meeting the criteria for the interdivisional communications provides reasonable assurance that these types of communications do not adversely affect the operability of safety functions. The following subsections discusses the staff positions related to interdivisional communication.

3.7.2.1.1 Staff Position 1, Point 1

ISG Staff Position 1, Point 1, states:

> A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE [Std] 603. It is recognized that division voting logic must receive inputs from multiple safety divisions.

[

]

[

]

3.7.2.1.2 Staff Position 1, Point 2 Evaluation

ISG Staff Position 1, Point 2, states:

> The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

[

]

3.7.2.1.3 Staff Position 3

ISG Staff Position 1, Point 3, states:

> A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system.
>
> Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function, and with the receipt of information in support of those functions, does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of “significantly” used in the demonstration.

[

]

3.7.2.1.4 Staff Position 4

ISG Staff Position 1, Point 4, states:

> The communication process itself should be carried out by a communications processor[ii] separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information.
>
> [ii] "Processor" may be a CPU or other processing technology such as simple discrete logic, logic within an FPGA, an ASIC, etc.

[

]

ISG Staff Position 1, Point 4, continues:

> The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B.

[

]

ISG Staff Position 1, Point 4, continues:

> Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

[

]

3.7.2.1.5 Staff Position 5

ISG Staff Position 1, Point 5, states:

> The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.

[

]

3.7.2.1.6 Staff Position 6

ISG Staff Position 1, Point 6, states:

> The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

Appendix D of NuPAC TR states:

> …NuPAC-based safety systems interdivisional communications is designed with no requirements for handshaking or acknowledgement while performing a safety function. The NuPAC platform is a deterministic state-machine based design that is not preempted by interrupts.

[

]

3.7.2.1.7 Staff Position 1, Point 7

ISG Staff Position 1, Point 7, states:

> Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-defined design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

[

]

3.7.2.1.8 Staff Position 1, Point 8

ISG Staff Position 1, Point 8, states:

> 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.

[

]

3.7.2.1.9 Staff Position 1, Point 9

ISG Staff Position 1, Point 9, states:

> Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.

[

]

3.7.2.1.10 Staff Position 1, Point 10

ISG Staff Position 1, Point 10, states:

> Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment.

[

]

ISG Staff Position 1, Point 10, continues:

> A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at

a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. “Hardwired logic” as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) which one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a “TRUE” or “1” at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

[

]

3.7.1.1.11 Staff Position 1, Point 11

ISG Staff Position 1, Point 11, states:

> Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.

[

]

3.7.2.1.12 Staff Position 1, Point 12

ISG Staff Position 1, Point 12, states:

> Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute “single failures” as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:
> 1. Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
> 2. Messages may be repeated at an incorrect point in time.
> 3. Messages may be sent in the incorrect sequence.
> 4. Messages may be lost, which includes, both failures to receive an uncorrupted message or to acknowledge receipt of a message.
> 5. Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
> 6. Messages may be inserted into the communication medium from unexpected or unknown sources.
> 7. Messages may be sent to the wrong destination, which could treat the message as a valid message.
> 8. Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
> 9. Messages may contain data that is outside the expected range.
> 10. Messages may appear valid, but data may be placed in incorrect locations within the message.

11. Messages may occur at a high rate that degrades or causes the system to fail (i.e. broadcast storm).
12. Message headers or addresses may be corrupted.

[

]

3.7.2.1.13 Staff Position 1, Point 13

ISG Staff Position 1, Point 13, states:

> Vital[iii] communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely, or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

[

]

[

]

3.7.2.1.14 Staff Position 1, Point 14

ISG Staff Position 1, Point 14, states:

> Vital[iii] communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.

[

]

3.7.2.1.15 Staff Position 1, Point 15

ISG Staff Position 1, Point 15, states:

> Communication for safety functions should communicate a fixed set of data (called the “state”) at regular intervals, whether data in the set has changed or not.

[

]

3.7.2.1.16 Staff Position 1, Point 16

ISG Staff Position 1, Point 16, states:

> Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criterion (“GDC”) 24, which states in part, “interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.”; and (2) IEEE 603-1991 Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3).

[

]

3.7.2.1.17 Staff Position 1, Point 17

ISG Staff Position 1, Point 17, states:

> Pursuant to 10 C.F.R. § 50.49, the medium used in a vital[iii] communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

[

]

3.7.2.1.18 Staff Position 1, Point 18

ISG Staff Position 1, Point 18, states:

> Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

[

]

3.7.2.1.19 Staff Position 1, Point 19

ISG Staff Position 1, Point 19, states:

> If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

[

]

3.7.2.1.20 Staff Position 1, Point 20

ISG Staff Position 1, Point 20, states:

> The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

[

]

DI&C-ISG-04, Section 2 – Command Prioritization

The NuPAC TR did not address this area. As a result, the staff did not evaluate the NuPAC platform against ISG-04, Section 2, "Command Prioritization." Licensees referencing this SE are to address plant-specific action items in Section 4.1 of this SE.

3.7.1.2 DI&C-ISG-04, Section 3 – Multidivisional Control and Display Stations

The NuPAC TR did not address this area. As a result, the staff did not evaluate the NuPAC platform against ISG-04, Section 3, Multidivisional Control and Display Stations. Licensees referencing this SE are to address plant-specific action items in Section 4.1 of this SE.

3.8 System, Hardware, Software and Methodology Modifications

This section of the SE is to addresses changes from what was previously approved. Since there are no prior approvals, there is nothing to address in this section.

3.9 Review of System and IEEE Std 603-1991 Requirements

The scope of IEEE Std 603-1991 includes all I&C safety systems (i.e., those typically described in Sections 7.2 through 7.6 of the Updated Final Safety Analysis Report (UFSAR)). Except for the requirements for independence between control systems and safety systems, IEEE Std 603-1991 does not apply directly to non-safety systems such as the control systems and diverse I&C systems (i.e., those typically described in Sections 7.7 and 7.8 of the UFSAR). Although intended only for safety systems, the criteria for IEEE Std 603-1991 can be applicable to any I&C system. Therefore, for non-safety I&C systems that have a high degree of importance to safety, the concepts of IEEE Std 603-1991 can be used for the review of these systems. Applicable considerations include design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing. Digital data communication systems as described in SRP Section 7.9 are support systems for other I&C systems. As such, they inherit the applicable requirements and guidance that apply to the supported systems. Consequently, IEEE Std 603-1991 is directly applicable to those parts of data communication systems that support safety system functions.

3.9.1.1 IEEE Std 603-1991 Clause 4.1 Identification of the Design Basis Events

Clause 4.1 requires the identification of the design bases events applicable to each mode of operation. This information should be consistent with the analyses of UFSAR, Chapter 15, events. SRP BTP 7-4 provides specific guidance on the failures and malfunctions that should be considered in identification of design bases events for systems that initiate and control auxiliary feedwater systems. SRP BTP 7-5 provides specific guidance on the reactivity control malfunctions that should be considered in the identification of design basis events. The malfunctions postulated should be consistent with the control system failure modes described in the UFSAR (typically Sections 7.6 and 7.7).

[

]

3.9.1.2 IEEE Std 603-1991 Clause 4.2 Identification of Safety Functions and Protective Actions

Clause 4.2 requires documentation of the safety functions and corresponding protective actions of the execute features for each design basis event.

[

]

3.9.1.3 IEEE Std 603-1991 Clause 4.3 Permissive Conditions for Operating Bypasses

Clause 4.3 requires documentation of the permissive conditions for each operating bypass capability that is to be provided.

[

]

3.9.1.4 IEEE Std 603-1991 Clause 4.4 Identification of Variables Monitored

Clause 4.4 requires the identification of variables that are monitored in order to provide protective action. Clause 4.4 also requires the identification of the analytical limit associated with each variable. Review considerations in assessing that an adequate margin exists between analytical limits and setpoints are discussed in Clause 6.8.

[

]

3.9.1.5 IEEE Std 603-1991 Clause 4.5 Minimum Criteria for Manual Protective Actions

Clause 4.5 requires the documentation of the minimum criteria under which manual initiation and control of protective actions may be allowed, including the points in time and the plant conditions during which manual control is allowed, the justification for permitting initiation or control subsequent to initiation solely by manual means, the range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations are to be performed, and that the variables in Clause 4.4 be displayed for use in taking manual action. If these have not changed, this should be clearly identified in the information provided. SRP BTP 7-6 provides specific guidance on determining if the timing margins for changeover from injection to recirculation mode are sufficient to allow manual initiation of the transition. Additionally, SRP Section 18-A contains guidance for evaluating manual actions. The information documented under this clause is used in assessing conformance with Clause 6.2.2 as well.

[

]

3.9.1.6 IEEE Std 603-1991 Clause 4.6 Identification of the Minimum Number and Location of Sensors

Clause 4.6 requires the identification of the minimum number and location of sensors for those variables in Clause 4.4 that have spatial dependence (i.e., where the variable varies as a function of position in a particular region). The analysis should demonstrate that the number and location of sensors are adequate. If these have not changed, this should be clearly identified in the information provided. The specification of the minimum number and location of sensors is used in evaluating the acceptability of single failures addressed by Clause 5.1.

[

]

3.9.1.7 IEEE Std 603-1991 Clause 4.7 Range of Transient and Steady-State Conditions

Clause 4.7 requires, in part, that the range of transient and steady-state conditions be identified for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. The range of conditions specified is used in evaluating the integrity of the equipment; see Clause 5.5.

For a generic platform TR, plant-specific conditions do not apply. Rather, the generic equipment is designed and qualified to a predefined envelope (e.g., see TR Appendix A, "NuPAC Application Design Guide," Section 5.0, "Environment and Location") and each application includes and evaluation of the plant-specific criteria against the equipment qualification envelope.

See Section 3.5, "Environmental Equipment Qualification," of this SE for the evaluation of the equipment qualification.

3.9.1.8 IEEE Std 603-1991 Clause 4.8 Conditions Causing Functional Degradation

Clause 4.8 requires the identification of conditions having the potential for causing functional degradation of safety system performance, and for which provisions must be incorporated to retain necessary protective action. This information should feed into additional evaluations, including Clauses 5.5, 5.6.1, and 5.6.3.

