FINAL SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION FOR SPINLINE 3 PLATFORM LICENSING TOPICAL REPORT ROLLS ROYCE CIVIL NUCLEAR TAC NO. ME3600

1.0 INTRODUCTION AND BACKGROUND

By letters dated July 8, 2009, January 31, 2011, and December 18, 2012 (References 1.1, 1.2, and 1.3), Rolls-Royce submitted a licensing topical report (LTR), "SPINLINE 3 Digital Safety I&C [Instrumentation and Control] Platform" (Proprietary version Reference 1.4 and Non-proprietary version Reference 1.5). In addition, by letters dated December 23, 2009, January 8, February 2, and March 5, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession Nos. ML093570361, ML100120087, ML100330793, and ML101480946, Rolls-Royce submitted supporting documentation for U.S. Nuclear Regulatory Commission (NRC) staff evaluation of this LTR.

The NRC staff performed an acceptance review of the subject LTR and supporting documentation in accordance with the Office Nuclear Reactor Regulation's Office Instruction, LIC-500, "Processing Requests for Reviews of Topical Reports" (ADAMS Accession No. ML051800651), and found that certain supplemental information was needed to complete the acceptance review. By letter dated May 14, 2010 (Reference 2.1), the NRC requested supplemental information from Rolls-Royce and by letter dated May 28, 2010 (Reference 1.10), Rolls-Royce provided the requested supplemental information. In addition, by letter dated June 15, 2010 (Reference 1.11), Rolls-Royce submitted additional information necessary for the acceptance review of the LTR. Based on this information, by letter dated December 1, 2010, the NRC staff accepted the Rolls-Royce LTR for review (Reference 2.2).

After acceptance of the LTR, Rolls-Royce submitted supporting documents for NRC staff evaluation, including submittal letters dated December 23, 2010, January 31, February 25, March 31, June 30, July 6, and November 18, 2011, March 14, May 31, July 19, September 21, and December 21, 2012 (References 1.12, 1.28, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19, 1.20, 1.21, and 1.22). Each submittal letter contained a set of new or revised supporting documents wherein varying portions or entire documents are identified as proprietary. On November 7, 2011, July 18, 2011, and March 28, 2013, the NRC staff submitted Requests for Additional Information (RAIs) (References 2.3, 2.4, and 2.5, respectively). Rolls-Royce provided the responses to these RAIs on its letters dated December 21, 2011 (Reference 1.22), August 3, 2012 (Reference 1.23), and April 4, 2013 (Reference 1.24).

By letter dated September 15, 2011 (Reference 1.25), Rolls-Royce requested an extension for the review of its LTR due to events and problems observed during equipment qualification (EQ) testing that required modifications to the system, as well as repeat of certain EQ tests. This request caused delays in the NRC staff review and schedule.

The NRC staff conducted an audit at the Rolls-Royce facility in Grenoble, France, on June 11-15, 2012. The purpose of the audit was to inspect Rolls-Royce procedures and processes that are referenced in the LTR and audit documented products of Commercial Grade Dedication (CGD) activities. During the site visit, thread audits were performed, the hardware configuration of the SPINLINE 3 qualification test specimen was observed, and performance characteristics and functional capabilities of the platform were observed. The results of the audit are documented in the September 19, 2012, audit report (Reference 2.6).

The SPINLINE 3 Platform LTR identifies the scope of the requested platform safety evaluation (SE) (see Reference 1.4). The SE of the SPINLINE 3 platform is limited to the development and test plans, specifications and procedures to design, verification and validation, and performance of the standardized circuit boards described in the LTR, including the generic software (i.e., library of software functions, the NERVIA+ communication software, the operational system software, and software embedded in electronic boards with electronic components). The SE scope excludes the development, integration and testing of a specific system, factory acceptance test of a system, or maintenance activities to support a fielded system. The SE also excludes any evaluation of the communication between the SPINLINE 3 platform and the Local Display Unit and platform's accuracy and response time specifications, as well as other Rolls-Royce components not described in the LTR (but described in docket documents) necessary to determine whether a given configuration will satisfy plant-specific or application-specific needs.

The SPINLINE 3 platform was initially designed, qualified, and manufactured in accordance with European Nuclear Safety and Quality Standards. The SPINLINE 3 platform is based on microprocessor technology and is being evaluated for general application within safety systems of current nuclear power generating stations. As such, this SE addresses criteria that apply to digital equipment for use in nuclear power plant safety systems.

Section 2.0 of this SE identifies the applicable regulatory bases and corresponding guidance and regulatory acceptance criteria against which the NRC staff evaluated the topical report submittals. Section 3.0 of this SE provides the technical evaluation of the topical report submittals. This section also includes a description of the SPINLINE 3 platform. Section 4.0 provides the NRC staff conclusion, Section 5.0 provides limitations and conditions that apply to applicants or licensees that reference this SE for use of the SPINLINE 3 platform in a safety system of a nuclear power generating station, and Section 6.0 provides a list of references.

For clarity, this SE uses the term "manufacturer" to refer to the applicant, Rolls-Royce, which submitted the "SPINLINE 3 LTR" for its platform while "applicant" refers to an "applicant for a license" and "licensee" refers to a holder of a license.

2.0 REGULATORY EVALUATION

NUREG-0800, "Standard Review Plan 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 Standard Review Plan (SRP), sets forth a method for reviewing compliance with applicable sections of Title 10 Part 50 of the *Code of Federal Regulations* (10 CFR Part 50), "Domestic Licensing of Production and Utilization Facilities." Specifically, SRP Chapter 7, "Instrumentation and Controls," addresses the requirements for instrumentation and control (I&C) systems in nuclear power plants based on light-water reactor designs. SRP Chapter 7 and Interim Staff Guidance (ISG), which augments and supplements SRP Chapter 7, principally establish the review process for digital I&C systems that was applied in this evaluation.

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

SRP Chapter 7, Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety," identifies design criteria and regulations from 10 CFR Part 50 that are applicable to I&C systems and relevant to the general review of the suitability of a digital I&C platform for use in SR applications. Many of the review criteria of the SRP depend on the design of an assembled system for a particular application, whereas the LTR presents the elements of hardware and system software in the SPINLINE 3 platform that can be used in a variety of safety applications. Since no plant-specific application of the platform as a safety system is associated with the LTR, this SE is limited to the evaluation of compliance with the relevant regulations and guidance documents to the degree to which they can be satisfied at the platform level. In effect, fulfillment of system-level requirements can only be partially evaluated on a generic basis based on the capabilities and characteristics of the SPINLINE 3 platform.

Determination of full compliance with the applicable regulations remains subject to a plant-specific licensing review of a full system design based on the SPINLINE 3 platform. Plant-

specific action items have been established to identify criteria that should be addressed by an applicant or licensee referencing this SE (see Section 5.0, Item 1). In part this criteria is provided to facilitate an applicant's or licensee's ability to establish full compliance with the design criteria and regulations identified in SRP Chapter 7, Table 7-1, that are applicable to the applicant's or licensee's digital I&C system and that were in effect at the time of the SPINLINE 3 platform review. Regardless, the plant-specific action items identified in Section 5.0 do not obviate an applicant's or licensee's responsibility to adequately address new or changed design criteria or regulations that apply in addition to those used to perform this SE when making a voluntary change to its facility.

The following regulations are applicable to the LTR:

- 10 CFR 50.55a (a)(1), "Quality Standards" requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.
- 10 CFR 50.55a(h), "Protection and Safety Systems" incorporates the 1991 version of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," by reference, including the correction sheet dated January 30, 1995.
- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants"
  - General Design Criterion (GDC) 1, "Quality standards and records"
  - GDC 2, "Design bases for protection against natural phenomena"
  - GDC 4, "Environmental and dynamic effects design bases"
  - GDC 13, "Instrumentation and control"
  - GDC 20, "Protection system functions"
  - GDC 21, "Protection system reliability and testability"
  - GDC 22, "Protective system independence"
  - GDC 23, "Protective system failure modes"
- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"

SRP Chapter 7, Table 7.1, identifies RGs (RGs), branch technical positions (BTPs), and industry standards that contain information, recommendations, and guidance and, in general, provide an acceptable basis to implement the above requirements for both hardware and software features of safety-related (SR) digital I&C systems. Based on the scope of the SPINLINE 3 platform and the limitations of a platform-level review, the following guides and positions are determined to be relevant for consideration in this SE:

- RG 1.22, "Periodic Testing of Protection Actuation Functions," Revision 0, describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.

- RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems,” Revision 1, describes a method acceptable to the NRC staff for complying with IEEE Std. 603-1991 in regard to bypassed and inoperable status indication for nuclear power plant safety systems.
- RG 1.53, “Application of the Single-Failure Criterion to Safety Systems,” Revision 2, describes a method acceptable to the NRC staff for satisfying the NRC’s regulations as they apply to the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.
- RG 1.62, “Manual Initiation of Protective Actions,” Revision 1, describes methods acceptable to the NRC staff for complying with IEEE Std. 603-1991 in regard to the manual initiation of protective actions.
- RG 1.75, “Criteria for Independence of Electrical Safety Systems,” Revision 3, describes a method acceptable to the NRC staff for satisfying physical independence of the circuits and electrical equipment that comprise or are associated with safety systems.
- RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” Revision 4, describes a method acceptable to the NRC staff for providing instrumentation to monitor variables for accident conditions.
- RG 1.100, “Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants,” Revision 3, describes a method acceptable to the NRC staff for satisfying the seismic qualification.
- RG 1.118, “Periodic Testing of Electric Power and Protection Systems,” Revision 3, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to periodic testing of electric power and protection systems.
- RG 1.152, “Criteria for Use of Computers In Safety Systems of Nuclear Power Plants,” Revision 3, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to high functional reliability and design requirements for computers used in safety systems of nuclear power plants.
- RG 1.153, “Criteria for Safety Systems,” Revision 1, endorsed IEEE Std. 603-1991 as a method acceptable to the NRC staff for satisfying the NRC’s regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants prior to IEEE Std. 603-1991incorporation by reference into the regulations.
- RG 1.168, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 1, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to the verification and validation of safety system software.
- RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” September 1997, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to the configuration management of safety system software.

- RG 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” September 1997, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to test documentation of safety system software.
- RG 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” September 1997, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to the unit testing of safety system software.
- RG 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” September 1997, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to preparation of software requirement specifications for safety system software.
- RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” September 1997, describes a method acceptable to the NRC staff for complying with the NRC’s regulations as they apply to the development processes for safety system software.
- RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Revision 1, describes a method acceptable to the NRC staff for design, installation, and testing practices to address the effects of electromagnetic and radio-frequency interference (EMI/RFI) and power surges on SR I&C systems.
- RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” describes a method acceptable to the NRC staff for satisfying the environmental qualification of SR computer-based I&C systems for service in mild environments at nuclear power plants.
- DI&C-ISG-02, “Task Working Group #2: Diversity and Defense-in-Depth Issues, Interim Staff Guidance,” Revision 2, describes methods acceptable to the NRC staff for implementing diversity and defense-in-depth (D3) in digital I&C system designs.
- DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc),” Revision 1, describes methods acceptable to the NRC staff to prevent adverse interactions among safety divisions and between SR equipment and equipment that is not SR.

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

- Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603”
- Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2”
- BTP 7-11, “Guidance on Application and Qualification of Isolation Devices”

- BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”
- BTP 7-17, “Guidance on Self-test and Surveillance Test Provisions”
- BTP 7-18, “Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems”
- BTP 7-19, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems”
- BTP 7-21, “Guidance on Digital Computer Real-Time Performance”

Since the SPINLINE 3 platform is an existing commercial off-the-shelf (COTS) digital I&C platform, certain industry guidelines that address dedication and qualification processes are applicable. The NRC staff has reviewed and accepted the following industry guidance documents based on conditions established in SE reports.

- Electric Power Research Institute (EPRI) Topical Report (TR)-102323, “Guidelines for Electromagnetic Interference Testing in Power Plants,” as accepted by the NRC SE dated April 30, 1996
- EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” as accepted by the NRC SE dated April 1997
- EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available programmable logic controller (PLC) for Safety-Related Applications in Nuclear Power Plants,” as accepted by the NRC SE dated July 30, 1998

It should be noted that industry standards, documents, and reports use the word “requirements” to denote provisions that must be implemented to ensure compliance with the corresponding document. Additionally, these standards, documents, and reports provide guidance or recommendations that need not be adopted by the user to ensure compliance with the corresponding document, and the optional items are not designated as “requirements.” The word “requirement” is used throughout the I&C discipline. However, licensee or vendor documentation of conformance to the “requirements” provided in industry standards, documents, and reports referenced in this SE only constitutes conformance with NRC regulatory requirements insofar as endorsed by the NRC. Furthermore, use of the word “requirements” in these documents does not indicate that the “requirements” are NRC regulatory requirements.

3.0 TECHNICAL EVALUATION

The following subsections identify and describe the SPINLINE 3 platform’s components and evaluate these components and its development against the regulatory evaluation criteria identified in Section 2.0.

3.1 System Background

The SPINLINE 3 platform is the third generation of the digital safety I&C platform developed by Data System and Solutions (now Rolls-Royce). This platform resulted from the evolution of Rolls-Royce software-based I&C system developed for the Électricité de France (EdF)'s fleet of P4 and N4 Pressurized Water Reactors (PWRs). Specifically, Rolls-Royce performed the MC3 project as a Research and Development (R&D) project with the purpose of using the technology implemented for the safety I&C systems on the EdF N4 1450 megawatt PWR in order to produce a modular digital platform, later called the SPINLINE 3 Platform.

The SPINLINE 3 platform's components were designed, implemented, and qualified in compliance with European nuclear standards, including the International Atomic Energy Agency 50-C-QA, "Quality Assurance for Safety in Nuclear Plants", and the French national code RCC-E, "Règles de Construction et de Conception des Matériels Electriques." RCC-E prescribes requirements for qualification of electrical equipment used in French-built nuclear power plants. Further, the life cycle processes for the SPINLINE 3 platform software were established according to the guidance provided in International Electrotechnical Commission (IEC) 880-1986, "Software for Computers in the Safety Systems of Nuclear Power Stations," and were documented in dedicated software plans (see Section 3.5 of this SE).

Rolls-Royce LTR (Reference 1.4) and Rolls-Royce "EPRI TR-106439 Critical Characteristics and EPRI TR-107330 Compliance Matrix Assessment Report" (Reference 1.70) provide a description on the evolution of the SPINLINE 3 platform, which is also described in Section 3.5 of this SE. The nuclear Quality Assurance (QA) program employed at I&C France originally was developed based on European nuclear QA standards. This original QA program has been revised to provide full compliance with 10 CFR Part 50 Appendix B. Rolls-Royce activities now are performed under the 10 CFR Part 50 Appendix B-compliant quality program documented in the "Rolls-Royce Civil Nuclear SAS Quality Manual" (Reference 1.26). Furthermore, activities to develop I&C systems for US nuclear Power Plants will be performed under the 10 CFR Part 50 Appendix B-compliant quality program documented in the "Instrumentation & Controls U.S. Quality Manual" (Reference 1.27). Because the SPINLINE 3 platform was not originally developed in accordance with currently endorsed NRC standards and regulations, Rolls-Royce dedicated the SPINLINE 3 platform to be qualified and accepted for use in safety related applications for U.S. Nuclear Power Plants (NPP). Section 3.5 of this SE describes the CGD of the SPINLINE 3 platform.

3.2 System Description

The SPINLINE 3 platform is a modular system that can be configured in different sizes according to the application. The SPINLINE 3 platform supports field input and output types including discrete inputs, relay contacts, analog current, analog voltage, resistance temperature detectors, and pulse signals. Due to the flexibility of the SPINLINE 3 platform design, Rolls-Royce can implement a variety of system architectures by combining the electronic boards. The numbers of components in a system are defined by the application specific design requirements

and by the number of slots available in the Parallel Asynchronous Bus (BAP acronym in French).

The SPINLINE 3 platform consists of components, such as, interface boards, daughter or main boards, power supply modules, communication modules, operator interfaces, and a chassis with a BAP backaplane board. Except for the central processing unit (CPU) board, each main board requires an interface board. The main board performs electronic functions. The interface board provides the connectors from sensor signals or to actuator controls, and from there to the main board. Note that the Resistance Temperature Detector (RTD) board uses a conditioning board instead of a main board. These boards are identified in the Rolls-Royce Master Configuration List (MCL) (Reference 1.29) and Table 3-1. The MCL also lists all components and documents associated with the SPINLINE 3 platform described in the LTR.

Table 3-1: SPINLINE 3 Platform Electronic Boards

Component ID	Name	Type	Part Number (Reference 1.29)
8PT100	RTD board	Conditioning	5 100 436 479
I.8PT100 Interface board		Interface	5 100 436 543
16E.ANA ISO	Analog input board	Main	5 100 436 656
I.16EANA Interface board		Interface	5 100 435 925
32ETOR TI SR	Digital isolated input board	Main	5 100 436 670
I.32ETOR TI interface board		Interface	5 100 435 567
ICTO	Calibrated pulse acquisition board	Main	5 100 436 662
I.ICTO interface board		Interface	5 100 435 557
32ACT	Actuator drive board (Discrete output)	Main	5 100 436 357
I.32ACT interface board		Interface	5 100 436 433
6SANA ISO	Analog output board	Main	5 100 436 664
I.6SANA interface board		Interface	5 100 435 547
UC25 N+	CPU board	Main	5 100 436 445
NERVIA+ board	NERVIA+ communication board	Main	5 100 436 197
I.NERVIA+ interface board		Interface	CAR0000065
ALIM 48V/5V-24V	Power supply board	Main	5 100 436 403
I.ALIM 48 interface board		Interface	5 100 435 486

In addition to the boards listed above, the SPINLINE 3 platform includes other components that support the functions performed by these boards. The most relevant components are listed in Table 3-2. Note that this list is not inclusive, and the MCL identifies all components that constitute the SPINLINE 3 platform.

Table 3-2: SPINLINE 3 Platform Components

Component ID	Name	Part Number (Reference 1.29)
120 VAC/48 VDC power supply chassis	Power supply	CNC0000031
48V DC/48-24 VDC power supply chassis	Power supply	CNCO000030
MV16	Actuation voting module	5100436646
32ETOR	Input terminal block	BOR0000009
8PT100 terminal block	Input terminal block	6 618 814
8SRELAY1	Output relays terminal block	5 100 436 731
8SRELAY2	Output relays terminal block	5 100 436 736
PCI NERVIA+ board	Interface board	CAR0000064
Hubs and twisted-pair to fiber optic (TP/FL) converters assembly	-	CAI0000002

The drawing provided in Reference 1.55 shows how the SPINLINE 3 platform's components were arranged in the cabinet for EQ testing.

The LTR and References 1.30, 1.22, and 1.23 identify the hardware design constraints for the SPINLINE 3 platform. In particular,

- The 21-slot BAP backplane board can host up to 12 digital, analog, and discrete input/output (I/O) boards
- Only one UC25 N+ CPU board can be installed in a BAP backplane board.
- The UC25 N+ CPU board uses two slots with or without the daughter board.
- One NERVIA+ daughter board can be mounted on the UC25 N+ CPU board
- One power supply module per BAP is used and occupies two slots.
- The RTD I.8PT100 Interface board uses two slots.
- Up to 6 chassis could be installed in a cabinet if only mechanical sizing was the restriction

Figure 3-1 shows the front and rear view of the SPINLINE 3 platform. A description of the SPINLINE 3 platform hardware is provided in the following sections.

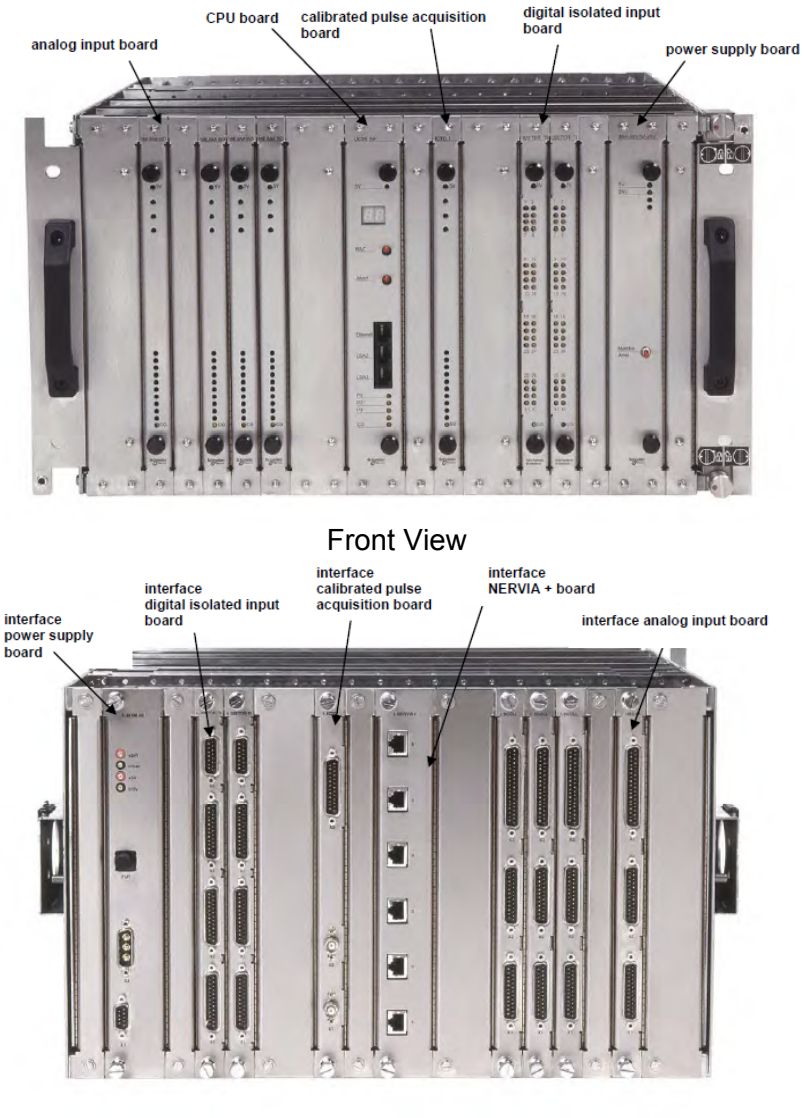

Figure 3-1: SPINLINE 3 Platform Chassis

3.2.1 SPINLINE 3 Platform Hardware

3.2.1.1 Chassis

The chassis for the SPINLINE 3 platform is a rack-mounted 19 inches 6U[1] assembly that houses the SPINLINE 3 platform's components. The chassis includes:

- A metallic frame consisting of riveted and bolted parts designed for EMI/RFI protection.
- Mounting rails for easy insertion and retrieval during maintenance.
- One or two printed circuit BAP backplanes with board connectors. These connectors are equipped with keys matching its associated board types.

The chassis hosts the main electronic boards on the front and the interface boards in the rear side. The BAP backplane fits in the middle of the chassis, in between the main boards and the interface boards. The main boards are connected to the BAP backplane on the front side, whereas the interface boards are connected to main boards through the BAP backplane on the rear side. The BAP backplane also supports the BAP bus.

The BAP backplane board is available in several sizes with 21, 11, and 10 slots. This allows for various arrangements of hardware components. For example, a 21-slot chassis can include the 10 and 11 slot BAPs, each with its own UC25 N+ CPU board and set of input, output, and communication boards.

3.2.1.2 Backplane Bus

The BAP backplane is the mechanical support to the BAP bus copper circuitry for power distribution and the parallel communication bus. The BAP backplane is placed in the middle of the chassis, between the main electronic boards and the interface boards. The main electronic boards are connected on the front side, whereas the interface boards are connected on the rear side.

The BAP bus is a passive bus that provides connection between the CPU and the I/O boards. Data is exchanged between the CPU and the I/O boards through a physical copper circuit made of parallel lines located on the BAP backplane. The Operating System Software (OSS) controls the BAP bus. The functions of the BAP bus are:

- Centralization of data acquisition performed by input boards.
- Transmit output signals from the CPU board to the output actuation boards.
- Supply power from the power supply board to the CPU board and to the I/O boards.
- Transmit status of the I/O boards to the CPU.

[1] 6U – this term refers to the size of the rack mount (for additional information: http://en.wikipedia.org/wiki/Rack_unit)

Section 3.2.3.1 describes data transmission through the BAP bus. The BAP backplane also performs the following functions:

- Connect main electronic boards to their associated interface boards.
- Data transfer from main electronic boards to their associated interface boards.

The BAP backplane has the following type of connectors:

- XF1 – connects the main boards to the BAP bus.
- XF2 – connects the main boards with their respective interface board. These are only pass-through connectors between the rear side and the front side for the external signals. These connectors are not used for the BAP bus.

