



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: i of 263  
Date: 04/14/2017

PROGRAM NAME: Cooperative Development of Safety Platform for Reactor Protection System and Reactor Protection System  
DOCUMENT TYPE: Licensing Topical Report (LTR)  
DOCUMENT TITLE: Generic Qualification of the NuPAC Platform for Safety-related Applications (Non-Proprietary)  
REFERENCE NUMBER(S): CONTRACT NUMBER 11HT10500001023 / Project Number 780  
CDRL: N/A

**PREPARED BY:** Jack Rosenthal  
Program Technical Licensing Manager  
(LMGI)

**CHECKED BY:** Jerry Mauck  
Licensing Consultant (LMGI)

**APPROVED BY:** Edward Brown Zhou Haixiang  
Project Manager (PM) (LMGI) Project Manager (PM) (SNPAS)

OFFICIAL  
ENGINEERING  
RELEASE

PIRA #: ORL201704021

\*Approvers listed on this cover page are for information only. Electronic approval records and the official release information are authenticated in the Windchill Configuration Management System.

|   |   |
|---|---|
| Lockheed Martin Global, Inc.<br>459 Kennedy Drive<br>Archbald, PA 18403-1598, USA | State Nuclear Power Automation<br>System Engineering Company<br>No. 428 East Jiangchuan Road<br>Shanghai, 200241, PRC |
|---|---|



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: ii of 263  
Date: 04/14/2017

This page intentionally left blank.



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: iii of 263  
Date: 04/14/2017

---

## USNRC SAFETY EVALUATION REPORT (SER)



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

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 (NON-PROPRIETARY)" (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.

J. Rosentel

- 2 -

In accordance with the guidance provided on the NRC website, we request that EPRI publish 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.

LMNS 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,



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

Project No. 780

Enclosure:  
Final Safety Evaluation (Nonproprietary)

**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)<br>and<br>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"                            |
| <br><b>Not Applicable:</b> 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"                            |
| <br><b>Not Applicable:</b> 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.<br><br><b>Not Applicable:</b> 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.<br><br><b>Not Applicable:</b> 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:

| <u>Part Number</u> | <u>Description</u>                       |
|--------------------|--|
| 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 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.

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 section 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 indicated 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  $\pm 1$  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**

| <b>MIL-STD-461E Test</b> | <b>Applicability</b>  | <b>Lockheed Martin Testing</b>  |
|--------------------------|---|---|
| RE101                    | <p>Radiated Emissions, Magnetic Field</p> <p>RE101 is applicable to equipment and subsystem enclosures and interconnecting leads. Figure 3.3 of RG 1.180 specifies the operating envelope.</p>  | <p>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).</p> <p>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.</p>   |
| RE102                    | <p>Radiated Emissions, Electric Field</p> <p>RE102 is applicable to equipment and subsystem enclosures and interconnecting leads.</p> <p>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.</p> | <p>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).</p> <p>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.)).</p> <p>Limitations: To fully comply with RE102, Lockheed Martin requires the following for plant-specific configurations:</p> <ul style="list-style-type: none"> <li>• [ ]</li> <li>• [ ]</li> <li>• [ ]</li> </ul> |

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 dB $\mu$ V.

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.

| <b>Table 3.5.3.5-2. Conducted Susceptibility Testing on Interconnecting Signal Leads</b> |   |   |
|--|---|---|
| <b>IEC Test</b>  | <b>Applicability</b>  | <b>Lockheed Martin Testing</b>  |
| 61000-4-4  | <p>Electrical Fast Transient (EFT)/Burst Immunity</p> <p>For medium exposure, RG 1.180, Table 16 specifies a Level 4, 2 kV test voltage.</p>            | <p>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).</p> <p>Test Data: [ ]</p> <p>Results: [ ]</p> <p>Limitations: [ ]</p>            |
| 61000-4-5  | <p>Surge Immunity</p> <p>For medium exposure, RG 1.180, Table 16 specifies a Level 3, 2 kV open circuit test voltage and 1 kA short circuit current</p> | <p>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).</p> <p>Test Data: [ ]</p> <p>Results: [ ]</p> |

**Table 3.5.3.5-2. Conducted Susceptibility Testing on Interconnecting Signal Leads**

| IEC Test  | Applicability   | Lockheed Martin Testing  |
|-----------|---|--|
|           |   | <p>[ ]</p> <p>Limitations: [ ]:</p> <ul style="list-style-type: none"> <li>• [ ]</li> <li>• [ ]</li> <li>• [ ]</li> <li>• [ ]</li> </ul> <p>] ]</p>  |
| 61000-4-6 | <p>Radio Frequency Conducted Susceptibility</p> <p>For medium exposure, RG 1.180, Table 16 specifies a Level 3, 140 dB<math>\mu</math>V test voltage.</p> | <p>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 dB<math>\mu</math>V level from 150 kHz to 80 MHz. (IEC 61000-4-6 identifies this test level as Level 3).</p> <p>Test Data: [ ]</p> <p>Results: [ ]</p> |

**Table 3.5.3.5-2. Conducted Susceptibility Testing on Interconnecting Signal Leads**

| IEC Test   | Applicability  | Lockheed Martin Testing  |
|------------|--|--|
|            |  | <p>Limitations: [ ]</p>  |
| 61000-4-12 | <p>Oscillatory Transients (Ring Wave) Immunity<br/>For medium exposure, RG 1.180, Table 16 specifies a Level 3, 2 kV test voltage.</p> | <p>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.<br/>Test Data: [ ]<br/>Results: [ ]<br/>Limitations: [ ]</p> |

**Table 3.5.3.5-2. Conducted Susceptibility Testing on Interconnecting Signal Leads**

| <b>IEC Test</b> | <b>Applicability</b>   | <b>Lockheed Martin Testing</b>  |
|-----------------|--|---|
| 61000-4-16      | <p>Immunity to Conducted, Common Mode Disturbances</p> <p>For medium exposure, RG 1.180, Table 16 specifies a Level 3 and refers to Table 11.</p> <p>Table 11 shows:</p> <ul style="list-style-type: none"><li>10-1 Vrms (15 – 150 Hz)</li><li>1 Vrms (150 – 1.5 kHz)</li><li>1 – Vrms (1.5 – 15 kHz)</li><li>10 Vrms (15 – 150 kHz)</li></ul> | <p>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).</p> <p>Test Data: [ ]</p> <p>Results: [ ]</p> <p>Limitations: [ ]</p> |

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**

| <b>IEC Test</b> | <b>Applicability</b>  | <b>Lockheed Martin Testing</b>   |
|-----------------|---|--|
| 61000-4-3       | <p>Radiated Susceptibility, Electric Field</p> <p>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.</p> | <p>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.</p> <p>Test Data: [ ]</p> <p>Results: [ ]</p> <p>Limitations: [ ]</p> <ul style="list-style-type: none"> <li>• [ ]</li> <li>• [ ]</li> </ul> |
| 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).<br>Test Data: [ ]<br>Results: [ ]<br>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).<br>Test Data: [ ]<br>Results: [ ] |

**Table 3.5.3.5-3. Radiated Susceptibility Testing**

| IEC Test   | Applicability   | Lockheed Martin Testing   |
|------------|---|---|
|            |   | <p>[ ]</p> <p>Limitations: [ ]</p>  |
| 61000-4-10 | Radiated Susceptibility, Magnetic Field (Damped Oscillatory Magnetic Field Immunity Test) | <p>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.)</p> <p>Test Data: [ ]</p> <p>Results: [ ]</p> <p>Limitations: [ ]</p> |

| <b>Table 3.5.3.5-3. Radiated Susceptibility Testing</b> |                      |                                |
|---|----------------------|--------------------------------|
| <b>IEC Test</b>   | <b>Applicability</b> | <b>Lockheed Martin Testing</b> |
|   |                      | ]                              |

### 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  $\pm 8$  kV for the contact discharge voltage and  $\pm 15$  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  $\pm 8$  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 [

- [1]. For this one case, [
- [2]. 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:

- [

- [

]

- No. 1.f.).
- [

] (See Section 4.2 Generic Open Item

- [

]

is a plant-specific action item.

] This

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 protection systems be independent of control systems. Digital communication between independent systems could compromise their independence unless appropriate measures 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 discuss 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<sup>ii</sup> 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.

<sup>ii</sup> “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<sup>iii</sup> 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<sup>iii</sup> 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<sup>iii</sup> 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 fulfills 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<sup>1</sup> 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."

---

<sup>1</sup> 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<sup>2</sup> 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.

[

]

---

<sup>2</sup> 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 is 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.<sup>3</sup> 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.

[

]

[

]

---

<sup>3</sup> 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"**

| <b>Page</b> | <b>Section</b> | <b>Line</b> | <b>Lockheed Martin Comment</b>  | <b>NRC Response</b> |
|-------------|----------------|-------------|---|---------------------|
| 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.<br><br>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 | <p>Consider rewording the sentence:</p> <p>"The <b>Netlist</b> testing is done in part to confirm the preservation of functionality after the software tools <b>has</b> converted the source code to <b>object code</b>"</p> <p>To read:</p> <p>"The <b>netlist</b> testing is done in part to confirm the preservation of functionality after the software tools <b>have</b> converted the source code to <b>a placed and routed FPGA netlist</b>."</p> <p><b>NOTE:</b> The term <b>object code</b> is software centric, and analogies to hardware are problematic.</p> | 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 | <p>Consider rewording the sentence:</p> <p>"After simulation testing, the <b>object code</b> is loaded onto the target FPGA, and the integrated assembly (FPGA &amp; 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"</p> <p>To read:</p> <p>"After simulation testing, the <b>placed and routed FPGA design</b> is loaded onto the target FPGA, and the integrated assembly (FPGA &amp; 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"</p> <p><b>NOTE:</b> The term <b>object code</b> is software centric, and analogies to hardware are problematic.</p> | Agreed.      |

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

| <b>Page</b> | <b>Section</b> | <b>Line</b> | <b>Lockheed Martin Comment</b>   | <b>NRC Response</b> |
|-------------|----------------|-------------|--|---------------------|
| 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.             |

| <b>Page</b> | <b>Section</b> | <b>Line</b> | <b>Lockheed Martin Comment</b> | <b>NRC Response</b>       |
|-------------|----------------|-------------|--------------------------------|---------------------------|
| 80          | 3.9.2          | 41 - 42     | [<br>]                         | Disagree. No change made. |

| <b>Page</b> | <b>Section</b> | <b>Line</b> | <b>Lockheed Martin Comment</b>                        | <b>NRC Response</b> |
|-------------|----------------|-------------|---|---------------------|
| 93          | 3.10.1.1.2     | 37 - 38     | With regards to the paragraph wording:<br>[<br>]<br>] | 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.      |

| <b>Page</b> | <b>Section</b> | <b>Line</b> | <b>Lockheed Martin Comment</b>   | <b>NRC Response</b>   |
|-------------|----------------|-------------|--|---|
| 104         | 4.2.4.f&g      | 30 - 46     | [<br><br>1]  | Disagree, the topical report includes commitments to the EPRI criteria, this action item is to ensure those commitments 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"<br>(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.<br>"Note: This document replaces the former "NuPAC Programmable Logic Test Plan - Core PLCI," NuPAC_TPL610400-001." | Agreed.   |



## ACKNOWLEDGEMENTS

**This report was submitted by:**

Lockheed Martin Global, Inc.  
459 Kennedy Drive  
Archbald, PA 18403-1598, USA

**Under a cooperative development project between Lockheed Martin Global, Inc. and the State Nuclear Power Automation System Engineering Company:**

State Nuclear Power Automation System Engineering Company  
No. 428 East Jiangchuan Road  
Shanghai, 200241, PRC

## ABSTRACT

This Licensing Topical Report (LTR) presents design, performance, and qualification information for the Nuclear Protection and Control (NuPAC) digital safety instrumentation and control (I&C) platform cooperatively developed by Lockheed Martin Global, Inc. (LMGI) and the State Nuclear Power Automation System (SNPAS) Engineering Company. The NuPAC system is a generic digital safety I&C platform devoted to the implementation of Class 1E safety-related applications in United States (US) nuclear power plants (NPPs).

This LTR is the summary licensing document for the NuPAC digital safety I&C platform and is organized as follows:

- Section 1.0, Introduction
- Section 2.0, Design Criteria
- Section 3.0, Description of the NuPAC Digital Safety I&C Platform
- Section 4.0, Technical and Support Processes
- Section 5.0, Software Development Process for NuPAC Programmable Logic
- Section 6.0, Equipment Qualification
- Section 7.0, Independent Verification and Validation
- Section 8.0, Secure Development and Operational Environment
- Section 9.0, Compliance with Standards and Interim Staff Guidance (ISG)
- Section 10.0, Reference Documents
- Appendix A, NuPAC Platform Application Design Guide
- Appendix B, IEEE Standard 603–1991 Compliance Matrix
- Appendix C, IEEE Standard 7-4.3.2-2003 Compliance Matrix
- Appendix D, DI&C-ISG-04 Compliance Matrix
- Appendix E, DI&C-ISG-06 Compliance Matrix
- Appendix F, Documentation Cross-Reference Matrix

## Keywords

- Instrumentation and Control System
- Digital Systems
- Safety Systems
- Control Systems
- Field Programmable Gate Array

## REVISION HISTORY

Revision information for this LTR is listed below. This table contains a listing and description of changed paragraphs for each succeeding revision.

| Revision | Date       | Paragraph | Description of Change   |
|----------|------------|-----------|---|
| -        | 04/14/2017 | All       | Initial Release<br>Minor editorial updates from previous releases are identified by change bars |
|          |            |           |   |
|          |            |           |   |
|          |            |           |   |

## CONTENTS

|   |             |
|---|-------------|
| <b>USNRC REQUEST FOR ADDITIONAL INFORMATION (RAI) AND SAFETY EVALUATION REPORT (SER).....</b> | <b>iii</b>  |
| <b>ACKNOWLEDGEMENTS .....</b>   | <b>iv</b>   |
| <b>ABSTRACT .....</b>   | <b>v</b>    |
| <b>REVISION HISTORY .....</b>   | <b>vi</b>   |
| <b>CONTENTS .....</b>   | <b>vii</b>  |
| <b>LIST OF APPENDICES.....</b>  | <b>viii</b> |
| <b>LIST OF FIGURES.....</b>   | <b>ix</b>   |
| <b>LIST OF TABLES.....</b>  | <b>x</b>    |
| <b>GLOSSARY OF ACRONYMS AND ABBREVIATIONS .....</b>   | <b>xi</b>   |
| <b>1.0 INTRODUCTION .....</b>   | <b>1</b>    |
| 1.1 Purpose.....  | 1           |
| 1.2 Licensing Topical Report Organization.....  | 2           |
| 1.3 Supporting Licensing Documents.....   | 3           |
| 1.4 Quality System.....   | 3           |
| 1.5 Diversity and Defense-In-Depth (D3).....  | 4           |
| <b>2.0 DESIGN CRITERIA.....</b>   | <b>5</b>    |
| <b>3.0 DESCRIPTION OF THE NUPAC DIGITAL SAFETY I&amp;C PLATFORM.....</b>                      | <b>11</b>   |
| 3.1 Overview.....   | 11          |
| 3.2 Hardware.....   | 19          |
| 3.3 Programmable Logic Architecture.....  | 44          |
| 3.4 Digital Communication.....  | 54          |
| 3.5 Additional Information .....  | 74          |
| <b>4.0 TECHNICAL AND SUPPORT PROCESSES .....</b>  | <b>75</b>   |
| 4.1 Organizational Relationships .....  | 75          |
| 4.2 TASP Structural Overview .....  | 76          |
| 4.3 Process Domains.....  | 77          |
| 4.4 Product Life Cycle .....  | 79          |
| 4.5 Planning Documentation.....   | 87          |
| 4.6 Software Tool Evaluation .....  | 90          |
| 4.7 Deleted .....   | 91          |
| <b>5.0 SOFTWARE DEVELOPMENT PROCESS FOR NUPAC PROGRAMMABLE LOGIC ..</b>                       | <b>93</b>   |
| 5.1 Programmable Logic Life Cycle Description .....   | 93          |
| 5.2 Programmable Logic Oversight .....  | 96          |
| 5.3 Deleted .....   | 96          |
| 5.4 Deleted .....   | 96          |

|   |            |
|---|------------|
| <b>6.0 EQUIPMENT QUALIFICATION .....</b>                                  | <b>97</b>  |
| 6.1 Description of Test Specimen and Test Equipment.....                  | 97         |
| 6.2 Qualification Test Program.....                                       | 101        |
| 6.3 Supporting Data for Analyses.....                                     | 107        |
| 6.4 Limited Life Components .....   | 110        |
| 6.5 Deleted .....   | 110        |
| <b>7.0 INDEPENDENT VERIFICATION AND VALIDATION .....</b>                  | <b>111</b> |
| 7.1 IV&V Independence .....   | 111        |
| 7.2 IV&V Process Overview .....   | 111        |
| 7.3 IV&V Testing and Documentation.....                                   | 116        |
| 7.4 IV&V Administrative Topics .....                                      | 118        |
| 7.5 IV&V Results for NuPAC Core PL.....                                   | 119        |
| <b>8.0 SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT .....</b>           | <b>121</b> |
| 8.1 System Security Planning .....  | 121        |
| 8.2 Vulnerability Assessment .....  | 121        |
| 8.3 Secure Development and Operational Environment Controls.....          | 122        |
| 8.4 Deleted .....   | 123        |
| <b>9.0 COMPLIANCE WITH KEY STANDARDS AND INTERIM STAFF GUIDANCE .....</b> | <b>125</b> |
| 9.1 Compliance with IEEE Standard 603-1991 .....                          | 125        |
| 9.2 Compliance with IEEE Standard 7-4.3.2-2003.....                       | 125        |
| 9.3 Deleted .....   | 125        |
| 9.4 DI&C-ISG-04, Rev. 1 .....   | 125        |
| 9.5 DI&C-ISG-06, Rev. 1 .....   | 126        |
| 9.6 Deleted .....   | 126        |
| <b>10.0 REFERENCES .....</b>  | <b>127</b> |

## LIST OF APPENDICES

|   |            |
|---|------------|
| <b>APPENDIX A: NuPAC Platform Application Design Guide .....</b>      | <b>145</b> |
| <b>APPENDIX B: IEEE Standard 603–1991 Compliance Matrix .....</b>     | <b>177</b> |
| <b>APPENDIX C: IEEE Standard 7-4.3.2-2003 Compliance Matrix .....</b> | <b>203</b> |
| <b>APPENDIX D: DI&amp;C-ISG-04 Compliance Matrix .....</b>            | <b>219</b> |
| <b>APPENDIX E: DI&amp;C-ISG-06 Compliance Matrix .....</b>            | <b>249</b> |
| <b>APPENDIX F: Deleted .....</b>                                      | <b>263</b> |

## LIST OF FIGURES

|                  |   |     |
|------------------|---|-----|
| Figure 3.1.2-1.  | NuPAC Context .....   | 12  |
| Figure 3.1.3-1.  | Generic Logic Module Configuration .....  | 14  |
| Figure 3.1.3-2.  | Chassis .....   | 15  |
| Figure 3.1.3-3.  | Chassis Installed GLMs and RTMs .....   | 16  |
| Figure 3.1.3-4.  | GLM/Backplane/RTM Configuration .....   | 17  |
| Figure 3.2.1-1.  | GLM Components and Assembly .....   | 20  |
| Figure 3.2.1-2.  | GLM Block Diagram .....   | 21  |
| Figure 3.2.1-3.  | Carrier Card .....  | 24  |
| Figure 3.2.1-4.  | Carrier Card Simplified Functional Block Diagram .....                                | 25  |
| Figure 3.2.1-5.  | Typical I/O Mezzanine .....   | 27  |
| Figure 3.2.1-6.  | Analog Input Mezzanine Simplified Block Diagram .....                                 | 29  |
| Figure 3.2.1-7.  | Discrete/Pulse Input Mezzanine Simplified Block Diagram .....                         | 31  |
| Figure 3.2.1-8.  | Temperature Input Mezzanine Simplified Block Diagram .....                            | 32  |
| Figure 3.2.1-9.  | RS-422/485 Mezzanine Simplified Block Diagram .....                                   | 33  |
| Figure 3.2.1-10. | Analog Output Mezzanine Simplified Block Diagram .....                                | 35  |
| Figure 3.2.1-11. | SSR Mezzanine Simplified Block Diagram .....  | 36  |
| Figure 3.2.1-12. | Logic Mezzanine .....   | 37  |
| Figure 3.2.2-1.  | Rear Transition Module .....  | 39  |
| Figure 3.2.3-1.  | Chassis .....   | 41  |
| Figure 3.3.1-1.  | Core PLCI Functional Architecture .....   | 45  |
| Figure 3.3.2-1.  | AS PLCI Programmable Logic Block Diagram .....  | 49  |
| Figure 3.4.2-1.  | NuPAC to NuPAC Communications .....   | 55  |
| Figure 3.4.2-2.  | Copper Cable Length vs Data Rate .....  | 57  |
| Figure 3.4.2-3.  | Division to Division Communications .....   | 57  |
| Figure 3.4.4-1.  | Full Mesh with Port Numbers .....   | 61  |
| Figure 3.4.4-2.  | Full Mesh Alternate View .....  | 61  |
| Figure 3.4.4-3.  | First 16 GLMs = 4 Groups of 4 .....   | 62  |
| Figure 3.4.4-4.  | NuPAC Internal to Chassis Communication Topology .....                                | 63  |
| Figure 3.4.4-5.  | Alternate port view of the two mesh/star communication connections .....              | 65  |
| Figure 3.4.5-1.  | ASPL Communication Block Function .....   | 69  |
| Figure 3.4.7-1.  | Inter-divisional Communication .....  | 73  |
| Figure 4.1-1.    | NuPAC Program Organizational Relationships .....                                      | 75  |
| Figure 4.2-1.    | TASP Structural Overview .....  | 77  |
| Figure 4.4-1.    | Perform Product Life Cycle Actions .....  | 81  |
| Figure 5.1-1.    | Software Development Process .....  | 94  |
| Figure 6.1.1-1.  | TSC Block Diagram .....   | 98  |
| Figure 6.1.2-1.  | Test System .....   | 99  |
| Figure 6.1.2-2.  | TSC Test Setup Block Diagram .....  | 100 |
| Figure 6.2.2-1.  | NuPAC Environmental Qualification Test Envelope .....                                 | 103 |
| Figure 6.2.3-1.  | NuPAC SSE -10% and OBE Qualification Spectra Seismic Withstand Response Spectrum .... | 104 |

## LIST OF TABLES

|   |     |
|---|-----|
| Table 2.0-1. Codes, Regulatory Guidance, and Design Standards Applied ..... | 5   |
| Table 3.1.4-1. Qualified Components .....                                   | 18  |
| Table 3.2.1-1. GLM Functions .....  | 22  |
| Table 3.2.1-2. Analog Input Mezzanine Functions .....                       | 29  |
| Table 3.2.1-3. Discrete/Pulse Input Mezzanine Functions .....               | 30  |
| Table 3.2.1-4. Temperature Input Mezzanine Functions.....                   | 32  |
| Table 3.2.1-5. RS-422/485 Mezzanine Functions .....                         | 33  |
| Table 3.2.1-6. Analog Output Mezzanine Functions.....                       | 34  |
| Table 3.2.1-7. SSR Mezzanine Functions .....                                | 36  |
| Table 3.4.4-1. LVDS Backplane Message Structure.....                        | 67  |
| Table 4.5-1. Generic NuPAC Platform Planning Documentation.....             | 87  |
| Table 6.2-1. Qualification Test Sequence .....                              | 101 |
| Table 6.2.5-1. Electromagnetic Compatibility Tess Sequence.....             | 105 |
| Table 6.2.5-2. Electromagnetic Compatibility Test Results Summary .....     | 106 |
| Table 10.0-1. USNRC Codes and Regulatory Guidance.....                      | 127 |
| Table 10.0-2. Industry Standards and Guidance.....                          | 132 |
| Table 10.0-3. NuPAC Program References.....                                 | 140 |

## GLOSSARY OF ACRONYMS AND ABBREVIATIONS

|                |  |
|----------------|--|
| $\Delta\Sigma$ | delta-sigma                                    |
| <b>A – B</b>   |  |
| ac             | alternating current                            |
| ADC            | analog-to-digital converter                    |
| ALWR           | Advanced Light-Water Reactor                   |
| AP             | assurance plan                                 |
| ANSI           | American National Standards Institute          |
| ASME           | American Society of Mechanical Engineers       |
| ASPL           | Application-specific Programmable Logic        |
| ASPLD          | Application-Specific Programmable Logic Device |
| ATWS           | Anticipated Transient Without Scram            |
| BIT            | built-in testing;<br>built-in test             |
| BGA            | ball grid array                                |
| BTP            | Branch Technical Position                      |
| <b>C</b>       |  |
| C              | Centigrade                                     |
| CAB            | Corrective Action Board                        |
| CCA            | circuit card assembly                          |
| CCB            | Change Control Board                           |
| CCF            | common cause failure                           |
| CDA            | Critical Digital Assets                        |
| [              | ] <sup>a,c,e</sup>                             |
| CFR            | Code of Federal Regulation                     |
| CGDP           | Commercial Grade Dedication Plan               |
| CI             | configuration item                             |
| CJC            | cold junction compensation                     |
| CM             | configuration management                       |
| CMP            | configuration management plan                  |

|          |   |
|----------|---|
| Core PLD | Core Programmable Logic Device              |
| COTS     | Commercial Off-The-Shelf                    |
| CRC      | cyclic redundancy check                     |
| CSA      | configuration status accounting             |
| CTIC     | communications and test interface connector |
| <b>D</b> |   |
| D3       | Diversity and Defense-in-Depth              |
| DAC      | digital-to-analog converter                 |
| DAE      | Diversity Attribute Effectiveness           |
| DAS      | Diverse Actuation System                    |
| DBE      | Design Basis Event                          |
| dc       | direct current                              |
| DCE      | Diversity Criterion Effectiveness           |
| DRS      | design requirements specification           |
| <b>E</b> |   |
| ECC      | error correction code                       |
| [        | ] <sup>a,c,e</sup>                          |
| EFT      | electrical fast transient                   |
| EMI      | electromagnetic interference                |
| EPRI     | Electric Power Research Institute           |
| ESD      | electrostatic discharge                     |
| ESFAS    | Engineered Safety Features Actuation System |
| <b>F</b> |   |
| F        | Fahrenheit                                  |
| FCA      | functional configuration audit              |
| FMC      | FPGA Mezzanine Card                         |
| FMEA     | failure modes and effects analysis          |

|              |   |
|--------------|---|
| FMECA        | failure modes, effect and criticality analysis            |
| FPGA         | field programmable gate array                             |
| FPL          | field programmable logic                                  |
| FRACAS       | failure reporting, analysis and corrective action system  |
| FVVP         | field programmable logic verification and validation plan |
| <b>G – H</b> |   |
| GDC          | General Design Criterion;<br>General Design Criteria      |
| GLM          | Generic Logic Module                                      |
| HDL          | hardware description language                             |
| HDP          | hardware development plan                                 |
| HW           | hardware  |
| <b>I</b>     |   |
| I/F          | interface   |
| I/O          | input/output  |
| I&C          | instrumentation and control                               |
| I&T          | Integration and Test                                      |
| I-V&V        | independent verification and validation                   |
| IAW          | in accordance with  |
| ICD          | interface control document                                |
| IDD          | interface design document                                 |
| IEC          | International Electrotechnical Commission                 |
| IEEE         | Institute of Electrical and Electronics Engineers         |
| ILS          | integrated logistics support                              |
| IMP          | integrated master plan                                    |
| IMS          | integrated master schedule                                |
| INH          | inherent use  |
| INT          | intentional use   |
| IP           | industry pack   |
| IPT          | integrated product team                                   |
| IRS          | interface requirements specification                      |
| ISG          | Interim Staff Guidance                                    |

|                  |   |
|------------------|---|
| ISO              | International Standards Organization              |
| <b>J – K – L</b> |   |
| JTAG             | Joint Test Action Group                           |
| kb               | kilobits  |
| kbps             | kilobits per second                               |
| KC               | key characteristic                                |
| kHz              | kilohertz   |
| LAR              | License Amendment Request                         |
| LED              | light emitting diode                              |
| LMGI             | Lockheed Martin Global, Inc.                      |
| LPE              | lead program engineer                             |
| LTR              | Licensing Topical Report                          |
| LVDS             | low-voltage differential signaling                |
| <b>M – N</b>     |   |
| Mb               | megabits  |
| Mbps             | megabits per second                               |
| MHz              | megahertz   |
| MICTOR           | Matched Impedance ConnecTOR                       |
| MOFSET           | metal-oxide semiconductor field-effect transistor |
| MSFIS            | Main Steam and Feedwater Isolation System         |
| MTP              | master test plan                                  |
| NPP              | nuclear power plant                               |
| NQA              | Nuclear Quality Assurance                         |
| NuPAC            | Nuclear Protection and Control                    |
| <b>O – P</b>     |   |
| OCD              | operational concept document                      |
| P/CR             | problem/change request                            |
| P/N              | part number                                       |
| PCA              | physical configuration audit                      |
| [                | ] <sup>a,c,e</sup>                                |
| PGA              | programmable gain amplifier                       |
| PL               | programmable logic                                |
| PLC              | programmable logic controller                     |

|              |  |
|--------------|--|
| PLCI         | programmable logic configuration item                      |
| PLD          | Programmable Logic Device                                  |
| PLDP         | programmable logic development plan                        |
| PLM          | priority logic module                                      |
| PLRS         | programmable logic requirements specification              |
| PLTP         | programmable logic test plan                               |
| PMP          | program management plan                                    |
| POST         | power-on self-test   |
| PPMC         | program planning, monitoring, and control                  |
| PM           | program manager  |
| PMP          | program management plan                                    |
| PRI          | program repository index                                   |
| PSPP         | Platform Safety Project Plan                               |
| [            | ] <sup>a,c,e</sup>   |
| <b>Q – R</b> |  |
| QA           | quality assurance  |
| QAP          | quality assurance plan                                     |
| RAM          | random access memory                                       |
| RG           | Regulatory Guide   |
| ROMP         | risk and opportunity management plan                       |
| RPP          | reliability program plan                                   |
| RPS          | Reactor Protection System                                  |
| RTD          | Resistance Temperature Detector                            |
| RTM          | requirements traceability matrix<br>Rear Transition Module |
| RTS          | Reactor Trip System  |
| Rx           | receiver   |
| <b>S</b>     |  |
| SD           | system design  |
| SDOE         | Secure Development and Operational Environment             |
| [            | ] <sup>a,c,e</sup>   |

|                          |   |
|--------------------------|---|
| SECY                     | Secretary of the Commission<br>Office of the (NRC)        |
| SEMP                     | systems engineering management plan                       |
| SER                      | safety evaluation report                                  |
| SiO <sub>2</sub>         | silicon dioxide   |
| SME                      | subject matter expert                                     |
| SMP                      | subcontract management plan                               |
| SNPAS                    | State Nuclear Power Automation System Engineering Company |
| SOW                      | statement of work   |
| SP                       | support plan  |
| SPI                      | serial peripheral interface                               |
| SQT                      | system qualification/acceptance test                      |
| SRA                      | system requirements analysis                              |
| [                        | ] <sup>a,c,e</sup>  |
| [                        | ] <sup>a,c,e</sup>  |
| SSP                      | system security plan                                      |
| SSR                      | solid state relay;<br>solid state resistor                |
| [                        | ] <sup>a,c,e</sup>  |
| Std.                     | standard  |
| <b>T – U</b>             |   |
| TEDP                     | test equipment development plan                           |
| [                        | ] <sup>a,c,e</sup>  |
| TSC                      | test specimen configuration                               |
| TASP                     | technical support process                                 |
| Tx                       | transmitter   |
| UART                     | Universal Asynchronous Receiver-Transmitter               |
| US                       | United States   |
| USNRC                    | United States Nuclear Regulatory Commission               |
| <b>V – W – X – Y – Z</b> |   |
| V                        | volt  |



|                 |  |
|-----------------|--|
| V&V             | verification and validation  |
| VA              | volt amperes   |
| V <sub>AC</sub> | volts alternating current  |
| V <sub>DC</sub> | volts direct current   |
| VDU             | visual display unit  |
| VHDL            | VHSIC (Very High-Speed Integrated Circuit) Hardware Description Language |
| VRCM            | verification cross-reference matrix                                      |

## 1.0 INTRODUCTION

### 1.1 Purpose

Lockheed Martin Global, Inc. (LMGI) is submitting this Licensing Topical Report (LTR) to the United States Nuclear Regulatory Commission (USNRC) for review and approval of the Nuclear Protection and Control (NuPAC) platform design. The NuPAC platform will be used as a digital system platform in safety-related applications in nuclear power plants (NPPs) in the United States (US). It is designed to replace existing analog and CPU-based instrumentation and control (I&C) systems currently used in US NPP applications and to be installed as original equipment for new NPP facilities.

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 will continuously monitor plant status through signals that are received from plant sensors or even manual commands. It performs computations (e.g., solves logic) to calculate appropriate commands based on the input signals. It provides output commands (e.g., trip signals) to the appropriate plant actuators. The NuPAC platform offers modularity and scalability, similar to a PLC, via the configuration of chassis installed logic solving modules.

The NuPAC platform is a state-of-the-art digital platform specifically designed for safety-related control and protection systems in NPP applications. Its design facilitates the development of highly safe and reliable digital I&C systems. The platform features a modular decentralized (distributed) field programmable gate array (FPGA)-based architecture. It is functionally similar to legacy analog measurement and trip modules, but takes advantage of the benefits of digital technology. The FPGA-based architecture facilitates implementation of nuclear safety requirements of redundancy, independence, determinacy, and diversity and defense-in-depth. In addition, the FPGA-based architecture allows simple programmable logic, avoiding unfavorable software-like behavior and integration of software operating systems and executables. NuPAC operational scenarios (typical NuPAC platform roles and applications) include, but are not limited to, the Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS).

The NuPAC platform design is based primarily on requirements of USNRC Regulatory Guides (RGs) and Institute of Electrical and Electronics Engineers (IEEE) standards applicable to NPP safety-related applications. The primary reference is Title 10 of the Code of Federal Regulation Section 50.55a(h)(2) (**Reference 104**) and USNRC RG 1.153 (**Reference 134**), which endorses IEEE Standard 603-1991 (**Reference 153**). Since the NuPAC platform is a digital device, USNRC RG 1.152 (**Reference 133**) and IEEE Standard 7-4.3.2-2003 (**Reference 356**) are used for guidance. The development process also considered the guidance provided in RGs 1.168, 1.169, 1.170, 1.171, 1.172, and 1.173 (**References 135 through 140**), as well as the Digital Instrumentation and Control Interim Staff Guidance (DI&C-ISG) associated with NPP digital I&C.

Generic qualification of the NuPAC platform includes both hardware components and the programmable logic used, which are detailed in Sections 3.2 and 3.3. The NuPAC platform provides the functionality that is typically required for safety-related control and protection systems in NPP applications. The qualification process involves technical evaluations and qualification tests. The equipment qualification test program is based on the Electric Power Research Institute (EPRI) Technical Report TR-107330 (**Reference 312**). Electromagnetic compatibility qualification is based on USNRC RG 1.180 (**Reference 141**). The qualification test results,

demonstrating both the adequacy and the robustness of the design, are provided as part of the Phase 2 documentation.

This LTR also demonstrates compliance to the licensing process of DI&C-ISG-06 (**Reference 119**). This LTR describes the NuPAC platform, development processes, and equipment qualification. Detailed compliance matrices, included as appendices to this LTR, document how the NuPAC platform complies with the requirements specified in IEEE Standard 603-1991, IEEE Standard 7-4.3.2 2003, DI&C-ISG-04 (**Reference 117**), and DI&C-ISG-06.

The platform defined in this LTR will be the basis of plant-specific systems supplied to utilities and other users. Plant-specific systems will be documented and submitted to the USNRC by the appropriate licensees, referencing, as appropriate, this topical report as part of the LAR process adopted by the licensee.

## 1.2 Licensing Topical Report Organization

This report is organized as follows:

- **Section 1.0, Introduction:** An overview of the LTR and identification of the supporting documents submitted for USNRC review. This Section also provides an overview of the quality assurance program.
- **Section 2.0, Design Criteria:** Lists regulatory requirements, design criteria, and guidelines applicable to the NuPAC platform.
- **Section 3.0, Description of the NuPAC Digital Safety I&C Platform:** Describes how the NuPAC platform works and how it can be applied in NPP safety-related applications. Identifies NuPAC platform hardware components and programmable logic, explains how they function, and describes how they are interrelated. In addition, addresses aspects of data communication, specifically identifying methodologies for the NuPAC platform to support compliance with DI&C-ISG-04 (**Reference 117**).
- **Section 4.0, Technical and Support Processes:** Describes the design process, organizational structure, and project control methods used during NuPAC platform development.
- **Section 5.0, Software Development Process for NuPAC Programmable Logic:** Explains software-based life cycle processes used to develop NuPAC programmable logic.
- **Section 6.0, Equipment Qualification:** Summarizes NuPAC platform qualification test plans. In addition, identifies the methodologies for the NuPAC platform to support plant-specific system-level analyses, including aspects of failure analysis, reliability/availability analysis, response time analysis, setpoint (inaccuracy) value analysis, and limited life component analysis.
- **Section 7.0, Independent Verification and Validation:** Explains the NuPAC Independent Verification and Validation (IV&V) organization, processes and results. The IV&V process follows the guidance of IEEE Standard 1012 (**Reference 328**) as endorsed by USNRC RG 1.168 (**Reference 135**).
- **Section 8.0, Secure Development and Operational Environment:** Explains the NuPAC platform vulnerability assessment and identifies the associated methodology to apply secure development and operational environment controls per USNRC RG 1.152 (**Reference 133**).
- **Section 9.0, Compliance with Standards and Interim Staff Guidance (ISG):** Explains how the NuPAC platform complies with IEEE Standard 603-1991 (**Reference 153**), IEEE Standard 7-4.3.2-2003 (**Reference 356**), DI&C-ISG-04 (**Reference 117**), and DI&C-ISG-06 (**Reference 119**).
- **Section 10.0, References:** Provides a cross-reference for all documents identified in this topical report.

- **Appendix A, NuPAC Platform Application Design Guide:** Provides design guidelines that future application (system) developers must consider in order to remain consistent with this platform baseline and anticipated approval.
- **Appendix B, IEEE Standard 603 Compliance Matrix:** Provides an IEEE Standard 603-1991 (**Reference 153**) compliance matrix, with the requirement listed; NuPAC platform compliance to each requirement defined; and references to confirmatory information.
- **Appendix C, IEEE Standard 7-4.3.2 Compliance Matrix:** Includes an IEEE Standard 7-4.3.2-2003 (**Reference 356**) compliance matrix, with the requirement listed, NuPAC platform compliance to each requirement defined, as well as references to the confirmatory information.
- **Appendix D, DI&C-ISG-04 Compliance Matrix:** Provides a DI&C-ISG-04 (**Reference 117**) compliance matrix, with the requirement listed, NuPAC platform compliance to each requirement defined, as well as references to the confirmatory information.
- **Appendix E, DI&C-ISG-06 Compliance Matrix:** Contains a DI&C-ISG-06 (**Reference 119**) compliance matrix, with the requirement listed, NuPAC platform compliance to each requirement defined, as well as references to the confirmatory information.

### 1.3 Supporting Licensing Documents

This topical report is provided in order to obtain generic approval from the USNRC of the NuPAC platform. As an unreviewed platform, the licensing information included herein, as well the docketed, supporting design and process documentation is provided for a Tier 3 review, as defined in DI&C-ISG-06 (**Reference 119**).

Appendix F provides a cross reference listing of the NuPAC documents, provided to support a Tier 3, Phase 1 review, against those documents identified for Phase 1 in DI&C-ISG-06 (Enclosure B) (**Reference 119**).

Appendix E provides a complete compliance matrix of NuPAC licensing, design, and processes against the review needs of the licensing process of DI&C-ISG-06 (**Reference 119**). For clarity, this compliance matrix also presents the alignment of the NuPAC documentation to the Phase 1 and Phase 2 expectations of the USNRC.

Note, the software documentation is associated with the software-based life cycle processes which were used as references to develop non-software, FPGA programmable logic of NuPAC.

### 1.4 Quality System

The development of NuPAC documented in this LTR is performed to a quality program that was developed to meet the requirements of Title 10 of the Code of Federal Regulations Part 50 (10 CFR 50) Appendix B, ASME Nuclear Quality Assurance (NQA)-1-2008 (**Reference 304**), ASME NQA-1a-2009, Addenda to ASME NQA-1-2008 (**Reference 305**), and USNRC RG 1.28 (**Reference 145**). All nuclear activities are subject to the policies and procedures described in the Lockheed Martin Energy Quality Systems Manual for Commercial Nuclear Programs (**Reference 731**) and the NuPAC Quality Assurance Plan (**Reference 719**).

In addition, LMGI facilities in Archbald, Pennsylvania, and Grand Prairie, Texas are certified to ISO 9001:2008 (**Reference 367**) and SAE AS9100C (**Reference 369**) requirements. The QA organizations are responsible for all quality assurance functions. Their primary tasks are to verify that documentation, fabrication, tests, shipments, and deliveries are complete and comply with all QA program requirements. The QA



organization performs ongoing evaluations to ensure quality objectives are accomplished in accordance with our NuPAC Quality Assurance Plan and program requirements.

### 1.5 Diversity and Defense-In-Depth (D3)

NuPAC is being designed as an integral element of the diversity and defense-in-depth approach for plant-specific applications. Diversity is being addressed within the design based on both hardware diversity and software (programmable logic) diversity. This will eliminate common cause failures within the platform and plant-specific applications. Detailed licensing material that addresses evaluation criteria in BTP 7-19 (**Reference 114**) and diversity/defense-in-depth considerations in NUREG/CR-6303 (**Reference 123**) will be provided in a future revision of this document.

## 2.0 DESIGN CRITERIA

This section identifies the applicable codes, regulatory guidance, and industry guidelines and standards used in the development of the design criteria for the NuPAC platform.

The NuPAC platform is designed for use in NPP safety-related systems which demand the highest quality of its components, its design process, and system implementation aspects, such as real time performance, independence, and self-diagnostic features such as Built-In Test (BIT) to support surveillance testing intervals.

The NuPAC platform was developed and is being supplied as qualified equipment. The NuPAC platform was developed based on the guidance provided in Regulatory Guides (RGs), endorsed industry standards, Branch Technical Positions (BTPs), and Interim Staff Guidance (ISG). By conforming to the acceptable methods set forth in that guidance, the NuPAC platform satisfies the applied design and regulatory criteria (Table 2.0-1).