Digital communications can cause functional degradation of one redundancy by another (see Clause 5.6.1) and of Safety Systems by other systems (see Clause 5.6.3). See Section 3.7, "Communications" for an evaluation of the digital communications mechanisms against the appropriate regulatory criteria.

[

]

3.9.1.9 IEEE Std 603-1991 Clause 4.9 Methods used to Determine Reliability

Clause 4.9 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that reliability goals imposed on the system design have been met.

The NRC staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the NRC's regulations for reliability of safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience can provide an added level of confidence, but alone is not sufficient.

For safety systems that include digital computers, both hardware and software reliability should be considered. Software errors that are not the consequence of hardware failures are caused by design errors and, therefore, do not follow the random failure behavior used for hardware reliability analysis. Consequently, different methodologies may be used to assess the unreliability introduced by hardware and software.

[

]

3.9.1.10 IEEE Std 603-1991 Clause 4.10 Control after Protective Actions

Performance criteria, including system response times, system accuracies, ranges, and rates of change, should also be identified in the system description. The analysis, including the applicable portion provided in Chapter 15 of the UFSAR, should conclude that the system performance criteria are adequate to ensure completion of protective actions.

Clause 4.10 requires that the minimum design basis documentation include the critical points in time or plant conditions, after the onset of a design basis event. The documentation of critical points in time for the initiation of protective actions is used to derive certain performance criteria (e.g., response time); the ability of the digital safety system to meet certain performance criteria is evaluated under Clause 5.4.

Clause 4.10.3 requires the documentation of information that will be used in Clause 6.1. The information documented under this clause should also be used in assessing conformance with Clause 6.2.3.

[

]

3.9.1.11 IEEE Std 603-1991 Clause 4.11 Equipment Protective Provisions

Clause 4.11 requires the documentation of the equipment protective provisions that prevent a safety system from accomplishing their safety function.

[

]

3.9.1.12 IEEE Std 603-1991 Clause 4.12 Special Design Bases

Clause 4.12 requires the documentation of any other special design basis.

[

]

3.9.2 IEEE Std 603-1991 Clause 5 System

Clause 5 of IEEE Std 603-1991 requires that the safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established by design basis events. This evaluation should confirm that the general functional criteria have been appropriately allocated to the various system components. The review in this regard should conclude that the system design fulfils the system design basis criteria established; this review should be from an integrated hardware/software perspective.

The licensee should ensure that the Requirements Traceability Matrix (RTM) is written such that each criteria and sub-criteria (whether hardware or software) is traceable throughout the design. The traceability should be possible both forwards and backwards, that is, the staff should be able to take any criterion, and trace it through from the system requirements specification to the design and associated validation tests or analysis. Tracing backwards, it should be possible to confirm what requirement is responsible for any aspect of the system. One of the things this should be used for is to assess whether there is unnecessary code in the product. Any application code which is not traceable back to a system or plant criteria is unnecessary and should be removed.

[

]

3.9.2.1 IEEE Std 603-1991 Clause 5.1 Single-Failure Criterion

Clause 5.1 requires that any single failure within the safety system shall not prevent proper protective action at the system level when needed. The analysis[1] should confirm that the single-failure criterion is satisfied. Guidance in the application of the single-failure criterion is provided in RG 1.53 Rev. 2, " Application of the Single-Failure Criterion to Safety Systems," which endorses IEEE Std 379-2000, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

[1] The analysis is sometimes documented in a Failure Modes and Effects Analysis (FMEA) report; see Section 3.9.2.1.1.

Components and systems not qualified for seismic events or accident environments and non-safety-grade components and systems are postulated to fail to function if failure adversely affects safety system performance. Conversely, these components and systems are postulated to inadvertently function in the worst manner if functioning adversely affects safety system performance. All failures in the safety system that can be predicted as a result of an event for which the safety system is designed to provide a protective function are postulated to occur if the failure adversely affects the safety system performance. In general, the lack of equipment qualification or a less than high quality development process may serve as a basis for the assumption of certain failures. After postulating the failures of non-safety-grade, non-qualified equipment and those failures caused by a specific event, a random single failure within the safety-related system is postulated. With these failures postulated, the safety system must be capable of performing the protective functions that are necessary to mitigate the consequences of the specific event. The information to reach a determination of adequate compliance with the single failure criterions with respect to equipment qualification should be contained in the system and hardware specifications, architecture, and descriptions, and in the Equipment Qualification Testing Plans, methods, FMEA, and test results.

Digital computer-based I&C systems share data, data transmission, functions, and process equipment to a greater degree than analog systems. Although this sharing forms the basis for many of the advantages of digital systems, it also raises a key concern with respect to I&C system vulnerability to a different type of failure. The concern is that a design using shared databases and process equipment has the potential to propagate a common-cause failure of redundant equipment. DI&C-ISG-04, Section 1, “Interdivisional Communications,” Staff Position 3, states that “A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system.” In order to comply with this staff position, the licensee or vendor should demonstrate what support or enhancement to the safety function is provided by the communications and that any communications failure should not allow a single failure within one channel to defeat the single failure concept. This demonstration is further discussed in Section 3.7, “Communications.” Per Section 3.7, the information to reach a determination of adequate data isolation should be contained in the system, hardware and software specifications, architecture, and descriptions. Depending on the complexity of the proposed communications, the NRC staff may also have to examine the actual circuitry as described in the circuit schematics and in the software code listings, and in detailed system and hardware drawings.

Another concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against common-cause failures within and between functions. The principle of defense-in-depth is to provide several levels or echelons of defense to challenges to plant safety, such that failures in equipment and human errors should not result in an undue risk to public safety. This is addressed further in Section 3.6; [

].

3.9.2.1.1 FMEA

The FMEA is a method of analysis of potential failure modes of modules within a system for determination of the effects on the system behavior. This information can then be used to assess the potential for an undetectable failure. The overall staff expectation is that each potential failure mode should be identified, and the effects should be determined. For a complex system, this is expected to be a complex analysis.

EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants," dated December 1996 was endorsed by the NRC by letter dated July 30, 1998 (ADAMS Accession No. ML12205A265). Guidance on FMEAs is contained in Section 1.4.3, "Generic vs. Application Specific Overview," Section 4.2.3.1, "Availability/Reliability Overview," Section 4.2.3.5, "Failure State/FMEA Requirements," and Section 6.4.1, "FMEA."

A generic platform FMEA is an input to an application specific FMEA. Each plant-specific application must be assessed to conclude that the application specific FMEA is sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures. For example, an FMEA is a method for documenting a single failure analysis which is conducted in accordance with IEEE Std 379-2000, as endorsed by RG 1.53 Rev. 2.

The review with respect to the failure of software is addressed in:

Section 3.4.1.9, "Software Safety Plan",
Section 3.4.1, "Safety Analysis", and
Section 3.6, "Defense-in-Depth & Diversity".

[

]

3.9.2.2 IEEE Std 603-1991 Clause 5.2 Completion of Protective Action

Clause 5.2 requires that the safety systems be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features continue until

completion, and that deliberate action is necessary to return the safety systems to normal. Appendix 7.1-C, Section 5.2, of the SRP provides acceptance criteria for this requirement.

In addition to a description of how “seal-in” features ensure that system-level protective actions go to completion, the information provided may include functional and logic diagrams to demonstrate this feature. The information should clearly demonstrate that deliberate action is needed to return the safety systems to normal operation. The information needed by the NRC staff to reach a determination that the “seal-in” features of the system are sufficient, should be contained in the system hardware and software specifications and associated descriptions. Depending on the complexity of the proposed seal-in features, the NRC staff may also have to examine (audit) the actual circuitry as described in the circuit schematics and in the software code listings.

[

]

3.9.2.3 IEEE Std 603-1991 Clause 5.3 Quality

Clause 5.3 requires that components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

The information provided should confirm that the quality assurance provisions of Appendix B to 10 CFR, Part 50, are applicable to the safety system. RG 1.28 provides an acceptable way to comply with the Appendix B regulation. The adequacy of the quality assurance program is addressed further in the evaluation against Clause 5.3 of IEEE Std 7-4.3.2-2003. It may be beneficial for a licensee to conduct a 10 CFR Part 50, Appendix B audit of the vendor to assess the adequacy of their quality assurance program. The information needed by the NRC staff to reach a determination that the vendor is planning to provide adequate quality should be contained in the quality assurance plans. The implementation of these plans may be audited by the NRC staff.

The NRC staff from both the quality and vendor branch and I&C branch conducted an audit to assess the Appendix B program (ADAMS Accession No. ML16069A237). In addition the quality assurance program is described in the following docketed material:

Section 1.4, “Quality System,” of the NuPAC TR,
Section 4.0, “Technical and Support Processes,” of the NuPAC TR, and
“NuPAC Quality Assurance Plan,” (Refs. 37.a. & 41.a.).

[

]

3.9.2.4 IEEE Std 603-1991 Clause 5.4 Equipment Qualification

Clause 5.4 states that safety system equipment shall be qualified[2] by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it should be capable of meeting the performance criteria as specified in the design basis (e.g., IEEE Std 603-1991 Clause 4.10), while being exposed to specified environmental conditions (e.g., IEEE Std 603-1991 Clause 4.7). Appendix 7.1-C, Section 5.4, of the SRP provides acceptance criteria for Clause 5.4. The information provided should confirm that the safety system equipment is designed to meet the performance criteria over the range of normal, abnormal, and accident conditions.

Section 3.5, “Environmental Equipment Qualification,” of this SE documents the evaluation against this criteria.

3.9.2.4.1 Response Time

The response time of a safety system is one of the performance criteria that must be addressed as described above. Response time criteria are established on an application specific basis (i.e., not applicable to a generic platform TR). The application specific response time is determined by analysis based on component specific response times and the application specific architecture. Subsequently response time is confirmed through testing.