The BAP backplane supplies power to the CPU board and to the I/O boards through the XF1 and XF2 connectors. In addition, specific pins in each XF2 connector are used to assign the address to each functional electronic board (front side). This address configuration is made through hardwired straps of 0 V or 5 V to these pins. The addresses are predefined for each given slot. The XF2 connectors are provided with keyed mechanisms to restrict the location of the given boards to their assigned and restricted slots during the design phase. References 1.22 and 1.23 provide additional details about these connectors.

3.2.1.3 Main Boards

The SPINLINE 3 platform includes the electronic boards listed in Table 3-1.
The LTR and Reference 1.30 group certain electronic boards depending on whether they include programmable components (e.g., Field Programmable Gate Array (FPGA)), firmware, and/or require software initialization. In Reference 1.24, Rolls-Royce explained this terminology and the comparison between the naming convention used in the LTR and in Reference 1.30. In summary, the following boards include programmable components:

- Microprocessor-based peripherals (also intelligent peripherals) – NERVIA+ and ICTO boards.
- Non-microprocessor-based peripherals (also non-intelligent peripherals) – 6SANA, 32 ACT, and 32ETOR.
- Configurable non-microprocessor-based peripherals (also configurable non-intelligent peripherals) – 16E.ANA ISO.

This classification is important for the discussion of initialization functions performed by the operating system. This information is provided in Section 3.4.2.1.1 of this SE.

The following subsections describe the main boards for the SPINLINE 3 platform. Note that SPINLINE 3 platform can be configured to use additional boards, such as UC16COM CPU

board (Reference 1.30). However, the NRC staff only evaluated the electronic boards listed in Table 3-1. Therefore, if a SPINLINE 3 platform board not evaluated in this SE is used for an application specific project, the configuration and use of this board should be separately evaluated (see Section 5.2, Item 2).

3.2.1.3.1 UC25 N+ Central Processing Unit

The central processing function is implemented in the UC25 N+ CPU board. This board uses microprocessors for processing and controlling unit functions (e.g., OSS and application software) and communication (BAP bus and the NERVIA network). It also has onboard memory devices for code and data in order to run software safety functions. One and only one UC25 N+ CPU board can be installed on a BAP bus. This board is installed with a NERVIA+ daughter board and the I.NERVIA+ interface board, if network communications are necessary for the application-specific design.

The LTR, Section 4.3.4.7, and References 1.22, 1.34, and 1.33 provide detailed functional descriptions for the components of the UC25 N+ CPU board. In particular, these references describe the following CPU components:

- FLASH EEPROM
  The Fast Programming (FLASH) Electrically Erasable Programmable ROM (EEPROM) contains the executable code and all configurable parameters required for the OSS and application program.

- Data Random Access Memory (RAM)
  The system uses the Data RAM to store and manage the variable calculated and used by the application software.
- Code RAM
  The Code RAM stores the code to be executed permanently by the Unit, including both the OSS and application software and the parameter tables necessary to activate the code in the OSS. This information is copied from the FLASH EEPROM to the Code RAM when the board is powered on, and after correct completion of the system self-test sequence.

- EEPROM
  The EEPROM is used to maintain values of configurable parameters to be accessed by the application software.

- Microprocessor 68040
  Hosts and runs the OSS and application software. The microprocessor includes a built-in math coprocessor and a memory management unit to access the Data RAM. This microprocessor is supported by a 68360 communication coprocessor.

- BAP bus interface and 68150 bus adaptor
  The 680150 microprocessor is used to control the BAP bus.

Section 3.4.2 of this SE describes the OSS.

The UC25 N+ CPU board manages the following communication:

- NERVIA+ Network
- BAP Bus
- Asynchronous Serial Links (RJ45 connectors)

Section 3.2.3 of this SE describes SPINLINE 3 System Communication.

The front panel of the UC25 N+ CPU board includes the following devices:

- RJ45 connectors for serial communication
- Liquid crystal display (LCD) to display error codes
- Hardware watchdog light emitting diode (LED) to display operation of the daughter board processors
- UC25 N+ watchdog LED
- RESET button
- ABORT button

3.2.1.3.2 Temperature Conditioning Module

The temperature conditioning (RTD) board performs amplification and shaping of the platinum temperature sensor signal. This board consists of the 8PT100 board, I.8PT100 interface board, and 8PT100 input terminal block. The 8PT100 conditioning board is installed in a temperature conditioning dedicated chassis with a 21, 11, or 10-slot BAP backplane, with a power supply board. The BAP backplane supplies power to the board and its interface.

The 8PT100 input terminal block defines the configuration of the PT100 sensor to the 8PT100 conditioning board. This module can process up to eight PT100 platinum temperature sensors, converting changes in resistance to either voltage (between 0 and 10 V) or current levels (between 4 and 20 mA). If the signal is converted to voltage, it is sent to the 16EANA for digital processing. If the signal is converted to current, it can be used by a temperature indicator.

This board does not connect to the UC25 N+ CPU board through the BAP bus.
Section 3.2.3.1.2 describes how data is acquired and exchanged between the UC25 N+ board and the RTD board.

The LTR, Section 4.3.4.1, and References 1.22 and 1.35 provide detailed description of the 8PT100 board.

3.2.1.3.3 Signal Input Module

3.2.1.3.3.1 Discrete Input

The discrete acquisition function is accomplished using the 32ETOR TI SR board, I.32ETOR TI interface board, and the 32ETOR terminal block. This board can acquire up to 32 dry contact signals, organized in 4 isolated groups of 8 inputs. For each group, the power supply for the sensors is provided from either the 48 VDC/48-24 VDC power supply chassis (in 24 VDC or in 48 VDC form) or the field power supply (in 24, 48 or 125 VDC). The 32ETOR TI SR board can also be used to acquire internal discrete signals of the SPINLINE 3 platform for monitoring and status (e.g., cooling fan operation).

The 32ETOR TI SR discrete acquisition board consists of the 32ETOR TI SR board and the I.32ETOR TI interface board. This board is installed in the chassis and connects to the BAP bus, which forwards discrete data to the UC25 N+ CPU board. Section 3.2.3.1 of this SE describes how data is transferred.

The 32ETOR terminal block is installed outside the chassis. The 32ETOR terminal block provides the interface between the field sensors and the 32ETOR TI SR discrete acquisition board.

The I.32ETOR interface board also provides access to the inputs for the Automated Testing Units (ATU) to perform periodic tests. Note that the LTR did not describe these periodic tests. Furthermore the SPINLINE 3 platform described in the LTR did not include an ATU because this will depend on the application specific system requirements. Therefore, the NRC staff did not evaluate the test support function provided by the 32ETOR terminal block. The use of this function is a plant-specific application (see Section 5.2, Item 2).

The 32ETOR TI SR board includes a complex programmable logic device (CPLD), which manages and provides the interface between the four input groups. The CPLD also provides status of the input groups to the BAP bus. Section 3.4.3 of this SE describes the development process followed for the logic embedded in this CPLD.

The LTR, Section 4.3.4.3, and References 1.22, 1.37, and 1.36 provide detailed descriptions of the 32ETOR TI SR discrete acquisition board and 32ETOR terminal block.

3.2.1.3.3.2 Analog Input

The analog input module performs the analog to digital conversion and the isolation of 16 analog inputs. The analog input acquisition function is accomplished using the 16E.ANA ISO, SPINLINE 3 terminal blocks, and I.16E.ANA interface board. This module can acquire up to 16 current or voltage analog signals and performs the analog-to-digital conversion. The digital conversion is performed by the FPGA included in the 16E.ANA ISO board. The FPGA

also performs board configuration, reading data, controlling data acquisition, communicating with BAP bus, and board self-testing. Section 3.4.3 of this SE describes the development process followed for FPGA embedded in electronic boards.

In Reference 1.22, Rolls-Royce explained that any analog input can be configured independently with its own acquisition range, and that the inputs are electrically isolated in groups of two. Specifically, the board provides the following possibilities:

- Input voltage measuring range: -10/+10 V
- Input voltage measuring range: -1/+1 V
- Input current measuring range: -20/+20 mA

The SPINLINE 3 terminal blocks used with the 16E.ANA ISO board are installed outside the chassis. The 16E.ANA ISO board is installed in the chassis and connects to the front of the BAP bus. The I.16E.ANA interface board is also installed in the chassis and connects to the back. The I.16EANA interface board provides electromagnetic compatibility (EMC) filtering for all analog inputs, connections for periodic testing, and checks the presence of analog input cables on its connectors.

The 8PT100 RTD conditioning board uses the 16E.ANA ISO board to perform the acquisition of the voltage signals originating from the 8PT100 RTD conditioning board. These signals are acquired in separate isolated groups to maintain isolation provided by the 8PT100 boards.

The LTR, Section 4.3.4.3, and References 1.22 and 1.38, and 1.36 provide detailed descriptions of the 16E.ANA ISO Board.

3.2.1.3.3.3 Pulse Input Board

The pulse input board is used for measuring count rate, which is used in the source range conditioning channel. This board acquires pulses with a count rate ranging from 1 count per second (cps) up to 6.5×10^6 cps. The ICTO boards acquire two pulse signals, the number of pulses and the duration of the counting time. This data is sent to the UC25 N+ CPU board to perform the count rate calculation. This count rate is expressed as a number of counts per second and so the processing unit must have both “TIME” and “COUNT” data. The range of operation and accuracy of the board will be defined in accordance with the operation of the source range conditioning for a plant-specific application. Configuration of this board is a plant-specific application (see Section 5.2, Item 2).

This module consists of the ICTO board and the I.ICTO interface board. The I.ICTO interface board provides EMC filtering for the pulse inputs. This interface board is installed on the back of the BAP bus.

The ICTO board communicates with the UC25 N+ CPU board via the BAP bus. The ICTO board includes an 8031 microcontroller for managing and checking counting time and number of pulses and for communication with the UC25 N+ CPU board. Section 3.4.3 of this SE describes the development process followed for the 8031 microcontroller embedded in electronic boards.

The LTR, Section 4.3.4.4, and References 1.22, 1.23, and 1.39 provide detailed description of the ICTO board.

3.2.1.3.4 Signal Output Module

3.2.1.3.4.1 Discrete Output

The discrete output module provides isolated on/off outputs that can be used to control low level relays. This module consists of a 32ACT board and I.32ACT interface board, MV16 Voting Module, and 8SRELAY relay terminal blocks. The MV16 Voting Module is not necessary for the board to perform its output functions. The design of a specific application will establish if the function of the Voting Module is necessary.

The relays are in turn connected to power actuators. The 32ACT board can manage up to 32 ON-OFF outputs resulting from commands generated in the CPU, which are transmitted via the BAP bus and an FPGA on the 32ACT board. The 32 outputs are divided in 4 groups of 8 isolated outputs.

The SPINLINE 3 platform does not include solid-state discrete output devices. Therefore, the output function is accomplished by relays with outputs designed for 125 VDC, 48 VDC, 24 VDC, and 120VAC.

The 32ACT board includes an FPGA to configure the output groups and transmit command orders to each output. It also provides the interface between the BAP bus and the 32 outputs, manages the logic for the 32 output commands, and ensures surveillance of the outputs, using a short impulse test and board self-tests. Section 3.4.3 of this SE describes the development process followed for FPGA embedded in electronic boards.

The 32ACT board's surveillance function of its output can be sent to the CPU to confirm that the state of the output is consistent with the received command. Rolls-Royce can program a default position for each group of 16 outputs when an error is detected during self-tests. This configuration will depend on the safety relevance of the outputs, and thus it depends on the system requirements specified by the licensee. The NRC staff did not evaluate this capability. Therefore the licensee should confirm this function is properly configured and tested for a project specific application. The use of this function is a plant-specific action (see Section 5.2, Item 2).

The I.32ACT interface board forwards up to 32 ON-OFF outputs from the chassis BAP to its front panel connectors. It also performs EMC filtering, voltage surge suppressors to ensure that each output on the 32ACT board is independently protected against external interference, and provides external power supplies for digital outputs. The 32ACT board is installed in the chassis and connects to the front of the BAP bus. The 32ACT interface board is installed on the back of the BAP bus.

Rolls-Royce provided a detailed description on the operation of the 32ACT board in the LTR, Section 4.3.4.5 and References 1.22 and 1.40.

All ON-OFF outputs from the 32ACT board are isolated from each other and are directly connected to the MV16 voting module. The MV16 voting module can then be used to perform an individual action resulting from the combination of the discrete outputs from 32ACT in a defined voting configuration that will be defined in a plant-specific application. The MV16 can perform different voting schemes, but only one type can be configured and implemented at a time for a dedicated module. The MV16 can manage either 8 or 16 outputs according to the voting function implemented. Note the MV16 module does not perform the division-level voting actions, such as two-out-of-four voting; the division-level voting actions are performed in the application software. The voting scheme will be defined for a plant-specific application. The following voting schemes are possible:

- 1-out-of-1 (16 outputs)
- 2-out-of-2 (16 outputs)
- 2 x 2-out-of-2 (16 outputs)
- 1-out-of-2 (16 outputs)
- 2 x 1-out-of-2 (16 outputs)
- 2-out-of-3 (8 outputs)

The MV16 includes a feature for inhibition of the control signal to the output relays. This information was not provided in the LTR. Therefore, the NRC staff did not evaluate this feature. The use of this feature is a plant-specific application (see Section 5.2, Item 2).

Rolls-Royce provided a detailed description on the operation of the MV16 board in the LTR, Section 4.3.4.5, and Reference 1.41.

The MV16 outputs drive the 8SRELAY terminal blocks through two cables carrying eight signals each. The 8SRELAY terminal blocks are located outside of the chassis. There are two types of 8SRELAY terminal blocks: Type 1 and Type 2. The relay characteristics (e.g., maximum switch current) define each relay type. Section 4.3.4.5 of the LTR defines these relay characteristics. The licensee should confirm that the specified relay type is properly selected and tested for a plant specific application (see Section 5.2, Item 2). Even though Rolls-Royce uses the 8SRELAY as part of the output module, the 8SRELAY terminal blocks could also be used to receive commands from a manual switch, which could be actuated by the operator in the control

room. The NRC staff did not evaluate the use of manual actuation. If this function is included in a project specific application, the licensee should evaluate it. The use of this function is a plant-specific application (see Section 5.2, Item 2).

Rolls-Royce provided detailed descriptions on the operation of the 8SRELAY terminal blocks in the LTR, Section 4.3.4.5 and Reference 1.42.

3.2.1.3.4.2 Analog Output

The 6SANA ISO board performs the digital to analog conversion and the isolation of up to six analog outputs. The term ISO stands for isolated board. This board provides the following outputs depending on the command received from the UC25 N+ CPU:

- Five outputs, configurable to current (4 to 20 mA) or voltage (0 to 10 V)
- One output, only configurable to voltage (0 to 10 V or -10 to +10)

This module consists of the 6SANA ISO boards, I.6SANA relevant interface board, and SPINLINE 3 terminal blocks. The I.6SANA board performs the segregation function between cables, and voltage configuration of channel 6 (only configurable to voltage). The I.6SANA interface board performs EMC filtering of the 6SANA ISO analog outputs. The I.6SANA board also provides recorder outputs for each of the six channels, and testing points available to the maintenance operator.

The 6SANA ISO board is installed in the chassis and connects to the front of the BAP bus, the interface board is installed on the back of the BAP bus, and the terminal blocks are located outside of the chassis.

Rolls-Royce provided detailed description on the operation of the 86SANA ISO board in the LTR, Section 4.3.4.6 and References 1.22 and 1.43.

3.2.1.3.5 NERVIA+ Communication Board

The NERVIA+ board implements the NERVIA digital communication network. This network was developed based on the Open System Interconnection model developed by the International Standards Organization (see LTR, Section 4.5.1). Section 3.2.3.2 of this SE describes NERVIA digital communication. This section describes the hardware components used in the communication board.

The NERVIA network requires the NERVIA+ daughter board and I.NERVIA+ interface board. The NERVIA+ board is mounted directly onto the UC25 N+ processor board. This board uses an MPC860 communication microprocessor, a CPLD, and a dual-port memory (DPM). The NERVIA+ board has no access to the BAP bus. Data from the UC25 N+ CPU is transferred via the DPM. The NERVIA+ board components are:

- MPC860 communication microcontroller
  The MPC860 executes the NERVIA+ executable code stored on a flash memory device for data processing, running the NERVIA+ protocol, and performing self-tests. The MPC860 can manage up to two NERVIA networks. The board can include up to 3 MPC860 processors, and thus be able to manage up to six NERVIA networks. The NERVIA+ board performs power conversion from 5 VDC provided by the UC25 N+ to 3.3 VDC for the MPC860 communication microprocessors, using a linear voltage regulator.

- Dual Port Memory
  The DPM on the NERVIA+ board enables data exchange between the UC25 N+ microprocessor and the NERVIA+ board's MPC860 microprocessor. Both the UC25 N+ and the NERVIA+ boards read data from and write data to the DPM.

- Flash memory
  The flash memory contains data transcribed when the RAM memory is initialized.

- RAM
  The RAM contains the program (constants) and associated data (variables and constants). These units are decoded by means of decoding signals integrated in the MPC860 processor.

- CPLD
  The CPLD has two functions in the NERVIA+ board, one during manufacturing and one during operation. During manufacturing, the CPLD allows write and read operations in the Flash memory via a JTAG link. During operation the CPLD arbitrates access to the DPM on the NERVIA+ board to preclude errors associated with simultaneous reading and writing to a specific memory location.

Section 3.4.3 of this SE describes the process followed for developing the CPLD and MPC860 embedded in the NERVIA+ board.

The I.NERVIA+ interface board is required to support each NERVIA+ board. The I.NERVIA+ interface board performs the function of network signal transceiver, which is used for transmitting and receiving data on the Ethernet network. The NERVIA+ board can have up to three transceivers, dictated by the number of MPC860 in the NERVIA+ board. Only two ports are used per transceiver on the NERVIA+ board. In addition, the I.NERVIA+ interface board is fitted with six RJ45 connectors and can support up to six NERVIA networks. This allows the UC25 N+ processor board to manage up to six NERVIA networks.

The NERVIA+ board is mounted with the UC25 N+ processor board and the I.NERVIA+ interface board is mounted on the back of the BAP slot occupied by the associated UC25 N+ processor board.

The NERVIA network uses two types of media:

- Copper cable inside cabinets: Shielded Foil Twisted Pair (SFTP), Category 5 Class D (IEEE Std. 802.3i-1990); and
- Optical fiber 62.5/125 (10BaseFL) or copper cable between cabinets. This allows for electrical isolation between equipment of different safety classes and between redundant equipment within separate divisions.

Rolls-Royce provided detailed descriptions on the operation of the NERVIA network hardware components in Sections 4.3.4.8 and 4.5.3 of the LTR, and References 1.22 and 1.44.

3.2.1.4 Power Supply

The power supply for the SPINLINE 3 platform consists of the following components:

- 120 VAC/48 VDC power supply chassis
- ALIM 48V/5V-24V power supply board in the chassis
- 48 VDC/48-24 VDC power supply chassis

The configuration of the power supply for a SPINLINE 3 platform-based system will depend on the configuration for a plant-specific application. In particular, only one ALIM 48V/5V-24V power supply board can be installed in a chassis.

3.2.1.4.1 120 VAC/48 VDC Power Supply Chassis

The 120 VAC/48 VDC power supply chassis is the first stage of the power conversion chain. It converts external power levels to power levels needed for the SPINLINE 3 platform's components. Two redundant power supplies in a separate chassis are normally mounted with the equipment cabinet. This chassis converts external power levels into ranges require by the SPINLINE 3 components (e.g., chassis, hubs, and cooling fans). This chassis includes the following converters:

- Each converter performs the conversion from 120 VAC to 24 VDC
- Each converter has two 24 VDC voltage outputs
- The two 24 VDC outputs are connected in series to provide 48 VDC.

The power supply chassis has several slots that will be used according to the cabinet internal power requirements, which will be defined in the system requirements as part of the plant-specific application.

3.2.1.4.2 48 VDC/48-24 VDC Power Supply Chassis

The 48 VDC/48-24 VDC power supply chassis is the second stage of the power conversion chain. It converts internal 48 VDC into isolated 24 VDC and 48 VDC for internal use and for loop power supplies. The 48 VDC/48-24 VDC power-supply (PS) chassis is based on two kinds of converters:

- converter with 2 connectors – 24 V/96W
- converter with 4 connectors – 24 V/48W

The converters can be connected in series to provide 48 VDC if needed. The type of converters used is a plant-specific application.

The 48 VDC/48-24 VDC PS chassis implements the following functions:

- Protection of the power supply (e.g., short-circuits)
- Filter power supply to sensors and for external use. For cabinet internal use, no filter is implemented.
- Provide a “correct operation” signal for all converters for diagnostic purposes.

After power is converted to 48 VDC, power is auctioneered to the 48 VDC bus to feed the ALIM 48V/5V-24V. The converters can also be connected in series. The configuration of the 48 VDC/48-24 VDC PS chassis is a plant-specific application.

3.2.1.4.3 ALIM 48V/5V-24V Power Supply Board

This board and its associated I.ALIM 48 interface board are mounted in the chassis. This board generates two regulated power supplies (5 VDC and 24 VDC) to the rack via the BAP backplane. The ALIM 48V/5V-24V board uses two hybrid converters to perform this function: one for the 5 V power supply and one for the 24 V power supply.

The ALIM 48V/5V-24V also performs the following functions:

- Monitor the 5 V and 24 V voltages and provide information on the values of the voltage outputs to the equipment in which the board is installed.
- Remote regulation input for each power supply in case of voltage drop for boards installed far away from receiving equipment.
- Indication of 5 V and 24 V power supply voltages status. The 5 V power supply monitoring system gives the command for a contact to open when the 5 V supply voltage value falls below 4.2 V, and the 24 V power supply monitoring system gives the command for a contact to open when the voltage value falls below 16.5 V. Also, the 5 V and 24 V power supplies are shut off when the On/Off input on each converter is below 0.65 V.

The ALIM 48V/5V-24V power supply board is implemented with the I-ALIM.48 power supply interface board. The ALIM 48V/5-24V is installed in the chassis and connects to the front of the BAP backplane. The I.ALIM.48 interface board is installed on the back of the BAP backplane. The I.ALIM 48 interface board provides EMC protection on the external 48 VDC power supply before it is sent to the ALIM 48V/5V-24V board. The I.ALIM 48 interface board also provides points for testing the 5 V and 24 V power supplies produced by the board. Reference 1.45 provides detailed information on the functioning of this board.

3.2.1.5 Operator Displays

The SPINLINE 3 system can be connected to the following operator displays:

- Local Display Unit (LDU)
- Operator Panel
- Automated Testing Unit (ATU)
- Monitoring and Maintenance Unit (MMU)

Rolls-Royce stated in the LTR that operator displays were not in the scope of the evaluation of the generic SPINLINE 3 platform because configuration of the operator displays will be defined for each plant-specific application. Therefore, the NRC staff did not evaluate the design, function, and operation of the operator displays listed above. The following sections only provide a brief description of the operator displays that can be used with the SPINLINE 3 platform. The licensee should evaluate what displays are used in a plant-specific application. Further, if an operator display is supplied for a plant-specific application, the licensee should evaluate its configuration and operation, as well as confirm that use of the operator display meets the guidance described in ISG-04 for communication between safety related and non-safety related equipment (see Section 5.2, items 7 and 8).

3.2.1.5.1 Local Display Unit

The LDU is a non-1E maintenance device, implemented on a dedicated laptop. The LDU is connected to the front panel of the CPU when performing maintenance related activities. For example, the LDU allows the operator to monitor and modify configurable parameters (e.g., setpoints). The LDU is not permanently connected to the system. Before the LDU is connected, the operator disables the division or part of the division to which the processing unit belongs.

The LDU is connected to the SPINLINE 3 platform via the RJ45 connectors (asynchronous link) in front of the UC25 N+ CPU board. The OSS in the CPU manages the data exchange with the LDU. Reference 1.30 provides a detailed description of the functions used by the OSS to communicate with the LDU.

Rolls-Royce installed an LDU in the qualification test specimen (QTS), which was used during EQ. But as mentioned before, the LDU was not part of the scope, and thus, the NRC staff did not evaluate capabilities and operation of the LDU.

LTR Section 4.6.9 and References 1.22 and 1.23 provide additional information about the LDU.

3.2.1.5.2 Operator Panel

The operator panel is the Human System Interface for the SPINLINE 3 platform to perform periodic testing, monitoring, and maintenance activities. The Operator Panel is a 1E device. The operator panel is used by the operators to perform periodic testing and local maintenance activities. Configuration of the Operator Panel depends on the application intended for the SPINLINE 3 platform.

Rolls-Royce configured the Operator Panel in the QTS to support EQ testing. Reference 1.22 describes the configuration and functions used during EQ testing. In References 1.22 and 1.23, Rolls-Royce explained that these functions were included in the QTS to only show that these functions would not adversely affect operation of the equipment during EQ testing.