NuPAC does not incorporate software. Guidance on software and software processes identified in the following table has been tailored and applied to the development and testing of the programmable logic of NuPAC. This is described in more detail in Sections 3, 4, and 5.

Table 2.0-1 lists the codes, regulatory guidance, and industry design standards which apply to nuclear safety-related I&C systems. The guidance and standards listed apply, generally, to a much broader definition of safety-related I&C than covered by this version of the NuPAC platform documented in this topical report and submitted for review and approval by the USNRC. As such, an applicability column is included in the table which identifies which of the documents applies to this submittal. Applicable documents, usually portions thereof, are identified with an “X” and the manner and extent of the applicability are described in related plans or technical documentation. Separate compliance traceability matrices for key standards are provided in the appendices to this document. Additionally, documents identified with a “G” are considered direct guidance and used to provide regulatory or technical insight. As the NuPAC platform is expanded in future versions, or incorporated in plant-specific applications by Licensees, additional regulatory guidance and industry standards may apply and will be identified at that time.

**Table 2.0-1. Codes, Regulatory Guidance, and Design Standards Applied**

| Reference Number | Document ID              | Subject                       | Applicability to This Topical Report Revision |
|------------------|--------------------------|-------------------------------|---|
| 100              | 10 CFR 21                | Defect Reporting              | [ ] <sup>a,c,e</sup>                          |
| 101              | 10 CFR 50                | Nuclear Facility Licensing    | [ ] <sup>a,c,e</sup>                          |
| 102              | 10 CFR 50 App. A         | Nuclear Plant Design Criteria | [ ] <sup>a,c,e</sup>                          |
| 103              | 10 CFR 50 App. B         | Quality Assurance Criteria    | [ ] <sup>a,c,e</sup>                          |
| 104              | 10 CFR Part 50.55a(h)(2) | Protection System Basis       | [ ] <sup>a,c,e</sup>                          |
| 106              | 10 CFR 810               | Foreign Atomic Activities     | [ ] <sup>a,c,e</sup>                          |

| Reference Number | Document ID                             | Subject  | Applicability to This Topical Report Revision |
|------------------|---|--|---|
| 304              | ASME NQA-1-2008                         | Nuclear Quality Assurance  | [ ] <sup>a,c,e</sup>                          |
| 305              | ASME NQA-1a-2009                        | Nuclear Quality Assurance  | [ ] <sup>a,c,e</sup>                          |
| 110              | BTP 7-12 Rev. 5                         | Establishing and Maintaining Instrument Setpoints  | [ ] <sup>a,c,e</sup>                          |
| 112              | BTP 7-14 Rev. 5                         | Nuclear SW Review Guide  | [ ] <sup>a,c,e</sup>                          |
| 113              | BTP 7-17 Rev. 5                         | Self-Test and Surveillance   | [ ] <sup>a,c,e</sup>                          |
| 115              | BTP 7-21 Rev. 5                         | Digital Computer Real-Time Performance   | [ ] <sup>a,c,e</sup>                          |
| 117              | DI&C-ISG-04 Rev. 1                      | Control Rooms & Digital Communication  | [ ] <sup>a,c,e</sup>                          |
| 119              | DI&C-ISG-06 Rev. 1                      | Licensing Process  | [ ] <sup>a,c,e</sup>                          |
| 153              | IEEE Std 603-1991                       | IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations; Institute of Electrical and Electronics Engineers | [ ] <sup>a,c,e</sup>                          |
| 154              | IEEE Std 603-1991 Correction Sheet 1995 | IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations; Institute of Electrical and Electronics Engineers | [ ] <sup>a,c,e</sup>                          |
| 155              | 10CFR50.54(jj)                          | Quality standards for 10CFR50.55a SSCs   | [ ] <sup>a,c,e</sup>                          |
| 156              | 10CFR50.55(i)                           | Quality standards for 10CFR50.55a SSCs   | [ ] <sup>a,c,e</sup>                          |
| 308              | EPRI NP-5652 Rev. -                     | Commercial Grade Dedication  | [ ] <sup>a,c,e</sup>                          |
| 309              | EPRI NP-102260 Rev. -                   | Supplemental Guidance on Commercial Grade Dedication (EPRI NP-5652)  | [ ] <sup>a,c,e</sup>                          |
| 310              | EPRI TR-102323 Rev. 1                   | Electromagnetic Interference Testing   | [ ] <sup>a,c,e</sup>                          |
| 311              | EPRI TR-106439 Rev. -                   | Evaluation and Acceptance of Commercial Grade Digital Equipment  | [ ] <sup>a,c,e</sup>                          |
| 312              | EPRI TR-107330 Rev. -                   | Commercial Digital Equipment   | [ ] <sup>a,c,e</sup>                          |
| 120              | GL 89-02                                | Detection of Counterfeit Products  | [ ] <sup>a,c,e</sup>                          |
| 121              | GL 91-05                                | Commercial Grade Procurement and Dedication  | [ ] <sup>a,c,e</sup>                          |

| Reference Number | Document ID                    | Subject   | Applicability to This Topical Report Revision |
|------------------|--------------------------------|---|---|
| 318              | IEC 61000-4-1 Ed. 1.0<br>1992  | EMC Testing and Measurement Techniques  | [ ] <sup>a,c,e</sup>                          |
| 319              | IEC 61000-4-2 Ed. 1.0<br>1995  | EMC Electrostatic Discharge Immunity Test   | [ ] <sup>a,c,e</sup>                          |
| 320              | IEC 61000-4-3 Ed. 1.0<br>1995  | EMC Radiated, Radio-Frequency, Electromagnetic Field Immunity Test                                  | [ ] <sup>a,c,e</sup>                          |
| 321              | IEC 61000-4-4 Ed. 1.0<br>1995  | EMC Electrical Fast Transient/Burst Immunity Test   | [ ] <sup>a,c,e</sup>                          |
| 322              | IEC 61000-4-5 Ed. 1.0<br>1995  | EMC Surge Immunity Test   | [ ] <sup>a,c,e</sup>                          |
| 323              | IEC 61000-4-6 Ed. 1.0<br>1996  | EMC Immunity to Conducted Disturbances, Induced by Radio-Frequency Fields                           | [ ] <sup>a,c,e</sup>                          |
| 324              | IEC 61000-4-8 Ed. 1.0<br>1993  | EMC Power Frequency Magnetic Field Immunity Test  | [ ] <sup>a,c,e</sup>                          |
| 325              | IEC 61000-4-9 Ed. 1.0<br>1993  | EMC Pulse Magnetic Field Immunity Test  | [ ] <sup>a,c,e</sup>                          |
| 315              | IEC 61000-4-10 Ed. 1.0<br>1993 | EMC Damped Oscillatory Magnetic Field Immunity Test   | [ ] <sup>a,c,e</sup>                          |
| 316              | IEC 61000-4-12 Ed. 1.0<br>1995 | EMC Oscillatory Waves Immunity Tests  | [ ] <sup>a,c,e</sup>                          |
| 317              | IEC 61000-4-16 Ed. 1.0<br>1998 | EMC Test for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz | [ ] <sup>a,c,e</sup>                          |
| 327              | IEEE STD 1008-1987             | SW Unit Testing   | [ ] <sup>a,c,e</sup>                          |
| 328              | IEEE STD 1012-2004             | SW Verification & Validation  | [ ] <sup>a,c,e</sup>                          |
| 330              | IEEE STD 1028-2008             | SW Reviews and Audits   | [ ] <sup>a,c,e</sup>                          |
| 331              | IEEE STD 1050-1996             | I&C Equipment Grounding   | [ ] <sup>a,c,e</sup>                          |
| 332              | IEEE STD 1058.1-1987           | SW Project Management Plans   | [ ] <sup>a,c,e</sup>                          |
| 333              | IEEE STD 1074-2006             | SW Life Cycle Processes   | [ ] <sup>a,c,e</sup>                          |
| 335              | IEEE STD 12207.0-1996          | SW Life Cycle Processes   | [ ] <sup>a,c,e</sup>                          |
| 336              | IEEE STD 15288-2004            | System Life Cycle Processes   | [ ] <sup>a,c,e</sup>                          |
| 337              | IEEE STD 1540-2001             | SW Risk Management  | [ ] <sup>a,c,e</sup>                          |
| 339              | IEEE STD 323-2003              | Nuclear Power Class 1E Equipment  | [ ] <sup>a,c,e</sup>                          |

| Reference Number | Document ID           | Subject  | Applicability to This Topical Report Revision |
|------------------|-----------------------|--|---|
| 342              | IEEE STD 344-2004     | Seismic Qualification of Class 1E Equipment                        | [ ] <sup>a,c,e</sup>                          |
| 343              | IEEE STD 352-1987     | Reliability Analysis of Safety Systems                             | [ ] <sup>a,c,e</sup>                          |
| 346              | IEEE STD 384-1992     | Independence of Class IE Equipment and Circuits                    | [ ] <sup>a,c,e</sup>                          |
| 350              | IEEE STD 577-2004     | Reliability Analysis in the Design and Operation of Safety Systems | [ ] <sup>a,c,e</sup>                          |
| 353              | IEEE STD 627-1980     | Qualification of Equipment Used in Nuclear Facilities              | [ ] <sup>a,c,e</sup>                          |
| 356              | IEEE STD 7-4.3.2-2003 | Digital Computer Safety Systems Criteria                           | [ ] <sup>a,c,e</sup>                          |
| 357              | IEEE STD 828-2005     | SW Configuration Management  | [ ] <sup>a,c,e</sup>                          |
| 358              | IEEE STD 829-2008     | SW and System Test Documentation                                   | [ ] <sup>a,c,e</sup>                          |
| 359              | IEEE STD 830-1998     | SW Requirement Specifications                                      | [ ] <sup>a,c,e</sup>                          |
| 366              | ISA S67.04-1994       | Setpoints for Nuclear Safety-Related Instrumentation               | [ ] <sup>a,c,e</sup>                          |
| 368              | MIL-STD-461E          | Electromagnetic Interference Control                               | [ ] <sup>a,c,e</sup>                          |
| 127              | NUREG-0800            | Safety Analysis Report Review Plan                                 | [ ] <sup>a,c,e</sup>                          |
| 122              | NUREG/CR-6101         | SW Reliability and Safety  | [ ] <sup>a,c,e</sup>                          |
| 145              | RG 1.28 Rev. 4        | Quality Assurance Criteria   | [ ] <sup>a,c,e</sup>                          |
| 148              | RG 1.62 Rev. 1        | Protective Action Initiation                                       | [ ] <sup>a,c,e</sup>                          |
| 149              | RG 1.75 Rev. 3        | Independence of Electrical Safety Systems                          | [ ] <sup>a,c,e</sup>                          |
| 129              | RG 1.100 Rev. 3       | Seismic Qualification  | [ ] <sup>a,c,e</sup>                          |
| 130              | RG 1.105 Rev. 3       | Setpoints for Safety-Related Instrumentation                       | [ ] <sup>a,c,e</sup>                          |
| 133              | RG 1.152 Rev. 3       | Nuclear Digital Computer Safety Systems Criteria                   | [ ] <sup>a,c,e</sup>                          |
| 134              | RG 1.153 Rev. 1       | Nuclear Safety Systems Criteria                                    | [ ] <sup>a,c,e</sup>                          |
| 135              | RG 1.168 Rev. 2       | Nuclear SW Verification & Validation                               | [ ] <sup>a,c,e</sup>                          |
| 136              | RG 1.169 Rev. 1       | Nuclear SW Configuration Management                                | [ ] <sup>a,c,e</sup>                          |

| Reference Number | Document ID     | Subject                               | Applicability to This Topical Report Revision |
|------------------|-----------------|---------------------------------------|---|
| 137              | RG 1.170 Rev. 1 | Nuclear SW Test Documentation         | [ ] <sup>a,c,e</sup>                          |
| 138              | RG 1.171 Rev. 1 | Nuclear SW Unit Testing               | [ ] <sup>a,c,e</sup>                          |
| 139              | RG 1.172 Rev. 1 | Nuclear SW Requirement Specifications | [ ] <sup>a,c,e</sup>                          |
| 140              | RG 1.173 Rev. 1 | Nuclear SW Life Cycle Processes       | [ ] <sup>a,c,e</sup>                          |
| 141              | RG 1.180 Rev. 1 | I&C System Interference               | [ ] <sup>a,c,e</sup>                          |
| 143              | RG 1.209 Rev. 0 | I&C Environmental Qualification       | [ ] <sup>a,c,e</sup>                          |
| 151              | RG 5.71 Rev. 0  | Cyber Security Programs               | [ ] <sup>a,c,e</sup>                          |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 10 of 263  
Date: 04/14/2017

This page intentionally left blank.

### 3.0 DESCRIPTION OF THE NUPAC DIGITAL SAFETY I&C PLATFORM

#### 3.1 Overview

##### 3.1.1 Topical Report Scope of Coverage

NuPAC is designed to be used in systems of the highest level of importance in an NPP I&C architecture, that of nuclear safety-related systems, for example, a Reactor Protection System. Therefore, this topical report demonstrates that the NuPAC equipment and development process satisfy the needs for protection, control, and mitigation for these types of systems within the scope of coverage of this report.

The scope of coverage of this report is the design basis and the design of:

- The hardware components described in Section 3.1.4, and described in detail in Section 3.2. This includes:
  - the chassis, all necessary wiring, interconnections, and its cooling
  - the backplane (mid-plane)
  - the Rear Transition Module,
  - The Generic Logic Module (GLM), including:
    - the family of six I/O mezzanine cards
    - the logic mezzanine, containing the Core and Application-specific PLDs
    - the carrier card
    - GLM power distribution and power auctioneering.
- The Core Programmable Logic (PL) on the logic mezzanine (of the Core PLD/FPGA), as described in Section 3.3.1, 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.

Any item not listed above is not covered by this report. For clarity, the following partial list of elements/components that are not covered:

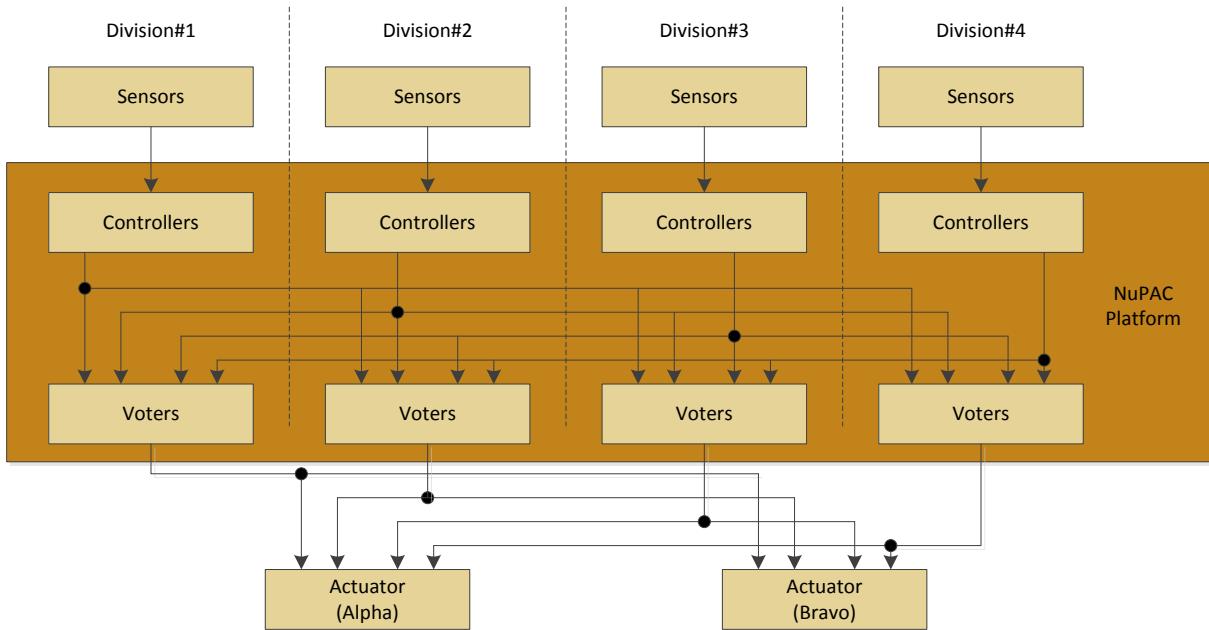
- Power supplies (external power source and cabinet-level)
- Application-specific (plant-specific) PL; note, however, that the AS PLD/FPGA is included as a hardware component
- Class 1E/non-Class 1E isolation
- Data communications outside of NuPAC (safety and non-safety)

- Safety-related display

For additional clarity, this topical report does not address system-level or application-specific topics.

### 3.1.2 NuPAC System Context

NPP protection and mitigation I&C safety systems are composed primarily of sensors, controllers (control electronics) including the voters (logic), and actuators. A simplified block diagram for a four-division, safety critical system is provided in Figure 3.1.2-1. The NuPAC system, as documented in this report, is used for the safety-related “controller” (control electronics) and “voter” (coincidence electronics) portions of the safety system. Input signals to NuPAC are obtained from sensors or discrete inputs located throughout the plant. The controllers would then send the status of the sensors to the divisional “voters”. Each voter compares the sensor status from the four controllers and decides whether to trip its outputs if two out of the four (2oo4) controllers vote to trip. These signals are then processed within NuPAC, described in detail below. After processing within NuPAC, the results are then sent out to the plant, typically to some form of actuator (for motors, valves, breakers, etc.).



*Figure 3.1.2-1. NuPAC Context*

### 3.1.3 Architecture

The NuPAC platform is an advanced, FPGA-based platform but is functionally and physically similar to commercially available programmable logic controllers (PLCs). However, the decentralized NuPAC FPGA-based architecture provides a unique paradigm akin to legacy NPP hardware-based solutions (e.g., analog measurement and trip modules).

An early development trade study concluded to avoid use of microprocessors and software in the NuPAC platform in favor of a true hardware-based solution using firmware. The physical size of a true hardware-based solution resulted in a solution in which FPGA devices were used to realize hardware structures. Although the

NuPAC platform is a FPGA-based product, the development process for the FPGA programmable logic follows accepted software development guidance, as described in Section 5.0.

The complexity and enhanced capability of FPGA products have made it possible to build, or to embed, whole microprocessor cores into an FPGA. This advance in programmable logic devices (PLDs) has resulted in a blurring of the lines between what was traditionally considered a software product and a programmable logic (PL) product. The cooperative development stayed true to the original intent of using PL as a method of producing hardware. Microprocessor-based structures are avoided in favor of discrete hardware based solutions.

The NuPAC platform contains no embedded software. Its design replaces the main operating loop (MOL) of a typical microprocessor-based platform by making use of dedicated independent state machines. The use of PL-based state machines is inherently safer than a reliance on microprocessors. The use of dedicated state machines also results in a distributed architecture that greatly improves processing throughput while simplifying verification and validation activities. In general, complex instruction sets, and the attendant risk of miss-operation that these instruction sets introduce, are avoided in the NuPAC platform design.

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 (Figure 3.1.3-1). Each GLM provides the capability to accomplish input/output processing, customizable control logic, diagnostics, and data communication.

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



***Figure 3.1.3-1. Generic Logic Module Configuration***

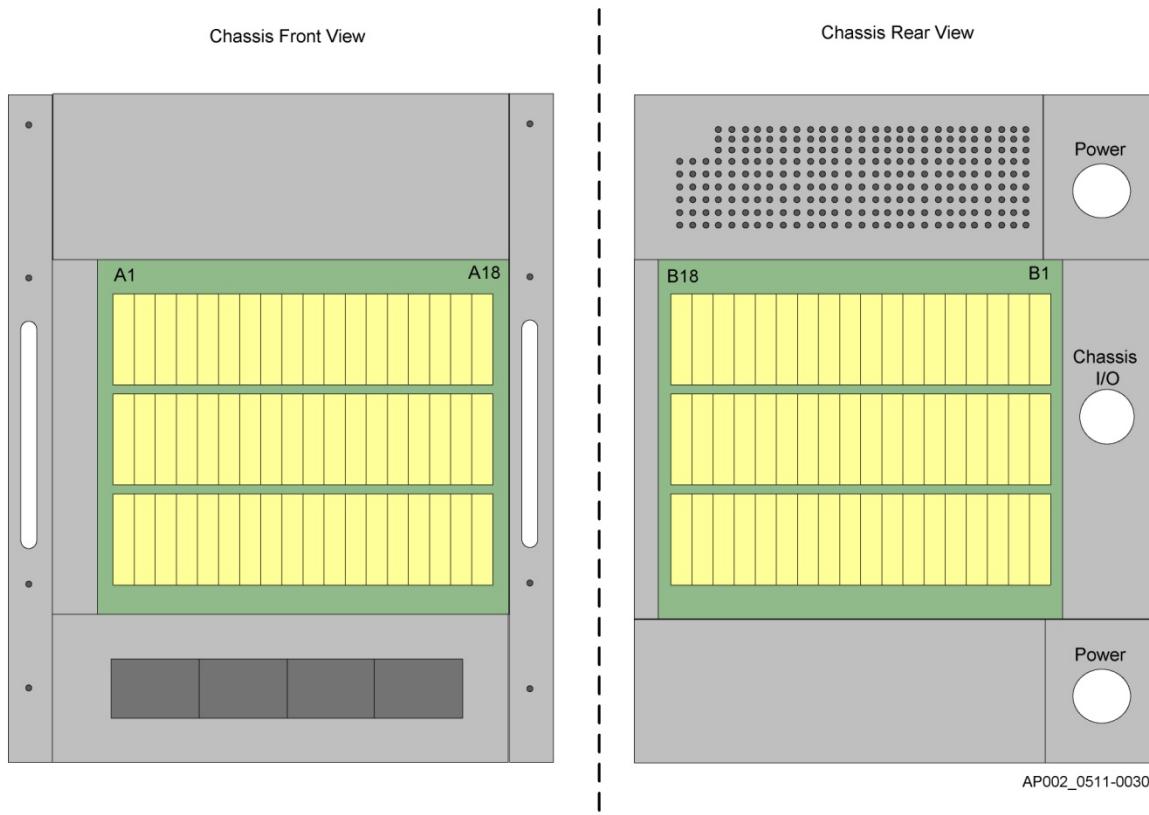
The Logic Mezzanine provides a logic solving capability implemented using two FPGAs. The Logic Mezzanine hosts a non-configurable FPGA and a configurable FPGA. The non-configurable FPGA, known as the Core FPGA or Core PLD, is utilized for general infrastructure-like logic. The Core PLD is reusable logic 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 GLMs are chassis installed. The GLMs are front-loaded and interface to a backplane (more accurately a mid-plane) within the chassis.

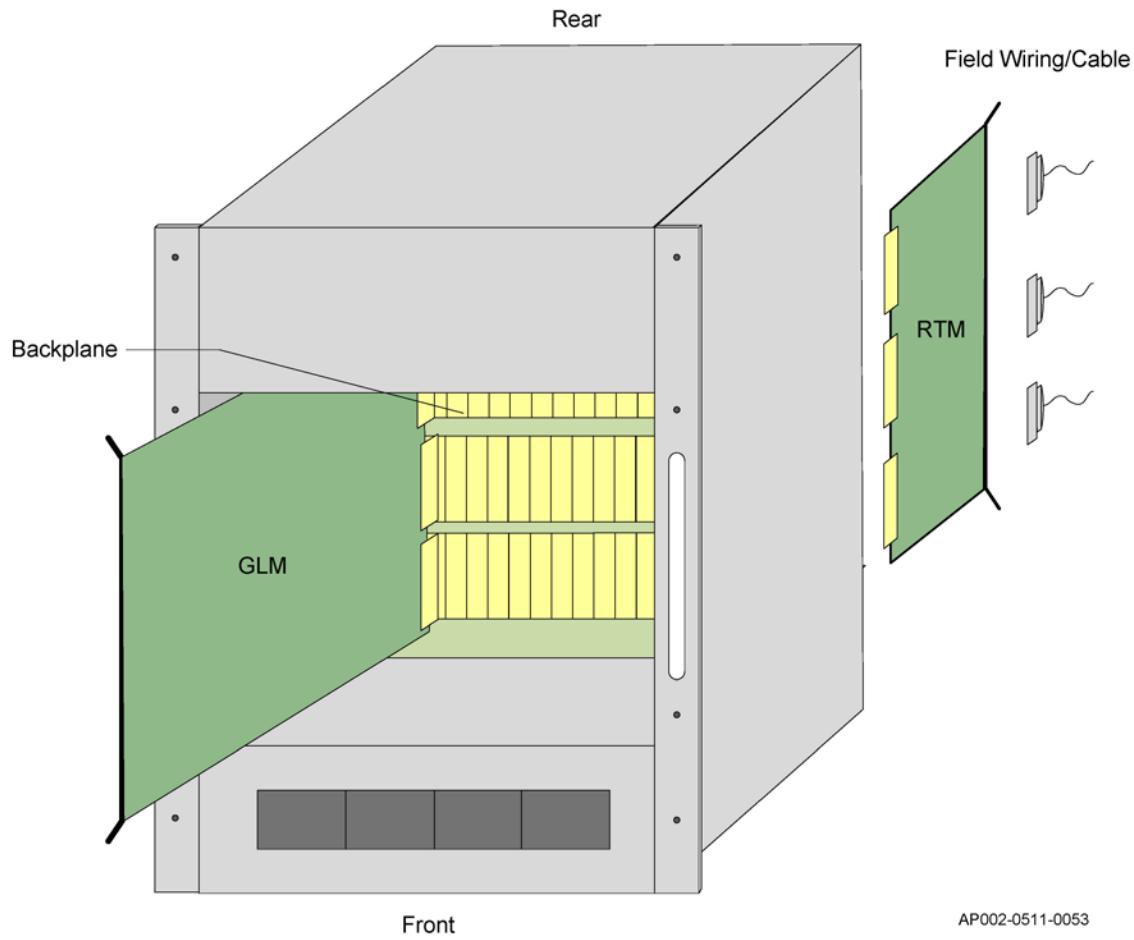
The chassis also supports Rear Transition Modules (RTMs), which plug into the back (rear) of the chassis (Figures 3.1.3-2 and -3) in slot locations that match the front-loaded GLMs. The RTMs and GLMs are interconnected through connectors on the backplane (Figure 3.1.3-4). The RTM interfaces field input 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).

Additional architecture details may be found in the NuPAC System Description NuPAC\_SYS610000-001 (Reference 727).



*Figure 3.1.3-2. Chassis*



AP002-0511-0053

*Figure 3.1.3-3. Chassis Installed GLMs and RTMs*



*Figure 3.1.3-4. GLM/Backplane/RTM Configuration*

### 3.1.4 Subject Components

Table 3.1.4-1 summarizes the qualified hardware components covered by this topical report as well as the programmable logic configuration items to be provided in the NuPAC Integration and Test Summary Report, NuPAC\_TR610000-100 (**Reference 730**).

*Table 3.1.4-1. Qualified Components*

| 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                          |

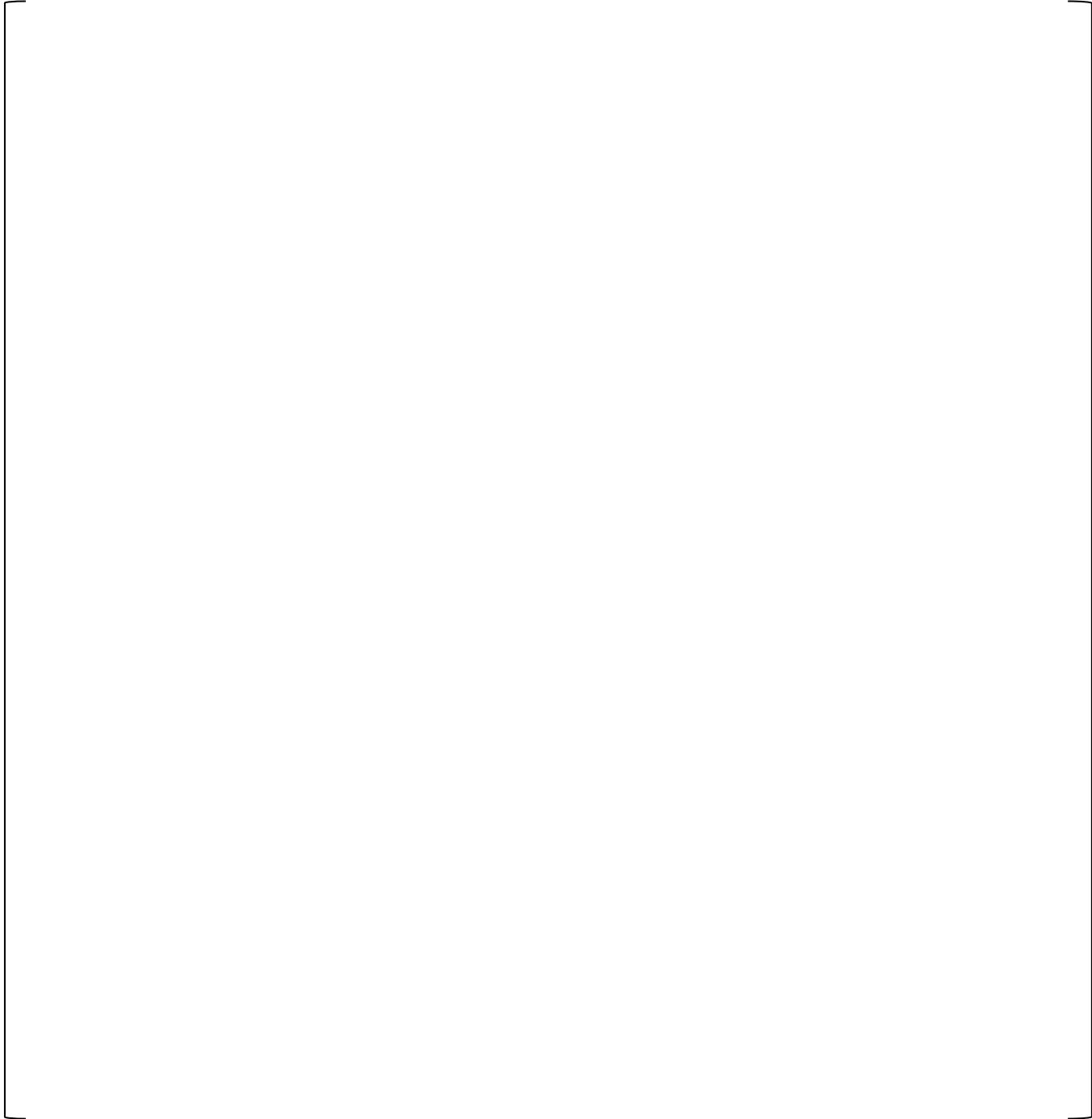
### 3.2 Hardware

From its inception, the NuPAC platform has been designed to be used in NPP I&C safety systems. The NuPAC platform utilized EPRI TR-107330 (**Reference 312**) guidance for functional and performance requirements. In addition, the NuPAC platform has been designed specifically to satisfy the environmental withstand envelope of EPRI TR-107330 when tested with the guidance identified in USNRC RG 1.209, USNRC RG 1.100 and USNRC RG 1.180 (**Reference 141**). The NuPAC platform is suitably rugged for NPP design basis events and long service life. With respect to reliability, electrical components used on the circuit card assemblies have been de-rated in terms of maximum electrical stress applied under worst-case conditions, including a [ ]<sup>a,c,e</sup> continuous operating environment cabinet internal temperature and [ ]<sup>a,c,e</sup> internal chassis temperature. The resultant reliability, combined with the NuPAC platform's extensive Built-In-Test (BIT) features, yields a highly available and safe system.

#### 3.2.1 Generic Logic Modules

The Generic Logic Module (GLM) is a circuit card assembly (shown previously in Figure 3.1.2-1) which consists of a Carrier Card, a Logic Mezzanine, and up to eight I/O mezzanines of which there are six variants. Limitations exist for power consumption [ ]<sup>a,c,e</sup> and weight [ ]<sup>a,c,e</sup>. Each GLM can be thought of as an entire PLC on a single card. Other than sharing the same input power, all GLMs within a chassis can function completely independent from one another. Each GLM offers the capability to accomplish input/output processing, control logic, diagnostics, and data communication. Figure 3.2.1-1 shows GLM components and assembly; Figure 3.2.1-2 shows a basic block diagram of the GLM.

*Figure 3.2.1-1. GLM Components and Assembly*



***Figure 3.2.1-2. GLM Block Diagram***

The GLM interfaces with signals external to the chassis through the RTM. The types of signals a GLM can process are identified in Table 3.2.1-1.

**Table 3.2.1-1. GLM Functions**

| Ref No. | I/O Type                        | Signal Direction | Additional Info (Range/Transmission Rate/etc.)       |
|---------|---------------------------------|------------------|--|
| 1       | Serial RS-422/485               | Input            | 9600 bps to 5 Mbps                                   |
| 2       | Analog Voltage                  | Input            | 0 – 5 VDC  |
| 3       | Analog Voltage                  | Input            | 0 – 10 VDC   |
| 4       | Analog Current                  | Input            | 4 – 20 mA  |
| 5       | Analog Current                  | Input            | 10 – 50 mA   |
| 6       | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 2-wire, USA Standard      |
| 7       | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 2-wire, European Standard |
| 8       | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 3-wire, USA Standard      |
| 9       | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 3-wire, European Standard |
| 10      | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 4-wire, USA Standard      |
| 11      | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 4-wire, European Standard |
| 12      | Analog Thermocouple Temperature | Input            | Type E, 0 to 1000°C (32 to 1832 °F)                  |
| 13      | Analog Thermocouple Temperature | Input            | Type J, 0 to 1200°C (32 to 2192 °F)                  |
| 14      | Analog Thermocouple Temperature | Input            | Type K, 0 to 1300°C (32 to 2372 °F)                  |
| 15      | Analog Thermocouple Temperature | Input            | Type B, 250 to 1800°C (482 to 3272 °F)               |
| 16      | Analog Thermocouple Temperature | Input            | Type N, 0 to 1250°C (32 to 2282 °F)                  |
| 17      | Analog Thermocouple Temperature | Input            | Type R, 0 to 1700°C (32 to 3092 °F)                  |
| 18      | Analog Thermocouple Temperature | Input            | Type S, 0 to 1700°C (32 to 3092 °F)                  |
| 19      | Analog Thermocouple Temperature | Input            | Type T, 0 to 400°C (32 to 752 °F)                    |
| 20      | Discrete AC                     | Input            | 120 VAC RMS  |
| 21      | Discrete AC                     | Input            | 24 VAC RMS   |
| 22      | Discrete DC                     | Input            | 125 VDC  |
| 23      | Discrete DC                     | Input            | 48 VDC   |
| 24      | Discrete DC                     | Input            | 24 VDC   |
| 25      | Discrete DC                     | Input            | 15 VDC   |
| 26      | Discrete DC                     | Input            | 12 VDC   |
| 27      | Discrete DC                     | Input            | 5 VDC (TTL input switching levels)                   |
| 28      | Discrete AC                     | Output           | 120 VAC RMS  |
| 29      | Discrete AC                     | Output           | 24 VAC RMS   |
| 30      | Discrete DC                     | Output           | 125 VDC  |
| 31      | Discrete DC                     | Output           | 48 VDC   |
| 32      | Discrete DC                     | Output           | 24 VDC   |
| 33      | Discrete DC                     | Output           | 15 VDC   |
| 34      | Discrete DC                     | Output           | 12 VDC   |
| 35      | Discrete DC                     | Output           | 5 VDC (TTL output switching levels)                  |
| 36      | Pulse <sup>1</sup>              | Input            | 20Hz – 100,000Hz (or 10us – 50ms period)             |
| 37      | Serial RS-422/485 <sup>2</sup>  | Output           | 9600 bps to 5 Mbps                                   |
| 38      | Analog Voltage                  | Output           | 0 – 5 VDC  |
| 39      | Analog Voltage                  | Output           | 0 – 10 VDC   |
| 40      | Analog Current <sup>3</sup>     | Output           | 4 – 20 mA  |

[

]a,c,e

As shown previously in Figure 3.1.3-3, the GLMs are installed from the front of the chassis. Each GLM plugs into three backplane connectors that connect each GLM to power—hardwired low-voltage differential signaling (LVDS) communication within the chassis via the backplane—and field input and output signals—including discrete, analog, and serial communication signals—via the Rear Transition Modules (RTMs).

### 3.2.1.1 Carrier Card, P/N 610310

The 610310 Carrier Card is a 360mm high and 340mm deep 9U size D Eurocard format circuit card assembly.

[

]<sup>a,c,e</sup>

The Carrier Card (Figure 3.2.1.1-1) is a circuit card providing nine mezzanine interfaces—one Logic Mezzanine and eight I/O mezzanine interfaces. The Carrier Card mechanically and electrically interfaces the Logic Mezzanine with the I/O mezzanine, while providing connectors to other peripheral interfaces via the chassis backplane. The Carrier Card facilitates a modular approach to system assembly because each Carrier Card is populated with one Logic Mezzanine and any combination of I/O mezzanines (up to eight). [

]<sup>a,c,e</sup> The integration of a Logic Mezzanine and I/O mezzanines forms an intelligent single-board system, the GLM. A simplified functional block diagram of the Carrier Card is depicted in Figure 3.2.1-4.



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 24 of 263  
Date: 04/14/2017



*Figure 3.2.1-3. Carrier Card*



**Figure 3.2.1-4. Carrier Card Simplified Functional Block Diagram**

The power interface is via backplane connectors. Onboard the Carrier Card, redundant input power is fused and diode auctioneered. Hot-swapping circuitry is employed to allow a GLM to be installed in or removed from a powered chassis without damage. From the auctioneered input power, onboard power supplies develop the required power for the local circuitry. In addition, power-sequencing circuitry controls the power up of I/O mezzanines to manage inrush currents.

The redundant input power, auctioneered power, and onboard derived power supply voltages are monitored for correct voltages. In addition, fuse monitoring is provided for both redundant input power sources. Temperature sensing is also provided to monitor forced air fan cooling effectiveness.

The Carrier Card provides an interface between the Logic Mezzanine and the circuitry of the I/O mezzanines and the Carrier Card itself. [

]a,c,e

[

]<sup>a,c,e</sup>

The backplane interface also links field input and output signals to the Carrier Card. Field input and output signals, including serial communication signals, are linked to the Carrier Card through the backplane connectors which interface with the RTM, which in-turn mate with the field connections (RTM card-top connectors). Onboard the Carrier Card, the field input and output signals are routed to the respective I/O mezzanines. The input and output signals interface to the I/O mezzanines through the respective board-to-board connectors.

The backplane interface also passes dedicated chassis/backplane signals to the Carrier Card. The signals include slot identification, chassis identification, memory write enable, and four system monitors.

[

]<sup>a,c,e</sup>

The Carrier Card provides LED type indicators that are visible from the GLM front panel (card-top). [

]<sup>a,c,e</sup>

The carrier card provides the output driver for each LED. The GLM logic located on the logic mezzanine card provides the ON/OFF output command. LED control signals are output from the Core PLD and passed to the Carrier Card through the board-to-board connectors. Onboard the Carrier Card, buffer circuits drive the LEDs.

Additional design details regarding the carrier card functionality are included in the NuPAC GLM Design Analysis Report (**Reference 710**).

### 3.2.1.2 I/O Mezzanines

The I/O mezzanines are modular circuit card assemblies physically based on a modified version of an industry standard form factor, [

]<sup>a,c,e</sup> The I/O mezzanines are approximately three inches by two inches. The connectors are installed parallel to the short side, almost at each end of the printed circuit boards. To avoid incorrect installation, one connector is male and the other connector is female. Figure 3.2.1-5 shows a typical I/O mezzanine.



*Figure 3.2.1-5. Typical I/O Mezzanine*

There are six variants of I/O mezzanines. Each input mezzanine provides a single input, whether analog, pulse, or discrete. Each output mezzanine provides a single output, whether analog or discrete. The serial communication mezzanine provides one receiver and one transmitter, each functionally independent of each other.

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

Each I/O mezzanine has onboard power management circuitry to galvanically isolate the mezzanine power from the Carrier Card power and provide the required regulated power for its respective circuitry.

All field inputs and outputs on the I/O mezzanines are made through the Carrier Card, Backplane, and RTM. All field inputs and outputs on the I/O mezzanines are isolated electrically from all other I/O mezzanines in the same GLM and in the same chassis. Isolation is accomplished with a high speed digital isolator with a maximum working insulation voltage of 560 Volts peak. Each I/O mezzanine has an isolated common, which is wired appropriately through the backplane connectors and RTM to field wiring.

### 3.2.1.2.1 Analog Input Mezzanine, P/N 610330

The Analog Input Mezzanine, P/N 610330, is a circuit card with the capability to monitor a single differential analog input. The Analog Input Mezzanine is capable of accepting either an analog input voltage or an analog input current, but not both at the same time. The Analog Input Mezzanine is capable of interfacing to any one of the voltage or current ranges identified in Table 3.2.1-2. The current input employs surge protection and the voltage input employs both surge and ElectroStatic Discharge (ESD) protection.

[

]<sup>a,c,e</sup>

*Table 3.2.1-2. Analog Input Mezzanine Functions*

| Ref No. | I/O Type       | Signal Direction | Additional Info (Range/Transmission Rate/etc.) |
|---------|----------------|------------------|--|
| 2       | Analog Voltage | Input            | 0 – 5 VDC                                      |
| 3       | Analog Voltage | Input            | 0 – 10 VDC                                     |
| 4       | Analog Current | Input            | 4 – 20 mA                                      |
| 5       | Analog Current | Input            | 10 – 50 mA                                     |
| 27      | Discrete DC    | Input            | 5 VDC (TTL input switching levels)             |



*Figure 3.2.1-6. Analog Input Mezzanine Simplified Block Diagram*

Additional design details are included in the NuPAC GLM Design Analysis Report (**Reference 710**).

### 3.2.1.2.2 Discrete/Pulse Input Mezzanine, P/N 610340

The Discrete/Pulse Input Mezzanine, P/N 610340, is a circuit card with the capability to monitor a single discrete or pulse input. The Discrete/Pulse Input Mezzanine is capable of accepting either a discrete AC input voltage, or a DC input voltage, or digital input pulses, but not more than one at the same time (i.e., mutually

exclusive). The Discrete/Pulse Input Mezzanine is capable of interfacing to any one of the voltage ranges identified in Table 3.2.1-3. Both the discrete input and pulse input employ surge and ESD protection.