[

]

3.9.2.4.2 Deterministic Behavior

SRP Chapter 7, BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” provides guidance for reviewing the deterministic behavior of a digital Safety System (DSS). This guidance was developed for microprocessor based systems.

[

]

[2] The information needed by the NRC staff to reach a determination of adequate environmental equipment qualification is discussed in Section D.5.

3.9.2.5 IEEE Std 603-1991 Clause 5.5 System Integrity

Clause 5.5 requires that the safety systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis.

See Section 3.5, “Environmental Equipment Qualification,” of this SE for the evaluation of the equipment qualification.

3.9.2.6 IEEE Std 603-1991 Clause 5.6 Independence

Clause 5.6 requires independence between: (1) redundant portions of a safety system, (2) safety systems and the effects of design bases events, and (3) safety systems and other systems.

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 is attained by physical separation and physical barriers. Electrical independence should include the utilization 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 that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety function of the redundant portions. Further, if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system.

[

] (See Plant-Specific Action Item No. 16).

See Section 3.7 for an evaluation of communication independence.

3.9.2.7 Clause 5.7 Capability for Test and Calibration

Clause 5.7 requires the capability for testing and calibration of the safety system equipment be provided while retaining the capability of the safety systems to accomplish their safety functions. It is expected that safety systems should be periodically tested and calibrated.

Guidance on periodic testing of the safety system is provided in RG 1.22, “Periodic Testing of Protection System Actuation Functions,” and in RG 1.118, Revision 3, “Periodic Testing of Electric Power and Protection Systems,” which endorses IEEE Std 338-1987, “Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems.”

The extent of test and calibration capability provided bears heavily on whether the design meets the single-failure criterion. Any failure that is not detectable must be considered concurrently with any random postulated, detectable single failure. Periodic testing should duplicate, as closely as practical, the overall performance of the safety system. The test should confirm operability of both the automatic and manual circuitry. The capability should be provided to permit testing during power operation. When this capability can only be achieved by overlapping tests, the reviewer should conclude that the test scheme overlaps leave no gaps.

The tests should address the increased potential for subtle system failures such as data errors and computer lockup. The system design should also support the compensatory actions documented in the nuclear plant technical specifications when limiting conditions for operation are not met. Typically, this should allow for tripping or bypass of individual functions in each safety system channel. SRP BTP 7-17 describes additional considerations regarding these topics.

In addition, if self-contained diagnostics within the digital system are being used as a reason for elimination of existing surveillances, or less frequent performance of existing surveillances, the information provided should show exactly what components and safety functions were previously tested, and how the new diagnostic functions will test these components to the same degree.

[

]

[

]

3.9.2.8 IEEE Std 603-1991 Clause 5.8 Information Displays

Clause 5.8 has four sub-clauses.

Clause 5.8.1 requires that display instrumentation provided for manually controlled actions for which no automatic control is provided and that are necessary for the safety systems to

accomplish their safety functions will be part of the safety systems. The design should minimize the possibility of ambiguous indications.

Clause 5.8.2 requires that display instrumentation provide accurate, complete, and timely information pertinent to safety system status, and that this information shall include indication and identification of protective actions of the sense and command features and execute features. Further, the design should minimize the possibility of ambiguous indications. The review of information displays for manually controlled actions should include assessment whether the displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary.

Clause 5.8.3 requires that protective actions that have been bypassed or deliberately rendered inoperative for any other purpose be continuously indicated in the control room; this display instrumentation does not need to be considered a part of the safety system. The indication must be automatically actuated if the bypass or otherwise inoperative condition is expected to occur more frequently than once per year and is expected to occur when the affected system is specified to be operable. Safety system bypass and inoperable status indication should conform with the guidance of RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems.”

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

[

]

3.9.2.9 IEEE Std 603-1991 Clause 5.9 Control of Access

Clause 5.9 requires that the safety system be designed to permit administrative control of access to the equipment. Administrative access limited to qualified plant personnel is acceptable if done with the permission of the control room operator. The system should be designed with alarms and locks to preclude inappropriate access. Additionally, electronic access to the system (e.g., via a network connection) should be sufficiently restricted. The information provided should sufficiently describe the hardware and software such that the NRC staff is able to conclude that Clause 5.9 has been met. The SDOE review area discusses this aspect in further detail. The information needed by the NRC staff to reach a determination that the system is designed such that administrative controls of access to the equipment is adequate should be contained in the system, hardware and software specifications, architecture, and descriptions.

[

]

3.9.2.10 IEEE Std 603-1991 Clause 5.10 Repair

Clause 5.10 requires that the safety system be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. It important to note that the acceptance criteria states that while digital safety systems may include self-diagnostic capabilities to aid in troubleshooting, the use of self-diagnostics does not replace the need for the capability for test and calibration systems as required by Clauses 5.7 and 6.5.

[

]

3.9.2.11 IEEE Std 603-1991 Clause 5.11 Identification

Clause 5.11 requires that the safety system equipment and documentation be distinctly identified for each redundant portion of a safety system. RG 1.75 Rev. 3, “Criteria for Independence of Electrical Safety Systems,” endorses IEEE Std 384-1992, “IEEE Standard for Independence of Class 1E Equipment and Circuits,” subject to the exceptions listed. IEEE Std 384 contains guidance regarding identification (e.g., Clause 6.1.2, “Identification”). Further, the safety system equipment must be distinguishable from any identifying markings placed on the equipment for other purposes, that the identification methods not necessitate the frequent use of reference materials (i.e., be “user friendly”), and that the associated documentation be distinctly identified. However, components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not, themselves, need identification.

[

]

3.9.2.12 IEEE Std 603-1991 Clause 5.12 Auxiliary Features

Clause 5.12 requires that auxiliary supporting features meet all requirements of IEEE Std 603-1991.

[

]

3.9.2.13 IEEE Std 603-1991 Clause 5.13 Multi-Unit Stations

This regulatory criteria is not applicable to a platform TR.

3.9.2.14 Clause 5.14 Human Factors Considerations

Clause 5.14 requires that human factors be considered at the initial stages and throughout the development process to assure that the functions allocated in whole or in part to the users and maintainers can be successfully accomplished to meet the safety system design goals.

[

]

3.9.2.15 IEEE Std 603-1991 Clause 5.15 Reliability

Clause 5.15 requires that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved.[3] The information provided should justify that 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. For computer systems, both hardware and software should be included in this analysis. The NRC staff considers software that complies with the quality criteria of Clause 5.3, and that is used in safety systems that provide measures for defense against common-cause failures also complies with the fundamental reliability requirements of GDC 21.

[

]

[

]

[3] A reliability analysis provides sufficient detail to support and justify that the system meets the reliability requirements.

3.9.3 IEEE Std 603-1991 Clauses 6. Sense and Command Features

Clause 6 of IEEE Std 603-1991 provides the requirements for sensors and command features, but does not contain any unique criteria, so no evaluation against this clause is required.

3.9.3.1 IEEE Std 603-1991 Clause 6.1 Automatic Control

This regulatory criteria is not applicable to a platform TR. Evaluation of this criteria should be performed for each plant specific application.

3.9.3.2 IEEE Std 603-1991 Clause 6.2 Manual Control

This regulatory criteria is not applicable to a platform TR. Evaluation of this criteria should be performed for each plant specific application.

3.9.3.3 IEEE Std 603-1991 Clause 6.3 Interaction with Other Systems

This regulatory criteria is not applicable to a platform TR. Evaluation of this criteria should be performed for each plant specific application.

3.9.3.4 IEEE Std 603-1991 Clause 6.4 Derivation of System Inputs

This regulatory criteria is not applicable to a platform TR. Evaluation of this criteria should be performed for each plant specific application.

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

Clause 6.5 requires that it must be possible to check, with a high degree of confidence, the operational availability of each sense and command feature input sensors needed for a safety function during reactor operation, including the availability of each sense and command feature needed during the post-accident period. SRP Chapter 7, Appendix 7.1-C, Section 6.5, “Capability for Testing and Calibration,” provides acceptance criteria for Clause 6.5.

The testing addressed under this clause is addressed at the time of applications development. Certain self-testing is addressed under the clause for “Repair” above in Section 3.9.2.10. [

]

3.9.3.6 IEEE Std 603-1991 Clause 6.6 Operating Bypasses

This regulatory criteria is not applicable to a platform TR. Evaluation of this criteria should be performed for each plant specific application.

3.9.3.7 IEEE Std 603-1991 Clause 6.7 Maintenance Bypass

This regulatory criteria is not applicable to a platform TR. Evaluation of this criteria should be performed for each plant specific application.

3.9.3.8 IEEE Std 603-1991 Clause 6.8 Setpoints

Clause 6.8 requires that the allowance for uncertainties between the process analytical limit documented in Clause 4.4 and the device setpoint must be determined using a documented methodology. Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design must provide a positive means of ensuring that the most restrictive setpoint is used. The setpoint analysis should confirm that an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system. Furthermore, the analysis should confirm that an adequate margin exists between setpoints and safety limits.

Guidance on the establishment of instrument setpoints can be found in RG 1.105 and Regulatory Information Summary (RIS) 2006-0017, “NRC Staff Position on the Requirements of 10 CFR 50.36, "Technical Specifications," Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels” (ADAMS accession number ML051810077). Where it is necessary to provide multiple setpoints as discussed in Clause 6.8.2, the NRC staff interpretation of “positive means” is that automatic action is provided to ensure that the most restrictive setpoint is used. SRP BTP 7-3 provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

[

] (see Plant-Specific Action Items No. 17).

3.9.4 IEEE Std 603-1991 Clause 7 Execute Features

The NuPAC TR did not address this area. Evaluation of this criteria should be performed for each plant specific application.

3.9.5 IEEE Std 603-1991 Clause 8 Power Source

The NuPAC TR did not address this area. Evaluation of this criteria should be performed for each plant specific application.