References 1.22 and 1.23 provide additional information about the Operator Panel.

3.2.1.5.3 Automated Testing Unit (ATU)

The ATU is a non-1E industrial computer used to perform periodic testing of the SPINLINE 3 platform described in Section 4.6.10 of the LTR and Section 3.7.3 of this SE.

The operator connects the ATU to the Operator Panel and starts automatic periodic testing. The ATU injects signals to the system and then receives the output signal from the tested unit, so it can identify hardware malfunctions. Upon test completion, the ATU switches test inputs back to the normal inputs from the process. The channel in test will be inhibited by the operator prior to the start of the periodic test.

The LTR Section 4.6.10 and References 1.22 and 1.23 provide additional information about the ATU.

3.2.1.5.4 Monitoring and Maintenance Unit (MMU)

The MMU is a non-1E computer used to process the result of self-diagnostic tests, and thus support system diagnostic and periodic testing. The MMU produces a list of recommendations based on the results of the self-diagnostic tests. In this manner operators can identify the location of a failure and performed the required corrective action.

The MMU is permanently connected to the SPINLINE network via one-way communication to the NERVIA network using a PCI NERVIA+ board. Section 4.5.7 of the LTR briefly describes

how one-way communication can be implemented through the PCI NERVIA+ board. The NRC staff did not evaluate the PCI NERVIA+ board. Therefore, if an applicant referencing this SE wants to use a non-safety MMU, then the applicant should confirm that data exchanged between safety and non-safety devices does not adversely affect the safety functions of the system, and that justification for not following D&IC-ISG-04 Position 10 guidance is provided (see Section 5.2, Item 7).

The LTR, Section 4.6.11, and References 1.22 and 1.23 provide additional information about the MMU.

3.2.2 SPINLINE 3 System Architecture

The SPINLINE 3 platform is built from a set of modular, standardized components, including chassis, electronic boards, and cabling, suitable to implement different nuclear safety I&C systems applications. In the LTR, References 1.22 and 1.23, and during the regulatory audit (Reference 2.6), Rolls-Royce explained the features and possibilities for establishing different system architectures for the SPINLINE 3 platform. Due to the modular nature of the SPINLINE 3 platform, Rolls-Royce did not describe a particular system architecture or application using SPINLINE 3 platform in the LTR. Instead the LTR explains that with the SPINLINE 3 modules, Rolls-Royce can implement different system architectures to support application specific requirements. Furthermore, the application-specific system architecture will define the redundancy, diversity, and other features appropriate to the specific application. In Section 4.2.4 of the LTR and Reference 1.22, Rolls-Royce provided information to describe possible system architectures using the SPINLINE 3 platform. The scope of this SE for diversity provides a generic SE of the design approaches to build diversity using SPINLINE platform components and application-specific system architectures. Below is a summary of this information.

The first level in the system architecture is the chassis. Each chassis will have an associated BAP backplane and boards. The size of the slots in the BAP will define the number of electronic boards to be installed, and thus the application to be run by the CPU board. The BAP backplane provides signal connectivity between boards, and the interface boards provide signal connectivity to the application specific devices (e.g., sensors). As noted in Section 3.2 of this SE, only one UC25 N+ board can be installed in a BAP at a given time. One NERVIA+ daughter board can be mounted on the UC25 N+ CPU board to provide communication. The UC25 N+ CPU board uses two slots with or without the daughter board. One power supply module is used and occupies two slots. The remaining slots are available for I/O boards in any combination or number of each type of boards. Note the RTD 1.8PT100 Interface board uses two slots. (The appropriate sizing of the chassis will be defined during the project design phase, according to Rolls-Royce).

The next level is the cabinet, in which several chassis (or units) are installed. A chassis can communicate with other chassis through the NERVIA+ network or using serial communication (hard-wired connection). The number of stations transmitting on a network and the amount of

data transmitted by each station will determine the overall network cycle time for the system. An applicant or licensee referencing this SE should describe the number of transmitting stations and their network configuration (see Section 5.2, Item 5). Note the number of chassis connected using serial configuration in a division can affect the overall system reliability and will affect the overall system performance. Therefore, for a specific project application, the system reliability and system performance should be evaluated for appropriateness. Furthermore, an applicant referencing this SE should perform plant-specific failure and reliability analyses for instances where the NERVIA network is used for communications between multiple chassis (see Section 5.2, Item 24).

At the system level, an application specification may require several cabinets (or divisions) to implement redundancy requirements for the system, as specified by the plant system requirements. The NERVIA+ network can be configured to transmit data among divisions for the voting logic. An applicant referencing this SE should demonstrate that overall system response time and reliability meet the plant-specific safety requirements (see Section 5.2, Item 10).

An applicant or licensee referencing this SE should confirm the system architecture for the plant-specific application meets the system requirements (see Section 5.2, Item 3).

3.2.3 SPINLINE 3 System Communication

This section describes the following communication capabilities provided in the SPINLINE 3 platform:

- BAP Bus
- NERVIA Network
- Passive Communication and Hubs and Converters
- Serial Links

Rolls-Royce did not define a specific communication architecture for the SPINLINE 3 platform in its LTR. Instead they described the different types of communication provided. Therefore, the NRC staff only reviewed the features provided for each type of communication. The licensee should review the communication architecture defined for a plant-specific application to confirm that it meets the NRC regulation (see Section 5.2, Item 4).

3.2.3.1 Backplane Bus

The BAP bus is a passive communication bus. The BAP bus is a Master/Slave parallel bus with the Master board being the UC25 N+ CPU board and one or several Slave boards, which are the I/O boards. Because of this, the I/O boards cannot initiate data transfer on the bus, and respond to access operations controlled by the UC25 N+ CPU board connected on the bus. The UC25 N+ CPU board controls the BAP bus through the OSS.

When the SPINLINE 3 platform-based system is configured for a plant-specific application, each board gets a predefined address. This address is unique and differs from the addresses of other accessible boards mounted on the chassis. The address of a given board, in a given position in the rack, is set during the design phase of the system using a hardwired connection of specific pins on the BAP panel. This address is associated to the location of the board in the rack in its position. To read or write information to or from a given board, the OSS sets the relevant bits of the address bus for a particular board. A board is then addressed when the bits on the address bus are equal to the address wired on the BAP panel. When the correct address and board status are verified, the CPU can read/transmit data.

The BAP bus uses the XF1 and XF2 connectors to receive and transmit data. References 1.22 and 1.23 provide detailed information about data exchange through the BAP bus. Figure 3-2 shows data exchange via the BAP bus. Specifically, when the UC25 N+ CPU wants to receive data from an input board, the data flows from the field instrument to the interface board (e.g., I.16EANA). Then the data is transmitted to its associated input board (e.g., 16E ANA) through the XF2 connector. The input board performs signal conversion and conditioning. The input board transmits this data to the UC25 N+ CPU board through the XF1 connector. Once data is acquired, the data is stored in the local data memory of the UC25 N+ CPU board, ready to be used by the application software when the application is launched in the OSS sequenced cycle.

When the UC25 N+CPU transfers data to an output board, data flows from the UC25 N+ CPU board to the output board (e.g., 32ACT board) through the BAP bus via the XF1 connector. The output board performs signal conversion and conditioning. The signal is then routed from the output board to its associated output interface board (e.g., I.32ACT board) through the XF2 connector. After this step, the signal is sent to the terminal blocks or actuator devices.

Data exchange from the UC25 N+ CPU board with the NERVIA+ board and with the RTD Conditioning board are slightly different; and therefore these communications are explained in the following subsections.

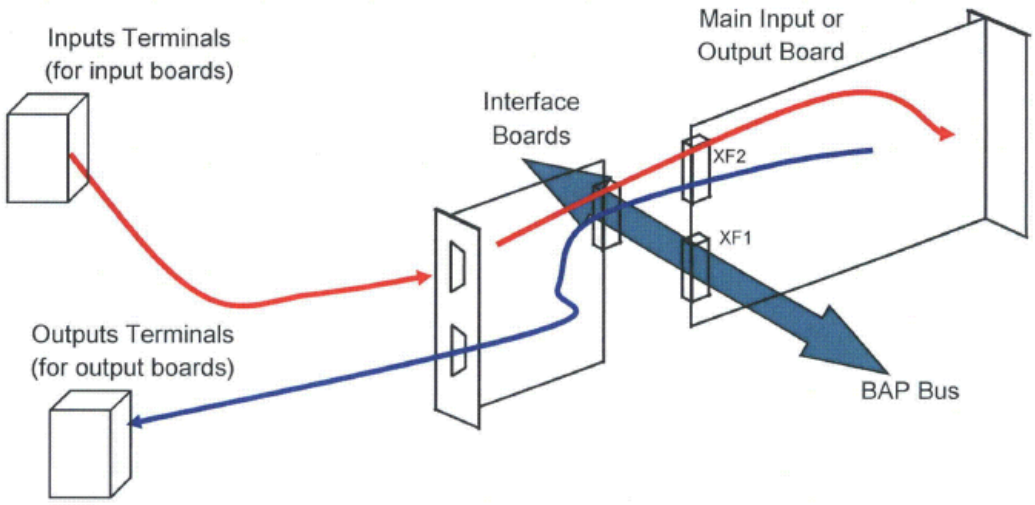

Figure 3-2: BAP bus Communication

3.2.3.1.1 Communication Between UC25 N+ CPU Board and NERVIA Board

The UC25 N+ CPU board communicates with the NERVIA network using the I.NERVIA+ interface board and the NERVIA+ board. The NERVIA+ board has no direct access to the BAP bus. Thus, the I.NERVIA+ interface board provides communication with the UC25 N+ CPU board through the XF2 connector, and its connection with the BAP bus. The data then flows from the I.NERVIA+ interface board to the NERVIA network hub through one of the RJ45 connectors. The data can then flow to other UC25 N+ CPU boards in the same cabinet through RJ45 connectors or through the NERVIA network (fiber optic) and then to other UC25 N+ CPU boards in different cabinets. Reference 1.22 provides detailed information about this data exchange.

3.2.3.1.2 Communication between UC25 N+ CPU board and RTD Conditioning Board

The 8PT100 conditioning board cannot communicate directly with the CPU using the BAP bus. Instead, the RTD signals are acquired by the I.8PT100 Interface board. The signals are then routed to the 8PT100 board through the XF2 connector for signal conversion and conditioning. After conversion, the signal is sent back to the I.8PT100 Interface board. If the signal is converted to voltage, the output signal from the I.8PT100 interface board is sent to an I.16EANA interface board as an analog input signal. At this point the signal will be transferred through the BAP bus to the CPU following the data exchange described in Section 3.2.3.1 of this SE.

If the signal is converted to current, the signal is not sent to the UC25 N+ CPU board. The signal can be used, for example, to drive a remote Class 1E temperature indicator or an appropriately isolated non-Class 1E device.

Reference 1.22 provides detailed information about this data exchange.

3.2.3.2 NERVIA Network

The NERVIA network is a SPINLINE 3 dedicated network. The NERVIA network can be used to exchange information within and among system divisions. Data in the NERVIA network is periodically exchanged among processing units, making the NERVIA a cyclic and broadcast network. Also, the NERVIA network allows a set of processing Units to exchange a predefined set of data within a bounded time frame, in order to ensure deterministic response time of safety actuations within design basis. The network physical topology is a star made of passive hubs. Configuration of the NERVIA+ network configuration (e.g., data and time frame to transmit data) is defined during the development process for a plant-specific application (see Section 5.2, Item 5).

Section 4.5 of the LTR describes the NERVIA digital network communication. The basic architecture for data exchange in the NERVIA network is shown in Figure 3-3. This figure shows that the NERVIA+ board and I.NERVIA+ interface board are known as “Station” and the UC25 N+ CPU is identified as “Unit.” The Station provides the network service to the Unit. Because the NERVIA+ daughter is mounted in the associated UC25 N+ CPU, up to 6 different Stations can communicate with the Unit, and therefore the Unit can communicate over 6 different NERVIA networks.

The first step in the data communication is to initialize the Station. Initialization of a Station is controlled by its Unit. The Station is initialized after the Unit power up or the Station hardware reset. During initialization, the Station verifies that the Unit has requested its initialization, and then proceeds to perform self-tests and diagnostics. After completing self-tests, the Station notifies the Unit that it is ready to operate. At this point the Station is initialized; this includes copying the NERVIA software into RAM, loading the network configuration tables. After initialization, the Station can insert itself in the network. If the Unit did not request initialization of the Station, the Station locks and an error message is generated and transmitted to the CPU. Rolls-Royce will define how this error is managed for a plant-specific application (see Section 3.4.2.3 of this SE for more information on error management).

The next step is to transfer the data from the Unit to the Station, so it is available to the NERVIA network. At this point, the data is transmitted to all Units connected to the network. Section 3.2.3.1.1 describes how data is transferred from the UC25 N+ CPU to the NERVIA+ board. Section 3.2.1.3.5 describes the hardware associated with the NERVIA network (see Figure 3-3).

The MPC860 processor on the NERVIA+ board controls the NERVIA network communication with the NERVIA software. The DPM on the NERVIA+ daughter board enables communication between the Unit’s 68040 microprocessor and the Station’s MPC860 microprocessor, so each microprocessor can read from and write to the DPM. Each microprocessor has independent cyclic process time, and therefore, will refresh data in the DPM independently (Reference 1.24).

Data in the DPM is grouped in Consistency Blocks (CBs), which are used to transfer information in the NERVIA network. In addition, the DPM memories are organized into [[ ]]. The OSS uses [[ ]] to control access to the buffers, in such manner that when data from either the Station's MPC860 microprocessor or the Unit's 68040 microprocessor is written to the DPM, the [[ ]] (References 1.22, 1.23, 1.24, and 1.30), and the data is written [[ ]]. Reference 1.24 provides a detailed description on how the [[ ]] and the DPM work, as well as [[ ]]. Configuration of the DPM is defined for each plant-specific application. Rolls-Royce will use the CLARISSE System and Software Development Environment (SSDE) tool to define and configure the DPM parameters. The licensee should verify that the requirement and design of the DPM is defined for a plant-specific application (see Section 5.2, Item 5).

During operation the [[ ]] access to the DPM on the NERVIA+ board to preclude errors associated with simultaneous reading and writing to a specific memory location (References 1.23, 1.24, and 2.5). The [[ ]]. Specifically, the [[ ]]. Reference 1.24 provides a detailed description on how the [[ ]] performs [[ ]].

Once the data is copied in the Station, the information is available to be broadcasted to all Stations in the network. A Station transmits a fixed amount of data organized in CBs. To deliver the CBs, the NERVIA network uses an Ethernet frame composed of: preamble bytes, Ethernet address field, source Ethernet address field, network protocol, data field, and frame check sequence field. Section 4.5.4.3 in the LTR describes the specific configuration of the frame used by the NERVIA network. The NERVIA uses the frame check sequence field (a 32 bit Cyclical Redundancy Check (CRC)) to check the integrity of the bits in the frame to ensure that the frame has arrived intact to the receiving Stations (to detect transmission errors). In addition, each CB includes a "refresh indicator" and a CB checksum that are used by the Stations to confirm the status of the message travelling in the NERVIA network.
These indicators are used by receiving Stations to determine if corruption or acquisition errors occurred during transfer of the CB. References 1.30 and 1.32 provide detailed descriptions on the configuration and operation of the CB in the NERVIA communication.

During the regulatory audit in Grenoble, France (Reference 2.5), the NRC staff reviewed a requirement thread that was central to management of access and access control to the DPM. The NRC staff also interviewed Rolls-Royce staff regarding the use of "consistency blocks" for data transfer. The NRC staff reviewed objective evidence during the audit that demonstrated

that the capability was properly implemented and rigorously tested. Note the NERVIA was not developed under a 10 CFR Part 50, Appendix B compliant program. Network components were, however, subjected to CGD. Thus, the NRC staff looked at evidence used for the evaluation of the CGD, such as Software Integration Test Plan and Report (Reference 1.49), Software Validation Test Plan (Reference 1.50), and Software Validation Test Report (Reference 1.51). These documents described the tests performed to verify and validate communication between the Unit and Station, NERVIA network (including CB status), and proper functioning of self-tests. An evaluation of Rolls-Royce's CGD effort is contained in Section 3.5 of this SE.

[[

]]

Figure 3-3: NERVIA+ Network Components

In Reference 1.24, Rolls-Royce described that although each Station operates independently, Stations are configured to operate in a coordinated manner. The network uses a time-based token bus protocol. The token is transmitted from one Station to another in the "Sequence Number" field defined in the network message. The token bus defines the order of the fixed cyclic sequence of transmissions. The token is transmitted from one Station to the others through the "next station sequence number" field included in all of its network messages. The next Station to transmit knows its turn through the positive comparison of its own Station number and the "next station sequence number" set in the received CB. Also, the CBs include several Network parameters to manage communication. For example, the token and related mechanism will allow synchronization while keeping the transmissions within a minimum and maximum propagation time, so Stations can be synchronized to receive messages or start transmission and a validation data to verify the integrity of the message for transmission errors.

The network and Station parameters are defined in the Network Description Table and Station Description Table. In this manner a sequence of cyclic and ordered transmitting Stations declared on the Network is established. Requirements, design, and configuration of the network and Station parameters and tables are a plant-specific application, which are defined during the design and configuration of the network (Section 5.2, Item 5).

The time allocated to each Station for transmission is called a “time window.” The time window is defined based on preparation of the message, transmission of the message, and reception and processing of messages transmitted in the NERVIA network. This time window is calculated and configured during the development of the software for a project based on the specific network configuration. An applicant referencing this SE should verify the time window for each Station is sufficient to meet the communication requirements for the plant-specific application (see Section 5.2, Item 5).

[[ ]] Data transmitted from one Station is received by all Stations in the NERVIA network. The Station will transmit the CB during its time window, established in the minimum and maximum propagation time. The Stations not transmitting listen for messages from other stations in the network. When a Station receives a message, it will check the integrity of the data for transmission errors. If the data received is correct (not transmission errors), additional checks are performed at application level based on the CB checksum (and the refresh indicator). If the Station determines that data has been corrupted or stale, the message will be flagged as invalid. Corrupted or stale data will be flagged by the Unit, and it won’t be used. Section 3.4.2.3 of this SE describes how errors and failures are detected and managed. After the data is checked, the Station will copy the data contained in the message in its DPM. [[ ]] Once data is in the buffer, the data is available to the Unit.

Section 4.5.2.4 of the LTR and Reference 1.24 explain how the NERVIA network is initialized. Specifically, the NERVIA network in a plant-specific application is initialized when the first Station in the network is powered up. This first emitting Station listens to the network traffic for a period of time greater than the defined Network cycle time. If during this time no message is received, this Station knows it is the first on the network and starts transmission. If a message is received, the Station determines where it is in the network time scheme. This first Station starts a timer used to identify its next transmission time window in the network cycle. The first Station will transmit again at the end of the timer, which corresponds to the network cycle time if no messages are received. The first Station message serves as a synchronization signal for the next Station to join the Network. The second Station to power up will initialize and listen for a message. The received message contains the token (i.e., [[ ]]). The second Station will transmit when the token [[ ]]. All other new Stations entering the network (after they are powered up and initialized) will follow the same procedure and steps as the second Station: listening, checking the token, setting its own timer, and transmitting in its pre-defined

time window. Once in the NERVIA Network, each Station operates in a coordinated manner as defined by the cyclic and sequenced time windows.

When a Station is reset or down, the next Station in the [[ ]] will transmit. When the Station is powered up again, it has to re-insert itself in the network. To do this, the Station listens for a pre-defined time (i.e., entire network cycle). If a message is not received during this time, the Station will start to transmit. On the other hand, if a message is received, the Station waits for its turn to transmit in accordance with [[ ]]. If a Station cannot reinsert itself after several attempts [[( ]]. In this case, the Station will send a message to the Unit to identify the error that occurred. Rolls-Royce will define how this error is managed for a plant-specific application (see Section 3.4.2.3). In addition, the fact that the Station cannot reinsert itself and transmit is detected by the other Stations through the refreshment indicator in the message. Other Stations will treat the message from the down Station as stale data, which are flagged as invalid. Rolls-Royce has stated it will define how this error is managed for a plant-specific application (see Section 3.4.2.3).

In Reference 1.24, Rolls-Royce describes a special case for network initialization. [[

]]

Section 4.5.4.2 of the LTR describes the typical failure mechanisms implemented to detect failures, and how these failures do not affect operation of the NERVIA network or the Unit. For example, [[

]]. Rolls-Royce has stated it will define how this error is managed for a plant-specific application (see Section 3.4.2.3).

In addition, the OSS continuously monitors communications status to indicate communications link failures or network problems. For this, the OSS performs the tests for Category 3 and 4 described in Section 3.4.2.3 of this safety evaluation. The NERVIA also performs self-diagnostic tests to detect communication failures. Section 4.5.6 of the LTR and Reference 1.24 describe the self-diagnostic tests performed. In particular, the NERVIA board performs self-tests, which consist of checking correct operation of the Station's MPC860 controller, correct addressing of memories, integrity of memories, etc. Rolls-Royce has stated it will define how these errors are managed for a plant-specific application (see Section 3.4.2.3).

Rolls-Royce defines two types of Stations in the NERVIA network, receive-only and transmitting. For two-way communication, the stations are configured as transmitting Stations. The receive-only Stations only receive data and cannot transmit (one-way communication) data. As a consequence, this type of station does not use time during the network cycle. The Station type is defined during the design and configuration of the system and the NERVIA network.

The NERVIA network configuration is defined during the development process using CLARISSE SSDE.

Section 4.5.7 of the LTR briefly describes how one-way communication can be implemented through the PCI NERVIA+ board. This board is a non-Class 1E board that establishes the physical interface between a non-Class 1E external computer and the SPINLINE 3 NERVIA communications network. The PCI NERVIA+ board can be installed in a PCI slot on an external non-safety PC (e.g., MMU). Rolls-Royce used this board to connect the qualification test specimen with the data acquisition system used during EQ testing.

During EQ testing, Rolls-Royce configured the QTS network to perform data transmission using the NERVIA network from Unit 1 to Unit 2 and unidirectional communication from Units 1 and 2 to the Data Acquisition System (DAS). References 1.22 and 1.46 provide descriptions of the system specification and requirements on the QTS network. In particular, Rolls-Royce defined 4 network connections for Unit 1 to send data to Unit 2, only one of these connections was bi-directional. In addition, Unit 1 included a fifth connection to send data to the DAS (one-way). For Unit 2, Rolls-Royce configured two network connections, one to send data back to Unit 1 and the other to send data to the DAS (one-way). When data was exchanged between Units 1 and 2, the system reads the validity indicator to determine if data transmission behaved as expected. In this manner, Rolls-Royce could collect data during EQ testing, as well as determine correct operation of the QTS and the DAS and validity of the data obtained.

The PCI NERVIA+ board was not included in the scope of the SPINLINE 3 platform submitted for review and approval; also, the PCI NERVIA+ board was not subject to the EQ testing performed on the rest of the platform components. Therefore, the NRC staff did not review and evaluate the PCI NERVIA+ board. Use of the PCI NERVIA+ board is a plant-specific action, and it should be evaluated as part of the specific system configuration (see Section 5.2, Item 2). Also, an applicant referencing this SE should confirm data exchanged between safety and non-safety devices does not adversely affect the safety functions of the system, and that justification for not following D&IC-ISG-04 Position 10 guidance is provided (see Section 5.2, Item 7).

In References 1.21 and 1.22, Rolls-Royce explained how transmission of invalid data was identified and treated during EQ testing. [[

]]
to perform the functions defined in the Tests Software Application Program (TSAP). The validity management used during EQ testing is only valid for the QTS configuration used. As stated before, the data validity management is project-specific and needs to be specified for a plant-specific application.

3.2.3.3 Passive Communication Hubs and Converters

Communications and their connections are implemented in passive hubs and converters installed outside the SPINLINE 3 chassis. Passive hubs and converters provide 10Mb/s connections between communications links and make the transition between copper cables and optical fibers, if needed. For example:

- Communication between safety units in the same division can use copper cables and 4TP hubs.
- Communication between safety units located in different divisions can use optical fiber and 3TP/2FL hubs or TP/FL converters. The optical fiber provides electrical isolation between safety divisions.
- Unidirectional communication between a Class 1E division and an external non-Class 1E unit can use a fiber optic cable and 3TP/2FL hubs or TP/FL converters. The fiber-optic cable of this communication path provides electrical isolation between a Class 1E I&C system and a non-Class 1E I&C system.

The communication hubs and converters do not embed microprocessors. These hubs are passive, and only manage the signal shape, amplitude of the data, and the correct operation of the hub. Hubs and converters are powered from the cabinet power supplies, with adequate redundancy in case of failure of one power supply. If an applicant decides to use hubs and TP/FL converters assembly different than the one used in the QTS and listed in Table 3-2 of this SE, then the applicant should confirm the hub or other network device used on the NERVIA network is truly passive and does not use an embedded microprocessor (see Section 5.2, Item 17).