A pulse input range of [

]<sup>a,c,e</sup>, with an operating frequency range of 20 Hz to 100 KHz. [

]<sup>a,c,e</sup>

**Table 3.2.1-3. Discrete/Pulse Input Mezzanine Functions**

| Ref No. | I/O Type           | Signal Direction | Additional Info (Range/Transmission Rate/etc.) |
|---------|--------------------|------------------|--|
| 20      | Discrete AC        | Input            | 120 VAC RMS                                    |
| 21      | Discrete AC        | Input            | 24 VAC RMS                                     |
| 22      | Discrete DC        | Input            | 125 VDC  |
| 23      | Discrete DC        | Input            | 48 VDC   |
| 24      | Discrete DC        | Input            | 24 VDC   |
| 25      | Discrete DC        | Input            | 15 VDC   |
| 26      | Discrete DC        | Input            | 12 VDC   |
| 36      | Pulse <sup>1</sup> | Input            | 20Hz – 100,000Hz (or 10us – 50ms period)       |

1 [

]<sup>a,c,e</sup>



*Figure 3.2.1-7. Discrete/Pulse Input Mezzanine Simplified Block Diagram*

Additional design details are included in the NuPAC GLM Design Analysis Report (**Reference 710**).

### 3.2.1.2.3 Temperature Input Mezzanine, P/N 610350

The Temperature Input Mezzanine, P/N 610350, is a circuit card with the capability to monitor a single temperature input. The Temperature Input Mezzanine is capable of accepting either a resistance temperature detector (RTD) or a thermocouple input, but not both at the same time. The Temperature Input Mezzanine is capable of interfacing to any one of the thermocouple types identified in Table 3.2.1-4. Both the temperature input and RTD drive output employ surge and ESD protection.

[

]<sup>a,c,e</sup>

**Table 3.2.1-4. Temperature Input Mezzanine Functions**

| Ref No. | I/O Type                        | Signal Direction | Additional Info (Range/Transmission Rate/etc.)       |
|---------|---------------------------------|------------------|--|
| 6       | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 2-wire, USA Standard      |
| 7       | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 2-wire, European Standard |
| 8       | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 3-wire, USA Standard      |
| 9       | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 3-wire, European Standard |
| 10      | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 4-wire, USA Standard      |
| 11      | Analog RTD Temperature          | Input            | 0 – 800 °C (32 – 1472 °F), 4-wire, European Standard |
| 12      | Analog Thermocouple Temperature | Input            | Type E, 0 to 1000°C (32 to 1832 °F)                  |
| 13      | Analog Thermocouple Temperature | Input            | Type J, 0 to 1200°C (32 to 2192 °F)                  |
| 14      | Analog Thermocouple Temperature | Input            | Type K, 0 to 1300°C (32 to 2372 °F)                  |
| 15      | Analog Thermocouple Temperature | Input            | Type B, 250 to 1800°C (482 to 3272 °F)               |
| 16      | Analog Thermocouple Temperature | Input            | Type N, 0 to 1250°C (32 to 2282 °F)                  |
| 17      | Analog Thermocouple Temperature | Input            | Type R, 0 to 1700°C (32 to 3092 °F)                  |
| 18      | Analog Thermocouple Temperature | Input            | Type S, 0 to 1700°C (32 to 3092 °F)                  |
| 19      | Analog Thermocouple Temperature | Input            | Type T, 0 to 400°C (32 to 752 °F)                    |

**Figure 3.2.1-8. Temperature Input Mezzanine Simplified Block Diagram**

Additional design details are included in the NuPAC GLM Design Analysis Report (**Reference 710**).

### 3.2.1.2.4 RS-422/485 Mezzanine, P/N 610360

The RS-422/485 Mezzanine, P/N 610360, is a circuit card with the capability to provide a serial data interface. The RS-422/485 Mezzanine provides one transmit port and one receive port. Transmit port and receive port are electrically independent of each other and galvanically isolated from external equipment. [

]<sup>a,c,e</sup>

At the maximum data rate of [ ]<sup>a,c,e</sup>, the transmit port provides the drive capability to permit communication over twisted pair wire up to a recommended maximum length [ ]

[ ]<sup>a,c,e</sup> The differential driver outputs are protected from short circuits.

[

]<sup>a,c,e</sup>

**Table 3.2.1-5. RS-422/485 Mezzanine Functions**

| Ref No. | I/O Type          | Signal Direction | Additional Info (Range/Transmission Rate/etc.) |
|---------|-------------------|------------------|--|
| 1       | Serial RS-422/485 | Input            | [ ]  |
| 37      | Serial RS-422/485 | Output           | [ ] <sup>a,c,e</sup>                           |

[

]<sup>a,c,e</sup>

a,c,e



**Figure 3.2.1-9. RS-422/485 Mezzanine Simplified Block Diagram**

Additional design details are included in the NuPAC GLM Design Analysis Report (**Reference 710**).

### 3.2.1.2.5 Analog Output Mezzanine, P/N 610370

The Analog Output Mezzanine, P/N 610370, is a circuit card with the capability of outputting a single differential analog output. The Analog Output Mezzanine is capable of providing either an analog output voltage or a loop-powered analog output current, but not both at the same time. The Analog Output Mezzanine is capable

of interfacing to any one of the voltage or current ranges identified in Table 3.2.1-6. Both the voltage output and current output employ surge protection.

The field I/O interface is via the Carrier Card through the board-to-board connectors. The scaled analog outputs are developed from the output of a digital-to-analog converter (DAC).

[

]<sup>a,c,e</sup>

For a current output, the output of a 16-bit DAC is applied to a two-wire current regulator, which generates a precisely controlled 4-20 mA current output. An external loop power supply (not included in this LTR) is required,

[<sup>a,c,e</sup> Like the field I/O, the loop power interface is via the Carrier Card through the board-to-board connectors. Circuitry limits the output current to approximately 32mA to protect the transmitter and loop power/measurement circuitry. ]

]<sup>a,c,e</sup>

The DAC features an internal reference, is monotonic, provides very good linearity, and minimizes undesired code-to-code transient voltages. The DAC incorporates a power-on-reset circuit that ensures its outputs power up at zero-scale until a valid code is written to it.

[

]<sup>a,c,e</sup>

**Table 3.2.1-6. Analog Output Mezzanine Functions**

| Ref No. | I/O Type       | Signal Direction | Additional Info (Range/Transmission Rate/etc.) |
|---------|----------------|------------------|--|
| 38      | Analog Voltage | Output           | 0 – 5 VDC                                      |
| 39      | Analog Voltage | Output           | 0 – 10 VDC                                     |
| 40      | Analog Current | Output           | 4 – 20 mA*                                     |
| 35      | Discrete DC    | Output           | 5 VDC (TTL output switching levels)            |

[

]<sup>a,c,e</sup>



**Figure 3.2.1-10. Analog Output Mezzanine Simplified Block Diagram**

Additional design details are included in the NuPAC GLM Design Analysis Report (**Reference 710**).

### 3.2.1.2.6 SSR Mezzanine, P/N 610380

The SSR Mezzanine, P/N 610380, is a circuit card with the capability of controlling either an AC or DC externally powered load. For AC-powered loads, the SSR is capable of switching 24 to 120 V<sub>AC</sub> RMS and is rated for continuous load currents in the range of [ ]<sup>a,c,e</sup>. For DC-powered loads, the SSR is capable of switching 12 to 125 V<sub>DC</sub> and is rated for continuous load currents in the range of [ ]<sup>a,c,e</sup>. The SSR's surge current rating exceeds [ ]<sup>a,c,e</sup>.

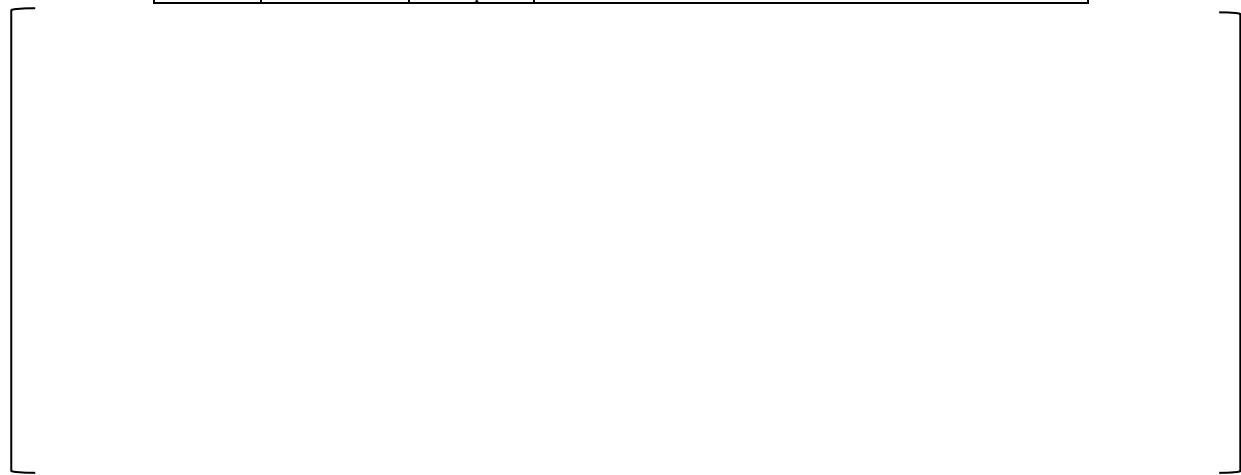
The SSR Mezzanine is capable of interfacing to any one of the voltage or current ranges identified in Table 3.2.1-7. The discrete output employs both surge and ESD protection.

[ ]<sup>a,c,e</sup>

Figure 3.2.1-11 shows the functional hardware blocks of the SSR Mezzanine. GLM functions previously identified in Table 3.2.1-1 that are allocated to the SSR Mezzanine are identified in Table 3.2.1-7.

**Table 3.2.1-7. SSR Mezzanine Functions**

| Ref No. | I/O Type    | Signal Direction | Additional Info (Range/Transmission Rate/etc.) |
|---------|-------------|------------------|--|
| 28      | Discrete AC | Output           | 120 VAC RMS                                    |
| 29      | Discrete AC | Output           | 24 VAC RMS                                     |
| 30      | Discrete DC | Output           | 125 VDC  |
| 31      | Discrete DC | Output           | 48 VDC   |
| 32      | Discrete DC | Output           | 24 VDC   |
| 33      | Discrete DC | Output           | 15 VDC   |
| 34      | Discrete DC | Output           | 12 VDC   |

**Figure 3.2.1-11. SSR Mezzanine Simplified Block Diagram**

Additional design details are included in the NuPAC GLM Design Analysis Report (**Reference 710**).

### 3.2.1.3 Logic Mezzanine, P/N 610320

The 610320 Logic Mezzanine is a custom modular circuit card assembly. The Logic Mezzanine is shown in Figure 3.2.1.3-1.



***Figure 3.2.1-12. Logic Mezzanine***

The mezzanine has onboard power management circuitry to provide the required regulated power for its respective circuitry.

The Logic Mezzanine provides an interface to the circuitry of the Carrier Card, and by extension, the circuitry of the I/O mezzanines. The interface is via four board-to-board receptacle connectors. All carrier card connectivity to the logic mezzanine is to or from pins on the Core PLD. No connections from the Carrier Card are made directly to the ASPLD.

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

Additional design details are included in the NuPAC GLM Design Analysis Report (**Reference 710**).

### 3.2.1.4 Hardware Acceptance and Design Verification Testing

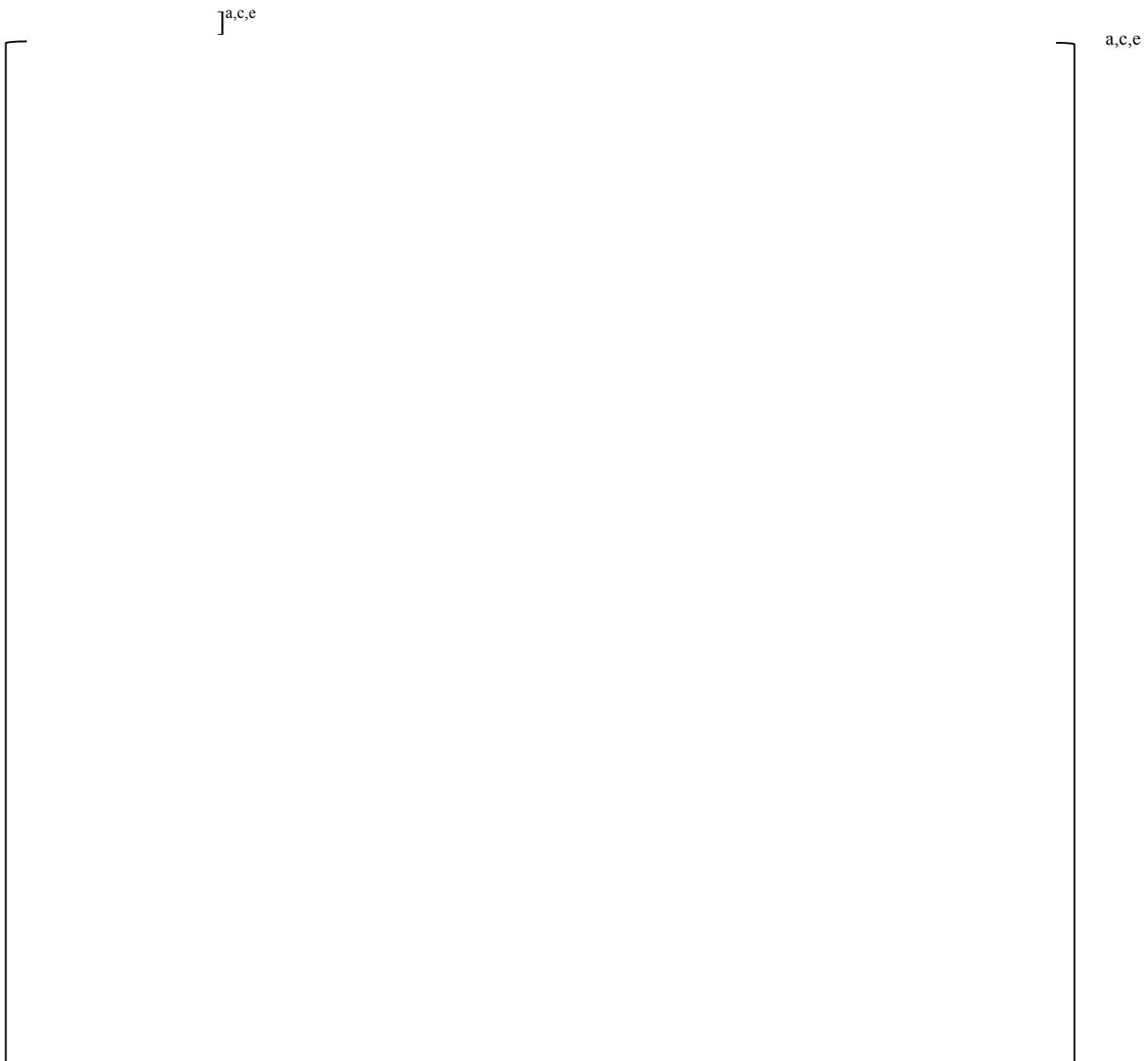
Prior to qualification testing, the NuPAC platform components underwent a series of acceptance tests. Acceptance test procedures were developed for each level of assembly, which includes the Carrier Card, Logic Mezzanine, individual I/O mezzanines, GLM, RTM, and chassis. These procedures are representative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

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 Test Specimen Configuration (TSC) DVT. DVT utilizes simulated inputs as required by the TSC to verify performance. The 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.

### 3.2.2 Rear Transition Module, P/N 610120

The 610120 RTM is a 360mm high and 80mm deep 9U size D Eurocard format circuit card assembly. [



**Figure 3.2.2-1. Rear Transition Module**

RTMs are installed from the rear of the chassis. A RTM plugs into the backplane in a slot location corresponding to each respective GLM, and thus the RTM is paired electrically with its corresponding GLM. RTMs provide a means of connecting the external field wiring to the inputs, outputs, and communication paths for

each GLM. [

]<sup>a,c,e</sup> The RTM provides jumpers for providing a path to chassis ground, isolated signal common, or floating for the external signal shield. There are no active or passive components on the RTM.

The RTMs attach to the backplane via three backplane connectors, explained in Section 3.1.3. [

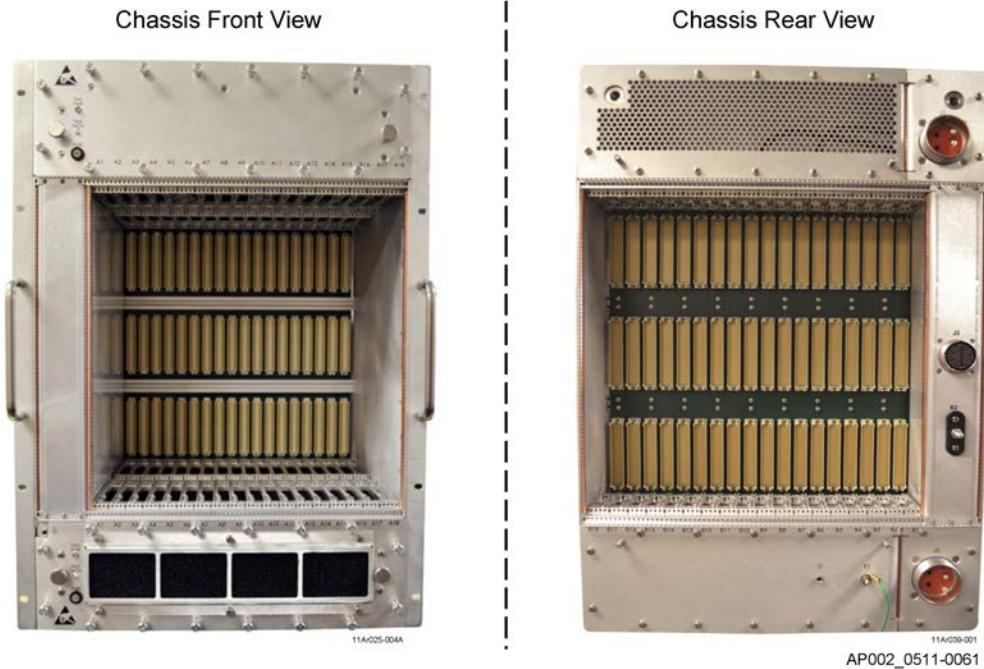
]<sup>a,c,e</sup>

Additional RTM design details are included in the Chassis/RTM Design Report (**Reference 709**).

### 3.2.3 Chassis, P/N 610100

The chassis, shown Figure 3.2.3-1, provides a structured, standards-based means to mount the NuPAC platform equipment in a standard 19-inch rack mount cabinet. [

]<sup>a,c,e</sup> The chassis is designed to provide a secure seismic structure. The chassis provides electromagnetic shielding.



*Figure 3.2.3-1. Chassis*

The chassis provides a structured means to mount up to 18 GLMs and their paired RTMs to the backplane (mid-plane) that runs vertically from side to side within the chassis, as shown in Figures 3.1.3-3 and 3.1.3-4.

The chassis provides slots with guides for mounting 18 GLMs, defined as A1 through A18. The chassis provides slots with guides for mounting 18 RTMs, defined as B1 through B18. The chassis provides additional slots for future expansion. Note that power supplies are not part of this LTR, and power is provided by external power supplies. All wiring to the NuPAC platform is attached to the rear of the chassis. Field inputs, outputs, and external communication ports interface by way of connectors on the RTMs. Redundant external power interfaces via two connectors integral to the chassis assembly itself. Miscellaneous chassis inputs and outputs interface via a third connector integral to the chassis assembly itself.

The chassis provides forced air fan cooling and air filtration for the GLMs. Integrated fan tray assemblies provide fan speed monitoring to provide remote alarms when fan failures occur. Two fan tray assemblies are provided, one on top and one on bottom. The effectiveness of the fans at controlling temperature is measured by temperature monitoring on each GLM. The cooling system is designed to maintain no greater than a [ ]<sup>a,c,e</sup> delta between the ambient environment outside of the chassis and the temperature within the chassis. The fan trays include an air filter which has a shelf life of three years and requires periodic cleaning.

The design of the NuPAC Chassis addresses seismic rigidity and electromagnetic shielding as required for nuclear safety applications.

Additional chassis design details are included in the Chassis/RTM Design Report (**Reference 707**).

### 3.2.3.1 Backplane

The backplane is a passive mid-plane, which is installed vertically within the chassis. The backplane allows installation of GLMs from the front of the chassis and RTMs from the rear. Each GLM is keyed to only one chassis and slot location. Within the chassis, the backplane is wired to the redundant external power supplies and miscellaneous chassis I/O connectors. The backplane electrically connects a GLM in the front to the power supplies, the GLM's paired RTM in the rear, and other GLMs installed within the chassis.

GLMs are plugged into three connectors in each backplane slot, as shown previously in Figure 3.1.3-4. The connectors provide the redundant [ ]<sup>a,c,e</sup> power supply connections, electrical communication interconnections between the GLMs, and the write protection and miscellaneous chassis input/output connections. The connectors provide electrical interconnections between the RTM and the GLM for interconnecting field input/output/communication signals with GLM I/O mezzanine slots.

The backplane connects the redundant regulated DC power and ground planes to the 18 GLMs. The backplane and its connectors provide sufficient current carrying capacity to provide [ ]<sup>a,c,e</sup> of power to each GLM.

The backplane provides built-in communication paths to interface GLMs within a chassis. The backplane communication is described in Section 3.4.1.

The backplane provides for distribution of the non-volatile memory lock signal (write protect input) to all GLMs within the chassis. The write protect input inhibits any write to the safety critical non-volatile memory when write protect is active.

The backplane provides each of the 18 GLM slots with a 5-bit binary slot address, which each GLM uses to verify, via Core PLD logic that it is installed in the correct slot. [ ]<sup>a,c,e</sup>

Valid GLM addresses start at 1 and end at 18.

The backplane also provides a 7-bit binary chassis address, which each GLM uses to verify that it is installed in the correct chassis. [ ]<sup>a,c,e</sup>

The chassis address values are determined at the plant specific application design phase.

Additional chassis design details are included in the Chassis/RTM Design Report (**Reference 709**).

### 3.2.4 Power Supply and Power Supplies (For Information Only)

The NuPAC platform chassis design provides provisions for utilizing redundant [ ]<sup>a,c,e</sup> power supply inputs; the mounting is chassis external. This capability to use redundant power supplies is included in the design of NuPAC but the actual power supplies are not part of this LTR.

For the NuPAC platform qualification, each chassis is powered by two independent supplies external to the NuPAC test specimen and are not considered part of the qualification unit. Each power supply providing a [ ]<sup>a,c,e</sup>

output that shall be capable of providing the full power requirements for the chassis. The NuPAC platform requires the following minimum characteristics from each power supply:

- Normal operating voltage tolerance of [ ]<sup>a,c,e</sup> maximum
- Maximum ripple voltage of [ ]<sup>a,c,e</sup>
- Maximum abnormal output voltage of [ ]<sup>a,c,e</sup> during a power supply overvoltage failure.

Under normal conditions, power may be drawn from one power supply. If that power supply or its supporting power source fails, the other power supply will support the full power requirements of the chassis.

### 3.3 Programmable Logic Architecture

The Logic Mezzanine consists of two FPGA processing elements—the Core Programmable Logic Device (PLD) and the Application Specific PLD (ASPLD). Each PLD hosts a programmable logic configuration item (PLCI). Figure 3.3-1 shows major functions of each PLCI.



*Figure 3.3-1. Programmable Logic Configuration Items*

The Core PLCI (or simply the “Core”) provides an I/O interface to the ASPLD. [

]<sup>a,c,e</sup> The AS PLCI designer can therefore concentrate on the plant-specific application instead of the infrastructure-like details such as parity, baud rate, routing, and BIT of I/O. [

]<sup>a,c,e</sup>

The AS PLCI provides plant-specific application functionality. [

]<sup>a,c,e</sup>

### 3.3.1 Core Programmable Logic Configuration Item

The following subsections provide a high-level summary of the Core PLCI architecture.

Figure 3.3.1-1 provides a functional architecture of the Core PLCI. The architecture is presented in terms of functional modules within the Core PLD. Additional Core PLCI architecture details are included in the Core PLCI Development Specification (**Reference 717**).



*Figure 3.3.1-1. Core PLCI Functional Architecture*



### 3.3.1.1 Core PLD Module

[

]<sup>a,c,e</sup>

#### 3.3.1.1.1 I/O Mezzanine Controllers

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 3.3.1.1.2 ASPLD Interface Controller

[

]<sup>a,c,e</sup>

### 3.3.1.1.3 Data Handlers

[

]<sup>a,c,e</sup>

### 3.3.1.1.4 Backplane Interface Controllers

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 3.3.1.1.5 Diagnostic/Maintenance Controller

[

]<sup>a,c,e</sup>

### 3.3.1.1.6 Non-Volatile Static RAM (NVSRAM) Controller

[

]<sup>a,c,e</sup>

## 3.3.2 Application Specific Programmable Logic Configuration Item (For Information Only)

The following subsections provide a high-level summary of the AS PLCI architecture.

Figure 3.3.2-1 provides a basic block diagram of the AS PLCI. The architecture is presented in terms of functional modules within the ASPLD. Note, that the Application-specific PL (ASPL) depends on the safety-critical system to be implemented, i.e., is plant-specific. As such, it is not included in this report for review. The ASPL will be created for each system application and will be reviewed at that time.



*Figure 3.3.2-1. AS PLCI Programmable Logic Block Diagram*

### 3.3.2.1 ASPLD Module

[

]<sup>a,c,e</sup>

#### 3.3.2.1.1 ASPLD Interface Controller

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 3.3.2.1.2 Diagnostic/Maintenance Controller

[

]<sup>a,c,e</sup>

### 3.3.2.1.3 SRAM Controller

[

]<sup>a,c,e</sup>

### 3.3.2.1.4 Plant-Specific Application Logic

The ASPLD implements the plant-specific application logic, which is responsible for the unique application specific processing in the ASPLD.

In general, the plant-specific application logic processes input data from backplane serial messages and/or I/O mezzanine inputs, and then provides outputs in the form of backplane serial messages and/or I/O mezzanine output commands. Examples of this processing include the following:

- Gathering input data from multiple I/O mezzanines, validating each one via range-checking against plant-specific limits, analyzing the validated data, and formatting the results into a backplane serial message to another GLM in the same chassis

- Accumulating messages from other GLMs within the same chassis, formatting an aggregate message and sending it to a RS-422/485 Mezzanine that is connected to a GLM in a different chassis
- Receiving an aggregated message from another chassis via an RS-422/485 Mezzanine, separating it into individual messages, and sending them to other GLMs in the same chassis
- Receiving a backplane serial message from another GLM in the same chassis, validating the source and content, and formatting the data into an output command to an I/O mezzanine.

Many possible plant-specific application logic designs can be developed to comply with IEEE Standard 603 (**Reference 153**) and IEEE Standard 7-4.3.2 (**Reference 356**).

### 3.3.3 Built In Test (BIT)

The term Built In Test (BIT) refers to automated and periodic diagnostics performed by the NuPAC platform while the Core PLCI and ASPLCI perform their safety function. BIT functionality is integrated into the Core PLCI and undergoes the same level of verification as the rest of the Core logic by IV&V. If an error is detected by BIT and the error is identified as Applicable, as described below, the error is provided to the System Monitoring identified in section 3.3.1.1.5. Any impact to response time by BIT is accounted for in NuPAC Supporting Data for Response Time Analysis (**Reference 707**). All BIT discussed below is applicable to the GLM including communication type errors the ASPL will detect as well. Application Specific Programmable Logic will have BIT specific to the application in addition to the communication errors identified below.

Any errors detected by BIT are indicated on the front panel of the GLM as well as made available to the ASPL for generating alarms. The Core logic can (application specific) do the following upon the detection of an error:

- Set an applicable error flag and make the flag available to the ASPL
- Enter Fault Mode and set all outputs to a safe (de-energized) state.

All BIT errors have masks available. The masks are as follows:

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

BIT allows for detection of errors occurring in hardware and programmable logic of the NuPAC. The NuPAC FMEA, described in section 6.3.1 identifies the hardware failures detected by BIT.

The sections below provide a high level identification of the errors that are detected by BIT. Additional details can be found in NuPAC\_EDD610400-001, NuPAC Error Description Document – Core PLCI (**Reference 735**)

### 3.3.3.1 GLM BIT

#### 3.3.3.1.1 General BIT

Identified below are BIT error types that are applicable to a GLM regardless of the GLM configuration:

[

]<sup>a,c,e</sup>

#### 3.3.3.1.2 ASPLD Bus BIT

Identified below are BIT error types that the Core logic monitors on the ASPLD bus. The errors that BIT can detect ensure the data being transferred between the ASPL and the Core is valid.

[

]<sup>a,c,e</sup>

#### 3.3.3.2 General Memory BIT

Identified below are BIT error types that are applicable to memory.

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 3.3.3.3 I/O Mezzanine BIT

Identified below are BIT errors that are applicable to I/O Mezzanines:

[

]<sup>a,c,e</sup>

### 3.3.3.4 LVDS BIT

Identified below are BIT errors that are applicable to LVDS communications:

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 3.3.3.5 ASPL BIT Constraints

Identified below are minimum sets of BIT errors that will be applicable to any future ASPL that processes communications.

[

]<sup>a,c,e</sup>

## 3.4 Digital Communication

This section provides a general description of the NuPAC platform Digital communication capabilities and how they are applied to realize intra-divisional and inter-divisional serial communications within a safety I&C system. For the purposes of this LTR, NuPAC communication capabilities are described given the constraint that each communication originates at one GLM card and terminates at another GLM. The GLMs may be located within the same chassis or in completely different chassis.

### 3.4.1 Overview

The GLM assembly (or simply “GLM”) is the basic system component of the NuPAC platform. All functions are performed by one or more GLMs. Each GLM provides an option to communicate outside the NuPAC chassis to other equipment using serial communications. To provide a GLM with this

external communication capability requires the installation of one or more RS-422/485 Mezzanine. The RS-422/485 Mezzanine is described in Section 3.2.1.2.4. As many as eight RS-422/485 Mezzanines can be selected for any GLM card at the expense of other, alternate, I/O mezzanine selections. It is not necessary to have any RS-422/485 Mezzanine communication option selected if not required for the safety application.

### 3.4.2 RS-422 to RS-422 Connectivity

The NuPAC RS-422/485 communication option can be used to establish communications between two GLMs. The GLMs could be located in the same chassis, or different chassis. These types of GLM to GLM communication will require external wiring to be supplied between the two corresponding RTM chassis external interface connections. Discrete shielded, twisted pair copper cabling connected between the respective RTMs can be used to implement the external communication pathway. All communications are unidirectional and point to point.

#### 3.4.2.1 NuPAC to NuPAC RS-422 Communication Connectivity

a,c,e

*Figure 3.4.2-1. NuPAC to NuPAC Communications*

Figure 3.4.2-1 provides a graphical representation of typical intra division (inside the division) communication between two NuPAC chassis in Division A. [

]<sup>a,c,e</sup>

The communication is RS-422 which generates a differential pair of voltages for each bit of serial information being transmitted. Differential voltages transmitted on the twisted pair copper conduction lines are the same in magnitude but opposite in polarity. The difference between a logical “1” and “0” is that the polarities of the two voltages are inverted when generating a zero. For more information see the TIA/EIA-422 electrical standard.

One important feature of RS-422, that gave rise to its popularity over RS-232 for industrial applications, is the noise immunity provided by the differential signal. The receiver records ones and

zeroes by detecting the voltage difference between the lines. A zero is not the absence of a signal but rather a full differential signal with inverse polarity. Electromagnetic interference (EMI) tends to induce common mode electrical noise, so resistance to EMI induced noise is high for RS-422 communications.

[

]<sup>a,c,e</sup>

The use of twisted pair conductors limits the maximum baud rate and/or the effective length of the cabling. The maximum RS-422/485 baud rate supported by NuPAC is [ ]<sup>a,c,e</sup>. Figure 3.4.2-2 shows that at the maximum baud rate of [ ]<sup>a,c,e</sup>, the standard transmission cable length for effective communication cannot exceed [

]<sup>a,c,e</sup>

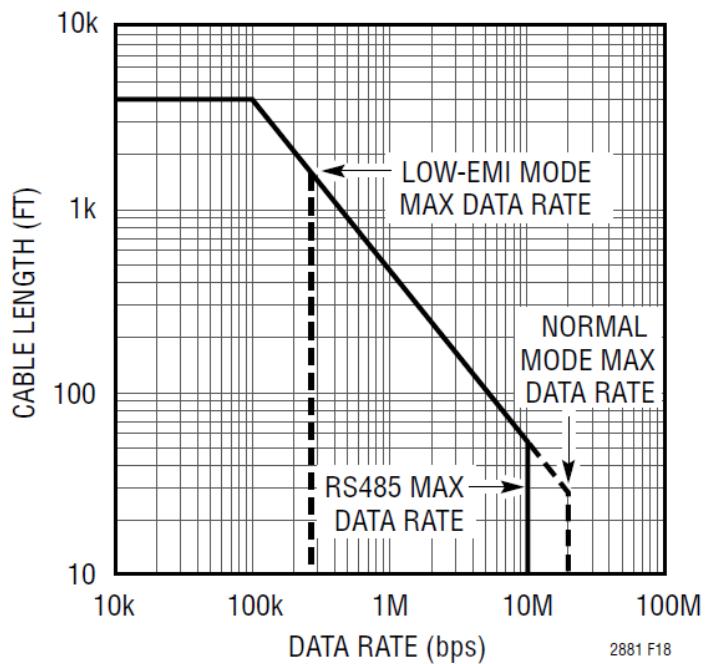


Figure 3.4.2-2. Copper Cable Length vs Data Rate

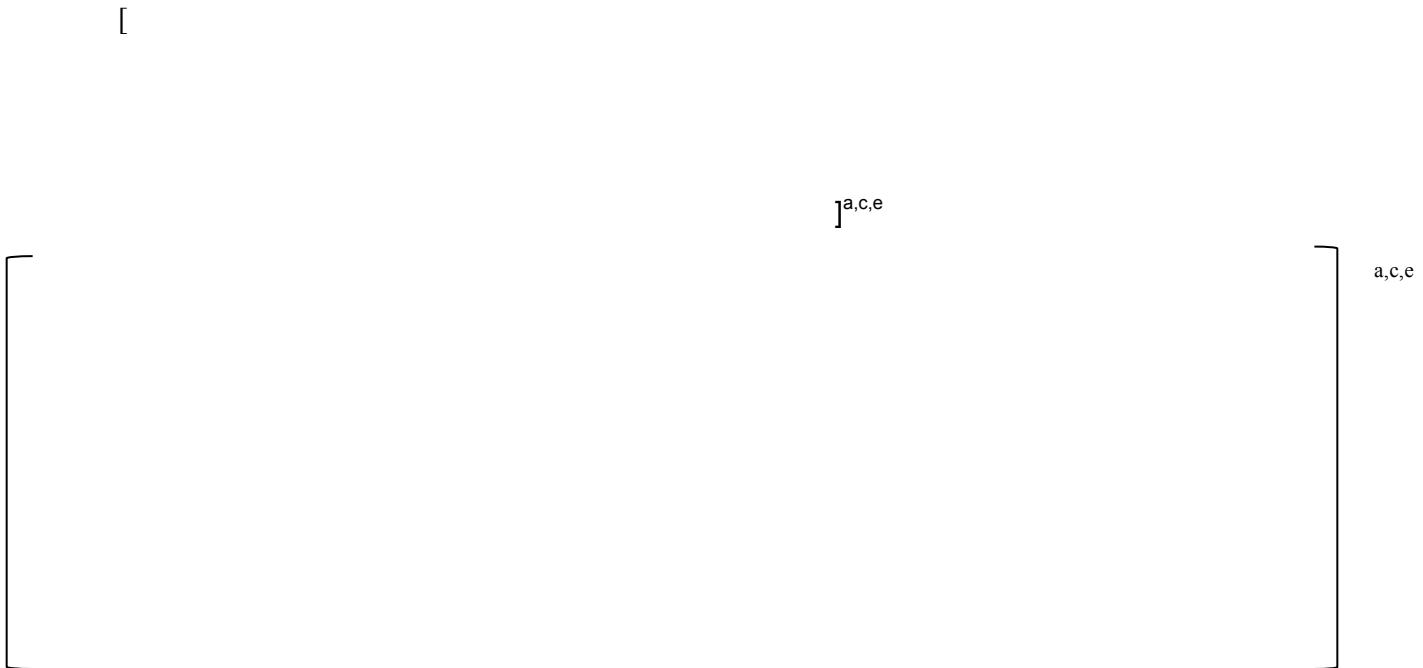


Figure 3.4.2-3. Division to Division Communications

[

]<sup>a,c,e</sup>

Aspects and features of the NuPAC external communication approach are provided in Section 3.4.3, followed by a full description of the chassis internal communication system in section 3.4.4.

### 3.4.3 RS-422/485 Mezzanine Serial Data Communication

For communications to occur outside a chassis, the external system must support the RS-422 electronic standard. For the purpose of this review, the external system will be another GLM card therefore this is supported. The NuPAC provides user selectable options for accommodating different baud rates, parity, stop bits, etc. Other than these restrictions, and the constraints specified in the ASC IDD, the message payload construction is at the discretion of the application developer.

Message payload received by NuPAC is managed in the ASPL pre-processing logic. This is intentional to allow alteration of the message processing rules based on the given future application without making any changes to the NuPAC Core logic.

[

]<sup>a,c,e</sup>

When external communications are NuPAC to NuPAC, there are specific constraints already established for how communications will be pre-processed by the ASPL. To facilitate robust communication, and to address concerns raised in ISG-04, all NuPAC to NuPAC communications are constrained to have the features of operation as defined in NuPAC\_ASCIDD610400-001 (**Reference 736**) and summarized in the following section: (section 3.4.3.1).

#### 3.4.3.1 NuPAC to NuPAC, RS422 ASPL Communication Constraints

When system communications are NuPAC chassis to NuPAC chassis there are several constraints imposed on the communication message structure. The full message constraints are contained in the Application Specific Communications Interface Description Document NuPAC\_ASCIDD610400-001.

The constraints form a minimum set of rules for the structure and communication of safety messages. The basic constraint information is provided here for reference when reviewing response to ISG-04 staff positions in Appendix D.

#### 3.4.3.1.1 Required Header Content

[

]<sup>a,c,e</sup>

#### 3.4.3.1.2 Required Message Content/ Format

[

]<sup>a,c,e</sup>

#### 3.4.3.1.3 Required Message Timing

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 3.4.4 Chassis Internal Backplane Serial Communication

A second method of communication is supported for GLMs located within the same chassis. This communication makes use of a network of fixed pre-wired point to point communication pathways that are available over the NuPAC chassis backplane. All hardware required for this internal communication is provided as a standard feature of NuPAC. Dedicated resources are used to support internal communication between GLMs. [

]<sup>a,c,e</sup> Connection to the allocated pathways is made by simply inserting the GLM into a given chassis slot. See Figure 3.4.4-4 for the network of available pathways.

The internal LVDS communications are not accessible outside the chassis. LVDS communications are configured during the initial system design phase when constructing future safety systems. Some or all may be used to fulfill the needs of future applications. It is never required that any LVDS link be used.

Chassis power is common, so splitting divisions within a single chassis is not allowed. For this reason any LVDS backplane communication is always intra-divisional communication. The details about the LVDS internal communications are given in the following sections.

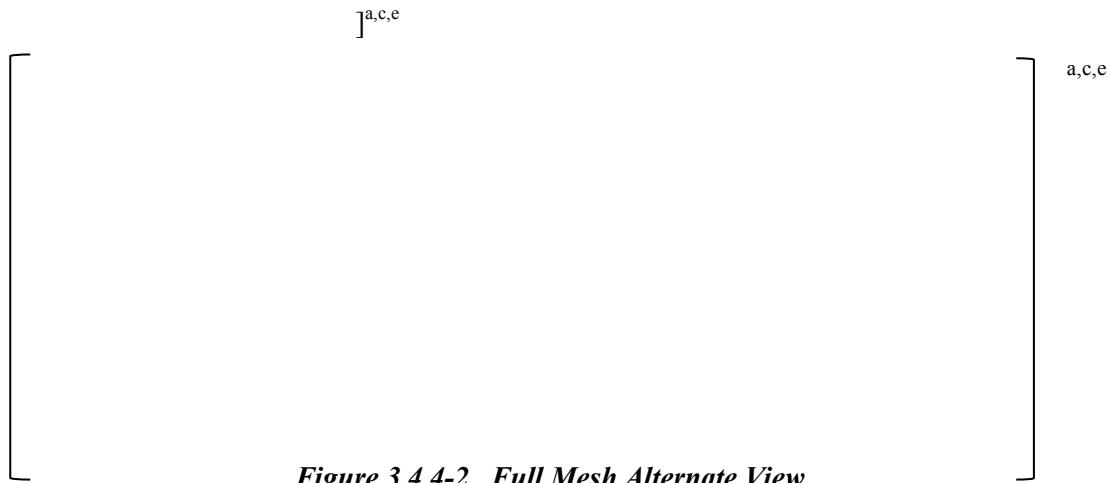
#### 3.4.4.1 NuPAC Mesh/Star Internal Communication Topology

Communication between all GLM cards within a single chassis is provided by pre wired point to point differential pair matched impedance copper traces located on the backplane circuit card. Point to point communication links were a desired feature of the NuPAC internal communications. There are 18 GLM card slots in a NuPAC chassis. [



*Figure 3.4.4-1. Full Mesh with Port Numbers*

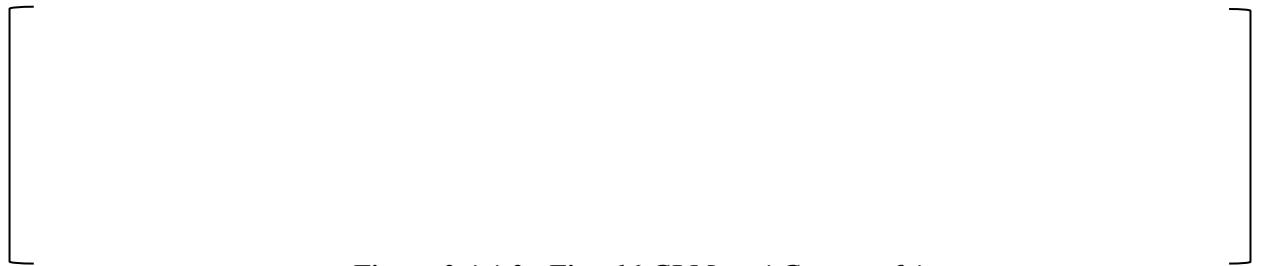
[



*Figure 3.4.4-2. Full Mesh Alternate View*

[

]<sup>a,c,e</sup>



*Figure 3.4.4-3. First 16 GLMs = 4 Groups of 4*

[

]<sup>a,c,e</sup>

To Increase capacity and flexibility, a second mesh star network was added. The second mesh star network provides additional overall communication capacity and additional communication options. For example, one mesh star can be used for the transmission of routine status information freeing, the other for important safety information. Alternately, the two mesh/star pathways could be used redundantly with the same message being transmitted on each network. [

]<sup>a,c,e</sup>

There are no connections from external communications into any of this internal communication network. This network is internal to the chassis only. There are no shared resources with external communications. Disruption, loss, or jamming of external communication will not have an effect on this internal network.