3.10 Review of IEEE Std 7-4.3.2-2003 Guidance

The scope of IEEE Std 7-4.3.2-2003 includes all I&C safety systems that are computer-based. IEEE Std 603-1991 does not directly discuss digital systems, but states that guidance on the application of its criteria for safety systems using digital programmable computers is provided in IEEE/ANS Std 7-4.3.2-1982. IEEE/ANS Std 7-4.3.2-1982 was subsequently revised into IEEE Std 7-4.3.2-2003 and endorsed by RG 1.152, Revision 3. IEEE Std 7-4.3.2-2003 serves to amplify the criteria in IEEE Std 603-1991. Within the context of IEEE Std 7-4.3.2-2003, the term computer is a system that includes FPGAs.

3.10.1 IEEE Std 7-4.3.2-2003 Clause 5 System

Clause 5 contains no additional criteria beyond those in IEEE Std 603-1991; however, some of the sub-clauses contain additional criteria. The sub-clauses that contain criteria are addressed below.

3.10.1.1 IEEE Std 7-4.3.2-2003 Clause 5.3 Quality

Clause 5.3 states that hardware quality is addressed by IEEE Std 603-1991, and contains two normative criteria:

> Computer development activities **shall** include the development of computer hardware and software. The integration of the computer hardware and software and the integration of the computer with the safety system **shall** be addressed in the development process.

Clause 5.3 also describes the typical digital system development life cycle. The licensee should describe the development life cycle actually used for the development of the system being proposed, and compare this to the typical life cycle. Any difference in the life cycle should be explained and justified. Clause 5.3 contains 6 sub-parts that are discussed in further detail below.

The evaluation of the hardware specific development process (i.e., conformance with Appendix B) is documented in Section 3.9.2.3, “Clause 5.3 Quality,” above. The evaluation of the software development process is documented in Section 3.4, “Software Development Process,” above. During the evaluation of the software development process, the staff considered the two normative criteria quoted above, and determined that the software development process included both the hardware and software, as appropriate and is therefore acceptable.

3.10.1.1.1 IEEE Std 7-4.3.2-2003 Clause 5.3.1 Software Development

The normative criteria in Clause 5.3.1 include:

> Computer software **shall** be developed, modified, or accepted in accordance with an approved software quality assurance (QA) plan. The software QA plan **shall** address all software that is resident on the computer at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics).

[

]

3.10.1.1.2 IEEE Std 7-4.3.2-2003 Clause 5.3.2 Software Tools

Clause 5.3.2 specifies that software tools used to support software development processes and V&V processes be controlled under the configuration management plan. The tools are further specified to be either developed to a similar standard as the safety-related software or the tools be used in a manner such that defects not detected by the tools should be detected by V&V activities. Furthermore, SRP Chapter 7 Appendix 7.1-D, Section 5.3.2, "Software Tools," contains additional criteria for software tools.

[

]

3.10.1.1.3 IEEE Std 7-4.3.2-2003 Clause 5.3.3 Verification and Validation

See Sections 3.4.1.10, "Software V&V Plan (SVVP)," and Section 3.4.2, "V&V Analysis and Reports," above.

3.10.1.1.4 IEEE Std 7-4.3.2-2003 Clause 5.3.4 Independent V&V (IV&V)

See Sections 3.4.1.10, “Software V&V Plan (SVVP),” and Section 3.4.2, “V&V Analysis and Reports,” above.

3.10.1.1.5 IEEE Std 7-4.3.2-2003 Clause 5.3.5 Software Configuration Management

See Sections 3.4.1.11, “Software Configuration Management Plan (SCMP),” and Section 3.4.2.3, “Configuration Management Activities,” above.

3.10.1.1.6 IEEE Std 7-4.3.2-2003 Clause 5.3.6 Software Project Risk Management

Software project risk management is a tool for problem prevention, which includes: identifying potential problems, assessing their impact, and determining which potential problems should be addressed to assure that software quality goals are achieved. Clause 5.3.6 defines the risk management activities for a software project. Furthermore, SRP Chapter 7 Appendix 7.1-D, Section 5.3.6, “Software Project Risk Management,” contains additional criteria.

[

]

3.10.1.2 IEEE Std 7-4.3.2-2003 Clause 5.4 Equipment Qualification

See Section 3.5, “Environmental Equipment Qualification,” above.

3.10.1.2.1 IEEE Std 7-4.3.2-2003 Clause 5.4.1 Computer System Testing

Clause 5.4.1 specifies that the system qualification testing be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Licensees should ensure that the test plans include these criteria, and that the test reports show what software was running during the tests.

Section 3.5.3.1, “Test System,” above, documents the evaluation of the NuPAC platform testing against IEEE Std 7-4.3.2-2003, Clause 5.4.1. The test report documentation includes references to the software and hardware versions tested.

Computer system qualification testing was performed with the computer functioning with actual platform software and diagnostics and applications software that is representative of those that will be used in an actual application. All portions of the computer necessary to accomplish safety functions, were exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the FPGA, inputs and outputs, LED display functions / diagnostics, associated components, communication paths, and interfaces. Testing demonstrated that the performance requirements related to safety functions have been met. Therefore the computer system testing met the criteria identified above and acceptable.

3.10.1.2.2 IEEE Std 7-4.3.2-2003 Clause 5.4.2 Qualification of Existing Commercial Computers

The NuPAC platform uses some commercial components that are assembled into modules, but does not have any commercial computers; therefore, the DI&C specific criteria identified in Chapter 7 of NUREG-0800 (the Standard Review Plan, SRP) are not applicable.

[

]

3.10.1.2.3 Deterministic System Behavior

Deterministic behavior requires that all cause and effect relationships be predictable for both the outcome and the time delay before the outcome is realized. True deterministic behavior would require that the outcome be invariant and that the time delay to achieve the outcome be exact. To satisfy the definition of deterministic behavior for digital control systems, such as NuPAC, it is sufficient that a worst case upper and lower bound is established for the time component of each outcome.

Although the regulatory requirements do not use the term “deterministic behavior,” this term summarizes various regulatory requirements such as IEEE Std 603-1991, Clause 5, which states, “The safety systems shall with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event.” SRP Chapter 7, BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” provides guidance for reviewing the deterministic behavior of a DSS. This guidance is specific to microprocessor based systems; therefore, it is not directly applicable.

[

]

3.10.1.2.4 Performance – Response Time

Regulatory requirements exist for application specific response times, but not for component specific response times; however, predictable component response time are necessary for determining system response times.

[

]

3.10.1.3 IEEE Std 7-4.3.2-2003 Clause 5.5 System Integrity

Clause 5.5 contains no additional criteria beyond those in IEEE Std 603-1991; however, some of the sub-clauses contain additional criteria. The sub-clauses that contain criteria are addressed below.

3.10.1.3.1 IEEE Std 7-4.3.2-2003 Clause 5.5.1 Design for Computer Integrity

Clause 5.5.1 specifies that the computer be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function.

[

]

3.10.1.3.2 IEEE Std 7-4.3.2-2003 Clause 5.5.2 Design for Test and Calibration

Clause 5.5.2 specifies that test and calibration functions not adversely affect the ability of the system to perform its safety function, and that it be verified that the test and calibration functions do not affect system functions that are not included in a calibration change. The clause further states that V&V, configuration management, and QA are necessary for test and calibration functions on separate systems such as test and calibration computers that provide the sole verification of test and calibration data. V&V, configuration management, and QA is not specified when the test and calibration function is resident on a separate system and does not provide the sole verification of test and calibration for the safety system.

[

]

3.10.1.3.3 IEEE Std 7-4.3.2-2003 Clause 5.5.3 Fault Detection and self-diagnostics

Clause 5.5.3 specifies that if reliability criteria warrant self-diagnostics, then the software should contain functions to detect and report computer system faults and failures in a timely manner, and that these self-diagnostic functions not adversely affect the ability of the system to perform its safety function nor cause spurious actuations of the safety function.

[

]

3.10.1.4 IEEE Std 7-4.3.2-2003 Clause 5.6 Independence

Clause 5.6 specifies that in addition to the requirements of IEEE Std 603-1991, data communication between safety channels or between safety and non-safety systems not inhibit the performance of the safety function.

Communication independence is addressed in Section 3.7, “Communications,” above.

3.10.1.5 IEEE Std 7-4.3.2-2003 Clause 5.7 Capability for Test and Calibration

There are no criteria beyond those in IEEE Std 603-1991. See Section 3.10.1.3.3, “Clause 5.5.3 Fault Detection and self-diagnostics,” and Section 3.10.1.3.2, “Clause 5.5.2 Design for Test and Calibration,” for related evaluations.

3.10.1.6 IEEE Std 7-4.3.2-2003 Clause 5.8 Information Displays

This regulatory criteria is not applicable to a platform TR. Evaluation of this criteria should be performed for each plant specific application.

3.10.1.7 IEEE Std 7-4.3.2-2003 Clause 5.11 Identification

Clause 5.11 specifies that firmware and software identification be used to assure the correct software is installed in the correct hardware component. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools and that physical identification of hardware is implemented in accordance with IEEE Std 603-1991. The identification should be clear and unambiguous, include revision level, and should be traceable to configuration control documentation. Licensees should ensure that the configuration management plans are sufficient to meet this clause, and when discussing compliance with the clause, point to the sections of the configuration management plans where this is discussed.

[

]

3.10.1.8 IEEE Std 7-4.3.2-2003 Clause 5.15 Reliability

Clause 5.15 specifies that, in addition to the requirements of IEEE Std 603-1991, when reliability goals are identified, the proof of meeting the goals should include the software. As stated in RG 1.152, the NRC does not endorse the concept of quantitative reliability goals as the sole means of meeting the NRC's regulations for reliability in digital computers for safety related applications. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the system.

[

]

3.11 Technical Specification changes

The NuPAC TR did not address this area.

3.12 Secure Development and Operational Environment

3.12.1 Applicable Regulations and Guidance

GDC 21, "Protection system reliability and testability", requires in part that "The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed."

10 CFR 50.55a(h) requires that protection systems for nuclear power plants meet the requirements of IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. With respect to the use of computers in safety systems, IEEE Std 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std 603-1991. In addition, RG 1.152 Rev. 3 contains regulatory positions (e.g., No. 2, "Secure Development and Operational

Environment for the Protection of Digital Safety Systems") to supplement the criteria in IEEE Std 7-4.3.2-2003.