Section 4.5.4.2 of the LTR describes the typical failures that can be observed at the hubs. Also, this section describes the behavior of the hubs if a failure is encountered. For example, if the hub detects that a Station is continuously transmitting, the hub will interrupt the transmission at the hub port. Rolls-Royce has stated it will define how these errors are managed for a plant-specific application (see Section 3.4.2.3).

The passive communication hubs and converters are commercial grade electronic devices. They are procured and qualified according to the Rolls-Royce nuclear quality assurance program. These items were part of the CGD performed for the SPINLINE 3 platform, which is described in Section 3.5 of this SE.

3.2.3.4 Serial Links

There are two serial links (i.e., RJ45 connectors) in the SPINLINE 3 platform. One connector can be used to connect to the LDU and the other for test purpose. They are located in the front panel of the SPINLINE 3 platform. These links will be used during maintenance. Use of these serial links must be defined for each plant-specific application (see Section 5.2, Item 4).

3.3 SPINLINE 3 Platform System Development

Rolls-Royce followed its "Project Execution Process," Document No. 8 303 314 (Reference 1.52), for the overall design of any Rolls-Royce product, including the SPINLINE 3 platform. Specifically, the Project Execution Process describes the organizational structure and generic process to be followed for management of contractual projects. The Project Execution Plan also identifies Rolls-Royce design and management processes and procedures throughout the development activities and lifecycle of the system. For a plant-specific application, this process would be adapted and described in the Project Management Plan (see Section 5.2, Item 9).

The Project Execution Process identifies the following procedures for the design and development of the SPINLINE 3 platform modules. Note that several procedures listed in this section were not submitted to the NRC, but were described in either the responses provided to RAIs or during the regulatory audit.

- 8 303 334, System Design (Safety Systems) (Reference 1.53)
- 8 303 603, Equipment Design Process (not docketed)
- 8 303 349, Electronic Design Process (not docketed)

Rolls-Royce procedure 8 303 334, "System Design (Safety Systems)," defines the generic design process, the project lifecycle phases, verification and validation activities, and review activities. In particular, this procedure defines the process for controlling the design and validation of SR I&C systems to meet system technical and functional requirements. In addition, Rolls-Royce has other design and development procedures that are used for the design of the SPINLINE 3 platform. In References 1.22 and 1.23, Rolls-Royce explained the process and the procedures used; Figure Q6-1 in Reference 1.22 illustrates the SPINLINE 3 platform development process. Furthermore, during the regulatory audit, the NRC staff reviewed these documents and observed how they are being used by Rolls-Royce personnel (Reference 2.5).

After the system design, Rolls-Royce staff followed procedure 8 303 603, "Equipment Design Process," for the implementation of the process described in the System Design (Safety Systems) and Project Execution Process. This procedure describes the design and development of the SPINLINE 3 platform.

For the design of the boards constituting the SPINLINE 3 platform, Rolls-Royce personnel followed the stages described in procedure 8 303 349, "Electronic Design Process." Rolls-Royce provided a summary of this document in Reference 1.22. In particular, this document describes the design activities of the equipment, which consists of the following phases:

- Specification – establishes requirements and functions to be performed by the board.
- Design – defines electronic design of the board according to its specification.
- Qualification – validates the design by confirming that the design met the specification.
- Industrialization – establishes manufacturing and control records.

Rolls-Royce Procedure 8 307 032, “Principle for Control of Design (Safety Systems)” (Reference 1.54), describes oversight and quality controls for the design and development of the SPINLINE 3 platform through the system lifecycle. This procedure will be followed to design and develop safety related systems.

Rolls-Royce staff follows Procedure 8 303 350, “Safety Software Design Process” (Reference 1.56) for software development. Particularly, this procedure will be used for the development of the application software for a plant-specific application.

In References 1.22 and 1.23, Rolls-Royce explained that all its activities are currently performed under the 10 CFR Part 50 Appendix B compliant quality program documented in the Rolls-Royce SAS Quality Manual (Reference 1.26). They also noted that modules would be updated or modified through a process called the New Offer Creation Process, described in Rolls-Royce Procedure 8 303 693. Rolls-Royce Procedure 8 303 314, Section 1.2, shows the relationship between the Project Execution Process and the New Offer Creation.

3.4 SPINLINE 3 Software Architecture

Section 4.4 of the LTR describes the software architecture for the SPINLINE 3 system. The OSS is part of each processing unit (CPU) to support configuration of hardware components and communication. The OSS will be configured for use with each application, but the code is not modified. The configuration of the OSS will consist of defining and configuring the I/O boards included in the SPINLINE 3 platform for a plant-specific application. On the other hand, the application software is developed for a plant-specific application. The adaptation of the system software to the application needs is performed using the processing units and networks configuration tool of the CLARISSE System and Software Development Environment. The application software performs the functions linked with the functional diagram and the operation of the system.

The software architecture in the SPINLINE 3 platform consists of:

- Non-Class 1E set of tools integrated in CLARISSE SSDE for the design and implementation of the system architecture, configuration of the units and networks and development of the plant-specific application software.
- Class 1E standardized OSS, which provides the interface between the local and remote data delivered by the I/O and communication link boards and the application software. The OSS also provides continuous self-diagnostic testing of the hardware and services to the application software.
- Class 1E application-oriented library of software functions.
- Class 1E software embedded in electronic boards with electronic components, such as the NERVIA+ board and ICTO Pulse Input board.
- Class 1E firmware embedded in electronic boards with electronic components, such as 6SANA board, 32 ACT board, 32ETOR board, and 16E.ANA ISO board.

In addition, the SPINLINE 3 platform includes programmable components, such as FPGA, to process data and perform specific functions, such as data conditioning. These programmable components include logic or firmware to perform their functions. These logic and code do not interface with the OSS or the application specific software.

The following section explains the software elements that constitute the SPINLINE 3 platform.

3.4.1 CLARISSE SSDE

The CLARISSE SSDE is the software development and automation environment used by Rolls-Royce to build a plant-specific application. In particular, CLARISSE SSDE is a standardized and independent software package that provides the software tools and libraries necessary to design and develop a SPINLINE 3 platform-based system. CLARISSE is a simple user interface that automates compilations, linking, transformation, setup, and configuration of the SPINLINE 3 platform. CLARISSE is only used for the development of SPINLINE 3 platform-based I&C systems for nuclear applications. No portion of the CLARISSE tool remains in a shipped system for a plant-specific application. The CLARISSE SSDE is not safety qualified; therefore Rolls-Royce has stated it will subject all outputs to thorough verification and validation (V&V) either directly or through validation of the integrated software.

This tool is used for the following functions:

- Definition and configuration of the system architecture, processing units, I/O boards, and NERVIA network
- Development of the application software
- Generation of executable code for the SPINLINE 3 platform-based system
- Perform informal verification and validation

Section 4.4.4 of the LTR describes and References 1.32, 1.34, and 1.57 describe the CLARISSE SSDE and how this is used for software development and configuration management. In particular, the CLARISSE links the different elements in the executable code for the plant-specific application. These elements are listed below, and illustrated in Figure 3-4.

- Bootstrap
- Hardware configuration table
- OSS
- application software

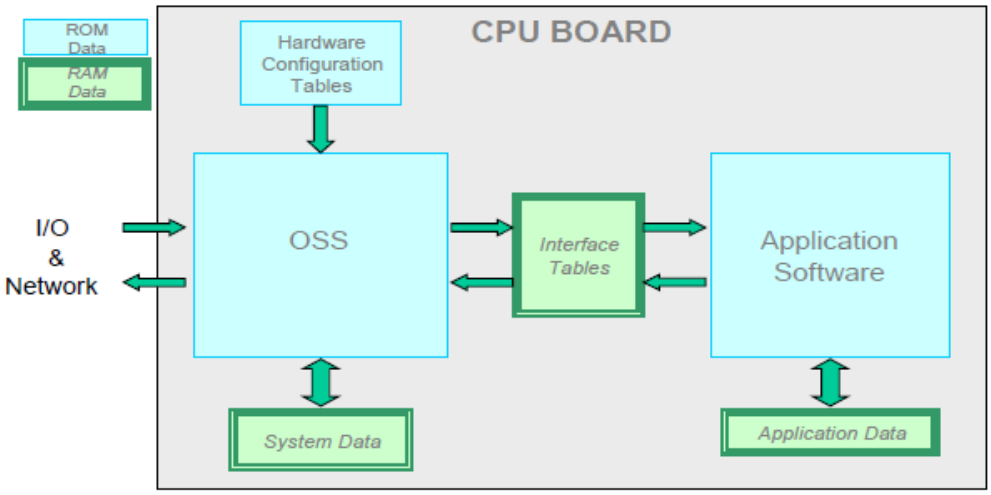

Figure 3-4: CLARISSE Configurable Components for the SPINLINE 3 Platform

The Rolls-Royce designer uses the Safety Critical Application Development Environment (SCADE) tool to define I&C functions to be implemented in the SPINLINE 3 platform-based system for a plant-specific application. The SCADE tool is part of the CLARISSE SSDE. The SCADE provides a functional block diagram language with a formally defined graphical and textual syntax and semantics. In addition, the SCADE is used to automatically generate the application executable code included in the Unit and executed the CPU.

Rolls-Royce document, "SPINLINE 3 Design Analysis Report" (Reference 1.58), explains that the SCADE tool was originally created by VERILOG and it is currently managed as a product of Esterel Technologies. Since this tool is not part of the running software system and performs no safety functions, it was not part of the CGD of the OSS. Rolls-Royce considered this a non-safety software tool, and therefore its output is subject to V&V activities necessary to find any errors introduced by the software tool.

The SCADE development environment includes a Rolls-Royce developed proprietary library of 1E application-oriented software functions (e.g., threshold function) for software development. If functions are not in the library, designers can create them using additional functions coded in C language. References 1.34 and 1.59 describe how this library was designed and it is currently maintained. Furthermore, Reference 1.34 explains that the library includes a checksum, which is used as a signature for the library version. When the CLARISSE is used to generate the executable code, the CLARISSE would verify the checksum matches the OSS library version used. During the regulatory audit, the NRC staff reviewed the software configuration management plan for the SCADE library and found this process was acceptable (Reference 2.5).

3.4.2 Operating System Software

Rolls-Royce developed the SPINLINE 3 platform OSS for the EDF P4 and N4 PWR fleet. Then, the I&C system for the N4 technology evolved into the current OSS for the SPINLINE 3 platform. The OSS was developed and validated according to European nuclear standards for software based 1E safety systems, mainly IEC 880-1986, IEC 60880-2006.

The OSS is a standard software component in each SPINLINE 3 processing unit to support any hardware configuration required for an application specific project. The OSS only requires simple configuration to fit the needs of the customer I&C systems. Configuration of the OSS is performed using the CLARISSE SSDE when developing the plant-specific application.

The OSS provides basic functions like communication, data acquisition, or services to be used by the application software. The OSS consists of the following elements:

- Core System Software (CSS)
  The CSS is responsible for initialization, testing, acquisition and restoration of data on a Unit's hardware I/O.

- Basic Functions (BFs)
  These functions are used to perform hardware functions, such as access to I/O modules, NERVIA network, and self-diagnostics.

- LDU Driver
  The LDU driver manages the exchange of data with the non-1E LDU device using an Asynchronous Serial Link (ASL). This interface module is called LDU_CPU in Rolls-Royce documents.

- Function for Access (FAS)
  Functions used by the application software to communicate and exchange specific hardware information with the OSS.

Rolls-Royce Reference 1.24 explains the relationship among these elements. In particular, the OSS is the assembled software that includes all these elements. The CSS is the main program responsible for running sequences and modules. Lastly, the BFs are the drivers that are used to interface between the CSS and the I/O boards. Figure 3-5 illustrates the layout of OSS elements.

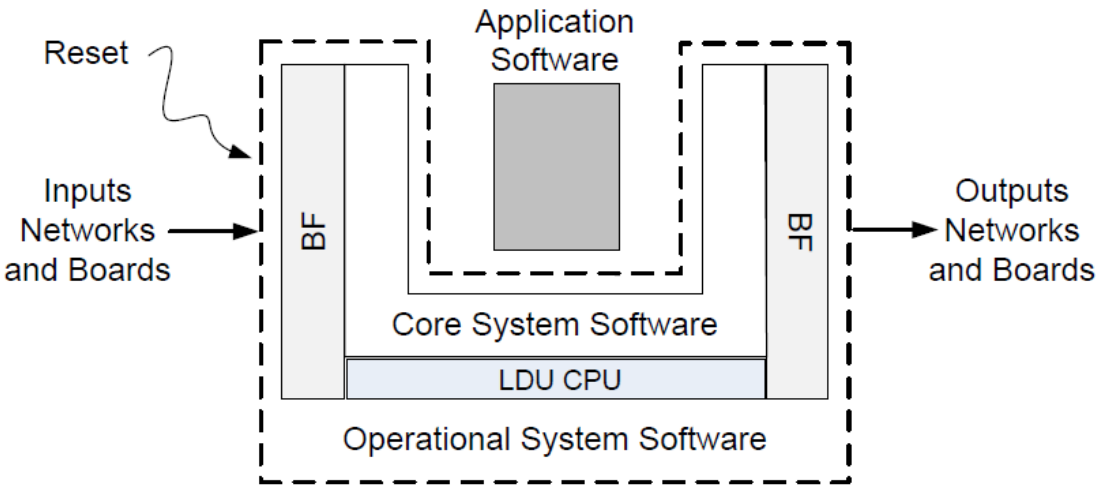

Figure 3-5: OSS Elements

The OSS uses configurable parameter tables to communicate with the I/O modules, application software, and LDU. These parameter tables define the values and/or assignments for each variable in the OSS necessary to perform its processing tasks. In this manner, Rolls-Royce can use a single code for the OSS, and just modify the configuration tables as necessary for a plant-specific application. The following generic configuration tables are configured for the SPINLINE 3 platform:

- Hardware Configuration Table
  This table defines the Unit's hardware configuration. This table includes the number of boards, station address, slot occupied by boards, channels used by boards, etc. This table is stored in CODE RAM.

- System Status Table
  This table is used by the OSS and LDU to determine and share information on rack hardware status and connected network status, LDU connection status data, and information on changes to individual parameters in the EEPROM made by the LDU (e.g., setpoints). This table is stored in DATA RAM.

- OSS/Application Interface Table
  This table is used for the data exchanges between the OSS and the application software. This table is stored in DATA RAM.

The tables are of fixed size and structure (regardless of the I/O boards installed for a plant-specific application). These generic parameter tables are configured using CLARISSE SSDE when configuring an application specific system. This customization is performed during design

activities of the system through static configuration parameters. In addition, Rolls-Royce implemented means (i.e., self-tests) to detect errors when the parameters in the tables do not match the system configuration. For example, the OSS verifies that the number and type of I/O boards presented in the chassis correspond to the I/O boards defined in the Hardware Configuration table. Each generic table is broken down into subsidiary tables necessary to perform specific functions; for example, the hardware configuration table includes an initialization table, which is used to initialize an intelligent board and a station. References 1.30 and 1.32 describe these tables and their configuration. For example, unused fields in a table (i.e., I/O board not used) are filled with a predefined value to avoid erroneous access to one of the fields.

Because the OSS is parameterized software, which can be adapted for different hardware configurations (i.e. I/O boards) for each plant-specific application, the OSS will include deactivated code[2]. Section 6.3 in Reference 1.31 explains the use of deactivated code for the MC3 project. Rolls-Royce controls the deactivated code during the design of the system; specifically, the code is linked to the configuration tables. Using these tables, the code will determine what part should be active (e.g., based on whether a board is present in the chassis and is defined in the configuration table). An applicant referencing this SE should verify that the I/O modules configured in the OSS correspond to the I/O modules evaluated in this SE. Furthermore, the applicant should confirm that the I/O modules are properly configured, and that the code for modules not installed does not adversely affect the safety functions to be implemented in the SPINLINE 3 system (see Section 5.2, Item 2).

The OSS is organized into modules (References 1.24 and 1.31). Specifically, the OSS includes the Treatment (or Initialization) Modules, which are constituted by Basic Modules, which in turn are divided into basic functions. For example, the Treatment Module is dedicated to the Initialization function of the system. This module uses a Basic Module associated to the functionality of a particular board (e.g., Initialization of the 6EANA board). Lastly, the Basic Module calls the basic function to perform a particular function (e.g., packing data). The Treatment Modules use the configuration tables to call the different Basic Modules associated with a particular function or task. The Basic Modules use the data in these tables for their processing tasks. Figure 3-5 illustrates the OSS structure.

[2] Rolls-Royce defined deactivated code in Reference 1.31 as "code which is present and has been validated, but has not been activated due the software configuration obtained by the parameter settings." In References 1.31 and 1.34, Rolls-Royce noted that this definition was taken from Avionics Standard, DO-178B, "Software Considerations in Airborne Systems and Equipment Certification." In these References Rolls-Royce clarifies that deactivated code is not considered dead code.

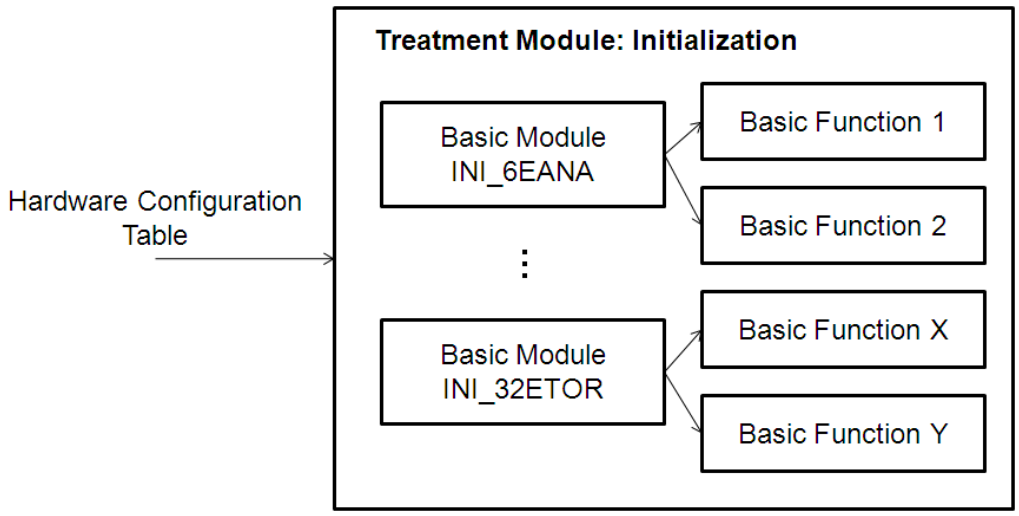

Figure 3-5: OSS Structure

3.4.2.1 OSS Functions

When the system is started, the OSS initializes the system by calling the Initialization Module. After initialization of the CPU, I/O boards, and Stations, the OSS calls the Bootstrap or launcher, which performs the following: copies the executable code from the FLASH EEPROM to the CODE RAM, copies the initialized variables to the DATA RAM, and activates the code in the CODE RAM. Once the executable code is in CODE RAM, it cannot be modified, and write access attempts will shutdown the system. After these tasks are performed, the OSS calls the CSS. The CSS will in turn call the different modules in the OSS and the application software to perform the functions configured in the system. Figure 3-6 shows the functions performed by the OSS.

The following sections describe these functions.

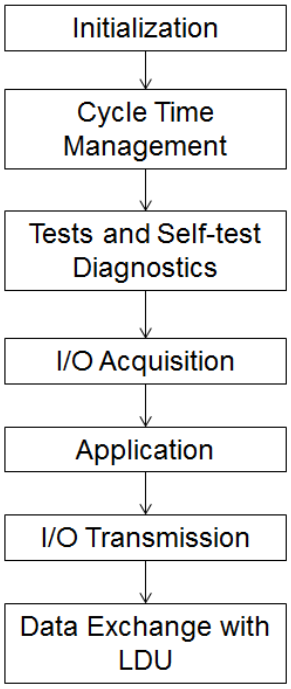

Figure 3-6: OSS Functions

3.4.2.1.1 Initialization

To initialize the system, the OSS calls the initialization function and uses the data in the Hardware Configuration Table to initialize the CPU by performing the tasks listed below. If a problem is encountered during initialization, the OSS will indicate the failure and manage it as described in Section 3.4.2.3 of this SE.

a. Initialization of the UC25 N+ board – This function initializes and verifies internal operation of the microprocessor and setting of the UC25 N+ board watchdog. If the initialization function encounters a failure, the CPU is stopped.

b. Initialization of intelligent peripherals – This function initializes the intelligent peripherals by resetting the intelligent device and transmits operation parameters to the board. If necessary, the OSS will perform 2 consecutive attempts to initialize the board. If it fails, the OSS will mark the board as faulted, and thus it would not be used by the system. These peripherals are NERVIA+ and ICTO boards.

c. Verification of intelligent peripheral (defined in Section 3.2.1.3) addressing – This function is performed to confirm the address of intelligent I/O boards and correct

operation of the board (this test is part of Category 2 diagnostics, which is described in Section 3.4.2.3). If an error is detected, the system would halt this function and the module is marked as faulted.

d. Verification of configurable non-intelligent peripherals (defined in Section 3.2.1.3) – This peripheral is 16 EANA board. This function is performed to confirm that the non-intelligent board is accessible and operating correctly (this test is part of Category 2 diagnostics, which is described in Section 3.4.2.3). If an error is detected, the system would halt this function and the module is marked as faulted.

e. Configurable non-intelligent peripherals (defined in Section 3.2.1.3) – This function initializes the non-intelligent peripherals by verifying the board status and updating the configuration registers for the board. These peripherals are the 6SANA, 32ACT, and 32ETOR boards. The OSS will perform one attempt to initialize this board and if it fails, the OSS will mark the board as faulted, and thus it would not be used by the system. Note, these boards require stabilization time after the CPU is reset to perform valid data acquisition and time to accept the updated registers. The stabilization time will be configured for a plant-specific application (see Section 5.2, Item 2).

f. Copying EEPROM data to RAM – This function copies the content of EEPROM data and the checksum to the RAM working area. After this is done the OSS will calculate the RAM checksum and compare it to the EEPROM checksum. If an error is detected in the checksum, the CPU is halted.

After these tasks are completed the OSS will determine and indicate its operating mode, as described in Section 3.4.2.2.

3.4.2.1.2 Cycle Time Management

The software in the SPINLINE 3 platform is run sequentially, deterministically, and periodically. To achieve this, the OSS maintains a fixed cycle time that consists of the CSS execution time and the application execution time. Further, the application execution time can be configured to be executed on a fixed time interval. The OSS uses a cycle time management function to monitor the defined cycle time. This function uses a CPU timer to count the elapsed time since the last call to the CPU timer initialization. If the elapsed time is less than the defined cycle time the OSS waits until the elapsed time is equal to the defined cycle time to continue operation. If the elapsed time is greater than the defined cycle time, the CPU is stopped. Section 3.7.1 of this SE describes the NRC staff's evaluation on system response time. An applicant referencing this SE should verify that the configured application execution time is sufficient to perform the safety functions, and that an evaluation of the system response time is performed (see Section 5.2, Item 10).

3.4.2.1.3 Tests and Self-tests Diagnostics

The test and self-tests are performed to detect failures in the system hardware. If a failure is detected, the OSS will change its operation mode and the failure will be indicated in the MMU, if the MMU is included with the system. Section 3.4.2.3 of this SE describes failure detection and management. The following tests and self-tests are performed.

a. CPU board self-tests – These tests confirm operation of the CPU and peripherals. These tests are considered Category 1 for error management, which is described in Section 3.4.2.3. In case a failure is detected, the CPU is stopped, which causes the front panel LED to go off.

b. Tests and check on peripherals – These tests confirm addressing status of all peripherals and the operating status of the intelligent peripherals. These tests are considered Category 2 and 3 for error management which are described in Section 3.4.2.3. These tests are not performed if the peripheral is not in faulted.

c. Tests of network communication – These tests confirm status of communication on the NERVIA network. These tests are considered Category 4 for error management, which is described in Section 3.4.2.3.

d. EEPROM parameter degradation test – This test verifies that parameters copied from the EEPROM to RAM have not degraded. This test is performed after initialization and it calculates and compares the checksum in the RAM against the checksum stored in EEPROM. If a checksum error is detected, the CPU is stopped. This test is performed during Category 1 diagnostic.