The twin mesh/star communication infrastructure is provided to be used if needed. There is no requirement that any given communication link must be used.

The total internal communication pathways are shown in Figure 3.4.4-4. Each box represents one of the 18 GLM cards. [

]<sup>a,c,e</sup>



***Figure 3.4.4-4. NuPAC Internal to Chassis Communication Topology***



国家核电  
国核自仪系统工程有限公司  
STATE NUCLEAR POWER AUTOMATION SYSTEM ENGINEERING COMPANY

No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 64 of 263  
Date: 04/14/2017

This page intentionally left blank.

The GLM Core logic maintains separation of the two Mesh/Star networks [

]<sup>a,c,e</sup>

a,c,e



***Figure 3.4.4-5. Alternate port view of the two mesh/star communication connections***

Figure 3.4.4-5 shows the same backplane network divided into the two mesh/star topologies designated as alpha and bravo. In this view, the boxes labeled A1-A18 represent GLMs installed in respective chassis/backplane slots. The numbers within the boxes represent the LVDS transmitter/receiver pairs. The lines between the boxes represent the backplane communication paths (copper traces) for full duplex LVDS serial data links. The color-coding is provided to facilitate the recognition of the logical grouping of GLMs.

### 3.4.4.2 LVDS Backplane Message pre-processing

A defined message structure is provided for the LVDS backplane communication. [

]<sup>a,c,e</sup> This ASPL function is required because the data content is subject to change based on the application.



国家核电  
国核自仪系统工程有限公司  
STATE NUCLEAR POWER AUTOMATION SYSTEM ENGINEERING COMPANY

No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 67 of 263  
Date: 04/14/2017

*Table 3.4.4-1. LVDS Backplane Message Structure*

a,c,e

### 3.4.4.3 Implementation of LVDS Backplane Serial Data Communication

NuPAC-based safety systems can be designed to collect and aggregate channel-level and/or divisional-level data or status information for all GLM cards in the chassis using a single or dual redundant GLM data collection card. A single GLM card can also act to distribute data to each of the other GLM cards. This aggregation of chassis data can reduce the number of external communication lines required for each chassis.

Intra-chassis communication supports the implementation of safety functions at the channel-level and divisional-level. To ensure that data independence is maintained, channels shall not receive any communication from another channel that is not necessary for supporting or enhancing the performance of the safety function, which may include communication of bypass information.

To enhance reliability, redundant intra-chassis communication paths could be implemented with two separate messages utilizing alternate backplane communication pathways.

[

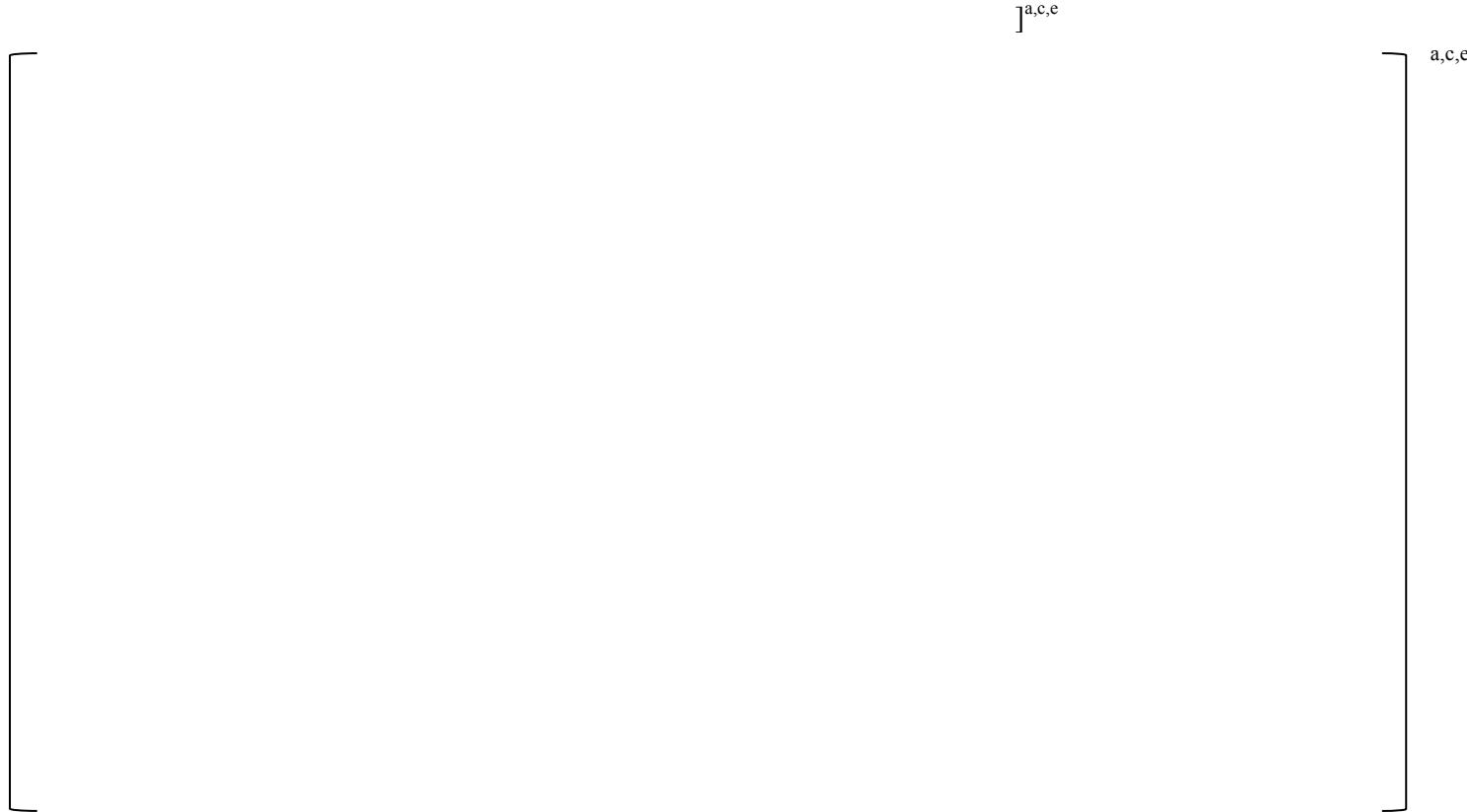
]<sup>a,c,e</sup>

### 3.4.5 Application Communication Function (Planned Approach)

This section is provided to describe the contribution to the communication system that is made by the logic that will be housed within the Application FPGA device (the ASPL).

The ASPL FPGA internal functions that support communications can be notionally broken down into general architectural function blocks as shown in Figure 3.4.5-1. The Figure is not intended to convey any relative size of the functional blocks. Just to show the general flow of data and processing within the ASPL FPGA. Also it should be understood that the blocks operate simultaneously without dependence on each other. This is a consequence of using hardware state machine logic rather than microprocessor/software based solution.

[



***Figure 3.4.5-1. ASPL Communication Block Function***

Many of the following functions have been implemented for the NuPAC TSC demonstration; however, the functions are not undergoing IV&V at this time. The communication functions implemented for the TSC are being used to help demonstrate the Core FPGA communication capability and verify the Core/Application interfaces

[

]<sup>a,c,e</sup>



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 70 of 263  
Date: 04/14/2017

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 3.4.6 General Communication Contribution to Response Time

The propagation and processing delays associated with communication are part of the overall delay through a NuPAC-based system. The methods for calculating delay from input to output are provided in section 6.3.3. Means are provided to calculate the maximum data delay associated with each GLM, which can then be totaled into the data delay through the system. Since the data delay is directly proportional to the amount of data sent and the baud rate for each message path is predefined as part of the plant-specific application design, each application for an individual system design will require confirmation of the maximum delay due to data transmission. This analysis will be part of the plant-specific total time delay analysis, which will include assumptions concerning additional delays associated with faults and failures in communicated messages.

The GLM card can process all eight I/O mezzanine RS422 communications and [ ]<sup>a,c,e</sup> LVDS communications simultaneously. The Core transfers bytes of message data to the ASPL as they arrive. No message buffering is necessary for messages being received by the ASPL. This is because the deterministic internal communication transfer is faster than the fastest ability to receive a byte of a message. Each of the [ ]

<sup>a,c,e</sup> Backplane Serial Interface (BSI) links and each of the eight (8) IO Mezzanines are provided with dedicated bandwidth to allow the transfer of one byte of data from each to the ASPL with a delay of at most one millionth of a second.

[

]<sup>a,c,e</sup>

Estimates of data throughput can be performed based on evaluation of the data items to be passed, communication protocol used, and processing times of both the sending and the receiving systems. Data throughput will be calculated for all functions under worst case conditions. The response times will be measured and compared with the accident analysis required times for acceptance.

### 3.4.7 RS-422 External Communications

A physically separate communication processor is not required for the RS-422/485 communication, since logically separate simultaneous communication processing is supplied for each of the eight possible RS-422/485 Mezzanines installed on a GLM.

Examples of future (not part of this review) RS-422 external systems or devices include:

- Bi- or unidirectional communication between safety systems, such as a neutron monitoring system sending data to a reactor trip system
- Bi- or unidirectional communications between a safety system and safety-related displays in the control room
- Unidirectional communications from a safety system to a non-safety system, such as a reactor trip system sending data to a plant computing system for data display, cross-channel comparisons and alarming.

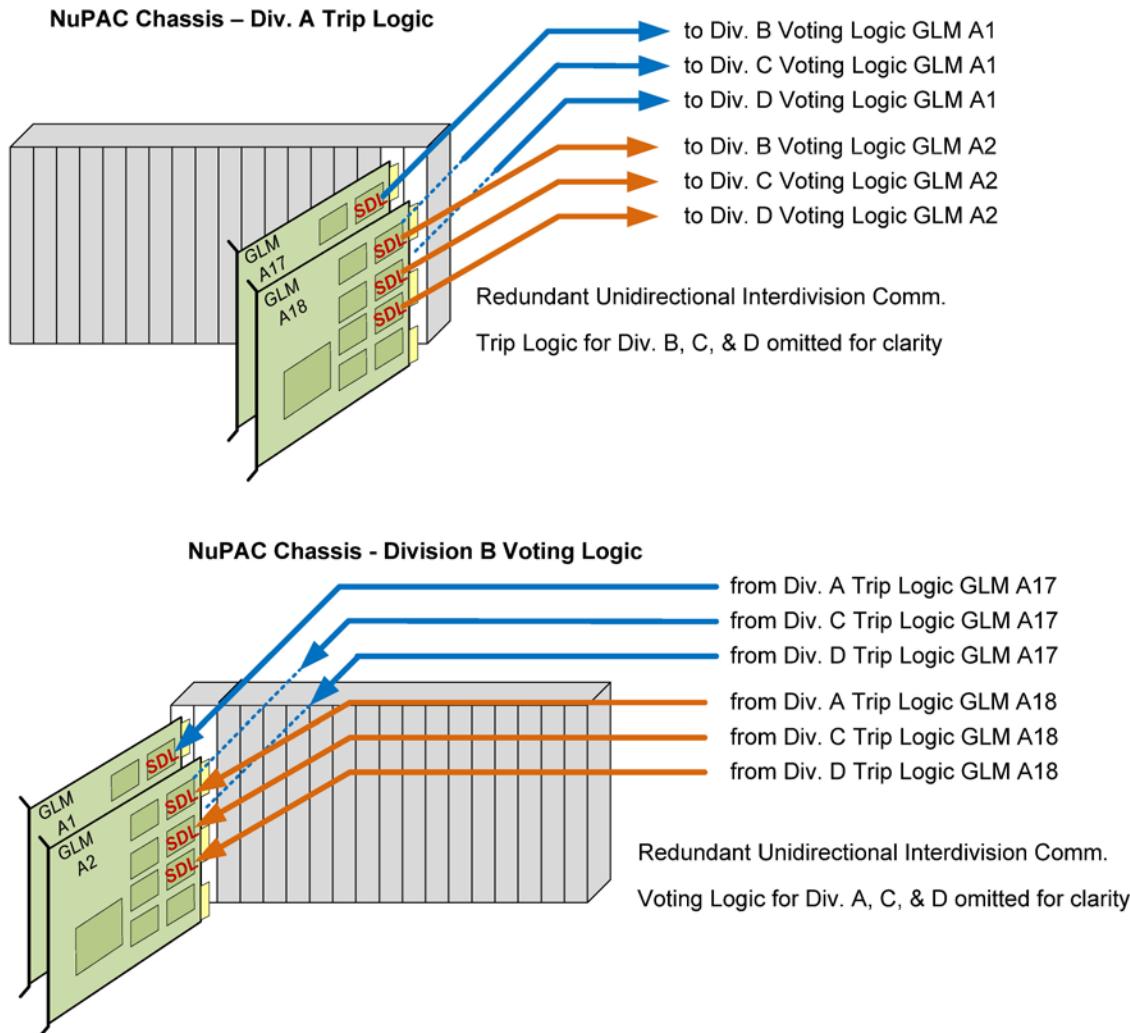
“Bi-directional” in the context of the NuPAC system, is always a pair of unidirectional communication links. One communication link dedicated to sending messages and the other dedicated to receiving messages. NuPAC never sends and receives any message using the same communication pathway.

[

]<sup>a,c,e</sup>

#### 3.4.7.1 Inter Divisional NuPAC to NuPAC Communications

All inter-divisional communications between NuPAC-based safety systems will be constructed with RS-422/485 mezzanines. The RS-422/485 mezzanines’ transmitter ports in the originating division will be wired to a RS-422/485 mezzanine’s receiver port in each of the other divisions.



AP002\_0511-0042

**Figure 3.4.7-1. Inter-divisional Communication**

As always, the communications are serial one directional send and forget. Messages are sent using a predefined periodicity. The GLMs that serve as the unidirectional inter-divisional communication interface provide functional and data isolation. Furthermore, to facilitate separation, [a,c,e]. The

separation distance between a division's and redundant divisions' circuits and cables shall be in accordance with IEEE Standard 384-1992 (**Reference 346**), with fiber optic cable separation in accordance with IEEE Standard 384-2008 (**Reference 347**). To enhance reliability, redundant inter-divisional communication paths could be provided with two separate GLMs and thus two separate unidirectional communication paths.

Requirements shall be imposed on the receiving GLM to verify the data being used meets the requirements of DI&C-ISG-04 (**Reference 117**), especially with regard to liveness and other critical aspects of ensuring the data transferred is correct. See section 3.4.3.1 for imposed constraints on NuPAC to NuPAC communications. Communication protocols are implemented, as required, in the ASPLD.

### 3.5 Additional Information

#### 3.5.1 Determinism

Architecturally speaking, one of the driving reasons to select firmware state machine logic over microprocessor embedded software was the desire to generate a highly deterministic system. The NuPAC platform contains no embedded software. Its design replaces the main operating loop (MOL) of a typical microprocessor-based platform by making use of parallel processing state machine elements and distributed logic. The NuPAC runs no program and has no interrupts to disrupt its intended functions. The NuPAC decomposes long complex tasks into manageable smaller parallel processes that can be readily reviewed for deterministic behavior and/or upper bounds on response time. Each state machine is implemented at design time to perform a specific dedicated function. NuPAC state machines, once implemented, are hardware designs and cannot be altered by software command.

The NuPAC response time, from event to outcome, can be computed by adding all contributions within the cause and effect process. The response time, from input(s), to final outcome, can be computed using document NuPAC\_ED610000-051 which provides the methodology for determining response time for any NuPAC function.

[

]<sup>a,c,e</sup>

## 4.0 TECHNICAL AND SUPPORT PROCESSES

The Technical and Support Processes (TASP) defines the core processes for conducting business in the Energy business area. The TASP is the generic operational architecture applied to each project and is part of the overall LMGI Quality System and is used as the basis for defining the plans and activities used for this NuPAC project.

### 4.1 Organizational Relationships

[

]<sup>a,c,e</sup>

a,c,e



*Figure 4.1-1. NuPAC Program Organizational Relationships*

[

]<sup>a,c,e</sup>



[

|

]<sup>a,c,e</sup>

## 4.2 TASP Structural Overview

[

]<sup>a,c,e</sup>



*Figure 4.2-1. TASP Structural Overview*

#### 4.3 Process Domains

[

]a,c,e



[

]<sup>a,c,e</sup>



[

]<sup>a,c,e</sup>

#### 4.4 Product Life Cycle

[

]<sup>a,c,e</sup>



[

]<sup>a,c,e</sup>



***Figure 4.4-1. Perform Product Life Cycle Actions***



[

]<sup>a,c,e</sup>



[

]<sup>a,c,e</sup>



[

]<sup>a,c,e</sup>



[

|

|

. ]<sup>a,c,e</sup>



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 86 of 263  
Date: 04/14/2017

[

]<sup>a,c,e</sup>

## 4.5 Planning Documentation

The TASP prescribes the “what” of managing and developing the NuPAC program. The TASP requires developing a set of program plans, which control “how” the TASP is to be implemented and executed for the NuPAC program. There are multiple program plans that govern the execution of the NuPAC program for achieving program excellence. The following subsections provide an overview of each program plan. Table 4.5-1 identifies references to the planning documentation specific to the generic NuPAC platform development program.

*Table 4.5-1. Generic NuPAC Platform Planning Documentation*

| Plan   | Reference |
|--|-----------|
| Commercial Grade Dedication Plan (CGDP)                          | 701       |
| Configuration Management Plan (CMP)                              | 702       |
| Field Programmable Logic Verification and Validation Plan (FVVP) | 711       |
| Hardware Development Plan (HDP)                                  | 712       |
| Master Test Plan (MTP)   | 714       |
| Program Management Plan (PMP)                                    | 718       |
| Programmable Logic Development Plan (PLDP)                       | 715       |
| Quality Assurance Plan (QAP)                                     | 719       |
| Reliability Program Plan (RPP)                                   | 721       |
| Subcontract Management Plan (SMP)                                | 724       |
| Platform Safety Project Plan (PSPP)                              | 726       |
| System Security Plan (SSP)                                       | 725       |
| Systems Engineering Management Plan (SEMP)                       | 723       |
| Test Equipment Development Plan (TEDP)                           | 728       |

### 4.5.1 Commercial Grade Dedication Plan (CGDP)

The CGDP is the controlling document for the dedication of NuPAC program commercial-grade items and services, when applicable. The design and manufacturing associated with the NuPAC program is considered safety-related under Appendix B so the amount of commercial-grade dedication is limited for NuPAC.

The CGDP is applicable to those NuPAC components purchased as commercial-grade and intended for safety-related use. This plan does not apply to components or services that are procured as basic components from suppliers in compliance with 10 CFR Part 50 Appendix B (**Reference 103**) or ASME NQA-1-2008 (**Reference 304**).

### 4.5.2 Configuration Management Plan (CMP)

The CMP is the controlling document for execution of configuration management on the NuPAC program. The CMP provides the instructions for configuration management and planning, configuration identification, configuration control, configuration status accounting, configuration audits, and control of documentation.

### 4.5.3 Field Programmable Logic Verification and Validation Plan (FVVP)

The FVVP defines the I-V&V activities and requirements to be applied to programmable logic developed for the NuPAC platform. The plan describes the organization, schedule, PL integrity level scheme, resources, responsibilities, tools, techniques, identification of anomalies, all methods necessary to perform the PL I-V&V activities.

#### 4.5.4 Hardware Development Plan (HDP)

The HDP details the NuPAC program hardware engineering effort. It provides technical supplements, with respect to hardware development, to the overall technical effort defined in the SEMP.

#### 4.5.5 Master Test Plan (MTP)

The MTP describes the NuPAC program test activities. The MTP includes the test flow through each level of test from subassembly acceptance tests through system-level integration and qualification testing.

#### 4.5.6 Program Management Plan (PMP)

The PMP provides the structure in managing the NuPAC program. The PMP is the top-level document describing the management approach. The contents of the PMP combined with the contents of other NuPAC plans, including those of the subcontractors/key suppliers form the foundation for program execution.

The NuPAC program management uses this PMP, along with applicable referenced plans, as key management documents to define, execute, and manage administrative/technical processes on the program. Program management is responsible for the life cycle development, which includes design, test, production, specialty engineering, and interfaces to independent verification and validation to satisfy the program requirements, quality standards, technical performance, budgetary constraints, and schedule requirements.

#### 4.5.7 Programmable Logic Development Plan (PLDP)

The PLDP is the basic governing document for the PL development activities. The PLDP defines the development of the PLCIs as a specific implementation of the software life cycle activities defined in IEEE Standard 1074 (**Reference 333**) as endorsed by the USNRC RG 1.173 (**Reference 140**).

The PLDP defines the technical processes, activities, and tasks needed to design, implement, and evaluate the Core and Application Specific (AS) PLCIs. The plan enforces a series of practices that provides structure and guidance to the systems engineering, design engineering, component engineering and evaluation activities associated with the complexity of the PLCIs.

##### 4.5.7.1 Programmable Logic Verification Procedure (PLPRC)

The PLPRC describes the scope, approach, resources, and schedule of the PL testing activities. It identifies the items being tested, the features to be tested, the testing tasks to be performed, and the personnel responsible for each task. The plan covers testing conducted on the PLCIs, including unit testing, integration testing, acceptance testing, and installation testing.

The plan complies with the software test plan and test activities sections of DI&C-ISG-06 (**Reference 119**), the integration through installation phases of IEEE Standard 1074- (**Reference 333**), the software test plan and the acceptance criteria for testing activities sections of NUREG-0800, BTP 7-14 (**Reference 112**), IEEE Standard 829 (**Reference 358**), and ANSI/IEEE Standard 1008 (**Reference 327**).

#### 4.5.8 Quality Assurance Plan (QAP)

The QAP supplements the “Energy Quality Systems Manual for Commercial Nuclear Programs,” D-D7210/2013P-5001 (**Reference 731**) and establishes the implementation details for the NuPAC program quality activities. The QAP is maintained throughout the life cycle of the NuPAC program.

This plan is also the controlling document for the quality assurance activities for the programmable logic development effort as described in Section 5.0

#### **4.5.9 Reliability Program Plan**

The RPP details the tasks, methodologies, organizational relationships, authority, and milestones relative to the management, analysis, design participation, surveillance, disclosure, and testing necessary to achieve the NuPAC program reliability requirements.

#### **4.5.10 Risk and Opportunity Management Plan (ROMP)**

The ROMP delineates how the program conducts and manages commercial risks and opportunities that are specific to the NuPAC program. The plan also provides a background for the risk and opportunity management process, lists reference documents, and defines personnel and processes that constitute the plan. The ROMP covers risk and opportunity management activities throughout the life cycle of the NuPAC program.

#### **4.5.11 Subcontract Management Plan (SMP)**

The SMP is the controlling document for subcontracts on the NuPAC program. This SMP sets forth the processes for developing subcontract strategies, managing and integrating activities with major program milestones, and driving excellent performance. It provides methods and guidance for the selection and management of subcontractors using proven concepts, tools, and techniques to assure successful NuPAC program execution.

This SMP provides guidance for subcontract management activities including:

- Organization, roles, and responsibilities for NuPAC program subcontract execution
- Techniques for subcontractor performance management
- An introduction to a subcontract management team concept
- Management of subcontractors during execution of the NuPAC program.

This plan provides consistent processes for developing subcontracting strategies and managing subcontractors of the NuPAC program with the following expectations:

- Early engagement with subcontractors
- Proactive planning of collaborative activities to enable excellent subcontract performance
- Consistent application of management oversight for all subcontractors
- Control of subcontractors through all phases of the program to minimize program impacts
- Defining and establishing coordinated supplier management teams with skill mixes focused on the program phases
- Defining and establishing appropriate business relationships with subcontractors to ensure NuPAC program success.

#### **4.5.12 Platform Safety Project Plan (PSPP)**

The PSPP provides instructions for planning and managing the system safety program activities. It defines the system safety management methodology and the system safety engineering methodology applied to the NuPAC program. In addition, it establishes the system safety design criteria and guidelines.

#### 4.5.13 System Security Plan (SSP)

The SSP specifies the Secure Development and Operations Environment (SDOE) controls for NuPAC platform.

#### 4.5.14 Systems Engineering Management Plan (SEMP)

The SEMP is the top-level controlling document for the system level execution of the NuPAC program. This document provides the detailed instructions for technical task planning and control, the system engineering process, and engineering specialty integration requirements to be applied to the NuPAC program.

#### 4.5.15 Test Equipment Development Plan (TEDP)

The TEDP describes the strategies, guidelines, and implementation details for the NuPAC program development of special test equipment, which is used for development, acceptance testing, and qualification. The TEDP outlines the process used to develop the test equipment required to perform the testing specified in the MTP. This plan applies throughout the life cycle of the NuPAC program.

### 4.6 Software Tool Evaluation

Position 6 of USNRC RG 1.168 (**Reference 135**) states, “Tools used in the development of safety system software should be handled according to IEEE Standard 7-4.3.2, as endorsed by Regulatory Guide 1.152.”

COTS software tools were used to develop programmable logic and perform IV&V for the NuPAC platform FPGAs. The Software Tool Evaluation Plan (**Reference 716**) provides the process for evaluating COTS software tools to ensure the guidance of IEEE Standard 7-4.3.2 (**Reference 356**) are met.

The NuPAC Platform LPE is responsible for the overall execution and maintenance of the above-referenced Software Tool Evaluation Plan for PL development (non-IV&V). The ILPE is responsible for the execution and maintenance of the tool evaluations used for IV&V, per the tool evaluation process defined in the FVVP (**Reference 711**). All other software tool evaluations are performed within the organization that uses them.

Each group (function) determines its need for a software tool. When a determinism is made that a tool is needed and available, each tool is identified in the individual development plans developed for the project, e.g., in the Programmable Logic Development Plan (**Reference 715**) and FPL Verification and Validation Plan (**Reference 711**). The function evaluates the tool per the requirements of the above-referenced software tool evaluation plan, or the IVV FVVP. The evaluated tool is then placed under configuration control and its operational history monitored.

[

]<sup>a,c,e</sup>



[

]<sup>a,c,e</sup>

#### 4.7 Deleted



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 92 of 263  
Date: 04/14/2017

This page intentionally left blank.

## 5.0 SOFTWARE DEVELOPMENT PROCESS FOR NUPAC PROGRAMMABLE LOGIC

This section summarizes the programmable logic (PL) development process for the NuPAC program. The process used in the development of the NuPAC platform PL follows an incremental waterfall life cycle model, based on the activities defined in IEEE Standard 1074 (**Reference 333**) as endorsed by USNRC RG 1.173 (**Reference 140**). The incremental waterfall life cycle model incorporates the strategy of developing the PL in a traditional waterfall approach that allows revisiting of requirements, design, implementation, and test based on the nature and evaluations of the safety critical aspects of the PL.

System-level requirements, system-level allocations (functional and physical architecture), and requirements of hardware components are defined as part of the overarching Product Life Cycle (section 4.0) of which the PL Development Process is integral. Hardware items provide the foundation to further allocate interface, functional, and performance requirements to PL configuration items (PLCIs). The PLCIs consist of the logic that is embedded in the programmable logic devices (PLDs). For each PLCI, the PL requirements are derived and the PL is designed, implemented, and evaluated against those requirements. Upon completion of PL validation, PL components are ready to be integrated with the PLDs and evaluated at the hardware-level.

The Programmable Logic Development Plan (**Reference 715**) addresses the management of PL process and establishes the infrastructure and systematic approach for development of the PLCIs for the NuPAC platform. The PLDP (**Reference 715**) also documents PL methods, tools, and techniques; standards; schedule and milestones; and technical documentation requirements. The PLDP is fully integral to the TASP which includes the configuration management process, the quality assurance process, and the IVV process.

### 5.1 Programmable Logic Life Cycle Description

The PL Incremental Waterfall Life Cycle is integral into the Product Life Cycle (Section 4.0) and consists of a Pre-Development Phase, a Development Phase, and a Post-Development phase. Activities in all life cycle phases are bounded by explicit milestones containing entry and exit criteria.

The Pre-Development Phase consists of a proposal activity and a pre-contract aware planning activity. The Development Phase consists of a planning activity, a requirements analysis activity, an architecture activity, a preliminary design activity, a critical design activity, an integration and test activity, and an acceptance test activity. The Post-Development Phase consists of an installation and check-out activity, an operation and support activity, and a retirement activity. See Figure 4.4-1, Perform Product Life Cycle Actions.

This process implements the Development Phase of the Product Life Cycle. Pre-Development and Post-Development Phases are not applicable.

The activities of the PL Incremental Waterfall Life Cycle are depicted in Figure 5.1-1, Software Development Process. For detailed application of the process shown in Figure 5.1-1, as used in the development of the NuPAC PL, refer to the Programmable Logic Development Plan (**Reference 715**).



*Figure 5.1-1. Software Development Process*

### **5.1.1 Management Activities**

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 5.1.2 Requirements Activity

[

]<sup>a,c,e</sup>

### 5.1.3 Architecture and Design Activities

[

]<sup>a,c,e</sup>

### 5.1.4 Implementation Activity

[

]<sup>a,c,e</sup>

### 5.1.5 Design Verification Activity

[

]<sup>a,c,e</sup>



### 5.1.6 Deleted

## 5.2 Programmable Logic Oversight

[

]<sup>a,c,e</sup>

### 5.3 Deleted

### 5.4 Deleted

## 6.0 EQUIPMENT QUALIFICATION

### 6.1 Description of Test Specimen and Test Equipment

#### 6.1.1 Test Specimen Configuration

The Test Specimen Configuration (TSC) is an example of a NuPAC-based application consisting of a mix of functions that match the relative mix of functions identified in NPP safety system operational scenarios. The TSC is the configuration of the NuPAC platform to be used for the qualification test program.

The TSC emulates a portion of a Reactor Trip System (RTS). An RTS is the overall system of instruments (sensors), trip logics, trip actuators, and scram logic circuitry that initiates rapid insertion of control rods (scram) to shut down a reactor. The system also establishes operating modes and provides status and control signals to other systems and annunciators. A RTS provides reliable single-failure-proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. This is accomplished through the combination of fail-safe equipment design and a redundant two-out-of-four logic arrangement. Although the TSC is RTS-centric, the general functionality is applicable to Engineered Safety Features Actuation System (ESFAS) and other systems.

The TSC, as specified, is representative of a single division (one of the four redundant logic arrangements) of reactor trip detect logic and coincidence logic. Each division samples sensors, performs trip detect logic, transmits/receives trip conditions to/from every other division, and provides trip output to the actuators (scram) when the same trip condition exists in any two or more divisions (coincidence logic).

The TSC consists of at least one of each type of NuPAC platform hardware component listed in Section 3.1.4, including the Carrier Card, Logic Mezzanine, I/O mezzanines, Rear Transition Module (RTM), and chassis. Figure 6.1.1-1 shows a block diagram of the TSC. The TSC is a system consisting of two chassis. Each chassis is populated with GLMs/RTMs. One chassis is allocated to trip detect logic and is comprised of GLMs that are configured to utilize each of the types of inputs offered by the NuPAC platform. The inputs to this chassis simulate the inputs that are present in a typical RTS. The application-specific programmable logic determines whether the input value is above or below the setpoint value and communicates the trip conditions to the second chassis. The second chassis is allocated to coincidence logic and is populated with GLMs configured to provide a sample of the output types offered by the NuPAC platform. The application-specific programmable logic of this chassis compares the trip conditions received from the trip detect chassis with trip conditions received from three other simulated divisions of trip detect logic. It performs two-out-of-four voting and controls outputs consistent with outputs that are present in a typical RTS.

After completion of design verification testing, the TSC continued to the pre-qualification, then the qualification test program.



*Figure 6.1.1-1. TSC Block Diagram*

#### 6.1.2 Test Equipment

[

]<sup>a,c,e</sup>

[



*Figure 6.1.2-1. Test System*

*Figure 6.1.2-2. TSC Test Setup Block Diagram*

## 6.2 Qualification Test Program

The qualification test program is a combination of the events of verification and validation, which confirm the NuPAC platform, as described in section 3.2, meets its requirements that are demonstrated by test. This process is described in the NuPAC Master Test Plan (**Reference 714**). After a series of acceptance and design verification tests and prior to the start of qualification testing, the TSC went through a series of pre-qualification testing described in Section 6.2.1. Upon successful completion of pre-qualification testing the TSC underwent a series of rigorous qualification tests described in Sections 6.2.2 through 6.2.5, as required by the NuPAC platform requirements to verify it is capable of performing its designed safety functions during specified operating conditions. Table 6.2-1 presents a summary of the qualification testing, including the sequence of tests.

*Table 6.2-1. Qualification Test Sequence*

| Order | Description              | Basis   |
|-------|--------------------------|---|
| 1     | Radiation Withstand      | EPRI TR-107330 ( <b>Reference 312</b> ), USNRC RG 1.209 ( <b>Reference 143</b> ), IEEE Standard 323-2003 ( <b>Reference 339</b> )                                 |
| 2     | Temperature and Humidity | EPRI TR-107330 ( <b>Reference 312</b> ), USNRC RG 1.209 ( <b>Reference 143</b> ), IEEE Standard 323-2003 ( <b>Reference 339</b> )                                 |
| 3     | EMI/RFI                  | USNRC RG 1.180 ( <b>Reference 141</b> ), MIL-STD-461E ( <b>Reference 368</b> ), IEC 61000-4 ( <b>References 315 thru 325</b> )                                    |
| 4     | Electrostatic Discharge  | EPRI TR-107330 ( <b>Reference 312</b> ), EPRI TR-102323 ( <b>Reference 310</b> ), IEC 61000-4-2 ( <b>Reference 319</b> ), USNRC RG 1.180 ( <b>Reference 141</b> ) |
| 5     | Seismic Withstand        | USNRC RG 1.100 ( <b>Reference 129</b> ), EPRI TR-107330 ( <b>Reference 312</b> ), IEEE Standard 344-2004 ( <b>Reference 342</b> )                                 |

Test procedures are used to define and document the detailed steps required to integrate and/or test the TSC. These procedures document integration/test conditions, prerequisite events, safety criteria, personnel responsibilities, and reporting requirements. Clearly defined pass/fail criteria are specified. The following test procedures were generated and submitted as part of Phase 2 information:

- Operability test procedure
- Prudency test procedure
- Pre-qualification test procedure
- Environmental test procedure
- Seismic test procedure
- Radiation test procedure
- EMI/RFI test procedure
- ESD test procedure

A summary test report has been developed to document results of the qualification test program. The test report describes the specific reason for conducting the tests, together with pertinent background information, as applicable. Following completion of each phase of testing, test report content was developed to document test conduct and results. The NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**) and NuPAC Environmental Equipment Qualifications (EQ) List of anomalies and Actions (**Reference 748**) were generated and submitted as part of Phase 2 information.

### 6.2.1 Pre-Qualification Testing

The TSC underwent various acceptance and operability tests prior to the qualification tests to confirm that the TSC operates correctly and to provide baseline data for some of the qualification tests. The pre-qualification

testing of the TSC is performed as described in NuPAC System Pre-Qual Test Procedure (**Reference 749**). The following tests were performed:

- A [ ]<sup>a,b,c,e</sup> burn-in conducted under ambient conditions was performed on the NuPAC platform components to detect any early life failures, which would corrupt the qualification test results.
- The operability tests were performed at various points in the qualification process to confirm that the TSC operation was satisfactory, and included accuracy measurements, response time measurements, and I/O and communication operability. The operability testing of the TSC was performed as described in the operability test procedure.
- The prudency tests exercise the TSC to verify its ability to perform under highly dynamic conditions, which includes toggling specified inputs and outputs and applying faults and noise interference to various locations in the TSC. The prudency testing of the TSC was performed as described in the prudency test procedure.

The results are documented in the NuPAC Pre-Qualification Test Report (**Reference 750**).

### 6.2.2 Temperature and Humidity Testing

Temperature and humidity testing of NuPAC using the TSC was performed as described in the NuPAC System Environmental Test Procedure (**Reference 739**), which is based on the guidance specified in EPRI TR-107330 (**Reference 312**) and follows the guidance of IEEE Standard 323-2003 (**Reference 339**) as endorsed by Regulatory Guide 1.209 (**Reference 143**). The NuPAC is qualified to perform its safety function in abnormal service conditions of temperature and humidity, up to the [ ]<sup>a,b,c,e</sup> Relative Humidity (RH) levels as defined in Figure 4.4 of EPRI TR-107330 (**Reference 312**), which includes the added and desired [ ]<sup>a,b,c,e</sup> margin, and to the Low Temperature/Humidity condition of [ ]<sup>a,b,c,e</sup> RH, and Low Humidity / Temperature condition of [ ]<sup>a,b,c,e</sup>. Figure 6.2.2-1 provides a visual envelope to which the NuPAC platform is qualified.



**Figure 6.2.2-1. NuPAC Environmental Qualification Test Envelope**

The detailed results of the temperature and humidity testing, as well as any restrictions, are provided in the NuPAC Environmental Test Report (**Reference 744**). Temperature and humidity testing is also summarized in NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**).

### 6.2.3 Seismic Withstand Testing

Seismic withstand testing of the NuPAC TSC was performed as described in the NuPAC System Seismic Test Procedure (**Reference 740**), which is based on the guidance specified in EPRI TR-107330 (**Reference 312**) and follows the guidance of IEEE Standard 344-2004 (**Reference 342**) as endorsed by Regulatory Guide 1.100 (**Reference 129**). Each chassis of the TSC was tested individually. Each chassis underwent a resonance search, five Safe Shutdown Earthquakes (SSE) and one Operating Basis Earthquake (OBE). The NuPAC platform is qualified to perform its safety functions to the seismic spectra provided in Figure 6.2.3-1.

### **Figure 6.2.3-1. NuPAC SSE -10% and OBE Qualification Spectra Seismic Withstand Response Spectrum**

The detailed results of the seismic testing are provided in the NuPAC Seismic Test Report (**Reference 745**). A summary of all EQ testing is provided in NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**). A summary of the restrictions is provided in NuPAC Environmental Equipment Qualifications (EQ) List of Anomalies and Actions (**Reference 748**).

#### **6.2.4 Radiation Withstand Testing**

Radiation withstand testing of the NuPAC TSC was performed as described in the NuPAC System Radiation Test Procedure (**Reference 741**), which is based on the guidance specified in EPRI TR-107330 (**Reference 312**) and follows the guidance of IEEE Standard 323-2003 (**Reference 339**) as endorsed by Regulatory Guide 1.209 (**Reference 143**). The radiation exposure consisted of the [ ]<sup>a,b,c,e</sup> radiation absorbed doses (RADs) requirement plus an additional [ ]<sup>a,b,c,e</sup> margin applied over the course of [ ]<sup>a,b,c,e</sup> above the required [ ]<sup>a,b,c,e</sup> of EPRI TR-107330 (**Reference 312**). The NuPAC Platform is qualified to perform its safety function when exposed to a cumulative radiation exposure of [ ]<sup>a,b,c,e</sup>.

The detailed results of the radiation testing are provided in the NuPAC Radiation Test Report (**Reference 746**). A summary of all EQ testing is provided in NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**). A summary of the restrictions is provided in NuPAC Environmental Equipment Qualifications (EQ) List of Anomalies and Actions (**Reference 748**).

### 6.2.5 EMI/RFI/ESD Testing

Electromagnetic compatibility testing of the NuPAC TSC was performed as described in the NuPAC System Electromagnetic Compatibility Test Procedure (**Reference 742**) and NuPAC System Electrostatic Discharge Test Procedure (**Reference 743**), in accordance with Regulatory Guide 1.180 (**Reference 141**), and as endorsed, the Military Standard MIL-STD-461E (**Reference 368**) and the International Electrotechnical Commission (IEC) 61000 series (**References 315 to 325**) of electromagnetic and radio-frequency Interference (EMI/RFI) test method requirements.

The specific tests conducted include the MIL-STD-461E (**Reference 368**) and the IEC 61000 series (**References 315 to 325**) test methods listed in Table 6.2.5-1.

*Table 6.2.5-1. Electromagnetic Compatibility Test Sequence*

| Test Method        | Test Description  |
|--------------------|---|
| MIL-STD-461E RE101 | Radiated Emissions, Magnetic Field Measurement  |
| MIL-STD-461E RE102 | Radiated Emissions, Electric Field Measurement  |
| IEC 61000-4-4      | Conducted Susceptibility, Electrical Fast Transient / Burst Immunity Test   |
| IEC 61000-4-12     | Conducted Susceptibility, Oscillatory Waves Immunity Tests  |
| IEC 61000-4-5      | Conducted Susceptibility, Surge Immunity Test   |
| IEC 61000-4-6      | Conducted Susceptibility, Immunity to Conducted Disturbances Induced by Radio-frequency Fields                            |
| IEC 61000-4-16     | Conducted Susceptibility, Test for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz |
| IEC 61000-4-8      | Radiated Susceptibility, Power Frequency Magnetic Field Immunity Test   |
| IEC 61000-4-9      | Radiated Susceptibility, Pulse Magnetic Field Immunity Test   |
| IEC 61000-4-10     | Radiated Susceptibility, Damped Oscillatory Magnetic Field Immunity Test  |
| IEC 61000-4-3      | Radiated Susceptibility, Radiated, Radio-frequency, Electromagnetic Field Immunity Test                                   |
| IEC 61000-4-2      | Electrostatic Discharge Immunity Test   |

The NuPAC platform is qualified to perform its safety functions to the levels identified in the EMI/ESD environments provided in Table 6.2.5-2.