IEEE Std 603-1991 Clause 4.8 requires that the design basis shall document as a minimum: "The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems)." Furthermore, IEEE Std 603-1991 Clause 5.5, "System Integrity," states, "The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis."

IEEE Std 603-1991 in Clause 5.6.3.1(2) under Interconnected Equipment states, "No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system."

IEEE Std 603-1991 in Clause 5.9 under Control of Access states, "The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof."

3.12.2 SDOE Evaluation

[

]

4.0 LIMITATIONS AND CONDITIONS

As discussed in Section 2.0, the staff did not directly evaluate the platform against the regulations and guidance at the system level. The staff only evaluated the capabilities and characteristics of the NuPAC 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 review of a full system design. If a plant-specific application is subject to regulatory requirements not specifically approved in this SE, they must be addressed in addition to the plant-specific action items listed below.

4.1 Plant-Specific Action Items

The following plant-specific actions are to be performed for a safety-related system based on the NuPAC platform.

1. As discussed in Section 3.4.1.5, the Software Installation Plan (SInstP) is a plant-specific plan and therefore not applicable to the generic NuPAC TR. An SInstP should be developed for each application.
2. As discussed in Section 3.4.1.6, the Software Maintenance Plan (SMaintP) is a plant-specific plan and therefore not applicable to the generic NuPAC TR. An SMaintP should be developed for each application.
3. As discussed in Section 3.4.1.7, the Software Training (STrngP) is a plant-specific plan and therefore not applicable to the generic NuPAC TR. A STrngP should be developed for each application.
4. As discussed in Section 3.4.1.8, the Software Operations Plan (SOP) is a plant-specific plan and therefore not applicable to the generic NuPAC TR. An SOP should be developed for each application.
5. As discussed in Section 3.4.3.5, the System Build Documents (SBDs) are application specific and therefore not applicable to the generic NuPAC TR. SBDs should be developed for each application.
6. As discussed in Section 3.5.3.1, address the following five elements in their qualification which were not part of the NuPAC qualification: (1) Power supplies. Licensees should address power quality related to power sources external to the NuPAC platform. (2) Application-specific (plant-specific) PL (3) Class 1E/non-Class 1E isolation. (4) Data communications outside of NuPAC (safety and non-safety). (5) Safety-related display.
7. (a) As discussed in Section 3.5.3.3, verify that the NuPAC platform is located in a mild environment and that their location of the NuPAC platform would preclude it from being subjected to dynamic effects such as missiles, discharging fluids, or pipe whipping resulting from other equipment failures or natural phenomena in accordance with GDC 4. (b) As discussed in Section 3.5.3.3, verify that temperature and relative humidity conditions, including abnormal and accident conditions where the NuPAC platform is installed would not exceed the qualification envelope. This verification includes heat management calculations in accordance with Section 5.3 of the Application Design Guide in Appendix A to the TR (Ref. 49.a.) and verification the initial heat up rate of [ ] degrees Fahrenheit per hour is not exceeded.
8. As discussed in Section 3.5.3.3, demonstrate the following constraints have been addressed: [

]

9. As discussed in Section 3.5.3.4, verify the NuPAC platform is located in a mild environment meeting the radiation environmental conditions for a lifetime gamma dose of not more than 1 krad consistent with Section 6.2.4 of the TR (Ref. 33.) and Section 5.5 of the Application Design Guide in Appendix A to the TR (Ref. 49.a.).
10. As discussed in Section 3.5.3.5.2, verify the location for the NuPAC platform and the administrative controls for establishing exclusion zones meet the criteria in RG 1.180, Regulatory Position 1 such that emissions in the vicinity of the NuPAC platform are within the tested susceptibility operating envelopes. RG 1.180 states that steps should be taken to ensure that systems are not exposed to EMI/RFI levels from identified sources that are greater than 8 dB below the specified operating envelopes.
11. (a) As discussed in Section 3.5.3.6, ensure the plant-specific In-Equipment Response Spectra (IERS) are enveloped by the NuPAC platform Test Response Spectra (TRS) qualification envelope. (b) As discussed in Section 3.5.3.6, demonstrate the following constraint has been addressed; [

]
12. As discussed in Section 3.7.2.1, implementation of interdivisional communication should produce the application specification(s) that govern the interface and demonstrate conformance of its application to DI&C-ISG-04, Section 1, “Interdivisional Communications,” staff positions 1, 2, 3, 4, 5, 7, 9, 10, 12, 13, 17, 18, 19, and 20.
13. As discussed in Section 3.7.2.2, implementation of command prioritization with NuPAC 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, Section 2, “Command Prioritization,” staff positions.
14. As discussed in Section 3.7.2.3, implementation of 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, Section 3, “Multidivisional Control and Display Stations,” staff positions.
15. As discussed in Section 3.6, implementation of an application should include a plant specific D3 analysis.
16. As discussed in Section 3.9.2.6, implementation of an application should include a plant specific electrical independence analysis.
17. As discussed in Section 3.9.3.8, implementation of an application should include a plant specific evaluation of the setpoint calculations against the criteria in RG 1.105.

4.2 Generic Open Items

The following generic open items are to be resolved.

1. Lockheed Martin should demonstrate the following trouble reports have been resolved:

   a. [

   ]

   b. [

   ]

   c. [

   ]

   d. [

   ]

   e. [

   ]

   f. [

   ]

   g. [

]

h. [

]

2. Atmospheric items: Lockheed Martin should address the following related to atmospheric qualification:

   a. [

]

3. All Power Supplies: Once Lockheed Martin identifies power supplies for the NuPAC platform, it should qualify the NuPAC platform in an EUT configuration that includes power supplies for atmospheric, radiation, EMI/RFI, and seismic withstand capability.

4. EMI/RFI, ESD items: Lockheed Martin should address the following related to EMI/RFI and ESD Qualification:

   a. [

]

   b. [

]

   c. [

]

d. [

]

e. [

]

f. [

]

g. [

]

h. [

]

i. Radiated Susceptibility: Lockheed Martin should address the following Open Items associated with radiated susceptibility:

1. [

]

2. [

]

5. [

]

5.0 CONCLUSION

The NRC staff determined the NuPAC 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 NuPAC 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 NuPAC platform is acceptable for use in safety-related I&C systems.

6.0 REFERENCES

1. Lockheed Martin letter to NRC Document Control Desk, June 28, 2011 (ADAMS Accession No. ML11201A323),docketing:
   a. NuPAC_ED610000-47-P, Revision -, "Generic Qualification of the NuPAC Platform for Safety-related Applications (Proprietary)"
      Note: Superseded by Ref. 49.a.
2. Lockheed Martin letter to NRC Document Control Desk, June 28, 2011 (ADAMS Accession No. ML11201A322) docketing:
   a. NuPAC_PLPMP610000-001, Rev. - , "NuPAC Programmable Logic Project Management Plan"
   b. NuPAC_PLDP610000-001, Rev. -, "NuPAC Programmable Logic Development Plan"
   c. NuPAC_QAP6 10000-001, Rev. A, "NuPAC Quality Assurance Plan"
   d. NuPAC_PLDP610000-004, Rev. -, "NuPAC Programmable Logic Integration Plan - Core PLCI"
   e. NuPAC_SSPP610000-001, Rev. A, "NuPAC System Safety Plan"
   f. NuPAC_FVVP610000-001, Rev. A, "NuPAC FPL Verification and Validation Plan"
   g. NuPAC_PLCMP610000-001, Rev. - , "NuPAC Programmable Logic Configuration Management Plan"
   h. NuPAC_PLDS610400-001, Rev. -, "NuPAC Programmable Logic Development Specification - Core PLCI"
   i. NuPAC_MTP610000-001, Rev. A, “Master Test Plan (MTP)"
   j. NuPAC_ED610300-011, Rev. -, "NuPAC Generic Logic Module (GLM) DAR"
   k. NuPAC_ED610100-003, Rev. -, "Chassis / Rear Transition Module (RTM) Design Report"
   l. NuPAC_PLDP610000-005, Rev. -, "Software Tool Evaluation Plan"
   m. NuPAC_ROMP610000-001, Rev. A, "NuPAC Risk and Opportunity Management Plan"
   n. NuPAC_CGDP610000-001, Rev. A, "NuPAC Commercial-Grade Item/Service Dedication Plan"
   o. NuPAC_ED610000-041, Rev. -, "NuPAC Vulnerability Assessment"
   p. NuPAC_SSP610000-001, Rev. -, "NuPAC System Security Plan"
3. Lockheed Martin letter to NRC Document Control Desk, January 19, 2012 (ADAMS Accession No. ML12040A265), docketing:
   a. NuPAC_ED610000-47-P, Rev. A, "Generic Qualification of the NuPAC Platform for Safety-related Applications (Proprietary)"
4. Lockheed Martin letter to NRC Document Control Desk, June 18, 2013 (ADAMS Accession No. ML13183A209), docketing
   a. “Lockheed Martin Responses to Requests for Additional Information Dated May 15, 2013; Numbers 1, 2, 3, 8, 9, 10 and 11.”
5. Lockheed Martin letter to Joseph Holonich, June 28 2013 (ADAMS Accession No. ML13198A076), docketing
   a. “Lockheed Martin Responses to Requests for Additional Information Dated May 15, 2013; Number 5.”