3.4.2.1.4 I/O Management

This function performs both I/O acquisition and transmission. The OSS will use the Hardware Configuration Table to identify the data to be acquired from and transmitted to I/O boards and/or network. Based on this data, the OSS will acquire information from the I/O boards, and the NERVIA network following these stages:

a. Acquisition of information
   During this stage, data is acquired from each type of board configured in the SPINLINE 3 system and the NERVIA network. Data is acquired from the input boards in the following order: digital input boards, analog input boards, and pulse inputs from the ICTO board. When data is acquired, the system performs data validation, and if an error is detected the data is identified as invalid and the operation status of the board is set to “fault.” Reference 1.30 provides detail information on the validation tests perform on each data and input board. The OSS will flag and address this failure in accordance with the system engineered fault management system (see Section 3.4.2.3). Afer the input boards data is acquired from the NERVIA network. In this instance, data is

acquired in a packed form (i.e., CB), which includes a validity flag to indicate if data is valid or invalid.

The SPINLINE 3 platform will not acquire data from input boards or NERVIA network stations that are identified in fault (due to addressing error or status, for more information See Section 3.4.2.3).

b. Transmit acquired data to the application software
In this stage the OSS supplies the data acquired and their validity indicators to the application software. If invalid values are transferred to the application software, these values will be flagged and not used in the logic (see Section 3.4.2.3).

c. Receive data from the application software
After data is used in the application software, the resulting values will be used to modify the data to be transmitted to the output boards and NERVIA network. This data is also transmitted with their validity indicators.

The signals marked as invalid are handled in accordance with the system engineered fault system (see Section 3.4.2.3).

The application software uses FAS to communicate with the OSS. References1.32 and 1.34 describe how these functions access the “OSS/Application interface table” for exchange with the OSS.

d. Transmit data to output boards and networks
After data is transferred from the application software to the OSS, data is sent to the output boards and the NERVIA network. Data is transmitted to the output boards in the following order: digital output boards, analog output boards, and then to the NERVIA network. When data is transferred the system performs data validation, and if an error is detected, the data is identified as invalid and the operation status of the board is set to “fault.” Reference 1.30 provides detailed information on the validation tests performed on each data and output board. Transmissions are not processed when operation status or address status of the station or board is set to the “fault” value.

3.4.2.1.5 Data exchange management with the LDU

This function in the OSS manages the communication between the LDU and the CPU board in the Unit through an ASL. Through the LDU the operator can modify parameters stored in the EEPROM and monitor selected values. As stated in Section 3.2.1.5, the LDU was not part of this review, so the NRC staff did not evaluate this function (see Section 5.2, Item 8).

3.4.2.2 OSS Operating Modes

After the OSS is initialized, the system will start operating in any of the following operating modes, assuming that errors or failures have not caused the CPU in the UC25 N+ board to stop working. Section 3.4.2.3 describes failure detection and management for the SPINLINE 3 platform.

a. Normal
   This mode is entered when all processing tasks are performed correctly. In this mode the CPU will perform its functions in a cyclical manner. If an error or fault is detected during normal operation, the system will transition to one of the other modes of operation, depending on the condition encountered; this will be defined for each plant-specific application.

b. Partially degraded
   In this condition, the CPU is working and performing its functions in a cyclical manner, but one of the peripheral boards was not initialized correctly. In this case, the CPU won't interface with the faulted board. If during this condition one of the CPU self-tests detects a failure, the CPU will stop working.

c. Totally degraded
   In this condition the CPU is stopped and the only functions performed are communicated to LDU and CPU self-tests, in this manner the operators can identify the error that caused this condition. After the fault is cleared, the system will have to be reinitialized.

3.4.2.3 OSS Failure Detection and Management

During the different functions of the OSS, the system performs error tests, detection, and indication. The LTR defines the process to manage failures identified by the OSS functions, and how these failures can modify the OSS operating mode and/or perform defined actions to address these failures. The tests performed to detect these failures are categorized in the following manner:

- Category 1 – self-tests on UC25 N+ board
- Category 2 – tests on intelligent and non-intelligent boards
- Category 3 – tests on NERVIA network stations
- Category 4 – tests on status of NERVIA network communication
- Category 5 – tests on I/O boards

Section 4.4.3.6.1 of the LTR and Reference 1.30 provide detailed information on the particular tests and self-diagnostic tests performed for each category. Below is a summary of this information.

If errors are encountered during self-tests or a test during one of the Category 2 through 4 tests, the OSS will perform pre-defined actions. In general, Rolls-Royce will define these actions in the application specific Failure Analysis for a plant-specific application. This failure analysis is used to design and configure the engineered fault management system built into the application software of the related CPUs. Section 4.4.3.6.1 describes generic actions to be taken for each test when errors or failures are detected. For example, if a self-test in Category 1 fails, the CPU is stopped. This causes the CPU's discrete outputs and analog outputs to switch to their fallback values. Stale data identified during this test is flagged and handled in accordance the system's engineered fault management system.

In addition to the pre-defined actions, the OSS can generate external and internal indicators. Internal indicators are used to flag and invalidate data transmitted to the application software and to manage data acquisitions/outputs. Specifically, these indicators are used to indicate: status of a board, access status of a board, and validity of data. This last indicator will identify if data obtained from input boards or the NERVIA network has been corrupted or if data becomes stale. The application software performs normal processing on valid data and safety-oriented exception processing on invalid data in accordance with the system's engineered fault management system.

External indicators are used to signal hardware failures in the MMU. Specifically, these indicators are used to identify: board addressing errors, board operating status, Station operating status, network status, and data status. This last indicator will identify: checksum status, refresh status, and identifier status.

3.4.2.4 OSS Development Process

The life cycle processes for the SPINLINE 3 platform software were established according to the guidance provided in IEC 880-1986, and were documented in dedicated software plans. The SPINLINE 3 software life cycle processes also took into account additional process enhancements employed on the N4 project and ongoing standardization efforts for a supplement to IEC 880, which was issued in 2000.

During evaluation of the CGD, the NRC staff reviewed the development process for the OSS. Section 3.5 provides a detailed description of this evaluation.

3.4.2.5 OSS Regulatory Review

The regulatory review for the OSS was performed as part of the CGD for the Rolls-Royce SPINLINE 3 platform, which is described in Section 3.5 of this SE.

3.4.3 Development Process of Boards with Programmable Components

As mentioned in Section 3.2.1.3, the SPINLINE 3 platform includes several boards that include programmable components (Reference 1.22), such as FPGAs, CPLDs, and microprocessors. These boards are:

- Actuator Drive Board 32ACT
- Calibrated Pulse Acquisition Board ICTO
- NERVIA+ Daughter Board
- 32ETOR TI SR module
- Analog Input Board 16EANA ISO

Section 6.2.10 of the LTR states that these modules were designed in accordance with the Civil Nuclear SAS Quality Manual (Reference 1.26). In addition, Rolls-Royce established a development process for each module that includes programmable components. These processes are described in detail in References 1.22 and 1.23. These processes are also illustrated in Figures Q5-1 and Q5-2 of Reference 1.22. This section summarizes the design process followed for programmable modules and the development process for the firmware or logic within the programmable components.

For design and development of these modules, Rolls-Royce followed the process described in Section 3.3 of this SE. Rolls-Royce Procedure 8 303 687A, "Design Process for Programmable Components for the design of electronic boards" (see Section 3.3), and Rolls-Royce Procedure 8 303 349, "Definition of the Electronic Design Process" are used for the design of the firmware to be embedded in the electronic boards.

Rolls-Royce Procedure 8 303 349, "Definition of the Electronic Design Process," was not docketed. However, in Section 6.2.10 of the LTR and Reference 1.23, Item 33, Rolls-Royce described the firmware development process used for FPGA/CPLD. Specifically, this process consisted of the following steps:

- Specification phase – Rolls-Royce defines the component requirements, features, and constraints (e.g., clock frequency).
- Design phase – using the requirement specification, Rolls-Royce designs the functions to implement the requirements.
- Test definition phase – Rolls-Royce defines validation tests, methods, and tools to be used.
- Coding phase – Rolls-Royce codes the logic.
- Simulation phase – Rolls-Royce performs simulations on the code.
- Synthesis, placement, and routing phase – Rolls-Royce converts the code into the appropriated file to embed in the FPGA/CPLD (e.g., netlist).
- In-situ measurement and testing – After the programmable component is placed on the board, Rolls-Royce performs functional testing of the board to verify the requirements.

- Archiving – file the data for maintenance and modifications.

Rolls-Royce prepared several documents summarizing the design, development, and testing of each board. These documents are identified in Reference 1.22. In addition, Reference 1.22 lists the configuration management documents prepared for each board.

During the regulatory audit (Reference 2.6), Rolls-Royce explained the process described in its document No. 8 303 687A was the original process followed to design and develop these boards. However, after Rolls-Royce implemented its 10 CFR Part 50 Appendix B compliant QA program, Rolls-Royce revised this procedure, and the most current revision is G. In Reference 1.23, Item 34, Rolls-Royce noted that any revision or modification to these boards will follow the current process described in Revision G.

In addition, during the regulatory audit, the NRC staff observed the development processes for logic to be embedded in the FPGA for the ACCG4 component. This FPGA is not part of the SPINLINE 3 platform, however, the processes and documents observed provided sufficient information for the audit team to confirm that the process described in 8 303 687 was properly implemented. The audit team observed that board requirements were traceable down to FPGA requirements. These requirements were used to design, develop, and test the FPGA. After being successfully tested, the FPGA was placed in the board. Then the CPLD/FPGA was re-tested along with the board.

The NRC staff found that the documentation prepared for the FPGA development provided acceptable evidence of the Rolls-Royce development processes.

Similar processes are followed for logic to be embedded in a CPLD and for firmware used in microprocessors or microcontrollers.

Because these modules were not developed in accordance with a 10 CFR Part 50 compliant QA program, Rolls-Royce qualified these modules as part of its CGD for SPINLINE 3 platform, which is described in Section 3.5 of this SE. Furthermore, validation of the firmware included in these boards was part of the validation testing performed for the OSS (References 1.49, 1.50, and 1.51).

The following sections describe the programmable components used, functions included, and implementation of the design process.

3.4.3.1 Actuator Drive Board 32 ACT

This board uses an FPGA to perform the following functions: bus interface, processor interface (registers), surveillance of the outputs (using a short impulse test), and board self-tests. Reference 1.40 describes the components and postulated failures for this board.

During the audit, the NRC staff reviewed the design documents prepared for the 32ACT's FPGA (Reference 2.5). The NRC staff observed that Rolls-Royce prepares a "Master" document with the component technical data, which identifies all design documents associated with the FPGA. In addition, Rolls-Royce prepared a Master document of the module in which the embedded electronic component is installed, which describes all documents that constitute the board's design basis (e.g., requirement specification, schematic, type testing, etc.), and a bill of materials for all components that comprise the module. The audit team observed that for the FPGA development, the FPGA requirement specification contained the requirements for the functions to be implemented in the FPGA. For example, for the 32ACT board, the audit team conducted a thread audit of the watchdog timer function included in the FPGA. The audit team identified the timer requirements and possible failures. With this information, the audit team reviewed the design schematics and observed implementation of this function. After the FPGA was developed, Rolls-Royce tested this function in accordance with a defined FPGA test program specification. The audit team reviewed the test specification, and then reviewed the test report to confirm that that the board met the acceptance criteria of the test program specification. In addition, because the FPGA is installed in the board, the audit team reviewed tests of the FPGA at the board level (integrated on the overall board). The audit team confirmed that these tests were completed successfully. In summary, the NRC staff found that the documentation prepared for the board and the FPGA development were acceptable evidence of the Rolls-Royce development processes.

3.4.3.2 Calibrated Pulse Acquisition Board ICTO

This acquisition board includes an Intel 8031 microcontroller to perform the following functions: Manage and check TIME and COUNT data each acquisition cycle, communicate with the UC25 N+ processor board, provide Ethernet link with two communication points, and perform board self-tests. Reference 1.39 describes the components and postulated failures for this board.

This board was validated during the validation testing performed for the OSS (References 1.50 and 1.51).

3.4.3.3 NERVIA+ Daughter Board

This board includes a Freescale MPC860 and CPLD to perform the following functions: handle communication data processing, run the NERVIA protocol, and perform self-tests. Reference 1.44 describes the components and postulated failures for this board.

During the audit, NRC staff reviewed the development documents for the CPLD installed in the NERVIA+ board (Reference 2.5). The audit team reviewed the documents associated with the CPLD memory management on the NERVIA+ board. This function serves to arbitrate access to the DPM (see Section 3.2.3.2). The audit team reviewed the documentation from the NERVIA+ board including its associated CPLD and traced this requirement in the documentation. The audit team observed the requirement specification included the memory management function, and the design specification included the code for the NERVIA CPLD function. The audit team reviewed the CPLD requirement specification, and observed the specification was properly verified by the V&V team. This document was also reviewed by the QA team. The audit team

reviewed the NERVIA CPLD test specifications and test report, which recorded the successful completion of the tests executed. In particular, the audit team observed the annex of the test report included the test scripts used for performing tests in the simulated environment. The audit team confirmed these tests were completed successfully.

During the audit, the NRC staff found that documentation prepared for the NERVIA+ board and the associated CPLD development provided acceptable evidence of the Rolls-Royce development processes.

3.4.3.4 32ETOR TI SR Module

This module includes a CPLD, which performs the following functions: provide interface between the input groups and the BAP and provide status of each input. The firmware for this board was developed in 1998. Reference 1.36 describes the components and postulated failures for this board.

Section 6.2.10 of the LTR, Rolls-Royce stated that modifications have not been made to this firmware since it was developed, and furthermore, the code was so simple and brief that it could be easily reviewed, if necessary. The NRC staff confirmed this statement by reviewing the code during the audit. In addition, this board was validated during the validation testing performed for the OSS (References 1.50 and 1.51).

3.4.3.5 Analog Input Board 16EANA ISO

This board uses an FPGA to perform the following functions: interface with the bus, interface with the processor (dual ported RAM), control of acquisition (16 inputs in 1 millisecond), processing of the input value for gain and offset adjustment, and board self-test. Reference 1.38 describes the components and postulated failures for this board.

3.4.4 Application Specific Software

According to Rolls-Royce, the application specific software for a SPINLINE 3 platform-based system is developed in accordance with the specifications and requirements established for a plant-specific application. Rolls-Royce personnel will use CLARISSE SSDE to build the plant-specific SPINLINE 3 application software. CLARISSE SSDE and SCADE are not SR software tool. Rolls-Royce plans to use CLARISSE SSDE to design and implement the system architecture and configure the units and networks. In particular, using CLARISSE SSDE, Rolls-Royce personnel create the data structure (i.e., Configuration Tables) used for the interface between the OSS and application software. Because the development of application software is a plant-specific action, an applicant referencing this SE should confirm that the system requirements were properly incorporated using the CLARISSE SSDE tools (see Section 5.2, Item 11).

Communication and data exchange between the OSS and the application software occurs in the UC25 N+ board's RAM data (References 1.4, 1.30, and 1.32). The OSS copies the data required by the application software in the RAM, and unpacks this data for the application software, if necessary. During the design of the application software, Rolls-Royce has the option of linking up data, using packing management process. This process is application dependent and was not evaluated as part of this SE. An applicant referencing this SE should coordinate with Rolls-Royce to establish appropriate parameters for the packing management process to ensure that application specific requirements will be correctly implemented (see Section 5.2, Item 11).

The application software runs as a subroutine within the OSS main program loop. It is executed periodically and sequentially during each program cycle. During each execution, the application software computes its outputs, which are then transferred to the OSS to be transferred to the system peripherals. The OSS also informs the application software of modifications to the system hardware, so data can be managed accordingly when a peripheral device is not working or connected.

3.4.4.1 Application Software Development Process

Digital I&C safety systems must be designed, developed, installed, and tested to quality standards commensurate with the importance of the safety functions to be performed. The development of safety system software should progress according to a formally defined software life cycle. Implementation of an acceptable software life cycle provides the necessary software quality.

Rolls-Royce will develop the application software for a plant-specific application using the SPINLINE 3 platform. The application software will implement plant-specific I&C control and logic functions. Section 6.4 of the LTR describes the proposed system life cycle to design, develop, verify, validate, test, and implement the application software for a plant-specific SPINLINE 3 platform-based system.

Because the LTR does not include a specific plant application, the NRC staff could not review or confirm implementation of the development processes for application specific software. An applicant referencing this SE should confirm that the implementation of the software development processes is conducted in accordance with the processes evaluated by the NRC for the application software (see Section 5.2, Item 11).

3.4.4.1.1 Application Software Plans

In Section 6.4 of the LTR, Rolls-Royce describes the Software Application Plans to be used for SPINLINE 3 platform-based systems. This section identifies how these plans match the software plans identified in BTP 7-14, and explains that even though Rolls-Royce prepared fewer software plans, they still cover all aspects of the plans defined by BTP 7-14 and RG 1.152.

In Reference 1.1, Rolls-Royce submitted templates for the application software plans. These plans represent a template to be used by Rolls-Royce when a plant-specific SPINLINE 3 system is developed. The templates were prepared for the following application specific software plans:

- Software Quality Assurance Plan
- Software Management Plan
- Software Safety Plan
- Software Verification and Validation Plan
- Software Configuration Management Plan
- Software Development Plan
- System Integration and Factory Test Plan
- System Installation and Site Test Plan
- System Operation and Maintenance Plan
- System Training Plan

The NRC staff evaluation is largely limited to a determination regarding whether the SPINLINE 3 platform satisfies the various sections of BTP 7-14. A single general plant-specific action item has been created to address full compliance to each BTP 7-14 section. Although these plans were designed to follow the guidance in BTP 7-14, the information submitted is not sufficiently complete for the NRC staff to evaluate full conformance of these plans to the guidance provided in BTP 7-14 when implemented on the application specific level. Implementation for each specific application must be further evaluated during the application software development process. The NRC staff reviewed these documents, but made no safety determinations on these software plans and, therefore, they are not approved by this SE. While the software plans describe a high-quality process and controls commensurate with the demands of safety at NPPs, the quality and safety of application software will rely heavily on the quality and coverage of test plans executed during the software life cycle process. The effort put in to the development of those test plans is paramount to ensuring the quality of the resultant application software. Thus, it is an application specific action item to confirm that development activities for a plant-specific application were governed by these software plans (see Section 5.2, Item 12).

3.4.4.1.2 Application Software Lifecycle

The LTR describes the software lifecycle to be followed for a plant-specific application. In particular, Figure 6.4-1 in the LTR illustrates the software lifecycle process for the application software. Rolls-Royce will follow a development process based on a “V” shaped lifecycle. The lifecycle is divided onto the following phases:

- Requirements
- Design
- Coding
- Tests and Integration

- Validation

Depending on the plant-specific application, the scope of the lifecycle phases may be modified. Applicant or licensee referencing this topical report is to describe the software lifecycle used for the application software (see Section 5.2, items 11 and 12).

In Sections 6.4.9 and 6.4.10 of the LTR, Rolls-Royce describes the documents that will be prepared to demonstrate proper implementation of the software lifecycle. These planned documents are:

- Safety Analysis Reports – Prepared after each lifecycle phase to demonstrate that no hazards were introduced into the software during that phase and that all software requirements, design, and code elements will not adversely affect safety.
- Verification Report – Summarizes the results of review and audit activities performed during the entire software development process.
- Software Validation Report – Summarizes the results of the tests performed after each release of the software application. This report will describe the anomalies detected and the corrective actions taken.
- Software Configuration Management Report – Summarize changes made to the application software.
- Configuration Management Final Report – Describes the results from performing the activities related to configuration management.
- Software Manufacturing File – Describes the release version of the application software, such as the software manufacturing file.
- Software Require Documents – Describes software requirements resulting from the system requirements. This will include the Software Requirements Traceability Matrix.

Because the LTR does not include a specific plant application, the NRC staff could not review or confirm implementation of the development processes for application specific software. An applicant referencing this SE should confirm the implementation of the software development processes is conducted in accordance with the processes described in the LTR for the application software (see Section 5.2, Item 11).

3.4.4.2 Regulatory Review

Rolls-Royce has committed to follow the design process described in BTP 7-14. In Sections 4.4.5.2 and 6.3 of the LTR, Rolls-Royce provided a comparison of the application software development process against BTP 7-14. However, the application software for a plant-specific application will depend on the system requirements, and thus the scope of the application software is beyond the scope of the LTR and this SE.

An applicant or licensee referencing this SE should provide application specification(s) to define the requirements necessary for the development of the plant-specific application. An applicant

or licensee referencing this SE should confirm that the development of its application software followed a development process consistent with the requirements in BTP 7-14 (see Section 5.2, items 11 and 12).

3.5 Commercial Grade Dedication

The Rolls-Royce SPINLINE 3 platform was originally developed by Data System and Solutions (DS&S) (now Rolls-Royce) for non-U.S. nuclear applications. Although the platform was developed under various European design, development, and regulatory standards in existence at the time, it was not specifically designed and developed to standards for SR digital systems currently endorsed by the NRC. As such, the SPINLINE 3 platform is considered a "commercial grade item" per the definitions of 10 CFR Part 21 and, therefore, must be subjected to a CGD activity prior to acceptance for use in the development of safety related applications for U.S. nuclear power plants. (The NRC staff notes the original development of SPINLINE 3 OSS was performed under the Rolls-Royce MC3 project. Specifically, the software life cycle processes used for the SPINLINE 3 platform resulted from the development of digital safety I&C systems for EdF P4 and N4 fleets. Thus, Rolls-Royce used documents prepared for the MC3 project, because they are applicable to the SPINLINE 3 platform development. In the LTR, Table 6.2-1, Rolls-Royce identifies the evolution of the MC3 software plans and documents applicable to the SPINLINE 3 platform.)

Section 1 of the LTR describes the licensing process followed for the SPINLINE 3 platform by Rolls-Royce to comply with US nuclear regulatory requirements. In particular, per 10 CFR Part 21, the dedication process must be conducted in accordance with the applicable provisions of 10 CFR Part 50, Appendix B. Rolls-Royce I&C France performed the role of the dedicating entity for the SPINLINE 3 platform. In preparation for this dedication effort, Rolls-Royce I&C France upgraded its internal processes (including QA program and procedures) to comply with 10 CFR Part 50, Appendix B. In addition, Rolls-Royce I&C France had audits performed by third-party firms Global Quality Assurance (GQA) (Reference 1.67) and MPR Associates (MPR) (Reference 1.58).

The NRC Quality and Vendor Branch (CQAB) reviewed these third-party audit reports. CQAB also discussed the audit conducted by GQA with the lead GQA auditor. The CQAB observed that the scope of the GQA audit was the design and manufacturing controls of safety I&C systems for the SPINLINE 3 platform work done by DS&S (now Rolls-Royce). Although DS&S did not have a QA manual compliant with 10 CFR Part 50 Appendix B (Appendix B), the project was conducted under the DS&S Quality Management Plan, Revision N, dated June 2008. The Quality Management Plan was structured to meet the requirements of the International Organization for Standardization (ISO) 9001-2000 Quality Management System, with the inclusion of additional requirements to address meeting the intent of Appendix B. The GQA audit was performance based and addressed all relevant Appendix B requirements and review of the implementation. No deficiencies were noted.

As mentioned above, a second audit was conducted by MPR, which was summarized in its Design Analysis Report (DAR) (Reference 1.58). The focus of the DAR was the documented evidence for the SPINLINE 3 platform software design and software life cycle processes to ensure an adequate technical basis would exist for dedication of the platform software. Additionally, MPR reviewed the EQ plan and plant-specific application software life cycle plans to ensure compliance with NRC requirements. MPR identified several recommendations, but no deficiencies were identified.

CQAB determined there was sufficient documented evidence to indicate that GQA and MPR had performed adequate audits of DS&S's quality programmatic controls for the design and manufacturing processes to develop a technical basis for the dedication of the SPINLINE 3 platform. However, Rolls-Royce is not currently on the Nuclear Procurement Issues Committee (NUPIC) list or included on an applicant's approved vendor List. Therefore, an applicant referencing the approval for this topical report must confirm that Rolls-Royce is currently on the NUPIC list and/or confirm that Rolls-Royce's quality processes conform to the applicant's Appendix B program – i.e., be put on the applicant's Approved Vendor List (see Section 5.2, items 14).

The regulation at 10 CFR 50.55a(h) requires protection and safety systems to comply with IEEE Std. 603-1991. IEEE Std. 7-4.3.2 provides further detail regarding application of IEEE Std. 603 criteria to digital systems. RG 1.152, Revision 3 endorses IEEE Std. 7-4.3.2-2003 as providing acceptable guidance for use of computers in safety related systems. Clause 5.4.2 of IEEE Std. 7-4.3.2-2003 provides elaboration of the IEEE Std. 603-1991 criteria as it should be applied to qualifying existing commercial digital systems. EPRI TR-107330 and EPRI TR-106439 reports were developed to provide more detailed guidance on the CGD of digital systems. These EPRI reports were reviewed by NRC in SEs issued July 30, 1998 (ADAMS Accession No. ML12205A265) and July 17, 1997 (ADAMS Accession No. ML092190664), respectively, as being appropriate for use in CGD for digital systems. It is noted that RG 1.152, Revision 3, also provides a pointer to EPRI TR-106439 as containing adequate guidance for CGD of computers for safety systems. Appendix 7.0-A of the NRC SRP (NUREG-0800) also identified EPRI TR-106439 as providing an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications. EPRI TR-106439 references several of the verification methods described in EPRI NP-5652 ("Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07)" June 1998) as being appropriate for supporting CGD.