*Table 6.2.5-2. Electromagnetic Compatibility Test Results Summary*

| Test                 | Compliance Category                                 |                 |                    |                |                        |            |
|----------------------|---|-----------------|--------------------|----------------|------------------------|------------|
| Emissions Tests      |   |                 |                    |                |                        |            |
| RE101                | [   |                 |                    |                |                        |            |
| RE102                |   |                 |                    |                |                        |            |
|                      |   |                 |                    |                |                        |            |
| Susceptibility Tests | Classification for Each I/O Type per Test Performed |                 |                    |                |                        |            |
|                      | Analog Inputs                                       | Discrete Inputs | Temperature Inputs | Analog Outputs | Discrete Outputs (SSR) | RS-422 I/O |
| IEC 61000-4-8        | [   |                 |                    |                |                        |            |
| IEC 61000-4-9        |   |                 |                    |                |                        |            |
| IEC 61000-4-10       | ■ P   | ■ P             | ■ P                |                |                        |            |
| IEC 61000-4-4        |   |                 |                    | ■              |                        |            |
| IEC 61000-4-16       |   |                 |                    |                | ■ P                    |            |
| IEC 61000-4-12       |   |                 |                    | ■ P            | ■ P                    |            |
| IEC 61000-4-3        | ■ P   | ■ P             | ■ P                |                |                        |            |
| IEC 61000-4-6        |   |                 |                    | ■              |                        |            |
| IEC 61000-4-2        |   |                 | ■                  | ■              | ■                      | ■          |
| IEC 61000-4-5        |   |                 |                    | ■              | ■                      | ]          |
| Notes:               |   |                 |                    |                |                        |            |
| [                    |   |                 |                    |                |                        |            |
|                      |   |                 |                    |                |                        |            |
| ] a,b,c,e            |   |                 |                    |                |                        |            |

The detailed results of the EMI/ESD testing, as well as any restrictions, are provided in the NuPAC System Electromagnetic Compatibility Test Report (**Reference 747**). A summary of all EQ testing is provided in NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**). A summary of the restrictions is provided in NuPAC Environmental Equipment Qualifications (EQ) List of Anomalies and Actions (**Reference 748**).

#### 6.2.6 Deleted

#### 6.2.7 Deleted

### 6.3 Supporting Data for Analyses

This section describes the following supporting data to establish the basis for future system-level analyses for plant-specific NuPAC-based systems:

- Failure analysis
- Reliability analysis
- Response time analysis
- Setpoint analysis.

#### 6.3.1 Supporting Data for Failure Analysis

A failure modes and effects analysis (FMEA) and failure modes, effects, and criticality analysis (FMECA) have been prepared for the NuPAC platform per EPRI TR-107330 (**Reference 312**) and per guidance in IEEE Standard 352 (**Reference 343**).

The FMEA, NuPAC\_ED610000-049 (**Reference 705**), identifies potential NuPAC platform failure modes and categorize the effect of each failure on performance in terms of the fault categories in EPRI TR-107330. The FMEA groups NuPAC platform failure modes by circuit card and by a specific fault associated with a function of that circuit card. Items included in the FMEA are the Carrier Card, Logic Mezzanine, I/O mezzanines, backplane, power sources, and external loop power supplies. Specific information provided by the NuPAC platform FMEA includes:

- System component: system or subsystem being analyzed for failure modes
- Failure mode: description of defect or function loss
- Failure mechanism: cause of failure
- Failure category: failure category from definitions in EPRI TR-107330
- Effect on I/O: result of failure mode on NuPAC platform inputs or outputs
- Effect on functionality: result of failure mode on overall NuPAC platform operability
- Method of Failure Detection: Identifies BIT capability of the NuPAC platform
- Compensating provisions: provisions for failure mode mitigation.

The likelihood of failure information is presented in the form of a component-level (electronic components on the circuit card assemblies) FMECA, NuPAC\_ED610000-050 (**Reference 706**). The component-level FMECA has been performed utilizing the guidance of IEEE Standard 352 (**Reference 343**). Failure rate information from the reliability prediction in conjunction with the fault information from the FMECA is used to rank the individual failure mode end effect fault categories by probability of occurrence.



The FMEA/FMECA results are to be applied to future system-level failures analyses for plant-specific applications of the NuPAC platform, following the guidance in IEEE Standard 352 (**Reference 343**).

The breakdown of failure modes by severity category is shown below:

[

]<sup>a,c,e</sup>

For the plant-specific application of the NuPAC in a redundant configuration, the operator or maintenance crew can simply replace the defective GLM or subassembly without interruption for all BIT Category A faults. BIT Category B faults (not detectable by BIT) must be detected by periodic surveillance testing. However, with proper determination of surveillance test intervals, based on NuPAC specific failure rate information, BIT Category B failures will cause no system level interruption or degradation.

### 6.3.2 Supporting Data for Reliability Analysis

#### 6.3.2.1 Reliability Analysis

The NuPAC Reliability Prediction Report, NuPAC\_ED610000-048 (**Reference 704**), has been prepared for the NuPAC platform in accordance with the guidance contained in IEEE Standard 352 (**Reference 343**).

The reliability analysis provides NuPAC platform reliability predictions to the circuit card level, based on the random hardware failure rate of its components. The failure rate data may represent prediction, test, or observed field failure data. The reliability predictions are performed using the parts stress analysis method. Component stress data, thermal data, and quality data are elements of the reliability prediction and are identified with other component characteristics as the Pi values in the failure rate calculations. The piece part stress level of the electrical components on circuit cards are calculated and recorded. These stress levels are used in the reliability prediction to verify stress level compliance with de-rating criteria. The component failure rates will also be applied to the FMECA. The summary of each of the CCA reliability predictions with failure rate (FR) data are provided in failures per million hours (FPMH) and MTBF values shown in hours. The FR and MTBF data are provided for both a best estimate value of 30 degrees C and a worst case of 60 degrees C.

In an actual nuclear power plant application, the GLM's I/O slots can be configured to hold as few as one (1) and as many as eight (8) I/O mezzanines. To assess a worst case FR and MTBF for a GLM (consisting of the generic I/O Carrier Card, a Logic Mezzanine Card, and the maximum of eight (8) I/O mezzanines), the highest FR (lowest MTBF) for an I/O mezzanine was used, [ ]<sup>a,c,e</sup>. The reliability prediction for this worst case GLM configuration was greater than an MTBF of [ ]<sup>a,c,e</sup> under best estimate temperature conditions and more than [ ]<sup>a,c,e</sup> under worst case temperature conditions.

In addition to the GLM, the RTM reliability prediction results are contained in Appendix C [ ]<sup>a,c,e</sup> and Appendix D [ ]<sup>a,c,e</sup> of NuPAC\_ED610000-048 (**Reference 704**). [ ]<sup>a,c,e</sup>

The reliability analysis results are to be applied to future system-level reliability and availability analyses for plant-specific applications of the NuPAC platform, following the guidance in IEEE Standard 352 (**Reference 343**).

### 6.3.3 Supporting Data for Response Time Analysis

A response time support document, "Supporting Data for Response Time Analysis", NuPAC\_ED610000-051 (**Reference 707**) has been prepared to facilitate future system-level response time calculations for its plant-specific applications. This approach provides a method for calculating the maximum expected discrete input-to-discrete output and analog input-to-discrete output response time, including effects of serial data communication (for both external and backplane links) for specific NuPAC platform hardware and application-specific programmable logic configurations.

### 6.3.4 Supporting Data for Setpoint Analysis

An inaccuracies and uncertainties document, "NuPAC Inaccuracies and Uncertainties", NuPAC\_ED610000-060 (**Reference 708**) has been prepared for the NuPAC platform to support future system-level setpoint calculations for plant-specific applications of the NuPAC platform, following the recommended practices of ISA

S67.04-1994 Part 1 (**Reference 366**) as endorsed by USNRC RG 1.105 (**Reference 130**). The NuPAC Inaccuracies and Uncertainties document has been prepared per the guidance of Section 4.2.4 of EPRI TR-107330 (**Reference 312**) and provides a Licensee input for accuracy, repeatability, drift, and other related data for supported input and output types.

#### 6.4 Limited Life Components

The NuPAC platform hardware was designed to be installed in a mild environment, which does not require establishing a qualified life for the equipment, since maintenance is possible during and after accidents, based on guidance in IEEE Standard 323 (**Reference 339**).

For NuPAC platform hardware described in Section 3.2, the non-volatile memory and fan tray air filter are identified as life-limited components. The non-volatile memory has a limitation on the number of times data can be erased and reprogrammed in memory. [

]<sup>a,c,e</sup>. The fan tray air filter requires to be cleaned at least every [ ]<sup>a,c,e</sup> and to be replaced every [ ]<sup>a,c,e</sup>. There are no other known life-limited components in the generic NuPAC platform hardware described previously in Section 3.2.

Plant-specific NuPAC-based systems will be examined during development to identify if any life-limited components are introduced in the application-specific hardware. If life-limited components are identified, the operational life is documented and an appropriate surveillance, testing, and maintenance program established to detect potential degradation.

#### 6.5 Deleted

## 7.0 INDEPENDENT VERIFICATION AND VALIDATION

This section describes the NuPAC Independent Verification and Validation (IV&V) organization, processes and results. The NuPAC IV&V organization is responsible for the verification and validation efforts related to the NuPAC Programmable Logic (PL). In accordance with IEEE Standard 7-4.3.2 Clause 5.3.3 and 5.3.4 (**Reference 356**) as endorsed by USNRC RG 1.152 (**Reference 133**), the NuPAC IV&V processes are integral to the NuPAC development lifecycle and are invoked for all safety-related PL. The IV&V processes described in this section are defined in detail by the NuPAC FPL Verification and Validation Plan (FVVP) (**Reference 711**) and follows the guidance of IEEE Standard 1012 (**Reference 328**) as endorsed by USNRC RG 1.168 (**Reference 135**). The results discussed in Sections 7.5 and 7.6 are the results of the NuPAC Core PL IV&V effort. When an implementation of the NuPAC platform for a specific application is developed, the ASPLD will be subject to an IV&V effort commensurate with the safety level of the application.

### 7.1 IV&V Independence

The NuPAC IV&V efforts are conducted by an organization that is technically, managerially, and financially independent from the NuPAC Design organization, as described in the NuPAC QA Plan (**Reference 719**) and NuPAC Program Management Plan (**Reference 718**). The level of independence correlates to the “classical” independence description as discussed in IEEE Standard 1012 Section C.4.1 (**Reference 328**). The IV&V independence ensures budget and schedule freedom from the Design organization. Managerially, the IV&V organization reports through a management chain separate from the Design organization. IV&V reports to an Assurance Manager, while the Design organization reports to a Program Manager and Director. Technical independence ensures that IV&V personnel have not participated in or contributed to the development of the NuPAC design artifacts that are under verification by the IV&V organization. The IV&V organization determines the methods and resources for verification independently of the NuPAC Design organization. These independence attributes meet the intent of IEEE Standard 7-4.3.2 Clause 5.3.4 (**Reference 356**) and ensure the IV&V organization is free to report technical issues identified during the various IV&V tasks.

### 7.2 IV&V Process Overview

The NuPAC FVVP defines the IV&V scope, organization, and processes used to verify the NuPAC PL. The FVVP was written to meet the intent of IEEE Standard 1012 (**Reference 328**) as endorsed by USNRC RG 1.168 (**Reference 135**). The extent of IV&V tasks performed per IEEE Standard 1012 is a function of the Software Integrity Level (SIL) chosen for a particular software design. The NuPAC PL is intended to provide a safety function in a nuclear power plant, and as such, the FVVP defines all NuPAC platform PL as SIL Level 4 which is the highest integrity level and requires a full scope IV&V effort. The following sections give an overview of the various IV&V tasks required by the FVVP. For each task, the FVVP defines the required Inputs, Outputs, and documentation requirements. The tasks follow the software life cycle activities defined in IEEE Standard 1012. The roles of “Acquirer” and “Supplier” for the NuPAC product follow the standard designation as described in IEEE Standard 1012, with the Acquirer being the customer organization and the Supplier being the NuPAC Design organization.

### 7.2.1 Acquisition Support Activity

The Acquisition Support Activity occurs at the beginning of the NuPAC lifecycle and consists of the following tasks:

1. Scoping the IV&V Effort - This activity consists of determining the SIL level (and subsequent tasks required), determining the IV&V independence, and determining budget and resource needs such as special tools or test facilities.
2. Planning the Interface between the IV&V Effort and Supplier - This task consists of refining the IV&V schedule based on the required tasks, identifying the Design processes and product that will be evaluated by IV&V, and coordinating the plan with the acquirer.
3. System Requirements Review - This task is a review of the system-level requirements to determine feasibility of implementation and testability of the requirements.
4. Acceptance support - This task refers to the development related tasks for the creation of test plans, test designs, test cases, and test procedure generation to aid in understanding of activity flow.

### 7.2.2 Planning Activity

The Planning Activity consists of two tasks:

1. Planning the Interface Between the IV&V Effort and Supplier - This task is focused on establishing plans for exchanging data and IV&V results with the Design organization and reviewing the Design development plans/schedules to coordinate the IV&V schedule of tasks.
2. Contract Verification - This task consists of verifying system requirements are consistent with and satisfy user needs and verifying procedures are in place for managing requirements changes, acceptance criteria, problem resolution and organizational interfaces.

### 7.2.3 Concept Activity

The Concept Activity begins the “Development Process” as defined in the FVVP and IEEE Standard 1012 (**Reference 328**), which concludes with the Test Activity. The Concept Activity includes the following tasks:

1. Concept Documentation Evaluation – In this task, the concept documentation is evaluated to ensure the documents meet user needs and is consistent with acquisition needs. System requirements are also analyzed against user needs.
2. Hardware/FPL/Software/User Requirements Allocation Analysis – this task consists of verifying NuPAC system level requirements were appropriately allocated to PL and hardware.
3. Traceability Analysis – This task begins the traceability effort for NuPAC IV&V and consists of verifying the system level requirements that will be implemented completely or partially by the PL are traceable to the GLM specification.

#### 7.2.4 Requirements Activity

The Requirements Activity consists of the following tasks:

1. Traceability Analysis – For this traceability analysis, the PL requirements allocated in the GLM specification are traced to the detailed PL requirements documents. Likewise, the traceability from the PL requirements documents are traced to the GLM specification.
2. FPL Requirements Evaluation – This task evaluates the PL requirements for correctness, consistency, completeness, accuracy, readability, and testability.
3. Interface Analysis – This analysis checks the PL requirements related to hardware interfaces for correctness, consistency, completeness, accuracy, and testability.
4. System Test Plan Generation – The System Test Plan is created to plan the extent of testing required at the NuPAC system level and determine what PL requirements will need to be validated at the system level. System level refers to the testing of NuPAC PL programmed onto NuPAC specific hardware at the GLM and Chassis level. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.
5. Acceptance Test Plan Generation – Similar to the System Test Plan, the Acceptance Test Plan is created to plan the extent of acceptance testing and the requirements validated at this level. Acceptance testing is executed at the chassis level to test the NuPAC system in an operational configuration. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.
4. Configuration Management Assessment – This task is an assessment of the PL development configuration management processes to determine if adequate procedures are in place for configuration control and that the processes are being followed to ensure changes are managed accordingly.

#### 7.2.5 Design Activity

The Design Activity consists of the following tasks:

1. Traceability Analysis – For the Design Activity, the Traceability Analysis traces the PL requirements to specific PL design elements and vice versa. This ensures that all PL requirements are included in the detailed PL design and that unnecessary functionality is not included in the design.
2. FPL Design Evaluation – This task evaluates the detailed PL design elements for correctness, consistency, completeness, accuracy, readability, and testability. This task is an extension of the FPL Requirements Evaluation from the Requirements Activity, but focused on the design details resulting from the requirements.
3. Interface Analysis – The Interface Analysis for the Design Activity is focused on the internal and external PL interfaces and evaluating the design details with respect to correctness, consistency, completeness, accuracy, and testability. Particular emphasis is placed on ensuring the PL design is consistent with the various external hardware interfaces.

4. Component and Integration Test Plan Generation – The Component and Integration Plans are generated to plan the extent of Component and Integration and the requirements that will be verified by the tests. The Test Plans will define the overall approach and identify any features that will not be tested at this level. The Component and Integration Test Plans also provide an overview of the required levels of PL test coverage with respect to code coverage and functional coverage. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.
5. Component and Integration Test Design Generation – The Component and Integration Test Designs are created to provide more detail on executing the Test Plans. Overall test cases are defined and the pass/fail criteria are outlined. The test configuration is also described. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.
6. System and Acceptance Test Design Generation – Similar to the Component and Integration Test Designs, the System and Acceptance Level test cases are defined and pass/fail criteria are outlined. An overview of the test configuration is described. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.

### 7.2.6 Implementation Activity

The Implementation Activity consists of the following tasks:

1. Traceability Analysis – This Traceability Analysis traces the PL requirements to the PL source code implementation and vice versa. The task confirms the PL requirements have been completely implemented and that the PL does not contain any unwanted or unused code.
2. Source Code and Source Code Documentation Evaluation – This task consists of an extensive review of the implemented PL code. This is conducted by a line-by-line review of the code to evaluate the design implementation against the design requirements as well as coding standards and guidelines established by the PL Design Team. The code is also evaluated for any potential unused or unnecessary code.
3. Interface Analysis – This task is similar to the Source Code and Source Code Documentation Evaluation but with an emphasis on the internal and external PL interfaces. The PL code is evaluated against interface requirements and the coding standards and guidelines mentioned previously.
4. Component and Integration Test Case Generation – The Component and Integration Test Cases are generated. The Test Case document defines all of the test cases in detail including the test case identifier, test case objectives, requirements to be tested, any special test case interdependencies and other special procedural requirements. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.
5. System and Acceptance Test Case Generation – The System and Acceptance Test Case documents contain similar content to the Component and Integration Test Case documents but are focused on the higher level System and Acceptance tests. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.
6. Component and Integration Test Procedure Generation – The Component and Integration Test Procedures provide the necessary detail for completing each of the test cases defined in the Test Case

document. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.

7. System Test Procedure Generation – Similar to the Component and Integration test procedure generation, the System Test procedures are generated. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.
8. Component Test Execution – Using the Component Test Procedure(s), the Component Test Cases are executed and the results recorded. Results are evaluated and discrepancies documented accordingly.

#### **7.2.7 Test Activity**

As defined in the FVVP, the Test Activity is the final activity that is applicable to the NuPAC platform IV&V effort. The Test Activity is defined by the following tasks:

- i. Integration and System Test Execution – Using the Integration and System test procedures, the Integration and System tests are each executed and results recorded. Results are evaluated and discrepancies are identified.
- ii. Acceptance Test Procedure Generation- The procedures for executing the Acceptance Test are created. The content is similar to the Component, Integration, and System level procedures. Refer to Section 7.3 for further discussion on NuPAC IV&V test documentation and the various levels of test.
- iii. Acceptance Test Execution – Using the Acceptance Test Procedure, the test is executed and results are recorded. The test results are evaluated and discrepancies identified.

#### **7.2.8 Installation and Checkout, Operation, Maintenance Activities**

The FVVP defines the overall process for IV&V activities related to the NuPAC generic platform. As described in the FVVP, the Installation and Checkout, Operation, and Maintenance Activities are outside of the current scope of the NuPAC IV&V effort. The activities that normally occur after the Test Activity as described by IEEE Standard 1012 (**Reference 328**) are more relevant to a project with an intended end-user application that will be installed into a specific plant operating environment. As such, these activities will be defined further in the FVVP and incorporated into the IV&V process when an application specific project is initiated.

#### **7.2.9 Repetitive Tasks**

There are several tasks that are repeated during each lifecycle activity (from Concept to Test Activity). These tasks are adapted based on the particular inputs from each activity:

1. Risk Analysis – The Risk Analysis task is performed to identify potential technical and project/programmatic risks. The tasks and the task inputs related to each Activity are reviewed and any risks identified are documented through the appropriate reporting system (e.g. anomaly database, corrective action database, or project risk register). The intent is to identify risks affecting the quality of the NuPAC PL design or the IV&V effort and mitigate or eliminate those potential risks.
2. Hazard Analysis – The Hazard analysis is adapted for each Activity. The task evaluates Activity-specific inputs (e.g. PL FMEA) to identify hazards at the PL, GLM, or System level.

3. Security Analysis – The Security Analysis task focuses on security related design details of the NuPAC system in the context of an operating environment, as well as the processes and environment in place for developing the NuPAC PL (e.g. Secure Development Environment). The task is repeated for each Activity and is tailored to the inputs from each Activity.

### 7.2.10 Deferred Tasks

The following tasks as described in the FVVP are not executed due to limitations in scope or to the lack of value added by task execution:

1. Criticality Analysis – This task as described in IEEE Standard 1012 (**Reference 328**) is aimed at verifying that the appropriate Software Integrity Level is assigned to each portion of the design and requirements throughout the development lifecycle. However, since the NuPAC FVVP designates all PL as SIL level 4, there is no need to evaluate the SIL assignment since it does not change.
2. User Documentation Evaluation – This task is deferred due to the NuPAC platform being generic in nature and the lack of an application-specific user defined. The necessary Inputs for this task have not been created for the NuPAC IV&V organization to evaluate.

## 7.3 IV&V Testing and Documentation

The NuPAC IV&V organization conducts various levels of testing to verify and validate the NuPAC PL design requirements. The testing is structured to build from the lower level detailed design requirements and end with higher-level system related requirements. Throughout the test process and hierarchy, the test documentation is structured to meet the intent of IEEE Standard 829 (Reference 358) as endorsed by USNRC RG 1.170 (Reference 137). Traceability from the design requirements to test case implementation is defined and maintained throughout the process. This section provides further details on the NuPAC IV&V testing and the documentation details.

### 7.3.1 Master Test Plan

The NuPAC IV&V Master Test Plan is contained in Section 8 of the FVVP. This Master Test Plan defines the levels of testing and the requirements for the contents of the various test documents. There are four levels of test defined for the NuPAC IV&V effort:

1. Component Testing – [

---

]<sup>a,c,e</sup>

2. Integration Testing – [

]<sup>a,c,e</sup>

3. System Testing – [

]<sup>a,c,e</sup>

4. Acceptance Testing – [

]<sup>a,c,e</sup>

In accordance with FVVP Section 8, each of these four levels of testing requires a hierarchy of test documentation. The following sections summarize the general content for the test documentation.

### 7.3.2 Test Plans

Test Plan is the upper level document for each level of test. The plan includes the test objectives and scope, a definition of the features to be tested and features not to be tested, the overall test approach and pass/fail criteria. The test environment is described and necessary resources are identified. The Test Plan can also identify any risks or contingencies associated with the level of test.

### 7.3.3 Test Designs

The Test Design further refines the test approach defined in the Test Plan. The test configuration is defined and the features to be tested may be elaborated in greater detail. Initial test cases are identified and described at a high level to aid in tracing requirements to test coverage. The test deliverables are also identified.

### 7.3.4 Test Case Documents

The Test Case Document defines the details for all test cases including a unique identifier for each test case, the objective of each test case, and the input and output specifications. Any special environmental needs, procedural requirements, or intercase dependencies for each test case are defined. The test case document will also identify how the test cases are traced to requirements and/or objectives.

### 7.3.5 Test Procedures

Test Procedures provide the detailed instructions on how to conduct the test. The test procedures may be different for each test case or may cover several or all of the test cases if the execution is generic in nature. The test procedures will have enough detail to ensure the test can be repeated. The test setup and configuration may also be described in the procedure.

### 7.3.6 Test Reports

The results of each test level are documented in a task report that describes the test results. The details regarding the pass/fail result of each test case are described. The test results will identify who performed the testing and when it was conducted. Any test failures or test discrepancies will be described and evaluated. Detailed test artifacts such as datasheets or automated log files may be attached as an appendix to the test results. Test failures will be documented in the IV&V anomaly database (see Section 7.4.2). The test results will include an overall evaluation of the test and conclusions reached based on the test.

## 7.4 IV&V Administrative Topics

### 7.4.1 IV&V Documentation Requirements

Throughout the NuPAC IV&V effort, the FVVP requires a structured approach to documenting the tasks performed and the results. For each task completed, a Task Report is created to describe the task, the results, an evaluation of any issues, and the conclusions reached. If an anomaly is identified during a task, an Anomaly Report will accompany the Task Report to describe the anomaly, the design artifact where the anomaly was identified, and other relevant details (See section 7.4.2 below). At the end of each IV&V activity, an Activity Summary Report is created that describes the tasks completed during the activity and a collective assessment of the results. Finally, at the completion of the IV&V effort, a Final Report is created to summarize the results of each activity. The Final Report will evaluate the results and provide a conclusion or assessment of the NuPAC PL quality. Any lessons learned, best practices, or recommendations can also be included in the Final Report.

### 7.4.2 Anomaly Reporting and Resolution

During IV&V task execution, any finding discovered by the IV&V organization that does not meet the acceptance criteria for a particular task or is shown to violate a regulatory or safety requirement will be documented as an anomaly in the IV&V anomaly reporting database. The use of the anomaly database is controlled by a procedure that defines the entire process from anomaly identification to anomaly resolution and closure. The IV&V organization documents anomalies and the Design organization addresses the anomaly by providing details on the implemented solution. Once the IV&V organization confirms the anomaly is addressed in a revised or newly released design artifact, the anomaly may be closed. The database provides the capability for tracking various anomaly metrics based on the artifact where the anomaly was identified, the task or activity associated the anomaly, who discovered the anomaly, anomaly status, etc. Anomaly criticality levels are defined in the FVVP and are used to prioritize resolution efforts and communicate the potential impact of the anomaly to the Design organization.

#### 7.4.3 Use of Software Tools

The NuPAC IV&V organization leverages software tools to conduct various portions of the IV&V test effort and other IV&V tasks. IEEE Standard 7-4.3.2 (**Reference 356**) as endorsed by USNRC RG 1.152 (**Reference 133**) states the following in clause 5.3.2:

*'One or both of the following methods shall be used to confirm the software tools are suitable for use:*

- a) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.*
- b) The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.*

*Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.'*

In accordance with IEEE standard 7-4.3.2, the IV&V organization conducts an evaluation on all software tools used in the verification and validation effort. The evaluation considers if the manner in which the tool is proposed to be used will allow other levels of IV&V activities to catch potential design anomalies masked due to a tool problem. Alternatively, the evaluation will describe any validation testing conducted on the tool by the IV&V organization to demonstrate that the tool features are reliable. In both cases, the tool evaluation discusses the industry or operating experience of the tool to support the conclusion that a tool is acceptable for use. The tool evaluation also documents the tool vendor/supplier, the version or release number, the task in which the tool will be used, and any relevant notes relevant to the tool such as vendor support or troubleshooting contacts.

#### 7.5 IV&V Results for NuPAC Core PL

This section describes the results of the NuPAC IV&V efforts for verifying and validating the NuPAC Core PL, which is the generic logic contained on each GLM Logic Mezzanine described in section 3.0. The Core PL design went through one full iteration and one regression effort of the IV&V process described in Section 7.2. The results of each iteration and the conclusions reached are summarized below.

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

### 7.5.3 Open Anomalies for the NuPAC Core PL

At the conclusion of the Baseline 1.3.2 IV&V effort, there are [ ]<sup>a,c,e</sup> anomalies remaining open that will need to be addressed in future applications. [

]<sup>a,c,e</sup> are mild or

moderate in nature and can be addressed with small changes to the design documentation or small changes to the PL code. [

]<sup>a,c,e</sup>

### 7.5.4 IV&V Conclusions

The NuPAC Core PL design has been extensively reviewed and tested by the IV&V organization for both Baseline 1.3.1 and 1.3.2. The design was fully exercised as demonstrated by the combined test coverage from Component, Integration, System, and Acceptance testing. The design documentation has been thoroughly reviewed with respect to completeness, correctness, accuracy, readability, and testability. Code evaluations confirmed the correct implementation of requirements and conformance to coding standards and guidelines. Additionally, requirements traceability tasks confirmed that the design requirements were appropriately implemented and tested. The overall quality of the design has strengthened from Baseline 1.3.1 to 1.3.2. Other than the remaining open anomalies, the Core PL design has been confirmed to be a correct, accurate, and complete implementation of the PL requirements and unused or nonessential code and features have not been introduced.

## 8.0 SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT

This section describes the NuPAC digital control system platform vulnerability assessment and identifies the associated methodology to apply the Secure Development and Operational Environment. As a safety-related platform, it is expected that all applications of NuPAC will be considered Critical Digital Assets (CDA), or a portion thereof, by a Licensee. Additionally, it will be an application requirement and expectation that the Licensee define the associated CDA (e.g., a Reactor Protection System) as a Level 4 CDA. A Level 4 CDA is defined not to have any potential externally-generated, inbound communication, which could make it susceptible to malicious intent. Therefore, this document and the NuPAC System Security Plan (**Reference 725**) only address the 10 CFR 50 (**Reference 101**) and USNRC RG 1.152 (**Reference 133**) secure development environment for a platform and do not address 1) the operational constraints of an SDOE defined in an application or 2) cyber-security requirements of 10 CFR73.54 (**Reference 105**) and guidance provided in USNRC RG 5.71 (**Reference 151**).

### 8.1 System Security Planning

[

]<sup>a,c,e</sup> This configuration is described in more detail in Appendix B of the security plan. The SDE is described in more detail in the Secure Development Environment Description (**Reference 751**).

### 8.2 Vulnerability Assessment

[

]<sup>a,c,e</sup>

[

]<sup>a,c,e</sup>

The NuPAC Vulnerability Assessment Report (VA) for Secure Development Environment (SDE), (**Reference 703**) presents a methodology, which can be applied as a basis for conducting future system-level analyses for plant-specific NuPAC-based systems.

### 8.3 Secure Development and Operational Environment Controls

[

]<sup>a,c,e</sup>

For the NuPAC platform development, the System Security Plan (**Reference 725**) specifies the security controls for the platform development. [

|

]<sup>a,c,e</sup>

---



[ ]  
]<sup>a,c,e</sup>

#### 8.4 Deleted



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 124 of 263  
Date: 04/14/2017

---

This page intentionally left blank.

## 9.0 COMPLIANCE WITH KEY STANDARDS AND INTERIM STAFF GUIDANCE

The suitability of a digital control system platform for use in NPP safety systems is dependent on the quality of platform components; quality of the design process; and aspects of system implementation, such as real time performance, independence, and ability to self-identify problems with system operation. The NuPAC platform was developed, qualified, and supplied under a quality program that was developed to meet the requirements of Title 10 of the Code of Federal Regulations Part 50 (10 CFR 50) Appendix B, ASME Nuclear Quality Assurance (NQA)-1-2008 (**Reference 304**), ASME NQA-1a-2009, Addenda to ASME NQA-1-2008 (**Reference 305**), and USNRC RG 1.28 (**Reference 145**).

DI&C-ISG-06 identifies the following 2 key standards to ensure compliance with I&C hardware and software requirements. The NuPAC platform design is in accordance with the applicable provisions of:

- IEEE Standard 603-1991 (**Reference 153**), “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”
- IEEE Standard 7-4.3.2-2003 (**Reference 356**), “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

In designing the NuPAC platform, the following USNRC Interim Staff Guidance (ISG) was also used as appropriate:

- DI&C-ISG-04 (**Reference 117**), ISG on Highly Integrated Control Rooms and Digital Communication Systems.

An important basis for preparing licensing review information presented in this document was:

- DI&C-ISG-06 (**Reference 119**), Licensing Process ISG.

For each of the above standards and guidelines, a compliance table is provided in the appendices. The tables describe how NuPAC complies with the applicable clauses of the document.

### 9.1 Compliance with IEEE Standard 603-1991

The NuPAC platform conforms to IEEE Standard 603-1991 (**Reference 153**) as set forth by 10 CFR 50.55a(h)(2) (**Reference 104**) and endorsed in USNRC RG 1.153 (**Reference 134**). Please refer to the IEEE Standard 603-1991 compliance matrix in Appendix B for more detailed data.

### 9.2 Compliance with IEEE Standard 7-4.3.2-2003

The NuPAC platform conforms to IEEE Standard 7-4.3.2-2003 (**Reference 356**) as endorsed in USNRC RG 1.152 (**Reference 133**). Please refer to the IEEE Standard 7-4.3.2-2003 compliance matrix in Appendix C for more detailed data.

### 9.3 Deleted

### 9.4 DI&C-ISG-04, Rev. 1

The aspects of DI&C-ISG-04 (**Reference 117**) area of interest #1, "Interdivisional Communication," as implemented by NuPAC, are described in detail in the compliance matrix included in Appendix D and in Section



3.4 of this report. The platform is designed consistent with this area of interest so that the NuPAC platform is directly usable for future safety-system applications. The generic NuPAC platform and plant-specific NuPAC-based systems will comply with DI&C-ISG-04 guidance regarding interdivisional communication. Compliance with the other aspects of DI&C-ISG-04, areas of interest #2 and #3, will be addressed as part of future system-level analyses for plant-specific NuPAC-based systems.

### 9.5 DI&C-ISG-06, Rev. 1

This LTR and the supporting documentation for review of the generic NuPAC digital safety I&C platform are consistent with the guidance, for a Tier 3 review, provided in USNRC document DI&C-ISG-06 (**Reference 119**). Refer to the DI&C-ISG-06 compliance matrix in Appendix E of this LTR and Appendix F as a cross-reference for documentation provided for the Phase 1 review.

### 9.6 Deleted

## 10.0 REFERENCES

The list of document references identified in Section 10 represents a comprehensive list of USNRC Regulatory Guidance, Industry Codes and Standards, related to instrumentation and control systems and their application, as well as NuPAC program specific references that may be incorporated into the overall NuPAC program. It is not intended that every reference be specifically described within the body of this topical report or used for the current review. Refer to Section 2.0 for the documentation applicable to this report and review. This table includes guidance and standards to be used as the platform is expanded and to be documented in future updates.

- The USNRC Codes and Regulatory Guidance references are identified as 100 thru 299
- The Industry Codes and Standards are identified as 300 thru 699
- The NuPAC program specific references are identified as 700 thru 999

**Table 10.0-1. USNRC Codes and Regulatory Guidance**

| Reference Number | Document Number           | Description  | Rev | Date       |
|------------------|---------------------------|--|-----|------------|
| 100              | 10 CFR Part 21            | Reporting of Defects and Noncompliance   | N/A | N/A        |
| 101              | 10 CFR Part 50            | Domestic Licensing of Production and Utilization Facilities  | N/A | N/A        |
| 102              | 10 CFR Part 50 Appendix A | Appendix A to Part 50 - General Design Criteria for Nuclear Power Plants                                 | N/A | N/A        |
| 103              | 10 CFR Part 50 Appendix B | Appendix B to Part 50 - Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants | N/A | N/A        |
| 104              | 10 CFR Part 50.55a(h)(2)  | Codes and Standards, paragraph (h), Protection Systems   | N/A | N/A        |
| 105              | 10 CFR Part 73 Section 54 | Protection of Digital Computer and Communication Systems and Networks                                    | N/A | N/A        |
| 106              | 10 CFR Part 810           | Assistance to Foreign Atomic Energy Activities   | N/A | N/A        |
| 107              | BTP 7-8                   | Guidance for Application of Regulatory Guide 1.22  | 5   | March 2007 |
| 108              | BTP 7-10                  | Guidance for Application of Regulatory Guide 1.97  | 5   | March 2007 |
| 109              | BTP 7-11                  | Guidance on Application and Qualification of Isolation Devices   | 5   | March 2007 |

| Reference Number | Document Number | Description   | Rev | Date          |
|------------------|-----------------|---|-----|---------------|
| 110              | BTP 7-12        | Guidance on Establishing and Maintaining Instrument Setpoints   | 5   | March 2007    |
| 111              | BTP 7-13        | Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors                                     | 5   | March 2007    |
| 112              | BTP 7-14        | Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems                             | 5   | March 2007    |
| 113              | BTP 7-17        | Guidance on Self-Test and Surveillance Test Provisions  | 5   | March 2007    |
| 114              | BTP 7-19        | Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems | 6   | July 2012     |
| 115              | BTP 7-21        | Guidance on Digital Computer Real-Time Performance  | 5   | March 2007    |
| 116              | Available       |   |     |               |
| 117              | DI&C-ISG-04     | Task Working Group #4: Highly-Integrated Control Rooms - Communications Issues (HICRc)                                  | 1   | March 2009    |
| 118              | DI&C-ISG-05     | Task Working Group #5: Highly-Integrated Control Rooms - Human Factors Issues (HICR-HF)                                 | 1   | November 2008 |
| 119              | DI&C-ISG-06     | Task Working Group #6: Licensing Process  | 1   | January 2011  |
| 120              | GL 89-02        | Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products                                      | N/A | March 1989    |
| 121              | GL 91-05        | Licensee Commercial-Grade Procurement and Dedication Programs   | N/A | April 1991    |
| 122              | NUREG/CR-6101   | Software Reliability and Safety in Nuclear Reactor Protection Systems   | N/A | June 1993     |
| 123              | NUREG/CR-6303   | Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems                             | N/A | December 1994 |

| Reference Number | Document Number | Description  | Rev | Date           |
|------------------|-----------------|--|-----|----------------|
| 124              | NUREG/CR-6463   | Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems - Final Report   | N/A | June 1996      |
| 125              | NUREG-0700      | Human System Interface Design Review Guidelines  | 2   | May 2002       |
| 126              | NUREG-0711      | Human Factors Engineering Program Review Model   | 3   | November 2012  |
| 127              | NUREG-0800      | Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition   | N/A | N/A            |
| 128              | USNRC RG 1.97   | Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants  | 4   | June 2006      |
| 129              | USNRC RG 1.100  | Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants | 3   | September 2009 |
| 130              | USNRC RG 1.105  | Setpoints for Safety-Related Instrumentation   | 3   | December 1999  |
| 131              | USNRC RG 1.118  | Periodic Testing of Electric Power and Protection Systems  | 3   | April 1995     |
| 132              | USNRC RG 1.151  | Instrument Sensing Lines   | 1   | July 2010      |
| 133              | USNRC RG 1.152  | Criteria for Use of Computers in Safety Systems of Nuclear Power Plants  | 3   | July 2011      |
| 134              | USNRC RG 1.153  | Criteria for Safety Systems  | 1   | June 1996      |
| 135              | USNRC RG 1.168  | Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants                               | 2   | July 2013      |
| 136              | USNRC RG 1.169  | Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants  | 1   | July 2013      |
| 137              | USNRC RG 1.170  | Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants  | 1   | July 2013      |

| Reference Number | Document Number | Description  | Rev | Date          |
|------------------|-----------------|--|-----|---------------|
| 138              | USNRC RG 1.171  | Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants                                       | 1   | July 2013     |
| 139              | USNRC RG 1.172  | Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants | 1   | July 2013     |
| 140              | USNRC RG 1.173  | Developing Software Life-Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants                    | 1   | July 2013     |
| 141              | USNRC RG 1.180  | Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems         | 1   | October 2003  |
| 142              | USNRC RG 1.204  | Guidelines for Lightning Protection of Nuclear Power Plants  | 0   | November 2005 |
| 143              | USNRC RG 1.209  | Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants  | 0   | March 2007    |
| 144              | USNRC RG 1.22   | Periodic Testing of Protection System Actuation Functions  | 0   | February 1972 |
| 145              | USNRC RG 1.28   | Quality Assurance Program Criteria (Design and Construction)   | 4   | June 2010     |
| 146              | USNRC RG 1.47   | Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems   | 1   | February 2010 |
| 147              | USNRC RG 1.53   | Application of the Single-Failure Criterion to Safety Systems  | 2   | November 2003 |
| 148              | USNRC RG 1.62   | Manual Initiation of Protective Actions  | 1   | June 2010     |
| 149              | USNRC RG 1.75   | Criteria for Independence of Electrical Safety Systems   | 3   | February 2005 |

| Reference Number | Document Number                         | Description  | Rev | Date         |
|------------------|---|--|-----|--------------|
| 150              | USNRC RG 1.89                           | Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants                             | 1   | June 1984    |
| 151              | USNRC RG 5.71                           | Cyber Security Programs for Nuclear Facilities   | 0   | January 2010 |
| 152              | 10 CFR Part 50.55a                      | Codes and Standards, Documents approved for incorporation by reference   | N/A | N/A          |
| 153              | IEEE Std 603-1991                       | IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations; Institute of Electrical and Electronics Engineers | N/A | 1991         |
| 154              | IEEE Std 603-1991 Correction Sheet 1995 | IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations; Institute of Electrical and Electronics Engineers | N/A | 1995         |
| 155              | 10 CFR Part 50.54(jj)                   | Quality standards for 10CFR50.55a SSCs   | N/A | N/A          |
| 156              | 10 CFR Part 50.55(i)                    | Quality standards for 10CFR50.55a SSCs   | N/A | N/A          |
| 157-300          | Reserved for future use                 |  |     |              |