6. Lockheed Martin letter to NRC Document Control Desk, August 5, 2013 (ADAMS Accession Nos. ML13226A026, ML13226A027, ML13226A028, and ML13226A029), docketing
   a. "Lockheed Martin Responses to Requests for Additional Information Dated May 15, 2013; Numbers 6 and 16."
7. Lockheed Martin letter to NRC Document Control Desk, August 15, 2013 (ADAMS Accession No. ML13234A129), docketing
   a. "Lockheed Martin Responses to Requests for Additional Information Dated May 15, 2013; Number 3, Item 8."
8. Lockheed Martin letter to NRC Document Control Desk, September 3, 2013 (ADAMS Accession No. ML13260A015), docketing
   a. "Lockheed Martin Responses to Requests for Additional Information Dated May 15, 2013; Numbers 14 and 15."
9. Lockheed Martin letter to NRC Document Control Desk, September 5, 2013 (ADAMS Accession No. ML13260A024), docketing "Submittal of Supporting Documentation Identified in Lockheed Martin Responses to Request for Additional Information (RAI) Number 3."
   a. NuPAC_PLDP610000-001 Rev, A, "NuPAC Programmable Logic Development Plan"
   b. NuPAC_PLCMP610000-001, Rev. A, "NuPAC Programmable Logic Configuration Management Plan" **Note:** Superseded by Ref. 20.a.
   c. NuPAC_PLPMP610000-001 Rev. A, "Programmable Logic Project Management Plan" **Note:** Superseded by Ref. 17.c and Ref. 23.c.
10. Lockheed Martin letter to NRC Document Control Desk, September 30, 2016 (ADAMS Accession No. ML13289A269), docketing:
   a. NuPAC_ED610000-47-P Rev. B, "Non-Redacted Public Version of the NuPAC Topical Report" (ADAMS Accession No. ML13289A270)
11. Lockheed Martin letter to NRC Document Control Desk, October 2, 2013 (ADAMS Accession No. ML13288A020), docketing "Submittal of Supporting Documentation Identified in Lockheed Martin Responses to Request for Additional Information (RAI) Number 3."
   a. NuPAC_PLDS610400-001 Rev. A, "NuPAC Programmable Logic Design Specification - Core PLCI"
   b. NuPAC_QAP610000-001 Rev. B, "NuPAC Quality Assurance Plan"
12. Lockheed Martin letter to NRC Document Control Desk, October 4, 2013 (ADAMS Accession No. ML13288A019), docketing "Submittal of Supporting Documentation Identified in Lockheed Martin Responses to Request for Additional Information (RAI) Number 3."
   a. NuPAC_MTP610000-001 Rev. B, "NuPAC Master Test Plan (MTP)"
13. Lockheed Martin letter to NRC Document Control Desk, October 9, 2013 (ADAMS Accession No. ML13295A009), docketing "Submittal of Supporting Documentation Identified in Lockheed Martin Responses to Request for Additional Information (RAI) Number 8, Item 1."
   a. NuPAC_ED610000-049 Rev, -, "NuPAC Failure Modes and Effects Analysis"

14. Lockheed Martin letter to NRC Document Control Desk, October 15, 2013 (ADAMS Accession No. ML13295A549), docketing "Transmital of Responses to Request for Additional Information Dated May 15, 2013 Numbers 12 and 17 through 20"
    a. Lockheed Martin Response to RAI #18 - #20, October 4, 2013 (ADAMS Accession No. ML13295A526),
    b. Lockheed Martin Response to RAI #18 - #20, October 4 2013 (ADAMS Accession No. ML13295A527).
    c. Lockheed Martin Response to RAI #12, September 30, 2013 (ADAMS Accession No. ML13295A529).
15. Lockheed Martin letter to NRC Document Control Desk, November 12, 2013 (ADAMS Accession No. ML13325A934), docketing:
    a. NuPAC_ED610000-048, Rev. -, "NuPAC Reliability Prediction"
    b. NuPAC_ED610000-051, Rev. -, "NuPAC Response Time Analysis"
    c. NuPAC_SSP610000-001 Rev. A, "NuPAC System Security Plan"
16. Lockheed Martin letter NRC Document Control Desk, February 7, 2014 (ADAMS Accession No. ML14051A679), docketing:
    a. NuPAC_ED610000-041, Rev. A, "NuPAC Vulnerability Assessment"
17. Lockheed Martin letter to NRC Document Control Desk, November 6, 2014 (ADAMS Accession No. ML14317A270), docketing:
    a. NuPAC_ED610000-055, Rev. -, "NuPAC Supporting Data for Setpoint Analysis"
    b. NuPAC_MTP610000-001, Rev. C, "NuPAC Master Test Plan"
    c. NuPAC_PLDP610000-001, Rev. B, "NuPAC Programmable Logic Development Plan"
    d. NuPAC_PLDP610000-005, Rev. C, "Software Tool Evaluation Plan"
    e. NuPAC_QAP610000-001, Rev. C, "NuPAC Quality Assurance Plan"
18. Lockheed Martin letter to NRC Document Control Desk, November 19, 2014 (ADAMS Accession No. ML14325A760), docketing:
    a. NuPAC_CGDP610000-001, Rev. C, "NuPAC Commercial Grade Item Dedication Plan"
19. Lockheed Martin letter to NRC Document Control Desk, March 6, 2015 (ADAMS Accession No. ML15084A009), docketing:
    a. NuPAC_CGDP610000-001 Rev. C, "Commercial Grade Item Dedication Plan"
    b. NuPAC_PLDS610400-001 Rev. E, "NuPAC Programmable Logic Design Specification"
    c. NuPAC_PSPP610000-001 Rev. -, "NuPAC Platform Safety Project Plan"
       Note: This document replaces the former "System Safety Program Plan," NuPAC_SSPP610000-001.
20. Lockheed Martin letter to NRC Document Control Desk, April 14, 2015 (ADAMS Accession No. ML15105A378), docketing:
    a. NuPAC_CMP610000-001 Rev. F, "NuPAC Configuration and Data Management Plan"
    b. NuPAC_ED610000-060 Rev. -, "NuPAC Inaccuracies and Uncertainties;"
    c. NuPAC_PLDP610000-005 Rev. D, "NuPAC Software Tool Evaluation Plan"
    d. NuPAC_QAP610000-001 Rev. D, "NuPAC Quality Assurance Plan"

21. Lockheed Martin letter to NRC Document Control Desk, April 17, 2015 (ADAMS Accession No. ML15117A099), docketing:
    a. NuPAC_PLDP610000-001 Rev. D, “NuPAC Programmable Logic Development Plan (PLDP)”
22. Lockheed Martin letter to NRC Document Control Desk, May 14, 2015 (ADAMS Accession No. ML15162A529), docketing:
    a. NuPAC_MTP610000-001 Rev. D, “NuPAC Master Test Plan (MTP)”
    b. NuPAC_TP610000-003 Rev. C, “NuPAC System Prudency Test Procedure”
    c. PR033271-10 (Cover Sheet) Rev. A, “Test Procedure for Environmental Testing on Nuclear Safety-Related Instrumentation and Control System”
    d. PR033271-10 Rev. A, “Environmental Testing on Nuclear Safety-Related Instrumentation and Control System”
23. Lockheed Martin letter to NRC Document Control Desk, June 17, 2015 (ADAMS Accession No. ML15170A374), docketing:
    a. NuPAC_CMP610000-001 Rev. G, “NuPAC Configuration and Data Management Plan”
    b. NuPAC_PLDP610000-001 Rev. E, “NuPAC Programmable Logic Development Plan”
    c. NuPAC_PMP610000-001 Rev. C, “NuPAC Project Management Plan (PMP)”
24. Lockheed Martin letter to NRC Document Control Desk, June 23, 2015 (ADAMS Accession No. ML15177A091), docketing:
    a. NuPAC_FVVP610000-001 Rev. D, “NuPAC FPL Verification and Validation Plan”
    b. NuPAC_TP610000-002 Rev. C, “NuPAC System Operability Test Procedure”
25. Lockheed Martin letter to NRC Document Control Desk, June 26, 2015 (ADAMS Accession No. ML15187A224), docketing:
    a. NuPAC_PLRS610400-001 Rev. F, “NuPAC Programmable Logic Requirement Specification - Core PLCI”
    b. NuPAC_ED610000-049 Rev. A, “NuPAC Failure Mode and Effects Analysis Report”
    c. NuPAC_SPC610000-003 Rev. A, “NuPAC System Test Specification”
26. Lockheed Martin letter to NRC Document Control Desk, July 9, 2015 (ADAMS Accession No. ML15190A108), docketing:
    a. NuPAC_PLDS610400-001 Rev. F, “NuPAC Programmable Logic Design Specification - Core PLCI”
    b. NuPAC_TP610000-004 Rev. B, “NuPAC System Environmental Test Procedure”
    c. NuPAC_ASCIDD610000-001 Rev. -, “NuPAC Application Specific Communications Interface Description”
27. Lockheed Martin letter to NRC Document Control Desk, July 8, 2015 (ADAMS Accession No. ML15194A012), docketing:
    a. NuPAC_TPL610400-001 Rev. E, “NuPAC Programmable Logic Test Plan - Core PLCI”
    b. PR033271-10 Rev. -, “Test House Environmental Test Procedure”
28. Lockheed Martin letter to NRC Document Control Desk, July 20, 205 (ADAMS Accession No. ML15204A065), dated docketing:
    a. NuPAC_TP610000-007 Rev. A, “NuPAC System Electromagnetic Compatibility Test Procedure”
    b. PR033273-10 Rev. A, “Test Procedure for NuPAC EMI Testing (Includes ESD Test)”
    c. NuPAC_TP610000-009 Rev. D, “NuPAC System Electrostatic Discharge Test Procedure”