In Section 1 of the LTR, Rolls-Royce identified use of the CGD guidance contained in EPRI TR-107330 and EPRI TR-106439. In addition the LTR describes the strategy that Rolls-Royce followed to qualify and accept the SPINLINE 3 platform under its 10 CFR Part 50, Appendix B compliant program. This strategy was defined in Rolls-Royce Quality Procedure – Commercial Dedication (Reference 1.47). This quality procedure defines the dedication process to be used by Rolls-Royce. In particular, this quality procedure requires preparation of a CGD plan and a CGD report to show compliance with EPRI TR-16439. In addition, this quality procedure identifies the roles and responsibilities for the Rolls-Royce personnel responsible for the

dedication process of commercial products. Thus, to support the dedication process for the SPINLINE 3 platform, Rolls-Royce prepared (and submitted) a CGD plan (Reference 1.68), a CGD report (Reference 1.69), and a compliance matrix with EPRI TR-16439 (Reference 1.70). Reference 1.69 documents the results from the dedication activities and acceptance of the SPINLINE 3 platform. Reference 1.70 documents the implementation of the plan and provides references to records that support CGD findings; in particular, it summarizes the results of the assessment for the critical characteristics of the SPINLINE 3 platform in accordance with EPRI TR-106439. Further, Table A-1 of this document provides a mapping of the attributes of CGD identified in EPRI TR-106439 to Rolls-Royce documents that address each requirement and/or activities performed by Rolls-Royce necessary to complete the dedication effort. When discrepancies between Rolls-Royce processes and documents and EPRI TR-106439 were identified, Rolls-Royce described, evaluated, and resolved them in Appendix B of Reference 1.70. Rolls-Royce also supplied additional information regarding its dedication process in Reference 1.22.

In response to discussions with NRC staff regarding Rolls-Royce's approach to use of the various EPRI NP-5652 critical characteristic verification methods, Rolls-Royce submitted a compliance matrix document (Reference 1.70) to more clearly illustrate its CGD approach. NRC staff reviewed this document as a supplement to the other information provided with the LTR to evaluate the acceptance of the SPINLINE 3 platform for safety related applications.

As previously noted, the Rolls-Royce SPINLINE 3 platform LTR describes a generic platform upon which digital safety applications can be developed. Because the application software and hardware configuration will be application specific, the scope of the dedication activities is limited to the SPINLINE 3 platform hardware and operating system software residing on the platform. Any application that may be developed using the SPINLINE 3 platform would need to be reviewed on an application-specific basis (see Section 5.2, Item 3).

In the LTR and References 1.69 and 1.70, Rolls-Royce stated that after the SPINLINE 3 platform was dedicated, it would be maintained under its 10 CFR Part 50, Appendix B compliant QA program. Furthermore, Rolls-Royce noted that if new boards are developed, or existing boards are modified, these activities will be performed in accordance with its Appendix B program and existing life cycle processes. Also, the components will be tested and qualified to maintain EQ to US standards.

Based on the information provided, the NRC staff found the hardware and software comprising the SPINLINE 3 platform, and described in the LTR, were properly dedicated and accepted into its 10 CFR Part 50, Appendix B compliant program (Rolls-Royce SAS Quality Manual). In addition, the NRC staff found the software life cycle for the OSS followed a rigorous development and software plans.

The following sections summarize the dedication and verification methods employed by Rolls-Royce, the results from these activities, and NRC staff evaluation of such activities.

3.5.1 Identification and Verification of Critical Characteristics

The LTR states the SPINLINE 3 platform is comprised of the software described in Section 3.4 and the hardware components described in Section 3.2.1 of this SE. These elements represent the scope for dedication activities that Rolls-Royce performed to dedicate and qualify the SPINLINE 3 platform. As mentioned before, Rolls-Royce used the CGD guidance contained in EPRI TR-107330 and EPRI TR-106439. Both EPRI-106439 and IEEE Std. 7-4.3.2-2003 provide guidance on the types of critical characteristics that need to be identified and verified for CGD of digital systems. These characteristics can be categorized into three groups: physical, performance and dependability. Rolls-Royce's dedication report makes use of these categories. Below is a summary of the information provided by Rolls-Royce and evaluated by NRC staff.

3.5.2 Critical Characteristics – Physical

Per the guidance in EPRI TR-106439 and IEEE Std. 7-4.3.2-2003, critical physical characteristics of the digital system should address the size, mounting, power requirements, hardware model number, software version number and data communications of system components. EPRI TR-106439 further notes that "special tests and inspections" (i.e., Method 1 per EPRI NP-5652) is typically appropriate for verifying these characteristics.

According to the Rolls-Royce CGD plan and report, the MCL (Reference 1.29) identifies the product and part information for the hardware and software components of the SPINLINE 3 platform. The NRC staff reviewed Revision G of the MCL document and noted the following:

- Table A-1 in the CGD report (Reference 1.69), identifies Revision A of the MCL. The NRC staff did not review this revision because Rolls-Royce docketed revisions D and G. The NRC staff compared Revision D and G and found that the revisions to updated documents identified information submitted to the NRC and included documents prepared to address issues encountered during EQ testing (e.g., Investigation Results of 2011 Qualification Tests).
- Table 3.1 of the MCL document lists each hardware item that is part of the system, along with a part number and revision identifier (if applicable). The equipment listed in the table maps to the hardware identified as being part of the SPINLINE 3 platform in Section 4.3 of the LTR (Reference 1.4). The NRC staff was able to match the equipment in the SPINLINE 3 topical report to items in Table 3.1; however, the NRC staff review of the list did not initially identify parts associated with the 8PT100 input terminal block or PCI NERVIA+ board. Rolls-Royce Reference 1.22 provides a pointer to the appropriate 8PT100 parts in the MCL. Rolls-Royce also clarified in its RAI response that PCI NERVIA+ board is not considered part of the "qualified" system and is thus not listed in the MCL. The PCI NERVIA+ board was not part of the NRC staff review.

- Table 3.2 of the MCL document contains identification (e.g., version numbers) for the software that Section 4.4 of the LTR identifies as being part of the SPINLINE 3 system and within the topical report scope. (Note: The software development environment tool (i.e., CLARISSE SSDE) is noted as being vital to application development for the SPINLINE 3 platform. However, since this tool is not part of the fielded platform, it is not included in the MCL) The NRC staff was able to match the items found in Table 3.2 to software described in the SPINLINE 3 topical report, with the exception of TS1 and TS2. Rolls-Royce Reference 1.22 clarifies the TS1 and TS2 manufacturing files that correspond to the Test Specimen application software used in the two processors for EQ testing.

Per the Rolls-Royce CGD report, Rolls-Royce I&C France has taken credit for an internal QA procedure and configuration management process, as well as an internal QA audit, to verify the SPINLINE 3 documentation is accurate and under appropriate version control. During the regulatory audit (Reference 2.5), the NRC staff interviewed Rolls-Royce staff and reviewed the Rolls-Royce records associated with the internal QA audit. The NRC staff found the Rolls-Royce internal audit was reasonably thorough and had captured 16 discrepancies. Rolls-Royce maintained a spreadsheet of the discrepancies and all follow-up actions taken to resolve them. The NRC staff noted no significant discrepancies among the 16 identified.

Appendix B of the LTR contains the equipment data sheets which describe the physical characteristics of the SPINLINE 3 hardware. The NRC staff reviewed the equipment data sheets in Appendix B and found that they provided a brief description of each component and its function and clearly identified size, weight, power requirements, electrical protective features, part numbers, permissible environmental conditions, and LED indications (if present). The NRC staff noted the power supply chasses were identified in the appendix, however, its associated equipment data was not included. Rolls-Royce Reference 1.22 provides three power supply component part number corrections and the manufacturer technical datasheets. The NRC staff also noted that in the equipment data sheets for the 10 Megabytes per second Ethernet Hub: 3TP/2FL, the TP/FL converters and MICROSENS TP/FL Converter lacked any environmental parameters for the equipment. Rolls-Royce Reference 1.22 states that the environmental qualification testing was being used to formally establish those parameters. Per the dedication report, the data contained in the topical report constitutes completion of the dedication activity associated with identifying the physical characteristics of the hardware and interface devices. The NRC staff concluded based upon the review of the documentation described above that Rolls-Royce has reasonably identified the critical physical characteristics for the SPINLINE 3 components.

During the regulatory audit of the Rolls-Royce Grenoble facility (Reference 2.5), NRC staff witnessed Rolls-Royce's receipt and handling of incoming parts – both mechanical and electrical. The processes were observed to be both thorough and disciplined. Checklists were used to ensure a complete inspection of each incoming parts delivery. Documentation providing technical details on each incoming part was readily available. The Rolls-Royce facility also

featured a locked, non-conforming parts area to “quarantine” any suspect parts. Based upon the audit results, the NRC staff concluded Rolls-Royce takes reasonable measures to assure that procured components of the SPINLINE 3 platform meet the identified critical physical characteristics.

Based on the data presented above, the NRC staff concluded that Rolls-Royce has identified and verified critical physical characteristics associated with the Rolls-Royce SPINLINE 3 platform in a fashion that is consistent with the guidance of EPRI TR-106439 and IEEE Std. 7-4.3.2-2003. In addition, the NRC staff observed that Rolls-Royce’s processes at its Grenoble facility provide reasonable assurance that parts received will conform to the critical physical characteristics required for platform performance.

3.5.3 Critical Characteristics – Performance

Per the guidance on EPRI TR-106439 and IEEE Std. 7-4.3.2-2003, performance characteristics are the functionality required from the device, as well as the performance attributes associated with that functionality. Performance characteristics may include items such as response time, memory allocation, reliability, required embedded functions, and environmental qualification requirements. In addition, failure management and “must-not-do” functions are also considered performance characteristics for digital systems. EPRI TR-106439 further notes that “special tests and inspections”, commercial grade surveys and supplier/item performance record (i.e., Methods 1, 2 and 4 per EPRI NP-5652) are typically appropriate for verifying these characteristics.

The Rolls-Royce CGD report (Reference 1.69) states:

> The dedication process uses a combination of three acceptance methods described in EPRI TR-106439 to verify the adequacy of the SPINLINE 3 platform:
>
> - Method 1 — Special Tests and Inspections of the SPINLINE 3 equipment
> - Method 2 — Commercial Grade Survey of the SPINLINE 3 hardware and software development processes
> - Method 4 — Acceptable Performance Record of the SPINLINE 3 platform

According to both the Rolls-Royce CGD plan and report, the performance characteristics are described at a high level in the LTR (Reference 1.4) and at a detailed level in the software requirement specification (Reference 1.30), software design document (Reference 1.31,) and software interface specification (Reference 1.32).

The NRC staff reviewed the referenced topical report sections and other referenced documents and noted the following:

- Since the scope of this review addresses only the SPINLINE 3 platform and not a specific application, the critical performance characteristics are viewed with that perspective.
- The Rolls-Royce SPINLINE 3 platform topical report does not contain a specific physical architecture for a system channel, so the identification of performance characteristics is focused on basic component capabilities and the ability of components to function together (see Section 5.2, Item 3).

Below is the NRC staff's evaluation of Rolls-Royce's use of EPRI NP-5652's verification Methods 1, 2, and 4 to confirm the acceptability of the SPINLINE 3 critical performance characteristics as part of its CGD effort.

3.5.3.1 Special Tests and Inspections (Method 1)

Per EPRI NP-5652, Method 1 consists of special tests and inspections applied to commercial grade items. These tests and inspections should be focused on verification of the critical characteristics identified for the item.

Rolls-Royce's CGD report (Reference 1.69) concluded that the validation testing (Reference 1.51) performed as part of the SPINLINE 3 development was of sufficient quality such that only hardware qualification testing need be performed to support the CGD effort, as well as to satisfy US regulatory requirements for hardware qualification. The basis for the conclusion was given as the rigor of the software and firmware development processes, the quality of the development documentation and validity of the results obtains (Reference 1.22). Since Rolls-Royce chose to take substantial credit in its CGD for its development processes and documentation generated at the time of SPINLINE 3 development, NRC staff spent additional review effort on its findings relative to Method 2 below.

The NRC staff's evaluation of the SPINLINE 3 EQ testing performed in support of CGD is found in Section 3.6 of this SE. In general, the EQ testing showed that SPINLINE 3 did not fully comply with EPRI TR-107330 requirements for seismic, EMI/RFI, and ESD, but met the criteria for the remaining qualification tests. The specific limitations are detailed in Section 15 of the "Summary Equipment Qualification Test Report" (Reference 1.78).

The NRC staff concluded this approach was acceptable, given the adequacy of their validation test plan, which is addressed in the section below, and the adequacy of their EQ testing, which is addressed in Section 3.6 of this SE.

3.5.3.2 Commercial Grade Survey (Method 2)

Per EPRI NP-5652, Method 2 consists of evaluating and crediting the quality controls on the development and manufacturing a commercial grade item. EPRI NP-5652 specifically notes that "Maximizing reliance on the supplier's controls will minimize the need to augment

acceptance with Method 1 upon receipt." These critical characteristics of the item must be controlled by the quality system in place.

As was noted previously, the SPINLINE 3 platform was not originally developed to standards currently endorsed by the U.S. NRC. However, as is noted in the LTR (Reference 1.4), the SPINLINE 3 platform was originally "designed, qualified, and manufactured to meet European nuclear safety and quality standards." In particular, the LTR indicates that the platform software life cycle processes were established to be consistent with the guidance of IEC 880-1986.

To support its case that its development approach was sufficiently disciplined to support CGD, Section 3 of the LTR provides a summary of Rolls-Royce's assessment of the SPINLINE 3 platform's compliance with NRC regulations, RGs, and endorsed standards. This section summarizes the results of comparing the software development process followed for SPINLINE 3 platform to the processes endorsed by BTP 7-14.

Rolls-Royce included a number of US industry processes standards, regulations, and guidance that are not specific to software development for which full compliance could not be determined on the basis of the platform alone. Therefore, the NRC staff could not fully evaluate these items, which will be subject to application specific review.

Appendix A of the LTR provides a detailed mapping of the SPINLINE 3 platform compliance to NRC-endorsed standards for software development – specifically quality assurance, configuration management, and V&V. Section 2.2 of Rolls-Royce's critical characteristic assessment report (1.70) provides an expanded description of Rolls-Royce's approach to use of Method 2 for verifying critical performance characteristics of the SPINLINE 3 platform. This information helped facilitate the NRC staff's review of these programmatic areas.

Rolls-Royce took significant credit for purposes of CGD for the quality of its original development processes of the SPINLINE 3 platform. Specifically, Rolls-Royce's LTR and CGD documentation explained that additional testing of critical performance characteristics under Method 1 was not considered necessary, as the quality of its original testing (and subsequent regression testing) was appropriately rigorous and still applicable to the current software. In the evaluation of this position, NRC staff reviewed several of Rolls-Royce's key process documents that governed the design, development and testing of the original SPINLINE 3 platform, in particular information related to OSS and software and firmware embedded in several components. Section 6.3 of the LTR provides a comparison between IEC 880-1986 and BTP 7-14, and discusses how the SPINLINE 3 platform software life cycle process and, as a result, the evaluations, reviews and analyses and ensuing documentation achieved equivalent results to those that would be attained using the guidance in BTP 7-14. The alignment of the SPINLINE 3 platform software life cycle documentation to the software plans described in BTP 7-14 is shown in Figure 6.3-1 of the LTR.

Since the scope of the CGD is on the SPINLINE 3 platform, the NRC staff focused on the BTP 7-14 documents for planning, implementation, and design outputs that would best ensure successful platform development.

3.5.3.2.1 Software Lifecycle Process Planning and Implementation

IEEE Std.603-1991 requires that the quality of components and modules be established and maintained in accordance with a QA program. IEEE Std.7-4.3.2-2003 amplifies this requirement for software quality. SRP BTP 7-14 describes the basis for accepting software for safety functions as including confirmation that acceptable plans were prepared to control software development activities.

SRP BTP 7-14, Section B.2.1, "Software Life Cycle Process Planning," identifies the software life cycle planning information subject to review in terms of the Software Plans. SRP BTP 7-14, Section B.2.2, "Software Life Cycle Process Implementation," identifies software documents and products subject to review to evaluate whether the software life cycle development process produced acceptable design outputs.

The NRC staff reviewed Rolls-Royce documents to ensure that they established a reasonable match to expectations outlined in BTP 7-14. The NRC staff noted all of the design phases and associated documentation described in BTP 7-14 are not provided as a result of the SPINLINE 3 platform software life cycle process, because they aligned with IEC 880. Rolls-Royce considered that missing design phases and associated documentation are accounted for through the process of combining certain life cycle phases, including the associated documentation. In addition, the NRC staff noted that several of the BTP 7-14 documents are more suited to development of applications, rather than platform development. The documents to be developed for a plant specific application were not evaluated by the NRC staff in this SE. These plans are:

- Software Installation Plan
- Software Training Plan
- Software Operation Plan

The SPINLINE 3 Platform software documents evaluated by the NRC staff, as well as its alignment to BTP 7-14, are described in the following subsections.

3.5.3.2.1.1 Software Quality Assurance Plan

Section B.3.1.3 of BTP 7-14 describes the review criteria for software QA plans. BTP 7-14 points out that Clause 5.3.1 of IEEE Std. 7-4.3.2-2003, which is currently endorsed by RG 1.152, Revision 3, contains guidance on software quality assurance. Clause 5.3.1 states, in part, that IEC 880 -1986 contains guidance on development of software QA plans. The MC3

project software quality plan (Reference 1.72, Section 2.1) identifies IEC 880-1986, which is an older, alternate identifier for IEC 880 – 1986, as a reference document for the project. (i.e., the SPINLINE 3 reference matches the IEC standard endorsed in IEEE Std. 7-4.3.2-2003.) The guidance in IEC 880 calls for the software quality plans to identify technical procedures for each phase of the software life cycle, identify methods, languages, tools, rules and standards used, identify provisions for tracking of quality issues, generation of quality records, and documentation of verification activities. The NRC staff review in this area focused on these quality assurance provisions of IEC 880.

Figure 6.3-1 of the LTR aligns this plan with the following parts of BTP 7-14: Software Management Plan, Software Quality Assurance Plan, and Software Development Plan.

The NRC staff notes the original development was not done under a 10 CFR Part 50, Appendix B quality plan as would normally be expected per BTP 7-14, which is why SPINLINE 3 is undergoing CGD.

The NRC staff reviewed the English translation of the original software quality plan (Reference 1.72) for the MC3 project, which was originally issued in November 1993, and evaluated its adherence to the guidance of IEC 880. Although the quality manual itself does not describe technical procedures in great detail, the NRC staff observed that Section 9.3 specifically identifies internal company processes, procedures and directives for use on the project. In addition, Section 5.3 does contain very specific inputs and outputs required for each lifecycle phase, as well as criteria to be met prior to advancing to subsequent lifecycle phases.

Section 9 of the quality manual specifically addresses the IEC 880 criterion for identification of methods, tools, software languages, and rules.

The NRC staff identified provisions for tracking of quality issues in Section 8 of the quality plan. The NRC staff also reviewed several examples of Rolls-Royce's follow-up on issues identified as non-conformances during the regulatory audit (Reference 2.5) and found those processes to be appropriately thorough.

Section 10 of the quality plan describes quality assurance activities and identifies quality records generated during the development. Documentation requirements for the MC3 project, which includes verification and validation activity records, are specifically identified in Section 6 of the quality plan.

The NRC staff also noted that Section 7 of the software quality plan described configuration management associated with the development effort. The NRC staff review of those provisions is discussed below.

Rolls-Royce submitted Software Modification Quality Plan (Reference 1.74) to describe the modifications made after the MC3 project. This quality plan establishes the process to manage evolution of software included in the SPINLINE 3 platform (e.g., OSS, NERVIA+ board software,

CLARISSE, etc.). In particular, this plan describes the process to modify SPINLINE 3 software, as well as management structure, activities (including validation tests) and responsibilities to perform such modification. This process also takes into consideration that a change to software embedded in an electronic component (e.g., CPLD in the NERVIA+ board) would affect other components and the system, thus requiring a modification plan to address them. In this document, Rolls-Royce noted that a software development plan will be created for each upgrade.

Based upon review of the software quality assurance provisions in the provided documentation, the NRC staff finds that reasonable quality controls are in place to support Rolls-Royce's CGD conclusions.

3.5.3.2.1.2 Software Development Plan

Section B.3.1.2 of BTP 7-14 describes characteristics expected of a software development plan for digital system development activities. The BTP indicates that the use of the software development plan should result in "a careful and deliberate development process which will result in high-quality software". Based on the BTP guidance, the NRC staff review focused on the definition of the development organization, identification of project risks, definition of lifecycle phase inputs and outputs, identification of methods and tools to be used, and identification of standards being followed.

Figure 6.3-1 of the LTR aligns this plan with the following BTP 7-14 provisions: Software Management Plan, Software Quality Assurance Plan, and Software Development Plan.

The NRC staff notes that the original development of SPINLINE 3 OSS was performed under the MC3 project. Thus, references that refer to the MC3 project are applicable to the SPINLINE 3 development.

As was noted above, the software development process for the OSS was not performed under a 10 CFR Part 50, Appendix B program. Table 6.2-1 of the LTR identifies the evolution of the SPINLINE 3 OSS software documents, and its revisions. Thus, the NRC staff reviewed an English translation of the original software development plan (Reference 1.71) for the MC3 project, which was issued in April 1994. The plan describes the overall project including major sub-projects, the methods and tools to be used, the resources applied to the development, schedules, budgets, and an assessment of project risks. The plan does not map exactly to the BTP 7-14 Software Development Plan acceptance criteria; however, the NRC staff observed that it describes a careful and deliberate development process. The software development plan primarily focuses on the development organization, working relationships, schedules and budgets for the development.

Assessment of risks to software development is specifically identified as an acceptance criterion for software development plans in BTP 7-14. For the SPINLINE 3 software development, risks

are specifically addressed in Section 8 of the document. The NRC staff finds that this is a reasonable treatment of identification of project risks.

BTP 7-14, Section B.3.1.2 also identifies discussion of tools, standards and internal oversight activities for the development. For SPINLINE 3, the software development plan references other program documentation (i.e., the MC3 software quality plan) for details on these facets of development.

The NRC staff reviewed the MC3 software quality plan (Reference 1.72) and observed that it defines the project organization, industry standards used in development, and the software development lifecycle. The description of the software lifecycle includes inputs and outputs of each phase, as well as conditions / criteria that would need to be met prior to moving to the next stage of development.

Project documentation is further defined in the software quality plan, along with the responsible parties for authoring, checking and approving each document. Section 9 of the software quality plan contains details of the methods and tools to be used for the software development effort. The methods elaborate on the products and activities contained in the life cycle phases identified earlier in the document. The rules include references to internal procedures on design control, team member training, software programming rules, and V&V. The project software quality plan (Reference 1.72, Section 2.1) identifies IEC 880 – 1986 as one of the primary reference standards for the project.

The NRC staff found the various documents governing the development planning activities for the SPINLINE 3 software contribute to a careful and deliberate development environment.

3.5.3.2.1.3 Software Configuration Management Plan

The acceptance criteria for software configuration management plans (SCMPs) is contained in SRP BTP 7-14, Section B.3.1.11, “Software Configuration Management Plan (SCMP),” and Section B.3.2.3, “Acceptance Criteria for Software Configuration Management Activities.” These sections state that both: (1) RG 1.173 that endorses IEEE Std. 1074-1995, Clause A.1.2.4, “Plan Configuration Management,” and (2) RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” that endorses IEEE Std. 828-1990, “IEEE Standard for Configuration Management Plans,” provide an acceptable approach for planning configuration management. SRP BTP 7-14, Section B.3.1.11 further states that additional guidance can be found in IEEE Std. 7-4.3.2-2003, Clause 5.3.5, “Software configuration management,” and in Clause 5.4.2.1.3, “Establish configuration management controls.” NUREG/CR-6101, Section 3.1.3, “Software Configuration Management Plan,” and Section 4.1.3, “Software Configuration Management Plan,” also contain guidance.

Figure 6.3-1 of the LTR aligns this plan with the following BTP 7-14 topic: Software Configuration Management Plan.