**Table 10.0-2. Industry Standards and Guidance**

| Reference Number | Document Number         | Description  | Rev | Date        | Owner  |
|------------------|-------------------------|--|-----|-------------|--|
| 301              | ANSI/IEEE Std 1042-1987 | IEEE Guide to Software Configuration Management  | N/A | 1987        | American National Standards Institute/ Institute of Electrical and Electronics Engineers |
| 302              | ANSI/VITA 4-1995        | American National Standards for IP Modules   | N/A | 1995        | American National Standards Institute/VMEbus International Trade Association             |
| 303              | ANSI/VITA 57.1-2008     | American National Standard for FPGA Mezzanine Card (FMC) Standard  | N/A | 2008        | American National Standards Institute/VMEbus International Trade Association             |
| 304              | ASME NQA-1-2008         | Quality Assurance Requirements for Nuclear Facility Applications   | N/A | March 2008  | American Society of Mechanical Engineers   |
| 305              | ASME NQA-1a-2009        | Addenda to ASME NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications             | N/A | August 2009 | American Society of Mechanical Engineers   |
| 306              | Available               |  |     |             |  |
| 307              | Available               |  |     |             |  |
| 308              | EPRI NP-5652            | Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07) | 0   | June 1988   | Electric Power Research Institute  |
| 309              | EPRI TR-102260          | Supplemental Guidance for the Application of EPRI NP-5652 on the Utilization of Commercial-Grade Items   | 0   | May 1994    | Electric Power Research Institute  |
| 310              | EPRI TR-102323          | Guidelines for Electromagnetic Interference Testing in Power Plants                                      | 1   | April 1997  | Electric Power Research Institute  |

| Reference Number | Document Number | Description   | Rev | Date          | Owner                                     |
|------------------|-----------------|---|-----|---------------|---|
| 311              | EPRI TR-106439  | Guideline on the Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications  | 0   | November 1996 | Electric Power Research Institute         |
| 312              | EPRI TR-107330  | Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants  | 0   | December 1996 | Electric Power Research Institute         |
| 313              | IEC 60297-3-100 | Mechanical structures for electronic equipment – Dimensions of mechanical structures of the 482,6 mm (19 in) series – Part 3-100: Basic dimensions of front panels, subracks, chassis, racks and cabinets | 1.0 | Nov 2008      | International Electrotechnical Commission |
| 314              | Available       |   |     |               |   |
| 315              | IEC 61000-4-10  | Electromagnetic Compatibility (EMC) - Part 4-10: Damped Oscillatory Magnetic Field Immunity Test  | 1.0 | June 1993     | International Electrotechnical Commission |
| 316              | IEC 61000-4-12  | Electromagnetic Compatibility (EMC) - Part 4-12: Oscillatory Waves Immunity Tests   | 1.0 | May 1995      | International Electrotechnical Commission |
| 317              | IEC 61000-4-16  | Electromagnetic Compatibility (EMC) - Part 4-16: Test for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz  | 1.0 | January 1998  | International Electrotechnical Commission |
| 318              | IEC 61000-4-1   | Electromagnetic Compatibility (EMC) - Part 4-1: Testing and Measurement Techniques - Overview of IEC 61000-4 Series   | 1.0 | December 1992 | International Electrotechnical Commission |

| Reference Number | Document Number | Description  | Rev | Date          | Owner                                     |
|------------------|-----------------|--|-----|---------------|---|
| 319              | IEC 61000-4-2   | Electromagnetic Compatibility (EMC) - Part 4-2: Testing and Measurement Techniques - Electrostatic Discharge Immunity Test                                 | 1.0 | January 1995  | International Electrotechnical Commission |
| 320              | IEC 61000-4-3   | Electromagnetic Compatibility (EMC) - Part 4-3: Testing and Measurement Techniques - Radiated, Radio-Frequency, Electromagnetic Field Immunity Test        | 1.0 | February 1995 | International Electrotechnical Commission |
| 321              | IEC 61000-4-4   | Electromagnetic Compatibility (EMC) - Part 4-4: Testing and Measurement Techniques - Electrical Fast Transient/Burst Immunity Test                         | 1.0 | January 1995  | International Electrotechnical Commission |
| 322              | IEC 61000-4-5   | Electromagnetic Compatibility (EMC) - Part 4-5: Testing and Measurement Techniques - Surge Immunity Test   | 1.0 | February 1995 | International Electrotechnical Commission |
| 323              | IEC 61000-4-6   | Electromagnetic Compatibility (EMC) - Part 4-6: Testing and Measurement Techniques - Immunity to Conducted Disturbances, Induced by Radio-Frequency Fields | 1.0 | April 1996    | International Electrotechnical Commission |
| 324              | IEC 61000-4-8   | Electromagnetic Compatibility (EMC) - Part 4-8: Power Frequency Magnetic Field Immunity Test   | 1.0 | June 1993     | International Electrotechnical Commission |
| 325              | IEC 61000-4-9   | Electromagnetic Compatibility (EMC) - Part 4-9: Pulse Magnetic Field Immunity Test   | 1.0 | June 1993     | International Electrotechnical Commission |

| Reference Number | Document Number      | Description  | Rev | Date      | Owner   |
|------------------|----------------------|--|-----|-----------|---|
| 326              | IEC 61784-3          | Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions            | 2.0 | June 2010 | International Electrotechnical Commission   |
| 327              | IEEE Std 1008-1987   | IEEE Standard for Software Unit Testing  | N/A | 1987      | American National Standards Institute/Institute of Electrical and Electronics Engineers |
| 328              | IEEE Std 1012-2004   | IEEE Standard for Software Verification and Validation   | N/A | 2004      | Institute of Electrical and Electronics Engineers                                       |
| 329              | IEEE Std 1023-1988   | IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations | N/A | 1988      | Institute of Electrical and Electronics Engineers                                       |
| 330              | IEEE Std 1028-2008   | IEEE Standard for Software Reviews and Audits  | N/A | 2008      | Institute of Electrical and Electronics Engineers                                       |
| 331              | IEEE Std 1050-1996   | IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations  | N/A | 1996      | Institute of Electrical and Electronics Engineers                                       |
| 332              | IEEE Std 1058.1-1987 | IEEE Standard for Software Project Management Plans  | N/A | 1987      | Institute of Electrical and Electronics Engineers                                       |
| 333              | IEEE Std 1074-2006   | IEEE Standard for Developing a Software Project Life Cycle Process   | N/A | 2006      | Institute of Electrical and Electronics Engineers                                       |
| 334              | IEEE Std 1101.1-1998 | IEEE Standard for Mechanical Core Specifications for Microcomputers Using IEC 60603-2 Connectors                                       | N/A | 1998      | Institute of Electrical and Electronics Engineers                                       |

| Reference Number | Document Number        | Description   | Rev | Date | Owner   |
|------------------|------------------------|---|-----|------|---|
| 335              | IEEE/EIA 12207.0-1996  | Industry Implementation of International Standard ISO/IEC 12207: 1995   | N/A | 1996 | Institute of Electrical and Electronics Engineers / Electronics Industry Alliance       |
| 336              | IEEE Std 15288-2004    | Adoption of ISO/IEC 15288:2002 Systems Engineering—System Life Cycle Processes  | N/A | 2004 | Institute of Electrical and Electronics Engineers                                       |
| 337              | IEEE Std 1540-2001     | IEEE Standard for Life Cycle Processes - Risk Management  | N/A | 2001 | Institute of Electrical and Electronics Engineers                                       |
| 338              | IEEE Std 323-1974      | IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations                                       | N/A | 1974 | Institute of Electrical and Electronics Engineers                                       |
| 339              | IEEE Std 323-2003      | IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations                                       | N/A | 2003 | Institute of Electrical and Electronics Engineers                                       |
| 340              | ANSI/IEEE Std 336-1985 | IEEE Standard Installation, Inspection, and Testing for Power, Instrumentation, and Control Equipment in Nuclear Facilities | N/A | 1985 | American National Standards Institute/Institute of Electrical and Electronics Engineers |
| 341              | ANSI/IEEE Std 338-1987 | IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems             | N/A | 1987 | American National Standards Institute/Institute of Electrical and Electronics Engineers |
| 342              | IEEE Std 344-2004      | IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations             | N/A | 2004 | Institute of Electrical and Electronics Engineers                                       |

| Reference Number | Document Number   | Description  | Rev | Date | Owner   |
|------------------|-------------------|--|-----|------|---|
| 343              | IEEE Std 352-1987 | IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems                         | N/A | 1987 | Institute of Electrical and Electronics Engineers |
| 344              | IEEE Std 379-2000 | IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems                         | N/A | 2000 | Institute of Electrical and Electronics Engineers |
| 345              | IEEE Std 383-2003 | IEEE Standard for Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations                        | N/A | 2003 | Institute of Electrical and Electronics Engineers |
| 346              | IEEE Std 384-1992 | IEEE Standard Criteria for Independence of Class IE Equipment and Circuits   | N/A | 1992 | Institute of Electrical and Electronics Engineers |
| 347              | IEEE Std 384-2008 | IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits   | N/A | 2008 | Institute of Electrical and Electronics Engineers |
| 348              | IEEE Std 494-1974 | IEEE Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations | N/A | 1974 | Institute of Electrical and Electronics Engineers |
| 349              | IEEE Std 497-2002 | IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations                                 | N/A | 2002 | Institute of Electrical and Electronics Engineers |
| 350              | IEEE Std 577-2004 | IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities             | N/A | 2004 | Institute of Electrical and Electronics Engineers |
| 351              | Available         |  |     |      |   |
| 352              | Available         |  |     |      |   |

| Reference Number | Document Number        | Description  | Rev | Date | Owner   |
|------------------|------------------------|--|-----|------|---|
| 353              | IEEE Std 627-1980      | IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations                   | N/A | 1980 | Institute of Electrical and Electronics Engineers |
| 354              | IEEE Std 665-1995      | IEEE Guide for Generating Station Grounding  | N/A | 1995 | Institute of Electrical and Electronics Engineers |
| 355              | IEEE Std 730-1998      | IEEE Standard for Software Quality Assurance Plans   | N/A | 1998 | Institute of Electrical and Electronics Engineers |
| 356              | IEEE Std 7-4.3.2-2003  | IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations                            | N/A | 2003 | Institute of Electrical and Electronics Engineers |
| 357              | IEEE Std 828-2005      | IEEE Standard for Software Configuration Management Plans  | N/A | 2005 | Institute of Electrical and Electronics Engineers |
| 358              | IEEE Std 829-2008      | IEEE Standard for Software and System Test Documentation   | N/A | 2008 | Institute of Electrical and Electronics Engineers |
| 359              | IEEE Std 830-1998      | IEEE Recommended Practice for Software Requirements Specifications   | N/A | 1998 | Institute of Electrical and Electronics Engineers |
| 360              | IEEE Std C37.90.1-2002 | IEEE Standard for Surge Withstand Capability (SWC) Tests for Relays and Relay Systems Associated with Electric Power Apparatus | N/A | 2002 | Institute of Electrical and Electronics Engineers |
| 361              | IEEE Std C62.23-1995   | IEEE Application Guide for Surge Protection of Electric Generating Plants  | N/A | 1995 | Institute of Electrical and Electronics Engineers |
| 362              | IEEE Std C62.41-1991   | IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits   | N/A | 1991 | Institute of Electrical and Electronics Engineers |

| Reference Number | Document Number              | Description  | Rev | Date          | Owner   |
|------------------|------------------------------|--|-----|---------------|---|
| 363              | IEEE Std C62.45-1992         | IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits                     | N/A | 1992          | Institute of Electrical and Electronics Engineers                           |
| 364              | Available                    |  |     |               |   |
| 365              | IPC-2221A                    | Generic Standard on Printed Board Design   | A   | May 2003      | IPC - Association Connecting Electronics Industries                         |
| 366              | ANSI/ISA S67.04, Part 1-1994 | Setpoints for Nuclear Safety-Related Instrumentation   | N/A | 1994          | American National Standards Institute / International Society of Automation |
| 367              | ISO 9001:2008                | Quality management systems – Requirements  | N/A | November 2008 | International Organization for Standardization                              |
| 368              | MIL-STD-461E                 | Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment | E   | August 1999   | ASC/ENSI  |
| 369              | SAE AS9100C                  | Quality Management Systems – Requirements for Aviation, Space and Defense Organizations                  | C   | January 2009  | Society of Automotive Engineers   |
| 370-700          | Reserved for future use      |  |     |               |   |

*Table 10.0-3. NuPAC Program References*

| Reference Number | Document Number      | Description   | Rev |
|------------------|----------------------|---|-----|
| 701              | NuPAC_CGDP610000-001 | NuPAC Commercial-Grade Item/Service Dedication Plan                                 | C   |
| 702              | NuPAC_CMP610000-001  | Configuration Management Plan   | H   |
| 703              | NuPAC_ED610000-062   | NuPAC Vulnerability Assessment Report (VA) for Secure Development Environment (SDE) | B   |
| 704              | NuPAC_ED610000-048   | NuPAC Reliability Prediction Report   | D   |
| 705              | NuPAC_ED610000-049   | NuPAC Failure Mode and Effects Analysis Report                                      | C   |
| 706              | NuPAC_ED610000-050   | NuPAC Failure Modes, Effects and Criticality Analysis Report                        | A   |
| 707              | NuPAC_ED610000-051   | NuPAC Response Time Analysis  | A   |
| 708              | NuPAC_ED610000-060   | NuPAC Inaccuracies and Uncertainties  | A   |
| 709              | NuPAC_ED610100-003   | Chassis/Rear Transition Module (RTM) Design Report                                  | G   |
| 710              | NuPAC_ED610300-011   | NuPAC Generic Logic Module (GLM) DAR  | D   |
| 711              | NuPAC_FVVP610000-001 | NuPAC FPL Verification and Validation Plan  | D   |
| 712              | NuPAC_HDP610000-001  | NuPAC Hardware Development Plan   | G   |
| 713              | NuPAC_IMP610000-001  | NuPAC Integrated Master Plan  | A   |
| 714              | NuPAC_MTP610000-001  | NuPAC Master Test Plan  | D   |
| 715              | NuPAC_PLDP610000-001 | NuPAC Programmable Logic Development Plan   | H   |
| 716              | NuPAC_PLDP610000-005 | Software Tool Evaluation Plan   | F   |
| 717              | NuPAC_PLDS610400-001 | NuPAC Programmable Logic Development Specification – Core PLCI                      | L   |
| 718              | NuPAC_PMP610000-001  | NuPAC Program Management Plan   | D   |
| 719              | NuPAC_QAP610000-001  | NuPAC Quality Assurance Plan  | E   |
| 720              | NuPAC_ROMP610000-001 | NuPAC Risk and Opportunity Management Plan  | B   |
| 721              | NuPAC_RPP610000-001  | NuPAC Reliability Program Plan  | B   |
| 722              | NuPAC_SDP610820-001  | NuPAC Test Equipment Software Development Plan                                      | C   |
| 723              | NuPAC_SEMP610000-001 | NuPAC Systems Engineering Management Plan   | F   |
| 724              | NuPAC_SMP610000-001  | NuPAC Subcontract Management Plan   | C   |
| 725              | NuPAC_SSP610000-001  | NuPAC System Security Plan  | D   |
| 726              | NuPAC_PSPP610000-001 | NuPAC Platform Safety Project Plan  | A   |
| 727              | NuPAC_SYS610000-001  | NuPAC System Description  | C   |
| 728              | NuPAC_TEDP610000-001 | NuPAC Test Equipment Development Plan   | B   |

| Reference Number | Document Number        | Description  | Rev |
|------------------|------------------------|--|-----|
| 729              | NuPAC_PLPRC610000-002  | NuPAC Programmable Logic Verification Procedure – Core PLCI                            | C   |
| 730              | NuPAC_TR610000-010     | NuPAC Environmental Equipment Qualifications (EQ) Summary Report                       | C   |
| 731              | D-D7210/2013P-5001     | Lockheed Martin Energy Quality Systems Manual for Commercial Nuclear Programs          | E   |
| 732              | NuPAC_TPL610800-001    | NuPAC Test Equipment Integration, Verification and Validation Plan                     | A   |
| 733              | NuPAC_PLRS610400-001   | NuPAC Programmable Logic Requirement Specification – Core PLCI                         | M   |
| 734              | NuPAC_ED610900-003     | Test Specimen Configuration (TSC) Design Report  | A   |
| 735              | NuPAC_EDD610400-001    | NuPAC Error Description Document – Core PLCI   | J   |
| 736              | NuPAC_ASCIDD610400-001 | NuPAC Application Specific Communications Interface Description                        | -   |
| 737              | NuPAC_ED610000-063     | Programmable Logic Failure Modes and Effects Analysis (FMEA) Report                    | -   |
| 738              | NuPAC_VDD610400-001    | NuPAC Version Description Document – Core Programmable Logic Configuration Item (PLCI) | P   |
| 739              | NuPAC_TP610000-004     | NuPAC System Environmental Test Procedure  | C   |
| 740              | NuPAC_TP610000-005     | NuPAC System Seismic Test Procedure  | E   |
| 741              | NuPAC_TP610000-006     | NuPAC System Radiation Test Procedure  | A   |
| 742              | NuPAC_TP610000-007     | NuPAC System Electromagnetic Compatibility Test Procedure                              | C   |
| 743              | NuPAC_TP610000-009     | NuPAC System Electrostatic Discharge Test Procedure                                    | F   |
| 744              | NuPAC_TR610000-004     | NuPAC Environmental Test Report  | B   |
| 745              | NuPAC_TR610000-005     | NuPAC Seismic Test Report  | A   |
| 746              | NuPAC_TR610000-006     | NuPAC Radiation Test Report  | B   |
| 747              | NuPAC_TR610000-007     | NuPAC System Electromagnetic Compatibility Test Report                                 | A   |
| 748              | NuPAC_TR610000-011     | NuPAC Environmental Equipment Qualifications (EQ) List of Anomalies and Actions        | B   |
| 749              | NuPAC_TP610000-001     | NuPAC System Pre-Qual Test Procedure   | B   |
| 750              | NuPAC_TR610000-001     | NuPAC Pre-Qualification Test Report  | -   |
| 751              | NuPAC_SDE610000-001    | Secure Development Environment Description (SRI)                                       | -   |

| Reference Number | Document Number      | Description   | Rev |
|------------------|----------------------|---|-----|
| 752              | ASR610000-100        | NuPAC V&V Activity Summary Report - Acquisition           | -   |
| 753              | ASR610000-101        | NuPAC V&V Activity Summary Report - Planning              | -   |
| 754              | ASR610000-102        | NuPAC V&V Activity Summary Report - Concept               | A   |
| 755              | ASR610000-103        | NuPAC V&V Activity Summary Report – Requirements          | A   |
| 756              | ASR610000-104        | NuPAC V&V Activity Summary Report - Design                | A   |
| 757              | ASR610000-105        | NuPAC V&V Activity Summary Report - Implementation        | -   |
| 758              | ASR610000-106        | NuPAC V&V Activity Summary Report - Test                  | -   |
| 759              | ASR610000-112        | BL 1.3.2 Core IV&V Concept Activity Summary Report        | A   |
| 760              | ASR610000-113        | BL 1.3.2 Core IV&V Requirements Activity Summary Report   | A   |
| 761              | ASR610000-114        | BL 1.3.2 Core IV&V Design Activity Summary Report         | -   |
| 762              | ASR610000-115        | BL 1.3.2 Core IV&V Implementation Activity Summary Report | -   |
| 763              | ASR610000-116        | BL 1.3.2 Core IV&V Test Activity Summary Report           | -   |
| 764              | IFR610000-001        | NuPAC V&V Final Report                                    | -   |
| 765              | IFR610000-103        | NuPAC Baseline 1.3.2 V&V Final Report                     | -   |
| 766              | NuPAC_VR610400-001   | NuPAC Programmable Logic Verification Report – Core PLCI  | C   |
| 767              | NuPAC_STER610000-029 | Software Tool Evaluation Report – [ ] <sup>a,c,e</sup>    | C   |
| 768              | NuPAC_STER610000-036 | Software Tool Evaluation Report – [ ] <sup>a,c,e</sup>    | A   |
| 769              | NuPAC_STER610000-063 | Software Tool Evaluation Report – [ ] <sup>a,c,e</sup>    | D   |
| 770              | NuPAC_STER610000-072 | Software Tool Evaluation Report [ ] <sup>a,c,e</sup>      | B   |



| Reference Number | Document Number         | Description  | Rev |
|------------------|-------------------------|--|-----|
| 771              | NuPAC_STER610000-016    | Software Tool Evaluation Report –<br>[ ] <sup>a,c,e</sup>  | A   |
| 772              | NuPAC_BL610000-005      | Status Accounting/Baseline Definition Report<br>for NuPAC Baseline 1.2.2 Hardware<br>Seismic/ESD/Surge Testing | E   |
| 773              | NuPAC_BL610000-008      | Status Accounting/Baseline Definition Report<br>for NuPAC Programmable Logic Baseline<br>1.3.2                 | A   |
| 774              | NuPAC_PLCI610400        | NuPAC Core Programmable Logic<br>Configuration Item (PLCI) Version 05.02.2B                                    | F   |
| 775-999          | Reserved for future use |  |     |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 144 of 263  
Date: 04/14/2017

This page intentionally left blank.



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 145 of 263  
Date: 04/14/2017

---

## APPENDIX A: NuPAC PLATFORM APPLICATION DESIGN GUIDE



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 146 of 263  
Date: 04/14/2017

This page intentionally left blank.

## 1.0 INTRODUCTION

This guideline document provides some design considerations and design constraints, when applicable, for future applications based on NuPAC platform. Design considerations may be modified, and will need to be supplemented, based on the scope of the application (e.g., an RPS). Some design constraints are those application rules which will be based on the regulatory review and that must be implemented, or if not implemented, or if implemented differently, must be identified for licensing (regulatory) evaluation as part of the application. This guide is provided as indicative information and not part of the regulatory review. Regulatory findings will be added upon review acceptance and completion.

The guidance provided in this document is intended to facilitate the use and application of the NuPAC platform and to remain within the basis of approval of this topical report. Additional requirements and limitations may apply to a plant-specific NuPAC-based system, based on plant-specific requirements.

Some of the guidance provided in this document is not specific to the NuPAC platform or software tools associated with the NuPAC platform, as some of the guidance is required by any installation of digital equipment in a nuclear facility. As an example, installation practices can create long-term problems, which are typically ascribed to faults and failures in the programmable logic. Correct initial system installation will enhance safe, reliable system operation.

Guidelines and/or constraints are provided for design, licensing, installation, operation, and maintenance of the system. Many of the guidelines in this document are interrelated. As an example, annunciation of alarms from faults and failures within the NuPAC platform have implications in design, operating and maintenance procedures, plant interface, the main control room design, and several other seemingly unrelated topics, including system power supply. Therefore, these guidelines should be considered as a whole, rather than as separate, individual, unrelated pieces.

A summary of the NuPAC platform, architecture, and theory of operation is provided in this LTR, which should be used as a reference by the developer and, ultimately, a Licensee.

The qualified equipment for the NuPAC platform includes:

- Generic Logic Module (GLM), P/N 610300
- Carrier Card for the GLM, P/N 610310
- Logic Mezzanine for the GLM, P/N 610320
- Rear Transition Module (RTM), P/N 610120
- Chassis, P/N 610100.

Qualified I/O mezzanine cards for the GLM include:

- RS-422/485 Mezzanine, P/N 610360
- Discrete/Pulse Input Mezzanine, P/N 610340
- SSR Mezzanine, P/N 610380
- Analog Input Mezzanine, P/N 610330
- Temperature Input Mezzanine, P/N 610350
- Analog Output Mezzanine, P/N 610370.

Redundant logic power supplies are not included in the qualified equipment. Field power supplies for the 4-20 mA analog loops are not included in the qualified equipment.

## 2.0 SYSTEM DESIGN GUIDANCE

### 2.1 NUPAC COMPONENTS SPECIFICATIONS

#### 2.1.1 Carrier Card

##### Input Power

- Power Consumption: [ ]<sup>a,c,e</sup>

##### Number of Interfaces

- Up to 8 external interfaces (types identified below)
- [ ]<sup>a,c,e</sup> LVDS internal communication interfaces [ ]<sup>a,c,e</sup>
- Twenty-three, I/O point status and fault LED output interfaces

##### Selectable Isolated Input Point Functionality (installed Input Mezzanine dependent)

- Analog voltage or current input (0-5 Vdc, 0-10 Vdc, 4-20 mA, 10-50mA)
- AC or DC bistable input (24/120 Vac, 12/15/24/48/125 Vdc)
- Pulse input (20 Hz-100 kHz)
- Thermocouple input (types T/E/J/N/K/R/S/B)
- RTD input (2/3/4 wire, 100/200 Ω)
- RS485 serial receive port [ ]<sup>a,c,e</sup>

##### Isolated Output Point Functionality (installed Output Mezzanine dependent)

- RS485 serial transmit port [ ]<sup>a,c,e</sup>
- Analog voltage or current output (0-5 Vdc, 0-10 Vdc, 4-20 mA)
- AC or DC bistable output (24/120 Vac, 0.5A; 12/15/24/48/125 Vdc, 1.0A)

##### Additional Features

- Hot swap capable
- On-card temperature sensor
- Card slot/rack detection
- Input and output status indicators
- NVM write protection

##### Physical Characteristics

- Overall dimensions: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>

#### 2.1.2 Logic Mezzanine

##### Input Power

- Power consumption: [ ]<sup>a,c,e</sup>

## Features

- FPGA state machine based processing (Core and Application Specific FPGAs)

[

] <sup>a,c,e</sup>

- Fault handling support
- Eight, I/O Mezzanine interfaces
- Card slot and rack identification interfaces
- [ ] <sup>a,c,e</sup> LVDS serial transmit and receive ports
- Twenty-three, I/O point status and fault LED output interfaces
- ADC interface for power supply voltage and temperature monitoring
- Core and Application Specific FPGA JTAG interfaces
- Separate [ ] <sup>a,c,e</sup> Core-to-AS FPGA read and write buses allow simultaneous reads/writes
- Diagnostic/maintenance serial interface
- System monitor interface

## Physical Characteristics

- Overall dimensions: [ ] <sup>a,c,e</sup>
- Weight: [ ] <sup>a,c,e</sup>

### 2.1.3 Analog Input Mezzanine

#### Input Power

- Power consumption: [ ] <sup>a,c,e</sup>

#### Input Characteristics

- Frequency (Voltage or Current) – DC
- Differential Voltage Amplitude Ranges (application selectable)
  - 0 to 5 Vdc, 0 to 10 Vdc
- Current Amplitude Ranges (ASPLD selectable)
  - 4 to 20 mA, 10 to 50 mA
- Update rate: [ ] <sup>a,c,e</sup>
- Voltage input impedance: [ ] <sup>a,c,e</sup>
- Current input impedance: [ ] <sup>a,c,e</sup>
- Resolution: [ ] <sup>a,c,e</sup>
- Noise rejection
  - Common mode: [ ] <sup>a,c,e</sup>

### Physical Characteristics

- Overall dimensions: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>

#### 2.1.4 Discrete/Pulse Input Mezzanine

##### Input Power

- Power consumption: [ ]<sup>a,c,e</sup>

##### Input Characteristics

- Bistable (nominal voltage application selectable)
  - AC bistable frequency range: 47 to 63 Hz
  - Bistable nominal voltage, switching levels (guaranteed) and maximum input voltage:

| Nominal Voltage | Default “ON” Threshold Voltage | Default “OFF” Threshold Voltage | Maximum Operating Voltage | Default Debounce “ON” | Default Debounce “OFF” |
|-----------------|--------------------------------|---------------------------------|---------------------------|-----------------------|------------------------|
| 120VAC*         | [ ]                            |                                 |                           |                       |                        |
| 24VAC*          |                                |                                 |                           |                       |                        |
| 125VDC          |                                |                                 |                           |                       |                        |
| 48VDC           |                                |                                 |                           |                       |                        |
| 24VDC           |                                |                                 |                           |                       |                        |
| 15VDC           |                                |                                 |                           |                       |                        |
| 12VDC           |                                |                                 |                           |                       | [ ] <sup>a,c,e</sup>   |

\* RMS values

- Pulse Input Detection for differential and single ended input pulse measurement options. [ ]<sup>a,c,e</sup>
  - Frequency range: 20 Hz to 100 kHz
  - Amplitude range: [ ]<sup>a,c,e</sup>
  - Logic range: [ ]<sup>a,c,e</sup>
  - Pulse Width of 1 microsecond or greater.

##### Physical Characteristics

- Overall dimensions: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>

#### 2.1.5 Temperature Input Mezzanine

##### Input Power

- Power consumption: [ ]<sup>a,c,e</sup>

#### Input Characteristics

- Update rate: [ ]<sup>a,c,e</sup>
- Thermocouple input impedance: [ ]<sup>a,c,e</sup>
- RTD input impedance: [ ]<sup>a,c,e</sup>
- Resolution: [ ]<sup>a,c,e</sup>
- Noise rejection
  - Common mode: [ ]<sup>a,c,e</sup>
  - Normal mode: [ ]<sup>a,c,e</sup>
- Input options:

| Input Type          | Temperature Range |
|---------------------|-------------------|
| Thermocouple Type T | 0 to 400°C        |
| Thermocouple Type E | 0 to 1000°C       |
| Thermocouple Type J | 0 to 1200°C       |
| Thermocouple Type N | 0 to 1250°C       |
| Thermocouple Type K | 0 to 1300°C       |
| Thermocouple Type R | 0 to 1700°C       |
| Thermocouple Type S | 0 to 1700°C       |
| Thermocouple Type B | 250 to 1800°C     |
| RTD 2-wire 100Ω     | 0 to 800°C        |
| RTD 3-wire 100Ω     | 0 to 800°C        |
| RTD 4-wire 100Ω     | 0 to 800°C        |
| RTD 2-wire 200Ω     | 0 to 800°C        |
| RTD 3-wire 200Ω     | 0 to 800°C        |
| RTD 4-wire 200Ω     | 0 to 800°C        |

#### Output Characteristics

- RTD excitation currents: 50, 100, 250, 500, 750, 1000, 1500 μA (Application selectable)

#### Physical Characteristics

- Overall dimensions: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>

### 2.1.6 RS-422/485 Mezzanine

Isolated, Single Transmit and Receive RS-422 Ports

#### Input Power

- Power consumption: [ ]<sup>a,c,e</sup>

### Range of Inputs and Outputs

- RS-422 Transmit Port (U1)
  - Maximum data rate: [ ]<sup>a,c,e</sup>
- RS-422 Receive Port (U2)
  - Maximum data rate: [ ]<sup>a,c,e</sup>

### Physical Characteristics

- Overall dimensions: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>

### 2.1.7 Analog Output Mezzanine

Single Point, Isolated, Current or Voltage Output

#### Input Power

- Power consumption: [ ]<sup>a,c,e</sup>

#### Output Characteristics

- Frequency (Voltage or Current) - DC
- Voltage output: 0 to 5 Vdc, 0 to 10 Vdc (application selectable), short circuit protected
  - Voltage output: maximum load [ ]<sup>a,c,e</sup>
  - Voltage output power: [ ]<sup>a,c,e</sup>
- Current output: 4 to 20 mA dc, short circuit protected
  - Current output: maximum load [ ]<sup>a,c,e</sup>
  - External current loop power: [ ]<sup>a,c,e</sup>

### Physical Characteristics

- Overall dimensions: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>

### 2.1.8 SSR Mezzanine

#### Input Power

- Power consumption: [ ]<sup>a,c,e</sup>

#### Output Characteristics

- Frequency – DC or AC (47 to 63 Hz)
- DC Voltage and Maximum Current Ratings
  - DC nominal voltages: 12 Vdc, 15 Vdc, 24 Vdc, 48 Vdc, 125 Vdc (ASPLD selectable)

- [ ]<sup>a,c,e</sup>
- [ ]<sup>a,c,e</sup>
- AC Voltage and Maximum Current Ratings
  - AC nominal voltages: 24 Vac, 120 Vac (ASPLD selectable)
  - AC voltage ranges: 24V (20-28V); 120V (90-130V)
  - [ ]<sup>a,c,e</sup>
- Overcurrent protection
  - Overcurrent trip time: [ ]<sup>a,c,e</sup>
  - Overcurrent trip level: [ ]<sup>a,c,e</sup>

#### Physical Characteristics

- Overall dimensions: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>

#### 2.1.9 Chassis

##### Chassis Physical Characteristics

- Overall dimensions: [ ]<sup>a,c,e</sup>
- Chassis maximum height: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>
- Weight: [ ]<sup>a,c,e</sup>
- GLM Card Slots: 18
- RTM Card Slots: 18
- Fan Trays: 2
- Interface Connectors: 3 (2 power, 1 user-defined)
- Chassis is designed for use in a standard 19.0-inch wide enclosure as defined in IEC 60297-3-100.

##### Chassis Power Requirements

##### Features

- [ ]<sup>a,c,e</sup>
- [ ]<sup>a,c,e</sup>
- Maximum ripple voltage of [ ]<sup>a,c,e</sup>

##### Card Rack Features

- 19-inch rack mountable
- Two rear shock bushings
- Electromagnetic Interference (EMI) shielding
- Chassis ground stud
- Alternate ground stud
- Electrostatic Discharge (ESD) test jack front and rear

- Hot swap fan trays
- Front-to-rear air flow
- Intake air filter
- Alpha and Bravo fan tray power and status LEDs
- Fan fuses
- Full internal wiring
- RTM cable support
- Installation handles
- 18 GLM card slots labeled A1 through A18, left to right from front
- 18 RTM card slots labeled B1 through B18, right to left from rear
- Power Distribution to all GLMs
- Slot addressing for each GLM
- Rack addressing to all GLMs
- Alpha and Bravo fan tray status output signals
- Two system monitor signals bused to all GLM slots
- Two system monitor signals to GLM slots A1, A5, A9, and A13 only
- Memory interlock signal bused to all GLM slots
- Hot swap capable for GLM and fan trays
- Low Voltage Differential Signal (LVDS) communication among GLM slots

## 2.1.9 Rear Transition Module

### RTM Features

- External signal termination using [ ]<sup>a,c,e</sup> connector interfaces
- Access to eight GLM Input/ Output (I/O) points
- Configurable shield termination for each I/O point
- EMI shielded mating connector options

## 2.2 POWER

### 2.2.1

The NuPAC platform has a defined response to loss of power. All discrete outputs turn off, all analog outputs go to a zero output value, and all communications links are disabled.

### 2.2.2

The NuPAC platform has a defined response to power restoration. When power is restored, power-on self-test (POST) starts and the platform logic holds all discrete and analog outputs in their safe state, [ ]<sup>a,c,e</sup>. When POST completes, outputs are set to the state commanded by the application logic. Serial output communication is not disabled during POST. If POST fails, it can be reported using serial output.

Power supplies are not included in the NuPAC topical report. However, requirements are still provided for power to ensure safe, reliable operation of the NuPAC platform. Power supply design considerations specific to the NuPAC platform are included in Sections 2.1.3 through 2.1.8 below.

## 2.2.3

The chassis is designed to accept dual redundant power supplies. Each supply shall be capable of providing 100% of the power requirements for the supplied chassis.

## 2.2.4

The cabinet, power supplies, and field wiring must be wired and grounded according to installation procedure requirements.

## 2.2.5

Redundant and independent paths to input power should be provided to the dual power supply connections on each NuPAC chassis. With this configuration, failure of either supply does not impact the NuPAC platform. The chassis power supplies shall meet the following minimum characteristics:

- Normal operating voltage tolerance of [ ]<sup>a,c,e</sup>
- Maximum ripple voltage of [ ]<sup>a,c,e</sup>
- Maximum abnormal output voltage of [ ]<sup>a,c,e</sup> during a power supply overvoltage failure.

## 2.2.6

The NuPAC platform shall be configured to provide a loss of a power alarm in the control room for both power input and power output from either or both redundant chassis and field power supplies. Conditions to be alarmed should include over and under voltage on the diode-auctioned power as well as over and under voltage on each of the regulated power supplies. Discrete outputs may be used to provide faults and failures to a plant annunciation system. Since power failures will be infrequent, maintenance procedures should be generated by the Licensee to respond to and resolve such faults and failures.

## 2.2.7

The method of auctioneering for field or Loop supplies could be provided by the supplies themselves or included as external devices located within the cabinet as part of RPS design. It is possible to purchase power supplies that are designed to work redundantly without any additional external aid. External auctioneering may need to be provided within the cabinet to achieve the desired redundancy.

## 2.2.8

For testing of field or loop supplies, it is recommended that each supply be monitored using available I/O mezzanine functionality. If the selected supply supports a “Power Good” discrete output signal then this signal can be monitored by one of the GLM backplane discrete input monitor points rather than using an I/O mezzanine card. Supplies should be monitored both before and after any auctioneering to facilitate fault isolation.

## 2.3 Connection to Plant Instrumentation and Controls

### 2.3.1

All analog field sensors/transmitters are hardwired to RTM connectors, which provide dedicated connection to analog input mezzanine cards. All discrete field sensors/transmitters are hardwired to RTM connectors, which provide dedicated connections to discrete input mezzanine cards.

### 2.3.2

All analog field actuated devices are hardwired to RTM connectors, which provide dedicated connection to analog output mezzanine cards. All discrete field actuated devices are hardwired to RTM connectors, which provide dedicated connections to discrete output mezzanine cards.

### 2.3.3

Each actuated discrete field device may be configured in the application logic either as a pair of programmable width pulses used separately to turn on and turn off a device or as a level.

### 2.3.4

If redundant inputs are provided to a single division, those redundant inputs shall not be processed on a single GLM. If redundant outputs are created in a single division, those redundant outputs shall not be sourced from a single GLM.

### 2.3.5

All shielded wiring between the RTM and field sensors/ transmitters should terminate shields at the field sensor/transmitter if possible. All shielded wiring between field actuators/receivers should terminate shields at the RTM. Terminating shields at both ends is discouraged.

## 2.4 System Configuration

### 2.4.1

Each GLM has a defined delay from input to output, based on the programmable logic on that GLM. Groups of GLMs are not synchronized, other than all GLMs start roughly together after power up. Messages are not internally synchronized. Section 6.3.3 of this LTR describes the methods needed to determine the maximum time delay from change in input to change in output for various configurations of GLMs, ranging from the cycle time for one GLM to respond where all inputs, all logic, and all outputs are on that single GLM through configurations where multiple GLMs, in multiple cabinets, and in multiple divisions are required to change outputs in response to the change in inputs.

### 2.4.2

The safety system response-time calculations shall 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.

**2.4.3**

The NuPAC platform is designed to support divisional redundancy. The NuPAC platform is designed to be provided in redundant systems. Each plant-specific system design shall provide redundant channels, divisions, and trains as required.

**2.4.4**

Selective internal redundancy can be applied within each channel, division, or train as necessary to enhance reliability or provide means to perform technical specification surveillance without entering a Limiting Condition for Operability (LCO) when taking a division's safety function out of service.

**2.4.5**

The NuPAC platform may be configured with individual field sensors split across separate I/O mezzanines and/or separate GLMs for redundancy.

**2.4.6**

The NuPAC platform may be configured with redundant voting on redundant GLMs.

**2.4.7**

The NuPAC platform may be configured to provide voting on the discrete outputs, using multiple series or parallel discrete outputs, as appropriate, to enhance reliability.

**2.4.8**

All external (through the Serial RS-422/485 Mezzanine) and internal (through the LVDS communication paths on the backplane) communication messages and processing shall be designed such that faults and failures do not adversely affect the safety function, except for the detectable loss of the data contained in that message. Plant-specific implementation of interdivisional communication shall demonstrate that communication supports or enhances the performance of the safety function.

**2.4.9**

All serial data communication outside a GLM platform chassis shall be performed only over point-to-point communication links.

**2.4.10**

The messages generated and transmitted in the application within NuPAC (i.e., NuPAC-to-NuPAC) shall be constrained by the applicable application-specific communications interface design guideline.

**2.4.11**

All messages shall be preformatted and shall have predefined content. The plant-specific application logic shall define the format and content of all serial data communication messages, with the exception of the routing data placed on internal communication messages by the platform logic.

**2.4.12**

Failure to receive a predefined number of periodic messages shall be treated appropriately by the receiving application logic. For messages that provide data to safety functions, this failure should be treated as if the

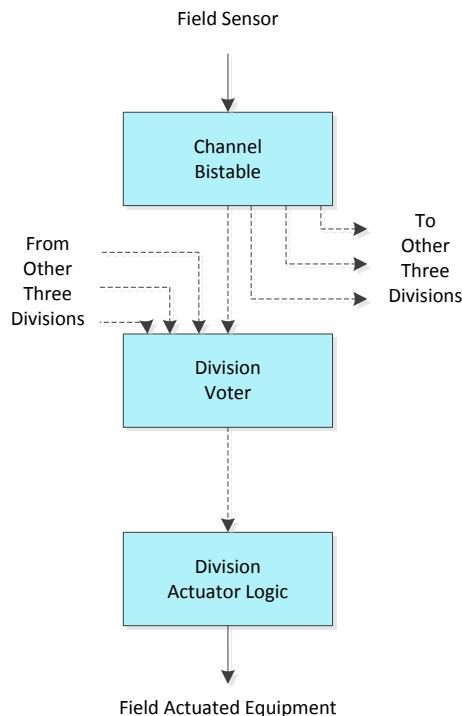
sending division has failed. Failure of multiple sending divisions shall be addressed in the plant-specific application logic.

#### 2.4.13

The serial communication pathways provided on the NuPAC platform backplane provide two mesh-star point-to-point networks. To minimize the transit time of bistable, voting, and status communications, one of the mesh-star networks may be dedicated to the transmission of these data types. All other data would be transmitted through the second mesh-star network.

#### 2.4.14

Figure 2.3.20-1 shows a typical architecture for an actuation arrangement, such as an RPS. The application architecture, using qualified NuPAC equipment, will depend on the specific application requirements. In the example below, divisional field sensors are hardwired to one or more GLM implementing the channel logic, shown as a solid line. The field sensor data is sampled through the I/O mezzanine cards on those GLM. The GLM includes application logic to compare input data against predefined setpoint values to determine whether this channel concludes that protective action is required.



**Figure 2.3.20-1. Channels and Divisions**

#### 2.4.15

The channel bistables provide votes to trip or actuate to separate GLMs that perform the voting at the division level, which may provide data to separate GLMs for the actuation logic. Connections from channels to divisions

are shown as dotted lines in Figure 2.3.20-1, which may be either hardwired or serial data communication connections. Connections to the field equipment are hardwired and shown as solid lines in the figure.

#### **2.4.16**

Except for quality calculations, Channels shall not make use of any engineering unit data from other divisions.

#### **2.4.17**

External isolation devices shall be used to provide the required electrical isolation between safety-related divisions and trains.

#### **2.4.18**

If fiber-optic cable is used for an application, separation shall be in accordance with IEEE Standard 384-2008 (**Reference 346**), “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.” Each fiber optic cable that crosses divisional boundaries shall be assigned to the division that would be affected by the loss of that cable. An external fiber optic converter is required to interface with the NuPAC platform.

#### **2.4.19**

If any hardwired connections cross-divisional boundaries, the copper cable shall be separated in accordance with IEEE Standard 384-1992 (**Reference 346**), as endorsed by USNRC RG 1.75 (**Reference 149**), “Criteria for Independence of Electrical Safety Systems.” In accordance with that standard, the cable shall be separated based on the division applying power to the cable.

#### **2.4.20**

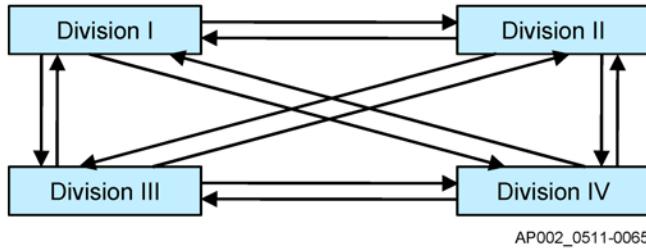
Voters will not access or be provided with engineering unit data from their own division or from other divisions. Voters shall have access only to status information (e.g., votes to trip or not trip, votes to actuate or not actuate, input sensor good/bad (quality information), division of sensors bypassed, division of outputs bypassed) as well as votes to actuate/trip from within the division and from other divisions.

#### **2.4.21**

Votes to trip or actuate and required status can be transferred between divisions using two methods. The preferred method for the plant-specific systems implemented with the NuPAC platform to transfer information is by use of communication links. With a communication link sending periodic messages, failure to receive and other faults (see DI&C-ISG-04) can be detected. Alternatively, with appropriate wiring and programming, data can be sent from discrete outputs in one division through qualified electrical isolation to discrete inputs in another division. Each bit of information to be sent requires a discrete output, electrical isolator, and discrete input.