29. Lockheed Martin letter to Joseph Holonich, August 6, 2015 (ADAMS Accession No. ML15222A255), docketing:
    a. NuPAC_ED610000-047-P Rev. D, “Generic Qualification of the NuPAC Platform for Safety- related Applications (Proprietary)”
       Note: Superseded by Ref. 49.a.
    b. NuPAC_TEDP610000- 001 Rev. B, “NuPAC Test Equipment Development Plan”
    c. NuPAC_TP610000-001 Rev. B, “NuPAC System Pre-Qualification Test Procedure”
    d. NuPAC_TP610000-002 Rev. D, “NuPAC System Operability Test Procedure”
    e. NuPAC_TP610000-003 Rev. D, “NuPAC System Prudency Test Procedure”
    f. NuPAC_TP610000-004 Rev. B, “NuPAC System Environmental Test Procedure”
    g. PR033271-TP-10 Rev. B, “Test Procedure for Environmental Testing of Nuclear Safety Related Instrumentation and Control System” [ ] Test Procedure
    h. NuPAC_TP610000-005 Rev. B, “NuPAC System Seismic Test Procedure”
    i. NuPAC_TP610000-006 Rev. A, “NuPAC System Radiation Test Procedure”
    j. PR033270-TP-15 Rev. -, “Test Procedure for Gamma Radiation Exposure of Two Card Racks”
    k. NuPAC_TP610000-007 Rev. A, “NuPAC System Electromagnetic Compatibility Test Procedure”
    l. PR033273-10A Rev. A, “Test Procedure for EMI Testing Performed on a Safety Control System Platform”
    m. NuPAC_TP610000-009 Rev. D, “NuPAC System Electrostatic Discharge (ESD) Test Procedure”
    n. NuPAC_TR610000-001 Rev. -, “NuPAC Pre-Qualification Test Report”
    o. NuPAC_TR610000-006 Rev. A, “NuPAC Radiation Test Report”
    p. PR033270-TR-15 Rev. -, “Test Report for Gamma Radiation Exposure of 2 Card Racks” [ ] Test Report
30. Lockheed Martin letter to NRC Document Control Desk, August 6, 2015 (ADAMS Accession No. ML15222A254), docketing:
    a. NuPAC_TP610000-002 Rev. D, “NuPAC System Operability Test Procedure”
    b. NuPAC_TP610000-003 Rev. D, “”NuPAC System Prudency Test Procedure”
    c. NuPAC_ED610000-048 Rev. D, “NuPAC Reliability Prediction Report”
    d. NuPAC_ED610000-047-P Rev. D, “Generic Qualification of the NuPAC Platform for Safety-Related Applications (Proprietary)”
       Note: Superseded by Ref. 46.a.
    e. PR033271-10 Rev. B, “Test Procedure for Environmental Testing on Nuclear Safety Related Instrumentation and Control System (cover page)”
    f. PR033270-TP-15 (Cover Page) Rev. -, “Test Procedure for Gamma Radiation Exposure of Two Card Racks Supplied by Lockheed Martin (cover Page)”
    g. PR033270-TP-15 Rev. -, “Test Procedure for Gamma Radiation Exposure of Two Card Racks Supplied by Lockheed Martin”
    h. PR033270-TR-15, “Test Report of Gamma Radiation Exposure of Two Card Racks Supplied by Lockheed Martin Corporation”
31. Lockheed Martin letter to NRC Document Control Desk, August 18, 2015 (ADAMS Accession No. ML15236A074), docketing:
    a. NuPAC_TP610000-005 Rev. D, “NuPAC System Seismic Test Procedure”

32. Lockheed Martin letter to NRC Document Control Desk, September 3, 2015 (ADAMS Accession No. ML15257A236), docketing:
    a. NuPAC_PLDS610400-001 Rev. G, “NuPAC Programmable Logic Design Specification – Core PLCI”
    b. NuPAC_PLRS610400-001 Rev. G, “NuPAC Programmable Logic Requirement Specification – Core PLCI”
33. Lockheed Martin letter to NRC Document Control Desk, September 17, 2015 (ADAMS Accession No. ML15265A163), docketing:
    a. NuPAC_ED610000-051 Rev. A, “NuPAC Response Time Analysis”
34. Lockheed Martin letter to NRC Document Control Desk, October 8, 2015 (ADAMS Accession No. ML15292A194), docketing:
    a. PR033271-01, Rev. B, “Environmental Testing on Nuclear Safety-Related Instrumentation and Control System,” [ ] Test Report
    b. PR033271-01, Rev. B, “Environmental Testing on Nuclear Safety-Related Instrumentation and Control System,” (Lockheed Martin Cover Page)
35. Lockheed Martin letter to NRC Document Control Desk, October 19, 2015 (ADAMS Accession No. ML15300A591), docketing:
    a. NuPAC_ED610000-003, Rev. F, “Chassis / Rear Transition Module (RTM) Design Report”
    b. NuPAC_ED610000-011, Rev. B, “NuPAC Generic Logic Module (GLM) DAR”
    c. NuPAC_ED610000-060, Rev. A, “NuPAC Inaccuracies and Uncertainties”
36. Lockheed Martin letter to NRC Document Control Desk, December 2, 2015 (ADAMS Accession No. ML15343A293), docketing:
    a. PR041411-TP-15, “Test Procedure for Seismic Testing of Two 19” NuPAC Card Racks,” [ ] Test Procedure
37. Lockheed Martin letter to NRC Document Control Desk, January 21, 2016 (ADAMS Accession No. ML16032A207), docketing:
    a. NuPAC_QAP610000-001 Rev. E, “NuPAC Quality Assurance Plan”
    b. NuPAC_TP610000-004 Rev. C, “NuPAC System Environmental Test Procedure,”
    c. NuPAC_TP610000-005, Rev. E, “NuPAC System Seismic Test Procedure”
    d. NuPAC_TP610000-007, Rev. C, “NuPAC System Electromagnetic Compatibility Test Procedure”
    e. NuPAC_TP610000-009, Rev. F, “NuPAC System Electrostatic Discharge Test Procedure”
38. Lockheed Martin letter to NRC Document Control Desk, February 9, 2016 (ADAMS Accession No. ML16054A275), docketing:
    a. NuPAC_TR610000-005 Rev. -, “NuPAC Seismic Test Report”
    b. PR041411-TR-15 Rev. NR 12/17/2015, “Test Report for Seismic Testing of Two 19” NuPAC Card Racks”
    c. NuPAC_PLDP610000-005 Rev. F, “Software Tool Evaluation Plan”
39. Lockheed Martin letter to NRC Document Control Desk, February 11, 2016 (ADAMS Accession No. ML16054A349), docketing:
    a. NuPAC_TR610000-004 Rev. A, “NuPAC Environmental Test Report”
40. Lockheed Martin letter to NRC Document Control Desk, March 23, 2016 (ADAMS Accession No. ML16096A158), docketing:
    a. NuPAC_TR610000-010 Rev. -, “NuPAC Environmental Equipment Qualifications (EQ) Summary Report”
    b. NuPAC_TR610000-011 Rev. -, “NuPAC Environmental Equipment - Qualifications (EQ) List of Anomalies and Actions”

41. Lockheed Martin letter to NRC Document Control Desk, April 15, 2016 (ADAMS Accession No. ML16120A049), docketing:
    a. NuPAC_QAP610000-001-NP, Rev. E, “NuPAC Quality Assurance Plan”
42. Lockheed Martin letter to NRC Document Control Desk, April 15, 2016 (ADAMS Accession No. ML16120A051), docketing:
    a. NuPAC_WP610000-005 Rev. A, “NuPAC Core PL Design Verification White Paper”
    b. WP610000-001 Rev. A, “NuPAC Independent Verification and validation Tool White Paper”
    c. WP610000-002 Rev. -, “NuPAC Verification and Tool Summary White Paper”
43. Lockheed Martin letter to NRC Document Control Desk, April 29, 2016 (ADAMS Accession No. ML16134A327), docketing:
    a. NuPAC_SSP610000-001, Rev. D, “NuPAC System Security Plan (SSP)” (ADAMS Accession No. ML16134A338)
    b. NuPAC_ED610100-003, Rev. G, “Chassis I Rear Transition Module (RTM) Design Report” (ADAMS Accession No. ML16134A332)
    c. NuPAC_ED610300-011, Rev. C, “NuPAC Generic Logic Module (GLM) DAR” (ADAMS Accession No. ML16134A333)
    d. NuPAC_PMP610000-001, Rev. D, “NuPAC Project Management Plan (PMP)” (ADAMS Accession No. ML16134A337)
    e. NuPAC_CMP610000-001, Rev. H, “NuPAC Configuration and Data Management Plan” (ADAMS Accession No. ML16134A330)
    f. NuPAC_ED610000-049, Rev. C, “NuPAC Failure Mode and Effects Analysis Report” (ADAMS Accession No. ML16134A331)
    g. NuPAC_PLDP610000-001, Rev. G, “NuPAC Programmable Logic Development Plan (PLOP)” (ADAMS Accession No. ML16134A328)
    h. NuPAC_PLDS610400-001, Rev. K, “NuPAC Programmable Logic Design Specification - Core PLCI” (ADAMS Accession No. ML16134A335)
    i. NuPAC_PLRS610400-001, Rev. L, “NuPAC Programmable Logic Requirement Specification-Core PLCI” (ADAMS Accession No. ML16134A336)
44. Lockheed Martin letter to NRC Document Control Desk, May 9, 2016 (ADAMS Accession No. ML16139A062), docketing:
    a. NuPAC_ED610000-0062, Rev. B, “Vulnerability Assessment Report (VA) for Secure Development Environment (SDE) (SUNSI //SRI)” (ADAMS Accession No. ML16193A063)
    b. NuPAC_TR610000-007, Rev. -, “NuPAC System Electromagnetic Compatibility Test Report”
45. Lockheed Martin letter to NRC Document Control Desk, May 12, 2016 (ADAMS Accession No. ML16146A727), docketing:
    a. NuPAC_ED610300-0011, Rev. D, “NuPAC Generic Logic Module (GLM) DAR” (ADAMS Accession No. ML16146A738)
    b. NuPAC_PLPRC610000-002, Rev. B, “NuPAC Programmable Logic Verification Procedure -Core PLCI” (ADAMS Accession No. ML16146A737)
       Note: This document replaces the former “NuPAC Programmable Logic Test Plan - Core PLCI,” NuPAC_TPL610400-001.