Since the original software development process for the OSS was not performed under a 10 CFR Part 50, Appendix B program, the NRC staff reviewed an English translation of the original software quality plan (Reference 1.72) for the MC3 project, which was issued in November 1993 and revised in September 1997. Section 7 of this plan addresses configuration management activities, including the purpose, responsibilities, a list of configuration elements, and procedures for element identification and entry into configuration control.

Section 6 of the software quality plan describes documentation requirements for the MC3 project. This section indicates the responsible individuals, who should author, check, and approve project management documents and technical documents related to the production and use of the software.

During the regulatory audit (Reference 2.5), the NRC staff observed Rolls-Royce's use of configuration management tools to control access to documents and software files, manage change requests, and track changes. The NRC staff also reviewed configuration management guidance documents and procedures. The NRC staff's observations during the audit support a finding of reasonable assurance that appropriate configuration management activities are being performed.

Based upon review of the provided documentation, as well as the results of the regulatory audit, the NRC staff finds that reasonable configuration management controls were in place during, and have been maintained throughout, the SPINLINE 3 software development.

3.5.3.2.1.4 Software Safety

The acceptance criteria for a software safety plan (SSP) are contained in SRP BTP 7-14, Section B.3.1.9, "Software Safety Plan (SSP)" and Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." These sections state that the SSP should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101, Section 3.1.5, "Software Safety Plan," and Section 4.1.5, "Software Safety Plan," contain guidance on SSPs. RG 1.173, Section C.3, "Software Safety Analyses," contains guidance on safety analysis activities while NUREG/CR-6101 also addresses guidance for these analyses.

Figure 6.3-1 of the LTR aligns this plan with the following BTP 7-14 topic: Software Safety Plan. This figure also shows software safety was described in the following Rolls-Royce Documents:

- SPINLINE 3 Safety of Processing Unit Software, Document 1 207 228 G (Reference 1.34)
- Analysis of Consequences of Errors (in Hardware Configuration Tables), Rolls-Royce Document 1 207 184

- Functional FMEA documented in Software Requirement document of LDU, Rolls-Royce Document 1 207 142

The NRC staff notes Rolls-Royce did not prepare a separate safety plan. However, Rolls-Royce captured the concepts of software safety in other plans. For example, the NRC staff reviewed Reference 1.34, which describes the overall testing strategy for the OSS. Further, this plan identifies the software test plan aimed at validating system performance in response to failures, which then would become objective evidence that the SPINLINE 3 OSS was originally developed with consideration of error handling. Therefore, Rolls-Royce identified requirements analysis, design analysis, code analysis, safety test analysis, and change analysis. Furthermore, the software safety requirements analysis for the OSS and embedded logic/firmware focused on identifying any necessary hardware/software development and determining means, such as existing or new platform safety design characteristics or platform architectural approaches, to mitigate the applicable abnormal conditions and events.

The NRC staff concluded that Rolls-Royce's provisions for software safety supported Rolls-Royce's findings on CGD.

3.5.3.2.1.5 Software V&V

The acceptance criteria for software V&V plans (SVVPs) are contained in SRP BTP 7-14, Section B.3.1.10, "Software V&V Plan (SVVP)." This section states that RG 1.168, Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the NRC staff for meeting the regulatory requirements as they apply to V&V of safety system software. RG 1.168 specifically notes that software to be used in safety systems should be assigned integrity level 4, as defined in IEEE Std. 1012-1998. The review guidance emphasizes independence of the review organization, the quantity and quality of V&V staff and documentation of V&V activities. The NRC staff review focused on the above noted aspects of V&V.

Figure 6.3-1 of the LTR aligns this plan with the following BTP 7-14 topic: Software V&V Plan and Software Test Plan.

Table 3.8-9 of Appendix A of the LTR states the original development of the platform software on the MC3 project (which resulted in the SPINLINE 3 platform) did not feature a single document describing the V&V plan for the development. The V&V provisions are described in a number of other original project documents, including the quality plan (Reference 1.72), the software validation test plan (Reference 1.50), and a technical instruction on rules for V&V (Reference 1.73).

Section 4 of the MC3 software quality plan depicts the organization chart in place during original system development and describes the responsibilities of the various managers. The V&V

manager did not report to the MC3 software project manager. The V&V manager and software project manager are shown both reporting to the Business Software Group. (Note: the plan shows the V&V manager is also independent from the QA manager and the Quality Department.0 The software project manager's responsibilities do not include any aspects of V&V, other than specifically defined participation in validation activities. The V&V manager's responsibilities include scheduling and monitoring of V&V activities, which include verification of documents associated with safety class software, verification of components, authoring software test and validation documents, and defining validation test cases. Based upon the review of the original project organization and the responsibilities defined for the development organization, the NRC staff finds there is reasonable assurance the V&V organization possess the necessary independence to effectively perform its activities.

In Reference 1.23, Rolls-Royce provided clarification of the differences in V&V activities between these original processes and the current SPINLINE 3 processes to ensure the original controls provided equivalent independence for V&V activities. Rolls-Royce responded (Reference 1.23) that tasks performed for V&V were equivalent to the tasks contained in its current plans and procedures.

Section 5.1 of the MC3 software quality plan depicts the software development life cycle. Verification activities are shown occurring during the specification, preliminary design, detailed design and implementation (i.e., coding) phases of development. Specific unit, integration, and validation testing phases are also shown. The plan section further states that "documents and code for safety class software are subject to verification by an independent team." Section 5.3 of the plan describes the phases in greater detail, including all the documentation subject to verification and validation test documents required before subsequent phases may be entered. Section 6 lists the documents to be generated as part of the development and identifies the responsible author, reviewer / verifier, and approval authority.

During the regulatory audit (Reference 2.5), the NRC staff examined several requirements threads, which entailed reviewing board specific requirements, design, implementation, test planning and test report documentation. In each requirements thread, the NRC staff specifically noted that all documentation was signed by appropriate personnel, including members of the V&V organization, in accordance with Rolls-Royce processes. The NRC staff noted that a representative of the V&V organization had signed an original code walk-through, which is objective evidence that appropriate verification activities had occurred in the initial implementation (i.e., coding) life-cycle phase.

Based upon the organization in place at the inception of the SPINLINE 3 system, the processes and products defined for each software life-cycle phase, and evaluation of SPINLINE 3 during the regulatory audit, the NRC staff concludes that there is reasonable assurance that appropriate V&V was provided during the original development of the SPINLINE 3 platform.

Section B.3.1.12 of BTP 7-14 contains review guidance for software test plans. Pointers are provided to the endorsements in RGs 1.170 and 1.171. Among the key attributes expected of a

software test plan are description of the test organization(s), testing strategy, testing criteria and testing records. The NRC staff review focused on the clarity and completeness of the validation test plans, with specific emphasis on the treatment of error handling / fault management functions.

Reference 1.34 describes the overall testing strategy for the OSS. Specifically, this document describes the different level tests performed. These tests included test of each OSS module, integration tests, and validation tests. In addition Reference 1.50 describes the procedures, activities, and techniques followed to develop the MC3 (now SPINLINE 3) OSS.

In Section 2 of the Reference 1.34 document, the OSS functions are identified, and the tasks subject to validation are listed. The NRC staff found this section to be a thorough evaluation of the software's functions.

Section 4 uses the information of section 2 to design the validation tests to be performed. The NRC staff also noted that section 4.4 also identifies certain tasks that were verified during unit testing and, thus, did not require specific re-testing. During the regulatory audit (Reference 2.5) of Rolls-Royce's Grenoble facility, the NRC staff performed several thread audits. In each thread audit, the NRC staff reviewed verification testing plans and reports associated with specific boards. The NRC staff found this unit testing documentation to be in good order during the audit and found that it was reasonable that certain functions were not re-tested during system validation.

Section 4.5 of the software test plan contains specific descriptions of the tests to be performed, the functions to be checked during each test and the points to be verified for each function. Of particular note to the NRC staff is that the software test plan includes tests that specifically address the OSS's response to error conditions. As was noted earlier in this section, EPRI TR-106439's guidance on CGD identifies failure management and "must-not-do" functions to be critical performance characteristics for digital systems. The NRC staff finds that specific tests in the software test plan aimed at validating system performance in response to failures are objective evidence the SPINLINE 3 OSS was originally developed with consideration of error handling as a critical characteristic.

Section 5 of the software test plan provides a mapping between the OSS functions of Section 2 and the tests to be performed in section 4 to ensure adequate coverage. Section 6 identifies regression tests to be performed following any upgrade to the OSS. Sections 7 through 10 discuss specific OSS upgrades performed since initial OSS development and analyze the need for any specific tests beyond those identified in Section 6. In the LTR, Table 6.2-1, Rolls-Royce identified the evolution of the MC3 software plans applicable to the SPINLINE 3 platform.

Rolls-Royce also prepared a software validation test plan (Reference 1.50) and software integration test plan and report (Reference 1.49). Reference 1.50 describes the OSS validation test analysis for safety class application. This plan defined the strategy to check that the OSS operates in accordance with the requirements specified in Reference 1.30. Reference 1.49

describes the integration tests performed to ensure that mutual relations among software modules, and relations between these modules and the target hardware meet the requirements and design. This document also describes the test strategy and test configuration, as well as the results observed during integration of the system.

The NRC staff noted that specific discussion of the testing organization and records to be generated was not in the software test plan. However, the MC3 software quality plan (Reference 1.72) specifically identifies the V&V manager as responsible for software test and validation documentation, verification of software components and definition of test cases for software. In addition, the software development life cycle in the original software quality plan identifies specific phases for both unit testing and validation. As noted earlier in this portion of the SE, Section 5.3 of the software quality plan provides details of life cycle phase inputs and outputs, and the generation of OSS test documentation is identified in appropriate phases. Section 6 of the software quality plan also identifies the authors, verifiers, and approvers of each test document.

The NRC staff concludes that the quality of the test planning documentation supports Rolls-Royce's findings for CGD.

3.5.3.2.1.6 System Integration and Test

BTP 7-14, Section B.3.1.4 describes expectations for software integration plans. (Note: software integration in this context refers to integration of the software with hardware components, rather than integration of various SPINLINE 3 hardware components.) The section indicates that such plans should contain information on tests to be performed on the integrated hardware / software system. The NRC staff review focused on the clarity and completeness of the integration plans, with specific emphasis on the treatment of error handling / fault management functions and any non-conformances found during testing.

Figure 6.3-1 of the LTR aligns this plan with the following BTP 7-14: Software Test Plan and Software Integration Plan.

The NRC staff reviewed the Rolls-Royce software integration test plan and report (Reference 1.49). The plan explains the different OSS versions and how they were tested. This document describes the integration activities, analysis, test procedures, and results of the integration tests on the 1E safety class. Rolls-Royce performed these tests to confirm the software modules interact with each other as required, and to confirm the software modules interacted with its respective hardware. Furthermore, these tests were performed to validate that the OSS, application software, firmware and software in electronic modules and the LDU communicated and exchanged data as defined in the system requirement specification.

The NRC staff noted the document contains detailed descriptions of the tests performed along with mapping to the functions exercised within various SPINLINE 3 components. The NRC staff also noted several tests addressed error handling of the system's components. This finding

supports SPINLINE 3's adherence to the EPRI-106439 CGD guidance that failure management is a critical characteristic of digital systems. Test run reports are contained in Section 8 of the plan. The NRC staff noted the integration test result summaries from multiple revisions of the system are contained in the document, along with conclusions from each revision tested. In a few instances, non-conformities were noted as a result of the integration tests. Section 9 (the appendix) to the plan contains summaries of the non-conformance records and resolutions associated with these test findings. During the regulatory audit (Reference 2.5) in Grenoble, the NRC staff reviewed the Rolls-Royce non-conformance system and observed it to be very thorough in its handling of such findings.

The NRC staff concludes the quality of the software integration planning documentation supports Rolls-Royce's findings on CGD.

According to Section B.3.2.4 of BTP 7-14, testing activities should consist of tests for required operating modes (including error recovery) and the testing should trace from the software requirements and design to the test documentation. The NRC staff review focused on the clarity and completeness of the test report, with specific emphasis on the treatment of any non-conformances found during testing.

The NRC staff reviewed the software validation test report (Reference 1.51), which references the software validation test plan (Reference 1.50). Section 4 of the document clearly describes the test procedures and provides detailed descriptions of the expected test results. Section 5 of the test report contains the actual test run reports for each version of the system software – original through the current version (i.e., OSS F / 5). The person responsible for the validation is identified, as well as the documentation (with its appropriate revision) used to support the execution of the tests.

Since test results were presented from all versions of the OSS, the NRC staff paid specific attention to the tests performed on the current version of the system software (i.e., OSS F / 5, the version that would be deployed on a SPINLINE 3 platform that references the SPINLINE 3 LTR). For the validation, Rolls-Royce used three racks with different configurations (i.e., different I/O boards and simulation (software configuration) to validate the SPINLINE 3 software and boards installed in each rack (i.e., parameter tables)). Rolls-Royce used an emulator to simulate I/O and to create communication between the OSS and the application software so data exchange and processing between them could be validated. The NRC staff noted that scope of the tests described was thorough. For example, a test was performed to validate automatic tests and self-test during system operation. The tests identified in this document were run for each rack.

Section 5.5 of software validation test report describes the validation tests performed in OSS version F/5. The results of these tests are summarized in Section 5.5.2.2. The NRC staff noted that Rolls-Royce performed several validation tests. The test report identifies non-conformity reports, as well as the corrections made to the software prior to additional tests. Rolls-Royce ran successfully after correcting non-conformities found. Similar to integration plan, the

appendix of the validation test plan contains summaries of the non-conformities that were found during validation testing.

The integration test plan and report (Reference 1.49) and the software validation test report (Reference 1.51) showed that Rolls-Royce fully and rigorously tested the SPINLINE 3 platform software. Based on this, the NRC staff concludes that the quality of the test planning documentation and results supports Rolls-Royce's findings for CGD.

3.5.3.2.1.7 Software Maintenance

The acceptance criteria for a software maintenance plan (SMaintP) are contained in SRP BTP 7-14, Section B.3.1.6, "Software Maintenance Plan (SMaintP)." This section states that NUREG/CR-6101, Section 3.1.9, "Software Maintenance Plan," and Section 4.1.9, "Software Maintenance Plan," contain guidance on software maintenance plans. These sections break the maintenance into three activities: failure reporting, fault correction, and re-release procedures. SRP BTP 7-14, Section B.3.1.6 further states that guidance on maintenance and configuration management of commercially dedicated items can be found in IEEE Std. 7-4.3.2-2003, Clause 5.4.2.3, "Maintenance of Commercial Dedication." Additionally, EPRI TR 106439, Section 5, "Maintenance of a Commercial Dedication," provides guidance addressing the need for adequate configuration control and change management to maintain the validity of a commercial grade item dedication. In the guidance, maintenance of the dedicated item and the impact of product changes, including software revisions, are covered.

Figure 6.3-1 of the LTR aligns this plan with the following BTP 7-14: Software Maintenance Plan.

Rolls-Royce submitted Software Modification Quality Plan (Reference 1.74) to describe the modifications made after the MC3 project. Section 3.11.2.3.1 of this SE provides the NRC staff evaluation on this plan.

3.5.3.2.2 Software Lifecycle Process Design Outputs

SRP BTP 7-14, Section B.2.3, "Software Life Cycle Process Design Outputs," identifies software documents and products subject to review to evaluate whether the software life cycle development process produced acceptable design outputs. The following documents are included in the review guidance:

- Software requirements specification (SRS)
- Hardware and software architecture description (SAD)
- Software design specification (SDS)
- Code listings
- Build documents
- Installation configuration tables

- Operations manuals
- Maintenance manuals
- Training manuals

Since the LTR does not identify a plant specific application, many of the documents identified in SRP BTP 7-14 are not relevant for generic review of a platform. Specifically, operations, maintenance, and training manuals primarily relate to the installed system and support the licensee as end product user. Thus, review of these documents is most appropriate in the context of a specific project. In addition, given that the design of a specific application is not within the scope of this review, some design outputs that are more particularly focused on application software as the object of the development process are not available for review.

Since SPINLINE 3 OSS and application software are designed, configured, compiled, and implemented using CLARISSE, the build documents and configuration tables for application software, which are not in the scope of the review, would give more conclusive indication of the effectiveness of the life cycle process. Finally, the OSS for the SPINLINE 3 platform was developed prior to the establishment of the Rolls-Royce QA Program so some design outputs are not aligned to BTP 7-14, and thus were evaluated from other documents that contained this information. Documents containing the SRS and SDS were submitted for review. Thus, the evaluation of the available design outputs that correspond to the OSS was focused on the requirements and design documents submitted as part of the dedication effort.

3.5.3.2.2.1 Software Requirements Specification

Section B.3.3.1 of BTP 7-14 describes NRC staff expectations for software requirements specifications. The BTP emphasizes clarity in the requirements and specifically cites thread audits as a method to check for completeness, consistency and correctness. The NRC staff review in this area focused on clarity and completeness of requirements and relied heavily on the thread audits to demonstrate that requirements were traceable through applicable design basis documentation.

The NRC staff reviewed the SPINLINE 3 OSS software requirement specification (Reference 1.30). The NRC staff noted that the document is written at a level where major system concepts of operation are described, such that it more closely resembles a system concepts document. The document does not use the modern convention of “shall” statements in its specification of system behaviors, as is recommended Section 5.3.2 of IEEE Std. 830-1993 (which is endorsed by RG 1.172). (During the regulatory audit, the NRC staff noted that the lower-tier board-specific requirements specifications more closely align with the guidance of IEEE Std. 830-1993 (i.e., use of “shall” in requirements).)

The NRC staff noted that a few of the hardware items addressed in the software requirement specification (e.g., LDU, audio boards) are not part of the scope of the LTR. Any use of components for SR applications that are not addressed in the SPINLINE 3 LTR would need to

be reviewed on an application-specific basis (see Section 5.2, items 2). Therefore, the use of these items in not generally approved.

Sections 5 and 6 of the software requirements specification describe the functions to be executed by the software and the relationship between the functions. The NRC staff noted that Section 5.12 describes “remote operation management.” The SPINLINE 3 topical report does not include any generic provisions for the platform to be operated remotely. Thus, at this time, use of remote operations is not generically approved for the SPINLINE 3 platform via this SE on the SPINLINE 3 LTR.

Section 7 defines constraints on system operations (e.g., frequency of self-tests, maximum time to complete functions, maximum number of specific boards that can be handled by the software). Section 8 describes the data formats to be used by the system.

The NRC staff also reviewed the OSS interface specification (Reference 1.32), which defines the interfaces among the system software and the application software, CLARISSE workshop and LDU. This document contains very specific details on the data exchanged between the CPU (UC25 N+) board and each other specific board in the system, including permissible values for each data field. Similar to the software requirement specification, descriptions of data exchanges for boards or hardware components not included in the LTR scope are included in the interface specification. If boards outside of the scope of the SPINLINE 3 LTR are to be used in a safety related system, those components would need to be reviewed on an application specific basis (see Section 5.2, Item 2).

In addition to the above document reviews, the NRC staff also performed audits of four separate requirements threads selected by the NRC staff during the regulatory audit in Grenoble (Reference 2.5). The threads were specifically selected by the NRC staff as the associated functions specifically dealt with capabilities of the system that were noted in the LTR as being safety critical regardless of the application developed. Conduct of the thread audits started with board-specific specifications derived from the top-level system specification. In each case, the NRC staff found that the requirements were clearly stated in the documentation and that the ‘master document’ for each SPINLINE 3 board contained a listing of the documents that comprised the design basis for the board. From these listed documents, the NRC staff was able to trace requirements through design documentation to test planning and results documents. The NRC staff considered the thread audits objective evidence that demonstrated that the requirements were traceable down to verification test results.

The NRC staff concluded that the quality of the software requirements specifications supported Rolls-Royce’s findings on CGD.

3.5.3.2.2.2 Software Design Description

Section B.3.3.3 of BTP 7-14 describes expectations for software design descriptions. The review guidance emphasizes the need for clarity in the descriptions of how the software requirements are to be implemented into code. BTP 7-14, Section B.3.3.2 contains review guidance for software architecture descriptions. Per the guidance, the software architecture description should sufficiently describe flow of data and deterministic operation of the software. The NRC staff review of the design documentation focused on clarity and completeness of its descriptions of the software architecture and information exchanges.

Rolls-Royce submitted its software preliminary design (Reference 1.31) document, which was originally developed at the time of the MC3 project. Rolls-Royce clarified in an RAI response (Reference 1.22) that the term “preliminary” in the title is just an artifact of the initial design development and that it does constitute the actual software design description. The design document references the software requirement specification (Reference 1.30) and interface specification documents (Reference 1.32) described above, which supports the traceability of requirements to design.

The NRC staff reviewed the software preliminary design document and found that it describes the software architecture and provide detailed descriptions of the major system software modules. In particular, Section 2 of the report describes the software architecture, and the appendix contains the technical memorandum detailing the original trade study performed to select the software architecture for the system. The appendix notes that the architecture chosen does present the potential for presence of “deactivated” code. This situation is the result of the standard OSS containing modules relating to all potential system hardware configurations, even if certain boards are not selected for use in a specific application. The design document states in numerous locations that “a basic module is not activated unless the number of boards belonging to the type associated with it is other than zero in the TAB_CONF table.” Further discussion of this situation is covered under Secure Development and Operational Environment in Section 3.12 of this SE. Section 2 also notes that the software code and hardware configuration table is located on Flash EEPROM, which is loaded into RAM upon initialization and executed from there.

Section 3 of the software preliminary design document describes the major system modules in detail. In particular, the NRC staff noted that details were provided on error handling – particularly during system initiation. As was noted above, failure management functions, such as error handling on system initiation, should be considered critical performance characteristics for purposes of CGD. The NRC staff also noted that similar to the software requirement specification, descriptions of software modules relevant to boards not included in the LTR scope are included in the design document. If boards outside of the scope of the SPINLINE 3 LTR are to be used in a safety related system, those components would need to be reviewed on an application specific basis (see Section 5.2, items 2).

Section 3.3 of the software preliminary design document describes the cycle time management module, which states that if an error occurs with respect to the length of a unit's cycle time, the system processor would be halted and an error message displayed. Description of the cycle time management is provided in Section 3.4.2.1.2.

The NRC staff finds that the software design descriptions were reasonably thorough and does capture data exchange, which supports Rolls-Royce's findings on CGD.

As described in Section 3.4 of this SE the SPINLINE 3 platform also includes software or firmware embedded in digital components (which are identified in Section 3.4.3 of this SE). Sections 2.2.4 and 2.2.5 of Reference 1.70 describe the strategy for commercial grade acceptance of the software. In particular these sections describe the process followed to design, developed, and tested the software or firmware embedded in these modules, as well as the documents prepared to record such activities. These sections describe the configuration management plans prepared for the software embedded in these components. In these sections, Rolls-Royce explained that these boards were included in the validation testing of the SPINLINE 3 OSS.

During the NRC regulatory audit (Reference 2.5) of Rolls-Royce's facility in Grenoble, NRC staff performed several requirement thread review activities. These requirement threads covered performance characteristics resident on the analog output board (6SANA ISO), digital output board (32ACT), the main processor board (UC25 n+), and communications board (NERVIA+). In each of the requirements threads, the NRC staff observed that Rolls-Royce had maintained a complete set of design basis documentation. This design basis documentation included a master document that identified all the design basis documentation for each board, requirements specifications, detailed design documents, test plans and test results. Each document noted the revision and date. The oldest document reviewed pre-dated the LTR by over two decades. The availability and quality of SPINLINE 3 documentation demonstrated the effectiveness of configuration management over the life of the platform. The documents also contained signatures of the author and approval authority, as well as the Rolls-Royce QA and V&V staff who reviewed the documentation. The NRC staff considered the collection of design basis documentation maintained by Rolls-Royce to be objective evidence that a system / software development process equivalent to what would currently be expected for such systems was followed in the development of the SPINLINE 3 components and software.

Based on the information observed during the regulatory audit, and the information provided in the software validation test report, the NRC staff concluded that Rolls-Royce used a robust design process for the software and firmware embedded in electronic modules, and that the integrated tests show that these components work properly with the SPINLINE OSS.

The NRC staff concluded that Rolls-Royce's findings using Method 2 were acceptable and that they support Rolls-Royce's findings regarding CGD.

3.5.3.3 Acceptable Performance Record (Method 4)

Per EPRI-5652, Method 4 entails collecting and evaluating historical performance of the commercial grade item to substantiate that the item is suitable for its intended application. Industry-wide performance is specifically noted as one applicable source of data to support Method 4.

In Table 2.3-1 of the LTR (Reference 1.4), Rolls-Royce presents the history of SPINLINE 3 systems, along with its predecessor lines from Rolls-Royce, currently in use in safety applications at nuclear installations. The cited operating experience is entirely in non-U.S. countries, with the majority of operating experience in French reactors. Rolls-Royce notes that none of the fielded SPINLINE 3 Class 1E systems have experienced a failure with software as a root cause. Rolls-Royce also states in the LTR that in no instances have SPINLINE 3 safety systems failed to function in the presence of anticipated operational occurrences. Rolls-Royce states in its RAI response (Reference 1.22) that SPINLINE 3 systems have not experienced an unsafe condition in more than 199 reactor-years of operating experience as of December 2011, which was when the RAI responses were submitted.