#### **2.4.22**

The interconnection of divisions is plant-specific. The interconnection of divisions shown in Figure 2.3.30-1 is an example of reactor trip system divisional interconnection, which could be implemented using the NuPAC platform. For engineered safety features systems, the number of voters and actuator outputs may vary, depending on the required number of various types of pumps and valves to meet the plant-licensing basis.



**Figure 2.3.30-1. Signal Paths between Divisions**

#### 2.4.23

Electrical separation shall be implemented between channels and divisions within the NuPAC-based plant-specific system in accordance with the Licensee's plant-specific requirements.

#### 2.4.24

Each division of plant-specific systems designed with the NuPAC platform may receive votes to trip or actuate, bypass status, and data status from other safety systems. This information types is used by the plant-specific system in voting to actuate or trip. Communication across divisional boundaries requires qualified isolation.

### 2.5 Chassis Configuration

#### 2.5.1

The NuPAC platform shall be installed in a mild environment.

#### 2.5.2

Each chassis shall be assigned to a specific electrical division. A chassis shall not be split between electrical divisions.

#### 2.5.3

Redundant communications cables should not be routed together outside the cabinet. For maximum protection from failure, the communication cables should be routed through separate routes within the cabinet.

### 2.6 Operational Interface

#### 2.6.1

The NuPAC platform design supports use of traditional switches, meters, recorders, and lights for human-system interface in accordance with plant-specific human-machine interface requirements.

#### 2.6.2

The NuPAC platform design supports provision of traditional contact closure signals to control room annunciators.

## 2.6.3

The NuPAC platform design supports communications to and from a video display safety system within the control room for human-system interface.

## 2.6.4

Each data item that is communicated to/from a video display safety system shall be checked (e.g., CRC) for correct data transmission. Each connection between programmable logic and configuration in the video display shall be verified and validated.

## 2.6.5

The plant-specific design shall provide appropriate control of the setpoint memory write protect line for each chassis. Appropriate key lock switches, or other physical and administrative processes, shall be supplied to ensure that changes to the setpoint values in each chassis are controlled and protected in accordance with the Licensee's cyber security program.

## 2.6.6

The plant-specific application logic should implement range checks for all NVM stored plant application variables, calibration constants and measurement limits. Modifications of NVM data should implement safeguards to prohibit access and limit modification of data or ranges to acceptable values. Any modifications of NVM should include a confirmation read-back/ validation.

## 2.7 Bypass Indication and Status Indication

### 2.7.1

Maintenance and operating bypass implementation is specific to the plant-specific system application. Bypasses shall be added as necessary and designed into the application logic in accordance with plant licensing, reliability, availability, surveillance, maintenance, and operations requirements.

### 2.7.2

Bypass inputs to the application logic should be provided through appropriate hardware interfaces (e.g. joystick or other such interface devices). Provisions in the application logic should be implemented to preclude multiple divisions simultaneously in bypass.

### 2.7.3

Operating bypasses are also provided through plant-specific design using a combination of application logic and hardware. Automatic operating bypasses may be designed into the plant-specific application logic.

### 2.7.4

For operating bypasses, more than one bypass can be active at any point in time based on the requirements of the operations procedures dealing with the plant conditions. Application logic shall verify permissive conditions are met for all active operating bypasses. If permissive conditions are not met, the application logic shall clear the bypass condition, restore permissive plant conditions, or initiate the appropriate safety feature.

## 2.7.5

Bypass, inoperable, and other status indication may be provided through discrete hardwired outputs to drive lamps in the control room or through serial communication to video displays in the control room.

## 2.7.6

If the NuPAC-based system communicates data to a non-safety system, then additional non-safety system software could be provided in that non-safety system to provide Bypassed and Inoperable Status Indication.

## 2.8 Self-Test and Surveillance Test Capabilities

### 2.8.1

A safety system design must provide the ability to conduct periodic testing consistent with the plant-specific requirements and procedures. The NuPAC-based system applications can be designed to provide these capabilities in accordance with the requirements established in the regulatory guidance documents referenced in BTP 7-17 (**Reference 113**). There is nothing inherent in the NuPAC platform or the software tools used with the NuPAC platform that fails to comply with the requirements of IEEE Standard 603-1991 (**Reference 351**), as required by BTP 7-17 (**Reference 113**). However, since the NuPAC platform architecture is different from any analog system it replaces, traditional surveillance test provisions for analog systems are likely not adequate or appropriate. The required surveillance testing support capabilities for each plant-specific application will be designed into the application logic. The surveillance tests and support for surveillance testing will be evaluated to assure adequacy to fulfill the requirements and the intent of the surveillance tests. The implications of surveillance capabilities on maintenance are discussed in Section 8.3.

### 2.8.2

Modifications to existing surveillance tests and Technical Specification licensing commitments will be considered based on the additional capabilities provided in the NuPAC-based system. An analysis shall compare the NuPAC-based system Built-In-Test (BIT) features, single failure analyses, FMEA, and application logic against the requirements established in the plant's Technical Specifications and USNRC requirements. BIT should be considered as means of reducing surveillance testing for the plant-specific system. Additional application logic should be considered to support surveillance testing by eliminating any requirements for lifted leads and temporary configuration changes. The analysis shall ensure that nothing done in these tests could prevent the performance of the system's safety function(s).

### 2.8.3

A NuPAC-based system may be configured to periodically test for coil presence and output switch functionality by verifying current flow or briefly changing state. This capability should be evaluated in lieu of manual surveillance testing, and for decreasing surveillance testing frequency.

### 2.8.4

The concepts used to determine test intervals for a NuPAC-based system should consider the reliability of the NuPAC-based system. Changes to surveillance frequency will require licensing change.

## 2.8.5

A NuPAC-based system shall be designed and validated to detect and identify failures to the greatest extent that is practical.

## 2.8.6

The application logic should provide the capability to confirm that BIT is still functional during plant operation.

## 2.8.7

A NuPAC-based plant-specific implementation shall include evaluation of the effects on the plant when a NuPAC-based system goes to a fail-safe state. Upon detection of faulted output conditions, a NuPAC-based plant-specific implementation should command all outputs to a fail-safe state.

## 2.8.8

Plant-specific application logic shall be designed to annunciate detected faults and failures in the control room. Mechanisms for operator notification of detected faults and failures shall comply with the system status indication provisions of IEEE Standard 603 (**Reference 351**) and should be consistent with, and support, plant-specific requirements, operating procedures, and maintenance procedures.

The plant-specific application logic BIT should be such that loss of GLM functionality, on any GLM card, is detected and reported by at least one other GLM within the system architecture. In addition to other methods of annunciating an alarm it is recommended that each GLM use the LVDS serial communication to report any local failure or alarm condition.

## 2.8.9

Procedures will be written or updated to support the NuPAC platform and the plant staff in operations and maintenance.

## 2.8.10

As required by IEEE Standard 603 (**Reference 351**), Section 5.8.3; and USNRC RG 1.47 (**Reference 146**), if the protective action of some part of a protection system is bypassed or deliberately rendered inoperative for testing, that fact shall be continuously indicated in the control room. Provisions shall also be made to inform the control room operator when the protection system is restored. Application logic with each NuPAC-based system shall be provided for bypass and status generation.

## 2.8.11

The field-actuated device testing specified in Regulatory Guide 1.22 (**Reference 144**) is still applicable. The NuPAC platform application logic can be configured to perform any of the testing described in USNRC RG 1.22, from complete function to judicious choice of components for several tests.

## 2.8.12

The risk associated with logic complexity associated with automating the required surveillance testing should be offset by the reduced risk associated with manual performance of such testing, including lifting leads. Consistent with the requirements of USNRC RG 1.118 (**Reference 131**), makeshift test setups, including

temporary modifications of data or plant wiring that must be removed to restore the system to service, shall be avoided.

#### 2.8.13

Hardware and programmable logic used to perform surveillance functions shall be classified as safety related and shall be integral to the NuPAC platform. The scope and extent of interfaces required to perform these tests shall be designed to maintain channel independence, maintain system integrity, and meet the single failure criterion. The scope and extent of interfaces between programmable logic that perform safety functions and programmable logic for testing functions should be designed to minimize the complexity of the logic and data structures.

#### 2.8.14

Plant procedures should specify manual compensatory actions and mechanisms for recovery from indicated faults and failures.

### 3.0 RESPONSE TIME

The response time data provided in Reference 707 shall be considered in the definition of architecture of the application and used to confirm that Licensee requirements can be met.

### 4.0 SETPOINT ANALYSIS AND ACCURACY

The accuracy, repeatability, thermal effects, and other necessary data for use in setpoint analyses provided in Reference 708 and shall be used in the development and/or provided to the Licensee for use in setpoint determination.

### 5.0 ENVIRONMENT AND LOCATION

The NuPAC platform will be qualified to a mild environment. A mild environment is defined in IEEE Standard 323-2003 (**Reference 339**) as an environment that would at no time be significantly more severe than the environment that would occur during normal plant operations, including anticipated operational occurrences.

The specific requirements and qualification testing pertaining to the environment in which a safety-related NuPAC platform may be located are discussed in this section.

Upon completion of environmental testing this guide will be updated with the test details and results if they differ from those described below. The test details will include a list of the specific hardware that underwent testing. The test results will specify the operating condition envelopes verified by testing for each of the following subsections.

A plant-specific evaluation will be performed to determine whether the as-tested limits bound the plant requirements. If not, additional evaluation or testing is required.

## 5.1 Mounting

### 5.1.1

The NuPAC chassis is designed to fit within industry-standard cabinets (19-inch minimum).

### 5.1.2

Each chassis shall be mounted consistently with the mounting methods and requirements used during seismic testing, which shall be updated in this guide at the completion of Equipment Qualification testing.

### 5.1.3

The NuPAC chassis do not require additional stand-off spacing between chassis.

## 5.2 Temperature and Humidity Testing

Temperature and humidity testing of NuPAC using the TSC was performed as described in the NuPAC System Environmental Test Procedure (**Reference 739**), which is based on the guidance specified in EPRI TR-107330 (**Reference 312**) to meet the intent of IEEE Standard 323-2003 (**Reference 339**) as endorsed by Regulatory Guide 1.209 (**Reference 143**). The NuPAC is qualified to perform its safety function in abnormal service conditions of temperature and humidity, up to the [ ]<sup>a,b,c,e</sup> Relative Humidity (RH) levels as defined in Figure 4.4 of EPRI TR-107330 (**Reference 312**), which includes the added and desired [ ]<sup>a,b,c,e</sup> margin, and to the Low Temperature/Humidity condition of [ ]<sup>a,b,c,e</sup>, and Low Humidity / Temperature condition of [ ]<sup>a,b,c,e</sup>. Figure 5.2-1 provides a visual envelope to which the NuPAC platform is qualified.



*Figure 5.2-1. NuPAC Environmental Qualification Test Envelope*

The detailed results of the temperature and humidity testing, as well as any restrictions, are provided in the NuPAC Environmental Test Report (**Reference 744**). Temperature and humidity testing is also summarized in NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**).

### **Heat Loads in Cabinets and Rooms**

When mounting the NuPAC chassis into enclosures, heat management calculations must be made to avoid exceeding the qualified ambient temperature ratings. For purposes of these calculations, all power consumed by the NuPAC platform should be assumed to be a source of heat inside the enclosure where the chassis is mounted. The NuPAC platform temperature range must be computed with cabinet doors open and closed.

If the room temperature plus any heat rise within the cabinet exceeds the NuPAC platform qualification envelope provided in this guide, Section 5.2, additional provision must be made for temperature control.

### **5.3 Seismic Withstand Testing**

Seismic withstand testing of the NuPAC TSC was performed as described in the NuPAC System Seismic Test Procedure (**Reference 740**), which is based on the guidance specified in EPRI TR-107330 (**Reference 312**) to meet the intent of IEEE Standard 344-2004 (**Reference 342**) as endorsed by Regulatory Guide 1.100 (**Reference 129**). Each chassis of the TSC was tested individually. Each chassis underwent a resonance search, five Safe Shutdown Earthquakes (SSE) and one Operating Basis Earthquake (OBE). The NuPAC platform is qualified to perform its safety functions to the seismic spectra provided in Figure 5.3-1.



**Figure 5.3-1. NuPAC SSE -10% and OBE Qualification Spectra Seismic Withstand Response Spectrum**

The detailed results of the seismic testing are provided in the NuPAC Seismic Test Report (**Reference 745**). A summary of all EQ testing is provided in NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**). A summary of the restrictions is provided in NuPAC Environmental Equipment Qualifications (EQ) List of Anomalies and Actions (**Reference 748**).

#### 5.4 Radiation Withstand Testing

Radiation withstand testing of the NuPAC TSC was performed as described in the NuPAC System Radiation Test Procedure (**Reference 741**), which is based on the guidance specified in EPRI TR-107330 (**Reference 312**) to meet the intent of IEEE Standard 323-2003 (**Reference 339**) as endorsed by Regulatory Guide 1.209 (**Reference 143**). The radiation exposure consisted of the [ ]<sup>a,b,c,e</sup> radiation absorbed doses (RADs) requirement plus an additional [ ]<sup>a,b,c,e</sup> margin applied over the course of [ ]<sup>a,b,c,e</sup> minutes above the required 10% margin of EPRI TR-107330 (**Reference 312**). The NuPAC Platform is qualified to perform its safety function when exposed to a cumulative radiation exposure of [ ]<sup>a,b,c,e</sup>.

The detailed results of the radiation testing are provided in the NuPAC Radiation Test Report (**Reference 746**). A summary of all EQ testing is provided in NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**). A summary of the restrictions is provided in NuPAC Environmental Equipment Qualifications (EQ) List of Anomalies and Actions (**Reference 748**).

## 5.5 EMI/RFI/ESD Testing

Electromagnetic compatibility testing of the NuPAC TSC was performed as described in the NuPAC System Electromagnetic Compatibility Test Procedure (**Reference 742**) and NuPAC System Electrostatic Discharge Test Procedure (**Reference 743**), in accordance with Regulatory Guide 1.180 (**Reference 141**), and as endorsed, the Military Standard MIL-STD-461E (**Reference 368**) and the International Electrotechnical Commission (IEC) 61000 series (**References 315 to 325**) of electromagnetic and radio-frequency Interference (EMI/RFI) test method requirements.

The specific tests conducted include the MIL-STD-461E (**Reference 368**) and the IEC 61000 series (**References 315 to 325**) test methods listed in Table 5.4-1.

*Table 5.4-1. Electromagnetic Compatibility Tess Sequence*

| Test Method        | Test Description  |
|--------------------|---|
| MIL-STD-461E RE101 | Radiated Emissions, Magnetic Field Measurement  |
| MIL-STD-461E RE102 | Radiated Emissions, Electric Field Measurement  |
| IEC 61000-4-4      | Conducted Susceptibility, Electrical Fast Transient / Burst Immunity Test   |
| IEC 61000-4-12     | Conducted Susceptibility, Oscillatory Waves Immunity Tests  |
| IEC 61000-4-5      | Conducted Susceptibility, Surge Immunity Test   |
| IEC 61000-4-6      | Conducted Susceptibility, Immunity to Conducted Disturbances Induced by Radio-frequency Fields                            |
| IEC 61000-4-16     | Conducted Susceptibility, Test for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz |
| IEC 61000-4-8      | Radiated Susceptibility, Power Frequency Magnetic Field Immunity Test   |
| IEC 61000-4-9      | Radiated Susceptibility, Pulse Magnetic Field Immunity Test   |
| IEC 61000-4-10     | Radiated Susceptibility, Damped Oscillatory Magnetic Field Immunity Test  |
| IEC 61000-4-3      | Radiated Susceptibility, Radiated, Radio-frequency, Electromagnetic Field Immunity Test                                   |
| IEC 61000-4-2      | Electrostatic Discharge Immunity Test   |

The NuPAC platform is qualified to perform its safety functions to the levels identified in the EMI/ESD environments provided in Table 5.4-2.

*Table 5.4-2. Electromagnetic Compatibility Test Results Summary*

| Test                 | Compliance Category                                 |                 |                    |                |                        |            |
|----------------------|---|-----------------|--------------------|----------------|------------------------|------------|
| Emissions Tests      |   |                 |                    |                |                        |            |
| RE101                | [   |                 |                    |                |                        |            |
| RE102                |   |                 |                    |                |                        |            |
|                      |   |                 |                    |                |                        |            |
| Susceptibility Tests | Classification for Each I/O Type per Test Performed |                 |                    |                |                        |            |
|                      | Analog Inputs                                       | Discrete Inputs | Temperature Inputs | Analog Outputs | Discrete Outputs (SSR) | RS-422 I/O |
| IEC 61000-4-8        | [   |                 |                    |                |                        |            |
| IEC 61000-4-9        |   |                 |                    |                |                        |            |
| IEC 61000-4-10       | IP  | IP              | IP                 |                |                        |            |
| IEC 61000-4-4        |   |                 |                    | IP             |                        |            |
| IEC 61000-4-16       |   |                 |                    |                | IP                     |            |
| IEC 61000-4-12       |   |                 |                    | IP             | IP                     |            |
| IEC 61000-4-3        | IP  | IP              | IP                 |                |                        |            |
| IEC 61000-4-6        |   |                 |                    | IP             |                        |            |
| IEC 61000-4-2        |   |                 | IP                 | IP             |                        | IP         |
| IEC 61000-4-5        |   |                 |                    | IP             | IP                     | IP         |
| Notes:               |   |                 |                    |                |                        |            |
| [                    |   |                 |                    |                |                        |            |
|                      |   |                 |                    |                |                        |            |
| ] a,b,c,e            |   |                 |                    |                |                        |            |



The detailed results of the EMI/ESD testing, as well as any restrictions, are provided in the NuPAC System Electromagnetic Compatibility Test Report (**Reference 747**). A summary of all EQ testing is provided in NuPAC Environmental Equipment Qualifications (EQ) Summary Report (**Reference 730**). A summary of the restrictions is provided in NuPAC Environmental Equipment Qualifications (EQ) List of Anomalies and Actions (**Reference 748**).

## 5.6 Constraints Resulting from EQ Testing

The following list of constraints are a result of environmental testing on the NuPAC platform that must be followed in order to use the NuPAC Platform in a safety system:

[

]<sup>a,b,c,e</sup>



[

] a,b,c,e

## 6.0 GUIDANCE FOR APPLICATION PROGRAMMING

The guidance provided in this section is intended to ensure that 1) the chance of design errors built into the application logic is minimized, 2) the chance of errors resulting from translation of human-readable software into machine instructions loaded into the NuPAC platform is minimized, and 3) the implementation of the software life cycle processes are ensured.

### 6.1 General

#### 6.1.1

Plant-specific application programming activities shall ensure that all applicable requirements of this topical report are implemented.

#### 6.1.2

The SDOE shall be used for all activities associated with the plant-specific application programming and shall be protected in accordance with guidance provided in USNRC RG 1.152 (**Reference 133**), supporting a secure development organization, and the cyber security requirements of USNRC RG 5.71 (**Reference 151**).

#### 6.1.3

The symbols on the design basis logic drawings should be reviewed prior to starting programming. Any special requirements in those logic drawings (e.g., logic that expects a set-reset flip-flop to preferentially treat the invalid simultaneous turning on of both set and reset inputs as ignoring one of the inputs) shall be understood and communicated to the entire applications development team. Special provisions shall be made to verify and validate the operation of these special requirements during V&V activities.

#### 6.1.4

Programs shall be created in accordance with application programming coding guidelines. The guidelines must conform to all guidance provided in the NuPAC topical report.

#### 6.1.5

Applications logic shall be a product of a disciplined implementation process, providing the traceability necessary to tie source code and testing with higher-level design documents to enhance verification, validation, systems safety, and other aspects required for high criticality software development.

#### 6.1.6

To support long-term maintainability of the plant-specific application logic, the structure of logic shall be maximized.

#### 6.1.7

Constant values shall be declared, and not just inserted as numeric values.

#### 6.1.8

Comments shall be provided either within the human-readable programmable logic HDL files, or referenced to a separate document. Each HDL file shall contain a human-readable purpose and reference the logic diagram from which the programmable logic was derived. Operations or series of operations shall be described in

comments, to maximize the ease of reading, understanding, and modifying the application logic. Comments shall be structured and preferably placed in the programmable logic to minimize interface ambiguities and errors.

#### 6.1.9

For any unusual or complex constructs, as well as any deviations from normal programming practices, comments shall be provided explaining the purpose and operation of the construct or the reason for the deviation.

#### 6.1.10

Names used in the programmable logic for variables, procedures, functions, data types, constants, exceptions, objects, methods, labels, and other identifiers should be descriptive, consistent, and traceable to higher-level documents. Naming conventions are an important part of coding style and practices. Using the same name for multiple variables should be avoided unless obviously advantageous. When the same name is reused, clear, consistent, and unambiguous notations in all locations where the variable is used shall accompany each reuse.

#### 6.1.11

To the extent required by reliability or safety, open and short circuits in the wiring between the NuPAC platform and critical field devices should be detected and annunciated.

#### 6.1.12

Detection that a GLM has not completed processing within the expected period, has stopped completely, has not been sending messages, and other detectable faults and failures shall be annunciated to the control room. Documentation from which procedures can be written by the Licensee for troubleshooting and resolution will be provided.

#### 6.1.13

[

]<sup>a,c,e</sup>

#### 6.1.14

Any open cabinet door on any cabinet containing NuPAC equipment shall annunciate the open cabinet door or doors in the control room.

#### 6.1.15

Each cabinet containing NuPAC platform equipment will be identified in accordance with plant-specific identification procedure and Clause 5.11 of both IEEE Standard 603-1991 (**Reference 351**) and IEEE Standard 7-4.3.2-2003 (**Reference 356**).

#### 6.1.16

The plant-specific application logic shall support I/O mezzanine card inventory check for correct installation of expected I/O mezzanine card, and shall not start operation if an incorrect mezzanine card is installed.

### 6.1.17

The plant-specific application logic shall support a slot and chassis check for correct installation in identified slot and chassis, and shall not start operation if the location is incorrect.

### 6.1.18

Chassis numbers are configured within the non-power (i.e., not the power supply connectors) rear chassis connector. No valid chassis address shall be set to the chassis number that results when the wiring to that connector is removed.

## 6.2 Communications

### 6.2.1

Communications-related message payload constraints and protocols shall follow the NuPAC Application Specific Communications Interface Description (**Reference 736**).

## 7.0 PREVENTATIVE MAINTENANCE PROCEDURES

### 7.1

The Operations and Maintenance (O&M) Manual shall be provided to customers.

### 7.2

The fans installed within each NuPAC platform chassis, and any associated filters, will require [ ]<sup>a,c,e</sup> inspection and cleaning, and replacement every [ ]<sup>a,c,e</sup>. The O&M Manual shall identify at least a refueling cycle frequency to be included in the Licensee maintenance procedures and schedules to support these tasks will be developed.

### 7.3

The O&M Manual shall specify preventive maintenance planning to ensure that [ ]<sup>a,c,e</sup>



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 176 of 263  
Date: 04/14/2017

---

This page intentionally left blank.



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 177 of 263  
Date: 04/14/2017

---

## APPENDIX B: IEEE STANDARD 603-1991 COMPLIANCE MATRIX



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 178 of 263  
Date: 04/14/2017

---

This page intentionally left blank.



| IEEE Standard 603-1991 Compliance Matrix |                                     |                           |
|--|-------------------------------------|---------------------------|
| Section No.                              | Section Title                       | NuPAC Platform Compliance |
| 1  | Scope                               | [                         |
| 2  | Definitions                         |                           |
| 3  | References                          |                           |
| 4  | Safety System Designation           |                           |
| 4.1                                      | Design Basis Events/Modes           |                           |
| 4.2                                      | Safety Functions/Protective Actions | ] <sup>a,c,e</sup>        |

| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title                                  | NuPAC Platform Compliance |
| 4.3                                      | Permissive Conditions for Operating Bypasses   | [ ]                       |
| 4.4                                      | Variables for Protective Actions               |                           |
| 4.5                                      | Minimum Criteria for Manual Protective Actions |                           |
| 4.6                                      | Spatial Dependency of Monitored Variables      | ] <sup>a,c,e</sup>        |



| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title                                  | NuPAC Platform Compliance |
| 4.7                                      | Motive and Control Power Conditions            | [ ]                       |
| 4.8                                      | Conditions of Potential Functional Degradation | ] <sup>a,c,e</sup>        |



| IEEE Standard 603-1991 Compliance Matrix |                                   |                           |
|--|-----------------------------------|---------------------------|
| Section No.                              | Section Title                     | NuPAC Platform Compliance |
| 4.9                                      | Reliability Method(s) and Goal(s) | [ ]                       |
| 4.10                                     | DBE Critical Points               | ] <sup>a,c,e</sup>        |



| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title                                    | NuPAC Platform Compliance |
| 4.10.1                                   | DBE Critical Points of Initiation                | [ ]                       |
| 4.10.2                                   | DBE Critical Points of Completion                |                           |
| 4.10.3                                   | DBE Critical Points of Automatic Control         |                           |
| 4.10.4                                   | DBE Critical Points – Return to Normal Operation |                           |
| 4.11                                     | Equipment Protection Limitations                 |                           |
| 4.12                                     | Special Design Bases                             | ] <sup>a,c,e</sup>        |



| IEEE Standard 603-1991 Compliance Matrix |                        |                                 |
|--|------------------------|---------------------------------|
| Section No.                              | Section Title          | NuPAC Platform Compliance       |
| 5  | Safety System Criteria | [<br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 185 of 263  
Date: 04/14/2017

| IEEE Standard 603-1991 Compliance Matrix |                          |                           |
|--|--------------------------|---------------------------|
| Section No.                              | Section Title            | NuPAC Platform Compliance |
| 5.1                                      | Single-Failure Criterion | [<br>] <sup>a,c,e</sup>   |



| IEEE Standard 603-1991 Compliance Matrix |                                 |                           |
|--|---------------------------------|---------------------------|
| Section No.                              | Section Title                   | NuPAC Platform Compliance |
| 5.2                                      | Completion of Protective Action | [ ]                       |
| 5.3                                      | Quality                         | [ ] <sup>a,c,e</sup>      |



| IEEE Standard 603-1991 Compliance Matrix |                         |   |
|--|-------------------------|---|
| Section No.                              | Section Title           | NuPAC Platform Compliance               |
| 5.4                                      | Equipment Qualification | [<br><br><br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 188 of 263  
Date: 04/14/2017

| IEEE Standard 603-1991 Compliance Matrix |                  |                           |
|--|------------------|---------------------------|
| Section No.                              | Section Title    | NuPAC Platform Compliance |
| 5.5                                      | System Integrity | [<br>] <sup>a,c,e</sup>   |



| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title  | NuPAC Platform Compliance |
| 5.6                                      | Independence   |                           |
| 5.6.1                                    | Between Redundant Portions of a Safety System            | [ ]                       |
| 5.6.2                                    | Between Safety Systems and Effects of Design Basis Event | [ ] <sup>a,c,e</sup>      |



| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title                            | NuPAC Platform Compliance |
| 5.6.3                                    | Between Safety Systems and Other Systems | [                         |
| 5.6.3.1                                  | (1) Classification/ (2) Isolation        |                           |
| 5.6.3.2                                  | Equipment Proximity                      |                           |
| 5.6.3.3                                  | Effect of Single Failure                 |                           |
| 5.6.4                                    | Detailed Criteria                        | ] <sup>a,c,e</sup>        |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 191 of 263  
Date: 04/14/2017

| IEEE Standard 603-1991 Compliance Matrix |                                     |   |
|--|-------------------------------------|---|
| Section No.                              | Section Title                       | NuPAC Platform Compliance               |
| 5.7                                      | Capability for Test and Calibration | [<br><br><br><br><br>] <sup>a,c,e</sup> |



| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title                            | NuPAC Platform Compliance |
| 5.8                                      | Information Displays                     |                           |
| 5.8.1                                    | Displays for Manually Controlled Actions | [ ]                       |
| 5.8.2                                    | System Status Indication                 |                           |
| 5.8.3                                    | Indication of Bypasses                   |                           |
| 5.8.4                                    | Location                                 | [ ] <sup>a,c,e</sup>      |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 193 of 263  
Date: 04/14/2017

| IEEE Standard 603-1991 Compliance Matrix |                   |                           |
|--|-------------------|---------------------------|
| Section No.                              | Section Title     | NuPAC Platform Compliance |
| 5.9                                      | Control of Access | [<br>] <sup>a,c,e</sup>   |



| IEEE Standard 603-1991 Compliance Matrix |               |   |
|--|---------------|---|
| Section No.                              | Section Title | NuPAC Platform Compliance                               |
| 5.10                                     | Repair        | [<br><br><br><br><br><br><br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 195 of 263  
Date: 04/14/2017

| IEEE Standard 603-1991 Compliance Matrix |                    |   |
|--|--------------------|---|
| Section No.                              | Section Title      | NuPAC Platform Compliance               |
| 5.11                                     | Identification     | [<br><br><br><br><br>] <sup>a,c,e</sup> |
| 5.12                                     | Auxiliary Features |   |



| IEEE Standard 603-1991 Compliance Matrix |                              |                           |
|--|------------------------------|---------------------------|
| Section No.                              | Section Title                | NuPAC Platform Compliance |
| 5.12.1                                   | Auxiliary Features           | [ ]                       |
| 5.12.2                                   | Other Auxiliary Features     |                           |
| 5.13                                     | Multi-Unit Stations          |                           |
| 5.14                                     | Human Factors Considerations | [ ] <sup>a,c,e</sup>      |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 197 of 263  
Date: 04/14/2017

| IEEE Standard 603-1991 Compliance Matrix |  |   |
|--|--|---|
| Section No.                              | Section Title  | NuPAC Platform Compliance                               |
| 5.15                                     | Reliability  | [<br><br><br><br><br><br><br><br><br>] <sup>a,c,e</sup> |
| 6  | Sense and Command Features- Functional and Design Requirements |   |



| IEEE Standard 603-1991 Compliance Matrix |   |                           |
|--|---|---------------------------|
| Section No.                              | Section Title                                     | NuPAC Platform Compliance |
| 6.1                                      | Automatic Control                                 | [ ]                       |
| 6.2                                      | Manual Control                                    |                           |
| 6.2.1                                    | Division-level Manual Control (Automatic Signals) | [ ] <sup>a,c,e</sup>      |



| IEEE Standard 603-1991 Compliance Matrix |                                |                           |
|--|--------------------------------|---------------------------|
| Section No.                              | Section Title                  | NuPAC Platform Compliance |
| 6.2.2                                    | Manual Control (Non-automatic) | [ ] <sup>a,c,e</sup>      |
| 6.2.3                                    | After Protective Actions       |                           |



| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title  | NuPAC Platform Compliance |
| 6.3                                      | Interaction Between the Sense and Command Features and Other Systems | [ ]                       |
| 6.4                                      | Derivation of System Inputs  | ] <sup>a,c,e</sup>        |



| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title                          | NuPAC Platform Compliance |
| 6.5                                      | Capability for Testing and Calibration | [ ]                       |
| 6.6                                      | Operating Bypasses                     | ] <sup>a,c,e</sup>        |



| IEEE Standard 603-1991 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section No.                              | Section Title  | NuPAC Platform Compliance |
| 6.7                                      | Maintenance Bypass                                   | [ ]                       |
| 6.8                                      | Setpoints  |                           |
| 7  | Executive Feature-Functional and Design Requirements |                           |
| 8  | Power Source Requirements                            | ] <sup>a,c,e</sup>        |



---

## APPENDIX C: IEEE STANDARD 7-4.3.2-2003 COMPLIANCE MATRIX



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 204 of 263  
Date: 04/14/2017

---

This page intentionally left blank.

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                                 |   |                           |
|--|---------------------------------|---|---------------------------|
| Section No.                                  | Section Title                   | Relationship to IEEE Standard 603-1991 Requirements | NuPAC Platform Compliance |
| 1  | Scope                           | No requirements                                     | [ ]                       |
| 2  | References                      | No requirements                                     |                           |
| 3  | Definitions and Abbreviations   | No requirements                                     |                           |
| 4  | Safety System Design Basis      | No requirements beyond IEEE Standard 603            |                           |
| 5  | Safety System Criteria          | See specific subsections, below                     |                           |
| 5.1  | Single-Failure Criterion        | No requirements beyond IEEE Standard 603            |                           |
| 5.2  | Completion of Protective Action | No requirements beyond IEEE Standard 603            | [ ] <sup>a,c,e</sup>      |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 206 of 263  
Date: 04/14/2017

## **IEEE Standard 7-4.3.2-2003 Compliance Matrix**

| Section No. | Section Title | Relationship to IEEE Standard 603-1991 Requirements  | NuPAC Platform Compliance               |
|-------------|---------------|--|---|
| 5.3         | Quality       | Section 5.3 requirements addresses software quality. These are in addition to IEEE Standard 603, which addresses hardware quality. | [<br><br><br><br><br>] <sup>a,c,e</sup> |

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                          |   |                           |
|--|--------------------------|---|---------------------------|
| Section No.                                  | Section Title            | Relationship to IEEE Standard 603-1991 Requirements | NuPAC Platform Compliance |
| 5.3.1  | Software Development     |   | [ ]                       |
| 5.3.1.1                                      | Software Quality Metrics |   | ] <sup>a,c,e</sup>        |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 208 of 263  
Date: 04/14/2017

## **IEEE Standard 7-4.3.2-2003 Compliance Matrix**

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                |   |                           |
|--|----------------|---|---------------------------|
| Section No.                                  | Section Title  | Relationship to IEEE Standard 603-1991 Requirements | NuPAC Platform Compliance |
| 5.3.2  | Software Tools |   | [<br>] <sup>a,c,e</sup>   |



| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                             |   |   |
|--|-----------------------------|---|---|
| Section No.                                  | Section Title               | Relationship to IEEE Standard 603-1991 Requirements | NuPAC Platform Compliance               |
| 5.3.3  | Verification and Validation |   | [<br><br><br><br><br>] <sup>a,c,e</sup> |

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                                      |   |                           |
|--|--------------------------------------|---|---------------------------|
| Section No.                                  | Section Title                        | Relationship to IEEE Standard 603-1991 Requirements | NuPAC Platform Compliance |
| 5.3.4  | Independent V&V (I-V&V) Requirements |   | [                         |
| 5.3.5  | Software Configuration Management    |   | ] <sup>a,c,e</sup>        |

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |  |   |                           |
|--|--|---|---------------------------|
| Section No.                                  | Section Title                                  | Relationship to IEEE Standard 603-1991 Requirements   | NuPAC Platform Compliance |
| 5.3.6  | Software Project Risk Management               |   | [                         |
| 5.4  | Equipment Qualification                        | Section 5.4 requirements are necessary to qualify digital computers for use in safety systems and are in addition to the equipment qualification criteria in IEEE Standard 603. |                           |
| 5.4.1  | Computer System Testing                        |   |                           |
| 5.4.2  | Qualification of Existing Commercial Computers |   | ] <sup>a,c,e</sup>        |

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |  |   |                           |
|--|--|---|---------------------------|
| Section No.                                  | Section Title                                    | Relationship to IEEE Standard 603-1991 Requirements | NuPAC Platform Compliance |
| 5.4.2.1                                      | Preliminary Phase of the COTS Dedication Process |   | [ ]                       |
| 5.4.2.2                                      | Detailed Phase of the COTS Dedication Process    |   |                           |
| 5.4.2.3                                      | Maintenance of Commercial Dedication             |   | ] <sup>a,c,e</sup>        |



| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                               |  |   |
|--|-------------------------------|--|---|
| Section No.                                  | Section Title                 | Relationship to IEEE Standard 603-1991 Requirements  | NuPAC Platform Compliance               |
| 5.5  | System Integrity              | Section 5.5 requirements are necessary to achieve system integrity in digital equipment for use in safety systems and are in addition to the system integrity criteria in IEEE Standard 603. |   |
| 5.5.1  | Design for Computer Integrity |  | [<br><br><br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 214 of 263  
Date: 04/14/2017

## **IEEE Standard 7-4.3.2-2003 Compliance Matrix**

| Section No. | Section Title                   | Relationship to IEEE Standard 603-1991 Requirements | NuPAC Platform Compliance |
|-------------|---------------------------------|---|---------------------------|
| 5.5.2       | Design for Test and Calibration |   | [<br>] <sup>a,c,e</sup>   |



| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                                      |   |                           |
|--|--------------------------------------|---|---------------------------|
| Section No.                                  | Section Title                        | Relationship to IEEE Standard 603-1991 Requirements | NuPAC Platform Compliance |
|  |                                      |   |                           |
| 5.5.3  | Fault Detection and Self-diagnostics |   | ] <sup>a,c,e</sup>        |

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                                     |   |                           |
|--|-------------------------------------|---|---------------------------|
| Section No.                                  | Section Title                       | Relationship to IEEE Standard 603-1991 Requirements   | NuPAC Platform Compliance |
| 5.6  | Independence                        | In addition to the requirements of IEEE Standard 603, this section addresses independence of data communication between safety channels or between safety and non-safety systems. | [ ]                       |
| 5.7  | Capability for Test and Calibration | No requirements beyond IEEE Standard 603  |                           |
| 5.8  | Information Displays                | No requirements beyond IEEE Standard 603  |                           |
| 5.9  | Control of Access                   | No requirements beyond IEEE Standard 603  | [ ] <sup>a,c,e</sup>      |

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |                             |  |                           |
|--|-----------------------------|--|---------------------------|
| Section No.                                  | Section Title               | Relationship to IEEE Standard 603-1991 Requirements  | NuPAC Platform Compliance |
| 5.10   | Repair                      | No requirements beyond IEEE Standard 603   | [ ]                       |
| 5.11   | Identification              | Section 5.11 supplements IEEE Standard 603 with additional requirements to ensure that the computer system hardware and software are installed in the appropriate system configuration |                           |
| 5.12   | Auxiliary Features          | No requirements beyond IEEE Standard 603   |                           |
| 5.13   | Multi-unit Stations         | No requirements beyond IEEE Standard 603   |                           |
| 5.14   | Human Factor Considerations | No requirements beyond IEEE Standard 603   | ] <sup>a,c,e</sup>        |

| IEEE Standard 7-4.3.2-2003 Compliance Matrix |   |   |                           |
|--|---|---|---------------------------|
| Section No.                                  | Section Title   | Relationship to IEEE Standard 603-1991 Requirements   | NuPAC Platform Compliance |
| 5.15   | Reliability   | In addition to the requirements of IEEE Standard 603, when reliability goals are identified, the proof of meeting the goals should include the software | [ ]                       |
| 6  | Sense and Command Features—Functional And Design Requirements | No requirements beyond IEEE Standard 603  |                           |
| 7  | Execute Features—Functional and Design Requirements           | No requirements beyond IEEE Standard 603  |                           |
| 8  | Power Source Requirements                                     | No requirements beyond IEEE Standard 603  | ] <sup>a,c,e</sup>        |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 219 of 263  
Date: 04/14/2017

---

## APPENDIX D: DI&C-ISG-04 COMPLIANCE MATRIX



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 220 of 263  
Date: 04/14/2017

---

This page intentionally left blank.



| DI&C-ISG-04 Revision 1 Compliance Matrix               |   |                                 |
|--|---|---------------------------------|
| Section/Staff Position                                 | Requirement   | NuPAC Platform Compliance       |
| 1. Interdivisional Communications/<br>Staff Position 1 | A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE Std. 603. It is recognized that division voting logic must receive inputs from multiple safety divisions. | [<br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 222 of 263  
Date: 04/14/2017

**DI&C-ISG-04 Revision 1 Compliance Matrix**

| DI&C-ISG-04 Revision 1 Compliance Matrix               |  |                               |
|--|--|-------------------------------|
| Section/Staff Position                                 | Requirement  | NuPAC Platform Compliance     |
| 1. Interdivisional Communications/<br>Staff Position 2 | 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. | [ ]<br><br>] <sup>a,c,e</sup> |



| DI&C-ISG-04 Revision 1 Compliance Matrix                |  |                           |
|---|--|---------------------------|
| Section/Staff Position                                  | Requirement  | NuPAC Platform Compliance |
| 1. Interdivisional Communications/<br>Staff Position 3a | 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.   | [ ]                       |
| 1. Interdivisional Communications/<br>Staff Position 3b | 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. | ] <sup>a,c,e</sup>        |



| DI&C-ISG-04 Revision 1 Compliance Matrix                |  |                             |
|---|--|-----------------------------|
| Section/Staff Position                                  | Requirement  | NuPAC Platform Compliance   |
| 1. Interdivisional Communications/<br>Staff Position 3c | 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. | [<br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 225 of 263  
Date: 04/14/2017

DI&C-ISG-04 Revision 1 Compliance Matrix

| DI&C-ISG-04 Revision 1 Compliance Matrix                |  |   |
|---|--|---|
| Section/Staff Position                                  | Requirement  | NuPAC Platform Compliance               |
| 1. Interdivisional Communications/<br>Staff Position 4a | The communication process itself should be carried out by a communications processor, separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. | [<br><br><br><br><br>] <sup>a,c,e</sup> |



| DI&C-ISG-04 Revision 1 Compliance Matrix                |   |                           |
|---|---|---------------------------|
| Section/Staff Position                                  | Requirement   | NuPAC Platform Compliance |
| 1. Interdivisional Communications/<br>Staff Position 4b | 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 CFR Part 50, Appendices A and B.  | [                         |
| 1. Interdivisional Communications/<br>Staff Position 4c | 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. | ] <sup>a,c,e</sup>        |



| DI&C-ISG-04 Revision 1 Compliance Matrix                |   |                                 |
|---|---|---------------------------------|
| Section/Staff Position                                  | Requirement   | NuPAC Platform Compliance       |
| 1. Interdivisional Communications/<br>Staff Position 4d | 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. | [<br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 228 of 263  
Date: 04/14/2017

**DI&C-ISG-04 Revision 1 Compliance Matrix**

| DI&C-ISG-04 Revision 1 Compliance Matrix               |  |                                 |
|--|--|---------------------------------|
| Section/Staff Position                                 | Requirement  | NuPAC Platform Compliance       |
| 1. Interdivisional Communications/<br>Staff Position 6 | The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division. | [<br><br><br>] <sup>a,c,e</sup> |



| DI&C-ISG-04 Revision 1 Compliance Matrix               |   |                           |
|--|---|---------------------------|
| Section/Staff Position                                 | Requirement   | NuPAC Platform Compliance |
| 1. Interdivisional Communications/<br>Staff Position 7 | Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be predetermined. 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. | [ ]                       |
| 1. Interdivisional Communications/<br>Staff Position 8 | Data exchanged between redundant safety divisions or between safety and non-safety 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.  | ] <sup>a,c,e</sup>        |



| DI&C-ISG-04 Revision 1 Compliance Matrix                 |   |                           |
|--|---|---------------------------|
| Section/Staff Position                                   | Requirement   | NuPAC Platform Compliance |
| 1. Interdivisional Communications/<br>Staff Position 9   | Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device. | [                         |
| 1. Interdivisional Communications/<br>Staff Position 10a | 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.   | ] <sup>a,c,e</sup>        |



| DI&C-ISG-04 Revision 1 Compliance Matrix                 |  |                           |
|--|--|---------------------------|
| Section/Staff Position                                   | Requirement  | NuPAC Platform Compliance |
| 1. Interdivisional Communications/<br>Staff Position 10b | A workstation (e.g., engineer or programmer station) may alter addressable constants, set points, 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) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes. | [ ]                       |
| 1. Interdivisional Communications/<br>Staff Position 11a | Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service.   | ] <sup>a,c,e</sup>        |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 233 of 263  
Date: 04/14/2017