46. Lockheed Martin letter to NRC Document Control Desk, May 25, 2016 (ADAMS Accession No. ML16159A366), docketing:
    a. NuPAC_PLDP610000-001 Rev. H, "NuPAC Programmable Logic Development Plan"
    b. NuPAC_PLDS610400-001 Rev. L, "NuPAC Programmable Logic Development Specification - Core PLCI"
    c. NuPAC_PLPRC610000-002 Rev. C, "NuPAC Programmable Logic Verification Procedure -Core PLCI"
    d. NuPAC_PLRS610400-001 Rev. M, "NuPAC Programmable Logic Requirement Specification - Core PLCI"
    e. NuPAC_TP610000-002 Rev. E, "NuPAC System Operability Test Procedure"
    f. NuPAC_TP610000-003 Rev. E, "NuPAC System Prudency Test Procedure"
    g. NuPAC_TR610000-006 Rev. B, "NuPAC Radiation Test Report"
    h. NuPAC_TR610000-005 Rev. A, "NuPAC Seismic Test Report"
47. Lockheed Martin letter to NRC Document Control Desk, May 27, 2016 (ADAMS Accession No. ML16169A057), docketing:
    a. IFR610000-103 Rev. -, "NuPAC Baseline 1.3.2 V&V Final Report"
    b. NuPAC_TR610000-004 Rev. B, "NuPAC Environmental Test Report"
    c. NuPAC_TR610000-007 Rev. A, "NuPAC System Electromagnetic Compatibility Test Report"
    d. PR033273-01 Rev. D, "Test Report for EMI Testing Performed on a Safety Control System Platform"
    e. NuPAC_TR610000-010 Rev. A, "NuPAC Environmental Equipment Qualifications (EQ) Summary Report"
    f. NuPAC_TR610000-011 Rev. A, "NuPAC Environmental Equipment Qualifications (EQ) List of Anomalies and Actions"
48. Lockheed Martin letter to NRC Document Control Desk, June 29 2016 (ADAMS Accession No. ML16195A148), docketing:
    a. NuPAC_TR610000-010 Rev. C, "NuPAC Environmental Equipment Qualifications (EQ) Summary Report"
    b. NuPAC_TR610000-011 Rev. B, "NuPAC Environmental Equipment Qualifications NuPAC (EQ) List of Anomalies and Actions"
49. Lockheed Martin letter to NRC Document Control Desk, July 8, 2016 (ADAMS Accession No. ML16195A387), docketing:
    a. NuPAC_ED610000-047-P Rev. E, "Generic Qualification of the NuPAC Platform for Safety-related Applications (Proprietary)" (ADAMS Accession No. ML16195A430)
50. Lockheed Martin letter to NRC Document Control Desk, July 19, 2016 (ADAMS Accession No. ML16214A021), docketing:
    a. PR033273-01 Rev. E, "Test Report for EMI Testing Performed on a Safety Control System Platform"
51. Lockheed Martin letter to NRC Document Control Desk, July 27, 2016 (ADAMS Accession No. ML16216A158), docketing:
    a. NuPAC_ED610000-063 Rev. -, "Programmable Logic Failure Modes and Effects Analysis (FMEA) Report"
52. Lockheed Martin letter to NRC Document Control Desk, August 5, 2016 (ADAMS Accession No. ML16224B112), docketing:
    a. NuPAC_PSPR610000-002 Rev. -, "NuPAC Plan (Concept) Phase Safety Report"
    b. NuPAC_PSPR610000-003 Rev. -, "NuPAC Requirements Phase Safety Report"

53. Lockheed Martin letter to NRC Document Control Desk, October 3, 2016 (ADAMS Accession No. ML16281A276), docketing:
    a. ASR610000-112 Rev. A, “BL 1.3.2 Core IV&V Concept Activity Summary Report”
    b. ASR610000-113 Rev. A, “BL 1.3.2 Core IV&V Requirements Activity Summary Report”
    c. ASR610000-114 Rev. -, “BL 1.3.2 Core IV&V Design Activity Summary Report”
    d. ASR610000-115 Rev. -, “BL 1.3.2 Core IV&V Implementation Activity Summary Report”
    e. ASR610000-116 Rev. -, “BL 1.3.2 Core IV&V Test Activity Summary Report”

Attachment: Appendix A, Comment Resolution Table

Principal Contributors: Division of Engineering, Office of Nuclear Reactor Regulation
Norbert Carte, Lead Reviewer
Deirdre Spaulding-Yeoman

Division of Engineering, Infrastructure, and Advanced Reactors,
Office of New Reactors
Tung Truong

Date: March 3, 2017

APPENDIX A

LOCKHEED MARTIN COMMENTS TO DRAFT SAFETY EVALUATION AND NRC STAFF RESPONSE ON NUPAC ED610000-47-P, REVISION -, "GENERIC QUALIFICATION OF THE NUPAC PLATFORM FOR SAFETY-RELATED APPLICATIONS"

Page	Section	Line	Lockheed Martin Comment	NRC Response
2	2.0	33	Editorial Comment: "SPR" should be "SRP" (for Standard Review Plan)	Agreed.
9	3.2	24 - 26	As written, the sentence implies that it is referring to the TSC / TSC DVT which would not be entirely correct. Suggest that a new paragraph be started for this last sentence and then change the sentence from: “The verification philosophy” to “The overall verification philosophy.” The statement is true when considering the overall verification testing philosophy applied by LM but not for the TSC alone.	Agreed.
9	3.4	41	The phrase "known as Field Programmable Logic (FPL) within Lockheed Martin" is inaccurate of design documentation. The Lockheed Martin prefers the term "Programmable Logic" as it is used in all design documentation. The terminology "Field Programmable Logic" was used by IV&V.	Agreed.

Page	Section	Line	Lockheed Martin Comment	NRC Response
12	3.4.1.4	13 - 14	Consider rewording the sentence: "The ***Netlist*** testing is done in part to confirm the preservation of functionality after the software tools ***has*** converted the source code to ***object code***" To read: "The ***netlist*** testing is done in part to confirm the preservation of functionality after the software tools ***have*** converted the source code to ***a placed and routed FPGA netlist***." **NOTE**: The term ***object code*** is software centric, and analogies to hardware are problematic.	Agreed. The SW centric term was used to facilitate referencing the applicable guidance.

Page	Section	Line	Lockheed Martin Comment	NRC Response
12	3.4.1.4	14 - 17	Consider rewording the sentence: "After simulation testing, the ***object code*** is loaded onto the target FPGA, and the integrated assembly (FPGA & Code) is tested using some of the same simulation test vectors to ensure there is a one for one correspondence between simulated and actual behavior" To read: "After simulation testing, the ***placed and routed FPGA design*** is loaded onto the target FPGA, and the integrated assembly (FPGA & Code) is tested using some of the same simulation test vectors to ensure there is a one for one correspondence between simulated and actual behavior" ***NOTE:*** The term ***object code*** is software centric, and analogies to hardware are problematic.	Agreed.

Page	Section	Line	Lockheed Martin Comment	NRC Response
12	3.4.1.4	8	The final TR does not include references to the PLTP, but instead to the PL Verification Procedure (NuPAC_PLPRC610000-002). Consider rewording the sentence: "The SIntP is described in the “NuPAC Programmable Logic Test Plan - Core PLCI,” (Ref. ***27.a***.)." To: "The SIntP is described in the “NuPAC Programmable Logic Verification Procedure - Core PLCI,” (Ref. ***45.c***.)."	Agreed.
22	3.5.1.3	22 - 23	Editorial Comment: In the first sentence change "...a redundant of the system…" to "…a redundant ***portion of*** the system…"	Agreed.
22	3.5.1.5	38	Editorial Comment: In the first sentence change "…in accordance with ***P*** requirements." to "…in accordance with ***IEEE Std 603-1991*** requirements."	Agreed.

Page	Section	Line	Lockheed Martin Comment	NRC Response
38 - 55	3.5.3.5	Various	The statement is made at various points that the testing should be reperformed with the actual programmable logic and installed in a cabinet. The Lockheed Martin position with regard to retest is documented in the white paper NuPAC_WP610000-006. Generic Equipment Qualification is achieved with a programmable logic load representative of a typical safety system application.Lockheed Martin's position with regards to EMI testing while installed in a cabinet: RG 1.209, Position 1, identifies type testing as the preferred method of environmental qualification. The NuPAC Test Specimen Configuration was developed with this NRC position in mind. When the NuPAC is installed in a cabinet, both the EMI imposed from the outside environment and the EMI radiated from the NuPAC will be attenuated; therefore the testing of the TSC without a cabinet represents the configuration of the worst possible EMI environment and envelopes the environment that would result with NuPAC installed within a cabinet.	Agreed
58	3.5.3.6	31	Editorial Comment: Add a space between "3.5" and "Hz"	Agreed.
70	3.7.2.1.8	3	Editorial Comment: Add an "I" to "SG"	Agreed.

Page	Section	Line	Lockheed Martin Comment	NRC Response
80	3.9.2	41 - 42	[ ]	Disagree. No change made.

Page	Section	Line	Lockheed Martin Comment	NRC Response
93	3.10.1.1.2	37 - 38	With regards to the paragraph wording: [ ]	Agreed.

Page	Section	Line	Lockheed Martin Comment	NRC Response
96	3.10.1.2.4	3	Editorial Comment: Add a carriage return at the end of the paragraph.	Agreed.
98	3.10.1.7	2	Editorial Comment: Add a carriage return at the end of the paragraph.	Agreed.
102	4.2.1.f	28 - 35	[ ]	Agreed.

Page	Section	Line	Lockheed Martin Comment	NRC Response
104	4.2.4.f&g	30 - 46	[ ]	Disagree, the topical report includes commitments to the EPRI criteria, this action item is to ensure those commitmments are realized.
105	6.1.a	43	Note should state "Superseded by Ref. 49.a"	Agreed.
107	6.9.b	2	Add note stating "Superseded by Ref. 20.a"	Agreed.
107	6.9.C	4	Add note stating "Superseded by Ref. 17.c and Ref. 23.c" (The PLPMP was integrated into the PMP and the PLDP)	Agreed.
108	6.25.a	44 - 45	Reference 25.a title should be changed from "NuPAC Programmable Logic Design Specification – Core PLCI" to "NuPAC Programmable Logic Requirement Specification – Core PLCI"	Agreed.
109	6.45.b	5 - 6	Should include a note stating this replaces Ref. 27.a, similar to the note in Ref. 19.c. "Note: This document replaces the former “NuPAC Programmable Logic Test Plan - Core PLCI,” NuPAC_TPL610400-001."	Agreed.