**DI&C-ISG-04 Revision 1 Compliance Matrix**

| DI&C-ISG-04 Revision 1 Compliance Matrix                 |   |                               |
|--|---|-------------------------------|
| Section/Staff Position                                   | Requirement   | NuPAC Platform Compliance     |
| 1. Interdivisional Communications/<br>Staff Position 11b | 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. | [ ]<br><br>] <sup>a,c,e</sup> |



| DI&C-ISG-04 Revision 1 Compliance Matrix                |   |                           |
|---|---|---------------------------|
| Section/Staff Position                                  | Requirement   | NuPAC Platform Compliance |
| 1. Interdivisional Communications/<br>Staff Position 12 | 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 CFR Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:<br><i>&lt;which are listed below&gt;</i> |                           |
|   | 1) Messages may be corrupted due to errors in communications, logic errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.  | [<br>] <sup>a,c,e</sup>   |



| DI&C-ISG-04 Revision 1 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section/Staff Position                   | Requirement  | NuPAC Platform Compliance |
|  | 2) Messages may be repeated at an incorrect point in time. | [                         |
|  | 3) Messages may be sent in the incorrect sequence.         | ] <sup>a,c,e</sup>        |



| DI&C-ISG-04 Revision 1 Compliance Matrix |   |                           |
|--|---|---------------------------|
| Section/Staff Position                   | Requirement   | NuPAC Platform Compliance |
|  | 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.   | ] <sup>a,c,e</sup>        |



| DI&C-ISG-04 Revision 1 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section/Staff Position                   | Requirement  | NuPAC Platform Compliance |
|  | 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. | ] <sup>a,c,e</sup>        |



| DI&C-ISG-04 Revision 1 Compliance Matrix |  |                           |
|--|--|---------------------------|
| Section/Staff Position                   | Requirement  | NuPAC Platform Compliance |
|  | 9) Messages may contain data that is outside the expected range. | [<br>] <sup>a,c,e</sup>   |



| DI&C-ISG-04 Revision 1 Compliance Matrix |  |   |
|--|--|---|
| Section/Staff Position                   | Requirement  | NuPAC Platform Compliance               |
|  | 10) Messages may appear valid, but data may be placed in incorrect locations within the message. | [<br><br><br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 240 of 263  
Date: 04/14/2017

**DI&C-ISG-04 Revision 1 Compliance Matrix**

| DI&C-ISG-04 Revision 1 Compliance Matrix |   |                           |
|--|---|---------------------------|
| Section/Staff Position                   | Requirement   | NuPAC Platform Compliance |
|  | 11) Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm). | [ ]<br>] <sup>a,c,e</sup> |



| DI&C-ISG-04 Revision 1 Compliance Matrix                |  |                           |
|---|--|---------------------------|
| Section/Staff Position                                  | Requirement  | NuPAC Platform Compliance |
|   | 12) Message headers or addresses may be corrupted.   | [ ]                       |
| 1. Interdivisional Communications/<br>Staff Position 13 | Vital communications, such as the sharing of channel trip decisions for 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. | [ ] <sup>a,c,e</sup>      |

| DI&C-ISG-04 Revision 1 Compliance Matrix                |   |                           |
|---|---|---------------------------|
| Section/Staff Position                                  | Requirement   | NuPAC Platform Compliance |
| 1. Interdivisional Communications/<br>Staff Position 14 | <p>Vital 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.</p> <p>Implementation of other communication strategies should provide the same reliability and should be justified.</p> | [ ]                       |
| 1. Interdivisional Communications/<br>Staff Position 15 | Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.  | ] <sup>a,c,e</sup>        |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 243 of 263  
Date: 04/14/2017

## **DI&C-ISG-04 Revision 1 Compliance Matrix**

| DI&C-ISG-04 Revision 1 Compliance Matrix                |   |   |
|---|---|---|
| Section/Staff Position                                  | Requirement   | NuPAC Platform Compliance               |
| 1. Interdivisional Communications/<br>Staff Position 16 | <p>Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. Note: This is also required by the independence criteria of:</p> <ul style="list-style-type: none"> <li>1) 10 CFR Part 50, Appendix A, General Design Criteria (“GDC”) 24, which states, “interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.”; and</li> <li>2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)</li> </ul> | [<br><br><br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 244 of 263  
Date: 04/14/2017

**DI&C-ISG-04 Revision 1 Compliance Matrix**

| DI&C-ISG-04 Revision 1 Compliance Matrix              |   |                                 |
|---|---|---------------------------------|
| Section/Staff Position                                | Requirement   | NuPAC Platform Compliance       |
| 1. Interdivisional Communications/ Staff Position 17a | Pursuant to 10 C.F.R. §50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. | [ ]<br><br>[ ] <sup>a,c,e</sup> |



| DI&C-ISG-04 Revision 1 Compliance Matrix                 |  |   |
|--|--|---|
| Section/Staff Position                                   | Requirement  | NuPAC Platform Compliance               |
| 1. Interdivisional Communications/<br>Staff Position 17b | 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. | [<br><br><br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 246 of 263  
Date: 04/14/2017

**DI&C-ISG-04 Revision 1 Compliance Matrix**

| DI&C-ISG-04 Revision 1 Compliance Matrix                |   |   |
|---|---|---|
| Section/Staff Position                                  | Requirement   | NuPAC Platform Compliance               |
| 1. Interdivisional Communications/<br>Staff Position 18 | Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication. | [<br><br><br><br><br>] <sup>a,c,e</sup> |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 247 of 263  
Date: 04/14/2017

DI&C-ISG-04 Revision 1 Compliance Matrix

| DI&C-ISG-04 Revision 1 Compliance Matrix                |  |   |
|---|--|---|
| Section/Staff Position                                  | Requirement  | NuPAC Platform Compliance               |
| 1. Interdivisional Communications/<br>Staff Position 19 | If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that 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. | [<br><br><br><br><br>] <sup>a,c,e</sup> |



| DI&C-ISG-04 Revision 1 Compliance Matrix                  |  |                           |
|---|--|---------------------------|
| Section/Staff Position                                    | Requirement  | NuPAC Platform Compliance |
| 1. Interdivisional Communications/<br>Staff Position 20   | 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. | [                         |
| 2. Command Prioritization/<br>Staff Positions 1 to 10     | Various requirements for Priority Logic Modules  |                           |
| 3.1 Independence and Isolation/<br>Staff Position 1       | Non-safety stations receiving information from one or more safety divisions.   |                           |
| 3.1 Independence and Isolation/<br>Staff Position 2       | Safety related stations receiving data from one or more safety divisions   |                           |
| 3.1 Independence and Isolation/<br>Staff Positions 3 to 5 | Various requirements for multi-divisional communication  |                           |
| 3.2 Human Factors Considerations                          | Various requirements for Human Factors Engineering for the associated system   |                           |
| 3.3 Diversity and Defense-in-Depth Considerations         | Various requirements for D3 analyses   | ] <sup>a,c,e</sup>        |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 249 of 263  
Date: 04/14/2017

## APPENDIX E: DI&C-ISG-06 COMPLIANCE MATRIX



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 250 of 263  
Date: 04/14/2017

This page intentionally left blank.

| DI&C-ISG-06 Revision 1 Compliance Matrix |                              |       |  |
|--|------------------------------|-------|--|
| Section No.                              | Section Title                | Phase | NuPAC Platform Compliance <sup>1</sup>   |
| A  | Introduction                 |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| B  | Purpose                      |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| C  | Digital I&C Review Process   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D  | Review Areas                 |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.1                                      | System Description           |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.1.1                                    | Scope of Review              |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.1.2                                    | Information to Be Provided   | 1     | <ul style="list-style-type: none"> <li>• System overview provided in Section 3.1 of this LTR.</li> </ul>   |
| D.1.3                                    | Regulatory Evaluation        |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.1.4                                    | Technical Evaluation         |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.1.5                                    | Conclusion                   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.2                                      | Hardware Development Process |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.2.1                                    | Scope of Review              |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.2.2                                    | Information to Be Provided   | 1     | <ul style="list-style-type: none"> <li>• Hardware design process described in Section 4.0 of this LTR. The quality assurance plan for digital hardware,” NUPAC document number NuPAC_QAP61000-001 (<b>Reference 719</b>). In addition to the hardware design process. Manufacturing processes are established for the following:             <ul style="list-style-type: none"> <li>○ Manufacturing instructions</li> <li>○ Inspection Instructions</li> <li>○ Acceptance Test Procedures</li> </ul> </li> </ul> |
| D.2.3                                    | Regulatory Evaluation        |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.2.4                                    | Technical Evaluation         |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.2.5                                    | Conclusion                   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.3                                      | Software Architecture        |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.3.1                                    | Scope of Review              |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.3.2                                    | Information to Be Provided   | 1     | <ul style="list-style-type: none"> <li>• Programmable logic architecture summarized in Section 3.3 of this LTR</li> <li>• Programmable logic architecture description provided in the “NuPAC Programmable Logic Development Specification - Core PLCI,” NUPAC document number NuPAC_PLDS610400-001 (<b>Reference 717</b>)</li> <li>• Programmable logic configuration items identified in Section 3.1.4 of this LTR</li> </ul>   |
| D.3.3                                    | Regulatory Evaluation        |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.3.4                                    | Technical Evaluation         |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |

| DI&C-ISG-06 Revision 1 Compliance Matrix   |  |       |  |
|--|--|-------|--|
| Section No.  | Section Title                                    | Phase | NuPAC Platform Compliance <sup>1</sup>   |
| D.3.5  | Conclusion                                       |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| NOTES: <sup>1</sup> Refer to Table 10-3 for applicable version of each document. |  |       |  |
| D.4  | Software Development Processes                   |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.4.1  | Scope of Review                                  |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.4.2  | Information to Be Provided                       | 1     | <ul style="list-style-type: none"> <li>• Software development process for programmable logic described in Section 5.0 of this LTR</li> <li>• Reference “NuPAC Programmable Logic Development Plan,” NUPAC document number NuPAC_PLDP610000-001 (<b>Reference 715</b>)</li> </ul> |
| D.4.3  | Regulatory Evaluation                            |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>  |
| D.4.4  | Technical Evaluation                             |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.4.4.1  | Software Planning Documentation                  |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.4.4.1.1  | Software Management Plan (SMP)                   | 1     | <ul style="list-style-type: none"> <li>• SMP summarized in Section 5.0 of this LTR</li> <li>• Reference “NuPAC Programmable Logic Development Plan,” NUPAC document number NuPAC_PLDP610000-001 (<b>Reference 715</b>)</li> </ul>  |
| D.4.4.1.2  | Software Development Plan (SDP)                  | 1     | <ul style="list-style-type: none"> <li>• SDP summarized in Section 5.0 of this LTR</li> <li>• Reference “NuPAC Programmable Logic Development Plan,” NUPAC document number NuPAC_PLDP610000-001 (<b>Reference 715</b>)</li> </ul>  |
| D.4.4.1.3  | Software Quality Assurance Plan (SQAP)           | 1     | <ul style="list-style-type: none"> <li>• SQAP summarized in Section 5.0 of this LTR.</li> <li>• Reference “Quality Assurance Plan,” NUPAC document number NuPAC_QAP610000-001 (<b>Reference 719</b>)</li> </ul>  |
| D.4.4.1.4  | Software Integration Plan (SIntP)                | 1     | <ul style="list-style-type: none"> <li>• Reference “NuPAC Programmable Logic Verification Procedure – Core PLCI,” NUPAC document number NuPAC_PLPRC610000-001 (<b>Reference 729</b>)</li> </ul>  |
|  |  | 2     | <ul style="list-style-type: none"> <li>• Software Test Report (STRpt)</li> </ul>   |
| D.4.4.1.5  | Software Installation Plan (SInstP)              |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>  |
| D.4.4.1.6  | Software Maintenance Plan (SMaintP)              |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>  |
| D.4.4.1.7  | Software Training Plan (STrngP)                  |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>  |
| D.4.4.1.8  | Software Operations Plan (SOP)                   |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>  |
| D.4.4.1.9  | Software Safety Plan (SSP)                       | 1     | <ul style="list-style-type: none"> <li>• Reference “Platform Safety Project Plan,” NUPAC document number NuPAC_PSPP610000-001 (<b>Reference 726</b>)</li> </ul>  |
| D.4.4.1.10   | Software Verification and Validation Plan (SVVP) | 1     | <ul style="list-style-type: none"> <li>• Reference “NuPAC Field-programmable Logic Verification and Validation Plan,” NUPAC document number NuPAC_FVVP610000-001 (<b>Reference 711</b>)</li> </ul>   |

| DI&C-ISG-06 Revision 1 Compliance Matrix |   |       |  |
|--|---|-------|--|
| Section No.                              | Section Title                                 | Phase | NuPAC Platform Compliance <sup>1</sup>   |
| D.4.4.1.11                               | Software Configuration Management Plan (SCMP) | 1     | <ul style="list-style-type: none"> <li>Reference “Configuration Management Plan,” NUPAC document number NUPAC_CMP610000-001 (<a href="#">Reference 702</a>)</li> </ul>   |
| D.4.4.1.12                               | Software Test Plan (STP)                      | 1     | <ul style="list-style-type: none"> <li>Reference draft of “NuPAC Programmable Logic Verification Procedure – Core PLCI,” NUPAC document number NuPAC_PLPRC610000-002 (<a href="#">Reference 729</a>) (available for audit); for V&amp;V testing, refer to “NuPAC FPL Verification and Validation Plan,” NuPAC_FVVP610000-001 (<a href="#">Reference 711</a>).</li> </ul>   |
| D.4.4.2                                  | Software Plan Implementation                  |       | <ul style="list-style-type: none"> <li>Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.4.4.2.1                                | Software Safety Analysis (SSA)                | 2     | <ul style="list-style-type: none"> <li>Reference “Programmable Logic Failure Modes and Effects Analysis (FMEA) Report,” NUPAC document number NuPAC_ED610000-063 (<a href="#">Reference 737</a>)</li> </ul>  |
| D.4.4.2.2                                | V&V Analysis and Reports                      | 2     | <ul style="list-style-type: none"> <li>IV&amp;V evaluated NuPAC Baseline 1.3.1 documentation and documented anomalies in the following activity summary reports:           <ul style="list-style-type: none"> <li>Acquisition: ASR610000-100 (<a href="#">Reference 752</a>)</li> <li>Planning: ASR610000-101 (<a href="#">Reference 753</a>)</li> <li>Concept: ASR610000-102 (<a href="#">Reference 754</a>)</li> <li>Requirements: ASR610000-103 (<a href="#">Reference 755</a>)</li> <li>Design: ASR610000-104 (<a href="#">Reference 756</a>)</li> <li>Implementation: ASR610000-105 (<a href="#">Reference 757</a>)</li> <li>Test: ASR610000-106 (<a href="#">Reference 758</a>)</li> </ul> </li> <li>IV&amp;V evaluated NuPAC Baseline 1.3.2 documentation which incorporated the 1.3.1 anomalies. These activities are documented in the following activity summary reports:           <ul style="list-style-type: none"> <li>Concept: ASR610000-112 (<a href="#">Reference 759</a>)</li> <li>Requirements: ASR610000-113 (<a href="#">Reference 760</a>)</li> <li>Design: ASR610000-114 (<a href="#">Reference 761</a>)</li> <li>Implementation: ASR610000-115 (<a href="#">Reference 762</a>)</li> <li>Test: ASR610000-116 (<a href="#">Reference 763</a>)</li> </ul> </li> </ul> |
| D.4.4.2.3                                | Configuration Management Activities           | 2     | <ul style="list-style-type: none"> <li>Reference “NuPAC Version Description Document – Core Programmable Logic Configuration Item,” NUPAC document number NuPAC_VDD610400-001 (<a href="#">Reference 738</a>)</li> <li>Reference “Status Accounting/Baseline Definition Report for NuPAC Baseline 1.2.2 Hardware Seismic/ESD/Surge Testing” NuPAC_BL610000-005 (<a href="#">Reference 772</a>)</li> <li>Reference “Status Accounting/Baseline Definition Report for NuPAC Programmable Logic Baseline 1.3.2”, NuPAC_BL610000-008 (<a href="#">Reference 773</a>)</li> </ul>  |

| DI&C-ISG-06 Revision 1 Compliance Matrix |   |       |  |
|--|---|-------|--|
| Section No.                              | Section Title                             | Phase | NuPAC Platform Compliance <sup>1</sup>   |
| D.4.4.2.4                                | Testing Activities                        | 2     | <ul style="list-style-type: none"> <li>Reference “NuPAC V&amp;V Final Report,” NuPAC document number IFR610000-001 (<b>Reference 764</b>)</li> <li>Reference “NuPAC Baseline 1.3.2 V&amp;V Final Report,” NuPAC document number IFR610000-103 (<b>Reference 765</b>)</li> <li>Reference “NuPAC Version Description Document – Core Programmable Logic,” NUPAC document number NuPAC_VDD610400-001 (<b>Reference 738</b>)</li> <li>Incidence/Anomalies tracked through the process using [ ]<sup>a,c,e</sup></li> </ul> |
| D.4.4.3                                  | Design Outputs                            |       | <ul style="list-style-type: none"> <li>Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.4.4.3.1                                | Software Requirements Specification (SRS) | 1     | <ul style="list-style-type: none"> <li>Reference “NuPAC Programmable Logic Requirement Specification - Core PLCI,” NUPAC document number NuPAC_PLRS610400-001 (<b>Reference 733</b>)</li> </ul>  |
| D.4.4.3.2                                | Software Architecture Description (SAD)   | 1     | <ul style="list-style-type: none"> <li>Programmable logic architecture summarized in Section 3.3 of this LTR</li> <li>Reference “NuPAC Programmable Logic Development Specification - Core PLCI,” NUPAC document number NuPAC_PLDS610400-001 (<b>Reference 717</b>)</li> </ul>   |
| D.4.4.3.3                                | Software Design Specification             | 1     | <ul style="list-style-type: none"> <li>Reference “NuPAC Programmable Logic Development Specification - Core PLCI,” NUPAC document number NuPAC_PLDS610400-001 (<b>Reference 717</b>)</li> </ul>  |
| D.4.4.3.4                                | Code Listings                             | 2     | <ul style="list-style-type: none"> <li>Reference “NuPAC Core Programmable Logic Configuration Item (PLCI) Version 05.02.2B”, NuPAC_PLCI610400 (<b>Reference 774</b>) listing available for thread audits</li> </ul>  |
| D.4.4.3.5                                | System Build Documents (SBDs)             | 2     | <ul style="list-style-type: none"> <li>Reference “NuPAC Version Description Document – Core Programmable Logic,” NUPAC document number NuPAC_VDD610400-001 (<b>Reference 738</b>)</li> </ul>   |
| D.4.4.3.6                                | Installation Configuration Tables         |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>  |
| D.4.4.3.7                                | Operations Manual                         |       | <ul style="list-style-type: none"> <li>Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>  |
| D.4.4.3.8                                | Software Maintenance Manuals              |       | <ul style="list-style-type: none"> <li>Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>  |
| D.4.4.3.9                                | Software Training Manuals                 |       | <ul style="list-style-type: none"> <li>Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>  |
| D.4.5                                    | Conclusion                                |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>  |
| D.5                                      | Environmental Equipment Qualifications    |       | <ul style="list-style-type: none"> <li>Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.5.1                                    | Scope of Review                           |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>  |

| DI&C-ISG-06 Revision 1 Compliance Matrix |   |       |   |
|--|---|-------|---|
| Section No.                              | Section Title   | Phase | NuPAC Platform Compliance <sup>1</sup>  |
| D.5.2                                    | Information to Be Provided                                | 1     | <ul style="list-style-type: none"> <li>Reference “Master Test Plan,” NUPAC document number NuPAC_MTP610000-001 (<b>Reference 714</b>)</li> </ul>  |
|  |   | 2     | <ul style="list-style-type: none"> <li>Reference “NuPAC System Environmental Test Procedure,” NUPAC document number NuPAC_TP610000-004 (<b>Reference 739</b>)</li> <li>Reference “NuPAC System Seismic Test Procedure,” NUPAC document number NuPAC_TP610000-005 (<b>Reference 740</b>)</li> <li>Reference “NuPAC System Radiation Test Procedure,” NUPAC document number NuPAC_TP610000-006 (<b>Reference 741</b>)</li> <li>Reference “NuPAC System Electromagnetic Compatibility Test Procedure,” NUPAC document number NuPAC_TP610000-007 (<b>Reference 742</b>)</li> <li>Reference “NuPAC System Electrostatic Discharge Test Procedure,” NUPAC document number NuPAC_TP610000-009 (<b>Reference 743</b>)</li> <li>Reference “NuPAC Environmental Equipment Qualification Summary Report,” NUPAC document number NuPAC_TR610000-010 (<b>Reference 730</b>)</li> </ul> |
| D.5.3                                    | Regulatory Evaluation                                     |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.5.4                                    | Technical Evaluation                                      |       | <ul style="list-style-type: none"> <li>Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>  |
| D.5.4.1                                  | Atmospheric   |       | <ul style="list-style-type: none"> <li>Reference “NuPAC System Environmental Test Report,” NUPAC document number NuPAC_TP610000-004 (<b>Reference 739</b>)</li> </ul>   |
| D.5.4.2                                  | Radiation   |       | <ul style="list-style-type: none"> <li>Reference “NuPAC System Radiation Test Report,” NUPAC document number NuPAC_TR610000-006 (<b>Reference 741</b>)</li> </ul>   |
| D.5.4.3                                  | Electromagnetic Interference/Radio Frequency Interference |       | <ul style="list-style-type: none"> <li>Reference “NuPAC System Electromagnetic Compatibility Test Report,” NUPAC document number NuPAC_TR610000-007 (<b>Reference 742</b>)</li> </ul>   |
| D.5.4.3.1                                | Susceptibility  |       | <ul style="list-style-type: none"> <li>Reference “NuPAC System Electromagnetic Compatibility Test Report,” NUPAC document number NuPAC_TR610000-007 (<b>Reference 742</b>)</li> </ul>   |
| D.5.4.3.2                                | Interference  |       | <ul style="list-style-type: none"> <li>Reference “NuPAC System Electromagnetic Compatibility Test Report,” NUPAC document number NuPAC_TR610000-007 (<b>Reference 742</b>)</li> </ul>   |
| D.5.4.4                                  | Sprays and Chemicals                                      |       | <ul style="list-style-type: none"> <li>Generic NuPAC platform design basis does not include exposure to sprays; therefore, requirement(s) not applicable</li> </ul>   |
| D.5.4.5                                  | Seismic   |       | <ul style="list-style-type: none"> <li>Reference “NuPAC System Seismic Test Report,” NUPAC document number NuPAC_TR610000-005 (<b>Reference 740</b>)</li> </ul>   |
| D.5.5                                    | Conclusion  |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.6                                      | Defense-in-Depth and Diversity                            |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.6.1                                    | Scope of Review   |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |

### DI&C-ISG-06 Revision 1 Compliance Matrix

| Section No. | Section Title   | Phase | NuPAC Platform Compliance <sup>1</sup>  |
|-------------|---|-------|---|
| D.6.2       | Information to Be Provided  |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.6.3       | Regulatory Evaluation   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.6.4       | Technical Evaluation  |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.6.4.1     | Adequate Safety System Diversity and Manual Actions               |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>   |
| D.6.4.2     | Diverse Displays and Controls for System Level Actuation          |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>   |
| D.6.5       | Conclusions   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.7         | Communications  |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>  |
| D.7.1       | Scope of Review   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.7.2       | Information to Be Provided  | 1     | <ul style="list-style-type: none"> <li>• Data Communication described in Section 3.4 of this LTR</li> <li>• DI&amp;C-ISG-04 Compliance Matrix provided in Appendix D of this LTR</li> </ul>       |
| D.7.3       | Regulatory Evaluation   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.7.4       | Technical Evaluation  |       | <ul style="list-style-type: none"> <li>• DI&amp;C-ISG-04 Compliance Matrix provided in Appendix D of this LTR</li> </ul>  |
| D.7.5       | Conclusions   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.8         | System, Hardware, Software, and Methodology Modifications         |       | <ul style="list-style-type: none"> <li>• Not Applicable</li> </ul>  |
| D.9         | Compliance with IEEE Std. 603                                     |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>  |
| D.9.1       | Scope of Review   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.9.2       | Information to Be Provided  |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix provided in Appendix B of this LTR</li> <li>• System Description provided in Section 3.1 of this LTR</li> </ul> |
| D.9.3       | Regulatory Evaluation   |       | <ul style="list-style-type: none"> <li>• The intent of this topical report is to show compliance with IEEE Standard 603-1991 and not propose compliance to an alternative standard.</li> </ul>    |
| D.9.4       | Technical Evaluation  | 1     | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.9.4.1     | IEEE Std 603, Clause 4, Design Basis                              |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 4, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.1.1   | IEEE Std 603, Clause 4.1, Design Basis Events                     |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 4.1, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.1.2   | IEEE Std 603, Clause 4.2, Safety Functions and Protective Actions |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 4.2, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.1.3   | IEEE Std 603, Clause 4.3, Permissive Conditions                   |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 4.3, provided in Appendix B of this LTR</li> </ul>   |

| DI&C-ISG-06 Revision 1 Compliance Matrix |  |       |  |
|--|--|-------|--|
| Section No.                              | Section Title  | Phase | NuPAC Platform Compliance <sup>1</sup>   |
| D.9.4.1.4                                | IEEE Std 603, Clause 4.4, Variables monitored                          |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.4, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.1.5                                | IEEE Std 603, Clause 4.5, Criteria for manual protective actions       |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.5, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.1.6                                | IEEE Std 603, Clause 4.6, Minimum number and location of sensors       |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.6, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.1.7                                | IEEE Std 603, Clause 4.7, Range of Conditions                          |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.7, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.1.8                                | IEEE Std 603, Clause 4.8, Conditions Causing Functional Degradation    |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.8, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.1.9                                | IEEE Std 603, Clause 4.9, Methods used to determine reliability        |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.9, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.1.10                               | IEEE Std 603, Clause 4.10, Critical Points in Time or Plant Conditions |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.10, 4.10.1, 4.10.2, 4.10.3 and 4.10.4, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.1.11                               | IEEE Std 603, Clause 4.11, Equipment Protective Provisions             |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.11, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.1.12                               | IEEE Std 603, Clause 4.12, Special Design Basis                        |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4.12, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.2                                  | IEEE Std 603, Clause 5, System   | 2     | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 5, provided in Appendix B of this LTR</li> <li>Program verification documents provide requirement traceability matrices within the documents themselves.</li> </ul>                                     |
| D.9.4.2.1                                | IEEE Std 603, Clause 5.1, Single Failure Criterion                     |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 5.1, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.2.1.1                              | Failure Modes and Effects Analysis                                     |       | <ul style="list-style-type: none"> <li>Reference “NuPAC Failure Mode and Effects Analysis Report,” NUPAC document number NuPAC_ED610000-049 (<b>Reference 705</b>)</li> <li>Reference “NuPAC Core Logic FMEA Report,” NUPAC document number NuPAC_ED610000-063 (<b>Reference 737</b>)</li> </ul> |
| D.9.4.2.2                                | IEEE Std 603, Clause 5.2, Completion of Protective Action              |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 5.2, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.2.3                                | IEEE Std 603, Clause 5.3, Quality                                      |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 5.3, provided in Appendix B of this LTR</li> </ul>  |

### DI&C-ISG-06 Revision 1 Compliance Matrix

| Section No. | Section Title   | Phase | NuPAC Platform Compliance <sup>1</sup>   |
|-------------|---|-------|--|
| D.9.4.2.4   | IEEE Std 603, Clause 5.4, Equipment Qualification             |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.4, provided in Appendix B of this LTR</li> <li>• Reference “NuPAC Response Time Analysis,” NUPAC document number NuPAC_ED610000-051 (<b>Reference 707</b>)</li> <li>• Reference “NuPAC Integration and Test (I&amp;T) Summary Report,” NUPAC document number NuPAC_TR610000-100 (<b>Reference 730</b>)</li> </ul> |
| D.9.4.2.5   | IEEE Std 603, Clause 5.5, System Integrity                    |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.5, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.2.6   | IEEE Std 603, Clause 5.6, Independence                        |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Sections 5.6.1, 5.6.2, and 5.6.3, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.2.6.1 | IEEE Std 603, Clause 5.6.1, Between Redundant Portions        |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.6.1, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.2.6.2 | IEEE Std 603, Clause 5.6.2, Effects of Design Basis Events    |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.6.2, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.2.6.3 | IEEE Std 603, Clause 5.6.3, Other Systems                     |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Sections 5.6.3, 5.6.3.1, 5.6.3.2, and 5.6.3.3 provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.2.7   | IEEE Std 603, Clause 5.7, Capability for Test and Calibration |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.7, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.2.8   | IEEE Std 603, Clause 5.8, Information Displays                |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Sections 5.8.1, 5.8.2, 5.8.3, and 5.8.4, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.2.9   | IEEE Std 603, Clause 5.9, Control of Access                   |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.9, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.2.10  | IEEE Std 603, Clause 5.10, Repair                             |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.10, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.2.11  | IEEE Std 603, Clause 5.11, Identification                     |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.11, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.2.12  | IEEE Std 603, Clause 5.12, Auxiliary Features                 |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Sections 5.12.1 and 5.12.2, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.2.13  | IEEE Std 603, Clause 5.13, Multi-Unit Stations                |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.13, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.2.14  | IEEE Std 603, Clause 5.14, Human Factors                      |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.14, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.2.15  | IEEE Std 603, Clause 5.15, Reliability                        |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 5.15, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.3     | IEEE Std 603, Clause 6, Sense and Command Features            |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.9.4.3.1   | IEEE Std 603, Clause 6.1, Automatic Control                   |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 6.1, provided in Appendix B of this LTR</li> </ul>  |
| D.9.4.3.2   | IEEE Std 603, Clause 6.2, Manual Control                      |       | <ul style="list-style-type: none"> <li>• IEEE Standard 603-1991 Compliance Matrix, Section 6.2, provided in Appendix B of this LTR</li> </ul>  |

| DI&C-ISG-06 Revision 1 Compliance Matrix |  |       |   |
|--|--|-------|---|
| Section No.                              | Section Title  | Phase | NuPAC Platform Compliance <sup>1</sup>  |
| D.9.4.3.3                                | IEEE Std 603, Clause 6.3, Interaction with Other Systems         |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 6.3, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.3.4                                | IEEE Std 603, Clause 6.4, Derivation of System Inputs            |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 6.4, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.3.5                                | IEEE Std 603, Clause 6.5, Capability for Testing and Calibration |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 6.5, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.3.6                                | IEEE Std 603, Clause 6.6, Operating Bypass                       |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 6.6, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.3.7                                | IEEE Std 603, Clause 6.7, Maintenance Bypass                     |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 6.7, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.3.8                                | IEEE Std 603, Clause 6.8, Setpoints                              |       | <ul style="list-style-type: none"> <li>IEEE Standard 603-1991 Compliance Matrix, Section 6.8, provided in Appendix B of this LTR</li> </ul>   |
| D.9.4.4                                  | IEEE Std 603, Clause 7, Execute Features                         |       | <ul style="list-style-type: none"> <li>Execute features are outside of the NuPAC platform.</li> </ul>   |
| D.9.4.5                                  | IEEE Std 603, Clause 8, Power Source Requirements                |       | <ul style="list-style-type: none"> <li>Power Source(s) is not part of the NuPAC platform</li> </ul>   |
| D.9.5                                    | Conclusion   |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.10                                     | Conformance with IEEE Std. 7-4.3.2                               |       | <ul style="list-style-type: none"> <li>Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>  |
| D.10.1                                   | Scope of Review  |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.10.2                                   | Information to Be Provided                                       | 1     | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, provided in Appendix C of this LTR</li> <li>Generic Logic Modules described in Section 3.2.1 of this LTR</li> <li>Programmable Logic Architecture described in Section 3.3 of this LTR.</li> </ul> |
| D.10.3                                   | Regulatory Evaluation  |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.10.4                                   | Technical Evaluation   |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.10.4.1                                 | IEEE Std 7-4.3.2, Clause 4, Safety System Design Basis           |       | <ul style="list-style-type: none"> <li>No additional criteria beyond those in IEEE Std 603-1991.</li> <li>IEEE Standard 603-1991 Compliance Matrix, Section 4, provided in Appendix B of this LTR</li> </ul>  |
| D.10.4.2                                 | IEEE Std 7-4.3.2, Clause 5, System                               |       | <ul style="list-style-type: none"> <li>No additional criteria beyond those in IEEE Std 603-1991.</li> <li>IEEE Standard 603-1991 Compliance Matrix, Section 5, provided in Appendix B of this LTR</li> </ul>  |
| D.10.4.2.1                               | IEEE Std 7-4.3.2, Clause 5.1, Single-failure criterion           |       | <ul style="list-style-type: none"> <li>No additional criteria beyond those in IEEE Std 603-1991.</li> <li>IEEE Standard 603-1991 Compliance Matrix, Section 5.1, provided in Appendix B of this LTR</li> </ul>  |
| D.10.4.2.2                               | IEEE Std 7-4.3.2, Clause 5.2, Completion of protective action    |       | <ul style="list-style-type: none"> <li>No additional criteria beyond those in IEEE Std 603-1991.</li> <li>IEEE Standard 603-1991 Compliance Matrix, Section 5.2, provided in Appendix B of this LTR</li> </ul>  |
| D.10.4.2.3                               | IEEE Std 7-4.3.2, Clause 5.3, Quality                            |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.3, provided in Appendix C of this LTR</li> <li>Reference Section 4.0 of this LTR.</li> </ul>   |

| DI&C-ISG-06 Revision 1 Compliance Matrix |  |       |  |
|--|--|-------|--|
| Section No.                              | Section Title  | Phase | NuPAC Platform Compliance <sup>1</sup>   |
| D.10.4.2.3.1                             | IEEE Std 7-4.3.2, Clause 5.3.1, Software development                 |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.3.1, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.3.2                             | IEEE Std 7-4.3.2, Clause 5.3.2, Software Tools                       |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.3.2, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.3.3                             | IEEE Std 7-4.3.2, Clause 5.3.3, Verification and Validation          |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.3.3, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.3.4                             | IEEE Std 7-4.3.2, Clause 5.3.4, Independent V&V (IV&V)               |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.3.4, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.3.5                             | IEEE Std 7-4.3.2, Clause 5.3.5, Software project risk management     |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.3.5, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.4                               | IEEE Std 7-4.3.2, Clause 5.4, Equipment qualification                |       | <ul style="list-style-type: none"> <li>Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>   |
| D.10.4.2.4.1                             | IEEE Std 7-4.3.2, Clause 5.4.1, Computer system testing              |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.4.1, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.4.2                             | IEEE Std 7-4.3.2, Clause 5.4.2, Computer system testing              |       | <ul style="list-style-type: none"> <li>Not applicable. All firmware for the NuPAC has been developed under a 10 CFR 50, Appendix B program.</li> </ul>   |
| D.10.4.2.5                               | IEEE Std 7-4.3.2, Clause 5.5, System integrity                       |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Sections 5.5.1, 5.5.2, and 5.5.3, provided in Appendix C of this LTR</li> </ul>   |
| D.10.4.2.5.1                             | IEEE Std 7-4.3.2, Clause 5.5.1, Design for computer integrity        |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.5.1, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.5.2                             | IEEE Std 7-4.3.2, Clause 5.5.2, Design for test and calibration      |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.5.2, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.5.3                             | IEEE Std 7-4.3.2, Clause 5.5.3, Fault detection and self-diagnostics |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.5.3, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.6                               | IEEE Std 7-4.3.2, Clause 5.6, Independence                           |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.6, provided in Appendix C of this LTR</li> <li>DI&amp;C-ISG-04 Compliance Matrix, provided in Appendix D of this LTR</li> </ul> |
| D.10.4.2.7                               | IEEE Std 7-4.3.2, Clause 5.7, Capability for test and calibration    |       | <ul style="list-style-type: none"> <li>No additional criteria beyond those in IEEE Std 603-1991.</li> <li>IEEE Standard 603-1991 Compliance Matrix Section 5.7. Reference Appendix B of this LTR.</li> </ul>                   |
| D.10.4.2.8                               | IEEE Std 7-4.3.2, Clause 5.8, Information Displays                   |       | <ul style="list-style-type: none"> <li>IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.8, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.9                               | IEEE Std 7-4.3.2, Clause 5.9, Control of access                      |       | <ul style="list-style-type: none"> <li>No additional criteria beyond those in IEEE Std 603-1991.</li> <li>IEEE Standard 603-1991 Compliance Matrix Section 5.9. Reference Appendix B of this LTR.</li> </ul>                   |

**DI&C-ISG-06 Revision 1 Compliance Matrix**

| Section No. | Section Title  | Phase | NuPAC Platform Compliance <sup>1</sup>  |
|-------------|--|-------|---|
| D.10.4.2.10 | IEEE Std 7-4.3.2, Clause 5.10, Repair                      |       | <ul style="list-style-type: none"> <li>• No additional criteria beyond those in IEEE Std 603-1991.</li> <li>• IEEE Standard 603-1991 Compliance Matrix Section 5.10. Reference Appendix B of this LTR.</li> </ul> |
| D.10.4.2.11 | IEEE Std 7-4.3.2, Clause 5.11, Identification              |       | <ul style="list-style-type: none"> <li>• IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.11, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.2.12 | IEEE Std 7-4.3.2, Clause 5.12, Auxiliary Features          |       | <ul style="list-style-type: none"> <li>• No additional criteria beyond those in IEEE Std 603-1991.</li> <li>• IEEE Standard 603-1991 Compliance Matrix Section 5.12. Reference Appendix B of this LTR.</li> </ul> |
| D.10.4.2.13 | IEEE Std 7-4.3.2, Clause 5.13, Multi-unit Stations         |       | <ul style="list-style-type: none"> <li>• No additional criteria beyond those in IEEE Std 603-1991.</li> <li>• IEEE Standard 603-1991 Compliance Matrix Section 5.13. Reference Appendix B of this LTR.</li> </ul> |
| D.10.4.2.14 | IEEE Std 7-4.3.2, Clause 5.14, Human Factor Considerations |       | <ul style="list-style-type: none"> <li>• No additional criteria beyond those in IEEE Std 603-1991.</li> <li>• IEEE Standard 603-1991 Compliance Matrix Section 5.14. Reference Appendix B of this LTR.</li> </ul> |
| D.10.4.2.15 | IEEE Std 7-4.3.2, Clause 5.15, Reliability Analysis        |       | <ul style="list-style-type: none"> <li>• IEEE Standard 7-4.3.2-2003 Compliance Matrix, Section 5.15, provided in Appendix C of this LTR</li> </ul>  |
| D.10.4.3    | IEEE Std 7-4.3.2, Clause 6                                 |       | <ul style="list-style-type: none"> <li>• No additional criteria beyond those in IEEE Std 603-1991.</li> <li>• IEEE Standard 603-1991 Compliance Matrix Section 6. Reference Appendix B of this LTR.</li> </ul>    |
| D.10.4.4    | IEEE Std 7-4.3.2, Clause 7                                 |       | <ul style="list-style-type: none"> <li>• No additional criteria beyond those in IEEE Std 603-1991.</li> <li>• IEEE Standard 603-1991 Compliance Matrix Section 7. Reference Appendix B of this LTR.</li> </ul>    |
| D.10.4.5    | IEEE Std 7-4.3.2, Clause 8                                 |       | <ul style="list-style-type: none"> <li>• No additional criteria beyond those in IEEE Std 603-1991.</li> <li>• IEEE Standard 603-1991 Compliance Matrix Section 8. Reference Appendix B of this LTR.</li> </ul>    |
| D.10.5      | Conclusion   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.11        | Technical Specifications                                   |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>  |
| D.11.1      | Scope of Review  |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.11.2      | Information to Be Provided                                 |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>   |
| D.11.3      | Regulatory Evaluation                                      |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>   |
| D.11.4      | Technical Evaluation                                       |       | <ul style="list-style-type: none"> <li>• Plant-specific requirement(s), not applicable to the generic NuPAC platform</li> </ul>   |
| D.11.5      | Conclusion   |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |
| D.12        | Secure Development and Operational Environment             |       | <ul style="list-style-type: none"> <li>• Summary-type requirement(s), compliance through sub-clauses, see below</li> </ul>  |
| D.12.1      | Scope of Review  |       | <ul style="list-style-type: none"> <li>• No requirements</li> </ul>   |

| DI&C-ISG-06 Revision 1 Compliance Matrix |                            |       |   |
|--|----------------------------|-------|---|
| Section No.                              | Section Title              | Phase | NuPAC Platform Compliance <sup>1</sup>  |
| D.12.2                                   | Information to Be Provided | 1     | <ul style="list-style-type: none"> <li>Generic NuPAC platform vulnerability assessment and associated methodology to apply secure development and operational environment controls summarized in Section 8.0 of this LTR</li> <li>Reference “NuPAC Vulnerability Assessment Report (VA) for Secure Development Environment (SDE),” NUPAC document number NuPAC_ED610000-062 (<b>Reference 703</b>)</li> <li>Reference “NuPAC System Security Plan,” NUPAC document number NuPAC_SSP610000-001 (<b>Reference 725</b>)</li> </ul> |
| D.12.3                                   | Regulatory Evaluation      |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.12.4                                   | Technical Evaluation       |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
| D.12.5                                   | Conclusion                 |       | <ul style="list-style-type: none"> <li>No requirements</li> </ul>   |
|  |                            | 2     | <ul style="list-style-type: none"> <li>Circuit Schematic Drawings</li> <li>Detailed system and Hardware Drawings</li> </ul>   |



No.: NuPAC\_ED610000-047-A-NP  
Rev: -  
Page: 263 of 263  
Date: 04/14/2017

---

**APPENDIX F: DELETED**  
**(INFORMATION WAS DUPLICATED FROM APPENDIX E)**