Rolls-Royce indicated in its RAI response (Reference 1.22) that it has a system in place to report and track non-conformities that is described in its I&C Quality Manual (Reference 1.26). The NRC staff reviewed the reference to verify that Rolls-Royce does have processes in place to field and evaluate any failures reported to them by the nuclear installations utilizing the SPINLINE 3 platform as cited in its LTR. Section 8.3 of the Quality Manual cites Rolls-Royce procedures SMQ 8 303 202 and SMQ 8 307 152 as addressing Rolls-Royce actions following receipt of any non-conformity (which would include customer initiated fault reporting). In Reference 1.70, Rolls-Royce noted that they did not use Method 4 to compensate for shortcoming in the legacy software, instead Rolls-Royce's intents for describing its operating experience was to demonstrate satisfactory performance of its SPINLINE 3 platform.

The NRC staff spent time during the regulatory audit of Rolls-Royce's Grenoble facility reviewing the performance of Rolls-Royce's non-conformity reporting system described in the RAI response. The NRC staff viewed several non-conformity examples. The records for all of the non-conformity items were contained in Rolls-Royce's ORIENT database. The NRC staff observed that Rolls-Royce's follow-up to non-conformity reports was thorough with respect to both technical evaluation and maintenance of relevant documentation.

In Rolls-Royce Reference 1.22, Rolls-Royce clarified that it is not taking credit for operating experience to either provide a basis for SPINLINE 3 module failure rates or compensate for shortcomings in legacy software, as it considers its original software development processes to be of high quality. The NRC staff, however, did conclude that the operating history does support a CGD of the SPINLINE 3 platform, based upon the NRC staff review of the SPINLINE 3 operating history provided and NRC staff review and audit of Rolls-Royce processes to address non-conformities in the platform.

3.5.4 Critical Characteristics – Dependability

Per the guidance on EPRI-106439 and IEEE 7-4.3.2-2003, dependability characteristics (or development process characteristics) include use of life cycle processes that support production and maintenance of a software product such that likelihood for introduction of design errors is minimized. These processes can include V&V activities, configuration management processes, and requirements traceability.

As noted above, the NRC staff performed a number of requirements thread reviews during the regulatory audit in Grenoble, France and was able to substantiate that requirements traceability was adequate to support a finding of CGD. Evaluations performed by the NRC staff in the areas of independence of the V&V organization and provisions for configuration management of the platform going forward were performed. Section 3.5.3.2.1.5 summarizes the evaluation of these areas for the OSS. Based on the information provided, the NRC staff noted verification activities establish suitable performance and dependability characteristics and are acceptable to contribute to CGD of the OSS of the SPINLINE 3 platform in accordance with the guidance in EPRI TR-106439 and EPRI TR-107330.

In addition, because the dependability category captures those critical characteristics that must be evaluated to form an appropriate judgment regarding built-in quality of a software-based device, the NRC staff reviewed certain characteristics of the current Rolls-Royce's software processes to ensure development of the application software is properly established and of high quality. Summaries of these evaluations are described below. Note, as stated in Section 3.4.4.1, the LTR does not include a specific plant application, and thus the NRC staff could not review or confirm implementation of the development processes for application specific software. An applicant referencing this SE should confirm that the implementation of the software development processes is conducted in accordance with the processes evaluated by the NRC for the application software (see Section 5.2, Item 11).

3.5.4.1 Independence of V&V

Per RG 1.68 and BTP 7-14, the V&V organization should have sufficient independence from the development organization to effectively perform its duties. Regulatory Position C.3 of RG 1.68 specifically cites "sufficient independence from cost and schedule limitations".

Rolls-Royce's "Quality Procedure, Safety Software Design Process" (Reference 1.56) describes its V&V organization in terms of composition and relation to a software development activity for "safety class" software. Section 3.1 identifies a project specific V&V organization that is formed which is distinct and separate from the software development team. The V&V group is headed by a Software V&V Manager. Section 3.2 notes that class B and C2 software may have employees reporting to the software project manager work on V&V activities. As was clarified in its RAI response (Reference 1.23), Class B and C software are defined in IEC standards. The RAI response also states that SPINLINE 3 software is exclusively Category A software. Thus, the NRC staff is basing its review upon the premise that Section 3.2's special case for V&V

staffing would not be used for SPINLINE 3 projects. The NRC staff understands that V&V personnel would report to the Software V&V Manager.

As stated in the Quality Procedure and clarified in the RAI responses, the Software V&V Manager is responsible for meeting commitments on cost and schedule for V&V work. However, it is noted that these commitments are made by the V&V group and not imposed on the V&V group by the Project Manager or project organization. In Section 6.2.7, the Quality Procedure states that the V&V Team Manager designates the Software V&V Manager and allocates resources to the project.

The Quality Procedure also describes the dispute resolution process. Disagreements between the Software V&V Manager and the Software Project Manager are resolved by the Software Group Manager with involvement of the Software QA Manager. If needed, issues may be further elevated to the Engineering Department Manager and the Quality & Infrastructure Department Manager.

The NRC staff concluded that sufficient independence existed in the V&V organization to support Rolls-Royce's finding on CGD.

3.5.4.2 Management of Software Configuration

The LTR states that Rolls-Royce documentation is consistent with RG 1.169 and IEEE Std. 828-1990 and IEEE Std.1042-1987 (see Section 3.3.13 of the LTR). In Table 3.8-7 of Appendix A of the LTR the applicant provided a mapping between Rolls-Royce documentation and the provisions of IEEE Std. 828-1998.

RG 1.169 states that for safety system software, the minimal set of activities must accomplish the following: identification and control of all software designs and code, identification and control of all software design interfaces, control of all software design changes, control of software documentation, control of software vendors supplying safety system software, control and retrieval of qualification information associated with software designs and code, software configuration audits, and status accounting.

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 both development and maintenance. The Software Configuration Management Plan (SCMP) needs to include an overview description of the development project and identify the configuration items that are governed by the plan. The plan should also identify the organizations, both technical and managerial, that are responsible for implementing configuration management.

Software configuration management (SCM) for the SPINLINE 3 platform is established by the SCMP, Rolls-Royce document 1 208 878 E (Reference 1.76) and the Configuration Management Process, Rolls-Royce document 1 207 875 G (Reference 1.75). These documents define the SCM roles and responsibilities for internal organizations and staff, identify the SCM tools, and describe the processes for SCM including item identification, configuration control activities, change control authority and request mechanisms, and change/error tracking and reporting. According to the Configuration Management Process, the Software Program Manager (SPM) has overall responsibility for SCM for the project and for the production and application of the SCMP; the Development and V&V teams perform technical SCM activities and create and identify configuration elements; and the Software Quality Assurance Manager (SQAM) verifies the application of requirements and conducts reviews and audits of SCM activities and software product configuration.

Section 2.2 of the SCMP defines life cycle models to control configuration items. When an item has been checked out for revision, the state is "to be defined". After having been checked in, the item is in the status “in progress;” after that, the item follows its life cycle. The state corresponds to the status of the item in the life cycle (e.g., “in progress,” “to verify,” “rejected,” “verified,” “incomplete,” “to be closed,” “closed,” “cancelled,” etc.).

Reference configurations are created at various stages in the software development life cycle. In the configuration management (CM) tool, the reference configurations are created by baselines, which are a set of configuration elements under a given version.

Each SCM item is given a unique identification for control and tracking purposes. Items under the SCMP are identified with a major version number (incremented for each new version of the component) and a minor version number (incremented to keep track of intermediate steps). For file-type items, which are elements of standard components, the version numbers are identified by major version numbers only.

Among the items identified in the SCMP for configuration control are: embedded software forming the basis of SPINLINE 3 (OSS, FAS, Microtec library, the software of intelligent boards, such as NERVIA+ and ICTO boards), software forming an integrated development environment (CLARISSE), the NERVIA network protocol export tool, LACRAL animation software, CMU, and ASA verification tools), various applications (Test Bench, LDU, MCC), tools, and documentation.

Archival is performed at the end of the software version development, when all the software configuration elements are finished. An archive is a set of elements defined from an archive baseline and intended to be archived electronically. An archived baseline contains every version of every managed element regardless of its state.

Rolls-Royce archives configuration tracking by using the following elements:

- The List of Software Documents (LSD) which identifies a software version and contains the list of the documents related to this software. It is produced manually and its configuration is managed in the CM tool.
- The List of Tools and Libraries Used for Software development (LTLUS) identifies the versions of the tools and libraries used to develop the software.
- The Software Configuration Management Report (SCMR) which ensures the visibility of the software configuration. It is produced manually and its configuration is managed in the CM tool with the other software documents. The SCMR identifies, for each software version, the changes taken into account as well as the corresponding baselines in order to ensure traceability in the CM tool. All the SCMRs for each managed component are referenced by a global SCMR.

SPINLINE 3 platform was initially developed without the use of a configuration management tool. The use of the tool was introduced in maintenance in order to facilitate the tracking of changes throughout the life cycle. Serena Dimensions CM is the configuration management tool selected by the Rolls-Royce. The CM tool (Dimensions CM) is running on a Windows server. The users utilize the Desktop client form of the tool, which also runs on Windows.

All types of configuration items (i.e., document or source code) are managed in the configuration management tool, whether they are in progress, verification, or testing. The PdM (Monitoring and Maintenance Unit) and the AS (System Workshop) software programs are managed using Visual SourceSafe and its configuration management plans are described in Rolls-Royce documents Nos. 3 000 342 and 1 208 868, respectively. The SCADE libraries have its own configuration management plan described in document Rolls-Royce document # 3 013 037. These documents were reviewed during the June 2012 Regulatory Audit (Reference 2.5) and were found to be consistent with the SCMP.

One of the purposes of the CM tool is to manage access to the items. When a document or safety software source file is checked-out, the file is locked and no other user can check-out the file. When parallel check out is allowed (i.e., for non-safety software source files), the tool gives an alert at check-in when the item has been checked-out by multiple users. A merge function can be performed by the integrator with a merge tool provided by Dimensions CM.

Under the Rolls-Royce Configuration Management Process, the change control process is managed to ensure that unauthorized access and software changes of inadequate quality are prevented.

There are two types of change requests:

- Change Requests relating to changes in the client's requirements or in the purpose of the software development.

- Non-conformities in cases where the current production status has been found to deviate from the purpose of the software development.

Rolls-Royce uses the following tools to manage and track change requests and non-conformities:

- GEVOL: system change management tool used throughout Rolls-Royce. It is used in accordance with Rolls-Royce document 8 303 197, Procedure - Definition of Change Management Process.
- ORIENT: product non-conformity management tool used throughout Rolls-Royce. It is used in accordance with Rolls-Royce document 8 303 202, Procedure - Nonconformities.
- Dimensions CM: tool specific to the Rolls-Royce Software group used for change management (including change request management and software configuration management).

The NRC staff reviewed Rolls-Royce documents 8 303 197 and 8 303 202 during the June 2012 Regulatory Audit (Reference 2.5).

When a non-conformity is identified in software, a request is systematically created on the product. The request is created in Dimensions on the impacted software if the software is managed in Dimensions. A non-conformity is recorded in a global Excel list of software non-conformities if the software is not managed in Dimensions CM (old product). The software anomaly resolution is identified and scheduled according to the impact of the problem and to the project status. If the non-conformity has been detected after the software validation (e.g., during interconnected tests, site tests, etc.), an analysis is also performed by the Software Method and Tools Manager in order to identify why and when the anomaly was introduced and why it has not been detected earlier. Following this analysis, improvement actions can be identified for the process, the methods, or the tools. The software improvement actions are managed in a global list. Each year, the Software Group Manager and the Software Method and Tools Manager identify the actions to be performed.

In Reference 1.69, Rolls-Royce explained that non-conformities that represent a potential risk for safety will be handled in accordance with Rolls-Royce procedure 8 307 512 B, Classified Non-Conformities, which will address the requirements in 10 CFR 21. In addition, Rolls-Royce will record equipment or parts returned to them in its ORIENT database. The NRC staff reviewed the performance of Rolls-Royce's non-conformity reporting system described in the RAI response during the regulatory audit of Rolls-Royce's Grenoble facility. The NRC staff viewed several non-conformity examples. The records for all of the non-conformity items were contained in Rolls-Royce's ORIENT database. The NRC staff observed that Rolls-Royce's follow-up to non-conformity reports was thorough with respect to both technical evaluation and maintenance of relevant documentation.

The NRC staff concluded that Rolls-Royce's provisions for configuration management supported Rolls-Royce's findings on CGD.

3.6 Environmental Equipment Qualification

The purpose of performing EQ testing for a safety system are (1) to demonstrate that the system will not experience failures due to abnormal service conditions of temperature, humidity, electrical power, radiation, electromagnetic interference, radio frequency interference, electrical fast transient, electrostatic discharge, power surge, or seismic vibration, and (2) to verify those tests meet the plant-specific requirements.

Criteria for environmental qualification of SR equipment are provided in 10 CFR Part 50, Appendix A, GDC 2, "Design Bases for Protection against Natural Phenomena," and GDC 4, "Environmental and Dynamic Effects Design Bases." Additionally, the regulation at 10 CFR 50.55a(h), "Protection and safety systems," incorporates by reference the requirements of IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," which addresses both system-level design issues and quality criteria for qualifying devices. RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," endorses and provides guidance for compliance with IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," for qualification of SR computer-based I&C systems installed in mild environment locations.

To comply with the requirements of GDC 4, 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," and IEEE Std. 603-1991, an applicant must demonstrate through environmental qualification that I&C systems meet design-basis and performance requirements when the equipment is exposed to normal and adverse environments.

SRP Chapter 7, Appendix 7.0-A (page 7.0-A-14), Section H, "Review of the Acceptance of Commercial-Grade Digital Equipment," contains guidance for the review of commercial equipment and references RG 1.152, Revision 2. RG 1.152, Revision 2, endorses IEEE Std. 7-4.3.2003. IEEE Std. 7-4.3.2-2003, Clause 5.4.2, defines the qualification of existing commercial computers for use in safety related applications in nuclear power plants. SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.4.2, "Qualification of Existing Commercial Computers," provides acceptance criteria for EQs (in accordance with IEEE Std. 7-4.3.2, Clause 5.4.2). This section states that EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," and EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants," provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” presents a specification in the form of a set of requirements to be applied to the generic qualification of PLCs for application and modification to SR I&C systems in nuclear power plants. It is intended to provide a qualification envelope corresponding to a mild environment that should meet regulatory acceptance criteria for a wide range of plant-specific SR applications. The qualification envelope that is established by compliance with the guidance of EPRI TR-107330 consists of the maximum (i.e., extremes) environmental and service conditions for which qualification was validated and the range of performance characteristics for the PLC platform that were demonstrated under exposure to stress conditions. Applicants using the SPINLINE 3 platform are obligated to verify that the requirements of the application are bounded by the qualification envelope established by qualification to the guidance of EPRI TR-107330.

Rolls-Royce used the guidance provided in EPRI TR-107330 to establish the testing approach to meet the requirements of IEEE Std. 323-2003 and other NRC guidance. The qualification program developed for the Rolls-Royce SPINLINE 3 addressed environmental qualification for a mild, controlled environment, such as a main control room and auxiliary electrical equipment rooms. The basis for the testing program was conformance with the guidance contained in EPRI TR-107330, Section 4.3. The results of the qualification program establish the qualification envelope of the Rolls-Royce SPINLINE 3 platform.

The testing program was conducted on a QTS composed of SPINLINE 3 modules that were configured into a representative system to execute a TSAP. Rolls-Royce used the DAS to simulate I/O and collect test data. Rolls-Royce Qualification Test Specimen and Data Acquisition System Specification (Reference 1.46) describes the requirements for the design of the QTS, TSAP, and DAS. The testing program was designed to exercise inputs and outputs and to demonstrate the capability of the SPINLINE 3 QTS to (1) perform basic functions within specified tolerances under normal environmental and operating conditions, and (2) perform design functions within specified tolerances under stress conditions, as specified in EPRI TR-107330, Section 6, “Qualification Testing and Analysis.” The qualification tests also inherently test the basic functionality of the SPINLINE 3 OSS, TSAP, and NERVIA communication software and the component firmware and software operating within the QTS hardware environment.

The SPINLINE 3 platform EQ Plan (Reference 1.77) describes the approach for qualification testing, including configuration of the test system, test requirements, and test plans for each of the tests performed. This plan states that the SPINLINE 3 QTS was placed under the specific stress conditions identified in EPRI TR-107330 to confirm that the SPINLINE 3 platform was able to function correctly during normal and abnormal plant operating conditions. Rolls-Royce performed pre-qualification, radiation, environmental, seismic, EMI/RFI, electrical fast transient (EFT), surge withstand, electrostatic discharge (ESD) and Class 1E to non-1E isolation tests; these tests were performed in the order listed in the EQ Plan (Reference 1.77) and in accordance with the requirements of EPRI TR-107330. Operability and prudency tests were

conducted before, during, and after the qualification testing. Rolls-Royce prepared test procedures for each test.

Rolls-Royce performed three qualification testing sessions, called “Campaigns.” In 2010, Rolls-Royce performed the first Campaign on the SPINLINE 3 platform. During the Campaign 2010, Rolls-Royce performed radiation and environmental testing. The qualification tests could not be completed at the time due to problems at the test facility, and thus Rolls-Royce performed the remaining tests during the Campaign 2011. Because most tests were performed in the Campaign 2011, Rolls-Royce is not crediting the results obtained for environmental testing during the Campaign 2010. During the Campaign 2011, the SPINLINE 3 platform experienced several problems that required investigations and reconfiguration. After these events were analyzed and resolved, Rolls-Royce performed additional qualification testing in Campaign 2012 to validate the solutions implemented to address the problems encountered during the Campaign 2011. Test plans, procedures, results, deficiencies, and results are discussed in each test section below.

Rolls-Royce was both the manufacturer and qualifier of the Rolls-Royce SPINLINE 3 platform. Rolls-Royce subcontracted national test laboratories with a 10 CFR Part 50, Appendix B compliant Quality Assurance Programs, to provide qualification testing services. Procurement, receipt, and acceptance of the test laboratory services were in accordance with Rolls-Royce QA Manual procedures for procurement, receipt and acceptance of nuclear grade services, including preparation of a services procurement specification. Rolls-Royce used Wyle Laboratories, located in Huntsville, AL, for the Campaign 2010, and the National Technical Systems (NTS), located in Acton, MA, for the Campaigns 2011 and 2012.

Rolls-Royce documented non-compliances and test anomalies in the individual qualification reports and in the summary EQ report as described below. The SPINLINE 3 did not fully comply with seismic requirements, EMI/RFI, and ESD, but met the criteria for the remaining qualification tests. The specific limitations are detailed in Section 15 of the “Summary Equipment Qualification Test Report” (Reference 1.78), “Investigations Results of 2011 NRC Qualification Tests” (Reference 1.79), and are summarized below. For clarity and to ensure full coverage, the NRC staff created plant-specific actions to address the limitations in the “Summary Equipment Qualification Report” (see Section 5.2, items 19, 20, and 21).

Table 3-3 lists test plans and test procedures prepared as part of the qualification program for the SPINLINE 3 platform.

Table 3-3 SPINLINE3 Platform EQ Tests and Procedures

Rolls-Royce Document	Document Title	ADAMS Accession Number
3 006 501 E	EQ Plan	ML12188A041
3 006 404 E	System Specification for the Qualification Test Specimen and the Data Acquisition System	ML101670096
3 010 612 G	MCL	ML12201A091
3 010 783 A 3 019 950 A	Factory Acceptance Test Procedures	ML12188A040 ML101670111
3 010 286 B	Radiation Exposure Test Procedure	ML101670117
3 010 287 B	Environmental Test Procedure	ML101670121
3 010 288 D	Seismic Test Procedure	ML12188A043
3 010 289 B	EMI / RFI Test Procedure	ML12188A042
3 010 290 B	Electrical Fast Transient Test Procedure	ML110910433
3 010 291 A	Surge Withstand Test Procedure	ML110910451
3 010 292 A	Electrostatic Discharge Test Procedure	ML110910453
3 010 293 A	Class 1E to Non-Class 1E Isolation Test Procedure	ML110910456
3 010 294 D	System Setup and Checkout Test Procedure	ML12188A039
3 010 295 D	Operability Test Procedure	ML12188A044
3 010 296 C	Prudency Test Procedure	ML12188A045

This SE evaluates the EQ type testing that the manufacturer performed on the SPINLINE 3 platform standardized circuit boards, representative BAP, and chassis, against applicable EQ regulations, standards, and guidance. This SE does not include plant-specific determinations for a specific application or installation. Therefore a plant-specific action for each applicant or licensee that references this SE to demonstrate the adequacy of the SPINLINE 3 platform's qualification in full consideration of the applicant's or licensee's environmental qualification program, SPINLINE 3 based I&C system, and installed operational environment (see Section 5.2, Item 15) is included. This plant-specific action is consistent the GDC 4, 10 CFR 50.49, IEEE Std. 603-1991, and the final conclusion of the "Summary Equipment Qualification Test Report" (Reference 1.78).

The next subsections summarize the QTS and DAS configurations, tests performed, events and limitations, and results observed during EQ testing. Each of these subsections also provides the NRC staff evaluation of the qualification test against its applicable regulatory evaluation criteria.

3.6.1 Test System Configuration

3.6.1.1 Qualification Test Specimen

The Rolls-Royce Qualification Test Specimen and Data Acquisition System Specification (Reference 1.46) describes the requirements for the design and configuration of the SPINLINE 3 QTS used for qualification testing. In Reference 1.55, Rolls-Royce provided a drawing illustrating the configuration and of the QTS.

As mentioned in previous sections, Rolls-Royce did not define a generic system or application based on the SPINLINE 3 platform. Instead, the LTR defined the different modules that can be used to meet any customer requirements. As a result, Rolls-Royce followed the guidance provided in EPRI TR-107330 to determine the number and type of hardware modules to include in the QTS. Based on this, Rolls-Royce used only one QTS, which included one of each module/board necessary to achieve the hardware requirements described in the LTR. Thus, the QTS represented a single-channel test configuration, which included the components listed in Tables 3-1 and 3-2 of this SE. (Reference 1.22 provides additional explanation for the use of only one QTS for EQ testing.) The Rolls-Royce MCL (Reference 1.29) lists the baseline configuration of the qualified SPINLINE 3 platform.

The QTS was reconfigured as necessary to support the protocol and worst-case loading scenario for each test.

The modules in the QTS were divided in two processing units (PU), PU1 and PU2. Each processing unit includes an UC25 N+ board and a NERVIA module. Each UC25 N+ includes the logic necessary to exercise the I/O modules installed in that processing unit. The NERVIA+ modules in each processing unit were used to implement the communication link between them, and thus defined the network architecture of the QTS. The “System Specification of the Qualification Test Specimen and Data Acquisition System” (Reference 1.46) describes the QTS architecture, physical connections, logic, and processing units’ arrangement. Also Reference 1.22 provided additional information about the QTS and DAS configuration. These documents identified the following limitations or constraints of the QTS:

- Rolls-Royce used both ICTO pulse acquisition channels in the QTS, but only one was tested because they are identical.
- The QTS configuration for acquisition of discrete signal could not meet the requirements for Prudency Test described in EPRI TR-107330, Section 5.4. Specifically, the 32 ETOR TI discrete acquisition board could not acquire 120 VAC discrete inputs. Each input channel of this module is configurable to operate at a maximum input voltage of 24 VDC, 48 VDC, or 125 VDC.
- Rolls-Royce did not test the MV16 inhibition function during qualification testing. This function is performed from the operator panel, whose configuration is application-specific (References 1.22 and 1.23), and was not part of the QTS EQ testing. If this function is

included on an application specific project, the licensee should evaluate how this function is implemented and if it meets regulations (see Section 5.2, Item 2).

- The SPINLINE 3 platform does not include solid-state discrete outputs, and thus the platform does not meet the EPRI TR-107330 requirements specified in Sections 4.3.3.2.1 for and 4.3.3.2.2.

The licensee should consider these limitations and constraints when an application specific system is supplied (see Section 5.2, Item 2).

The QTS is powered by the cabinet power supply assembly. This assembly was arranged to provide versatility in applying and controlling power to the QTS components, as well as to operate during the different operating modes applied during EQ testing (Reference 1.46). The power supply assembly was composed of several cabinet power supply chassis to provide the 120 VAC source, and then convert it to various AC and DC voltage levels required to operate the QTS. Reference 1.46 provides details of the QTS power supply assembly and distribution.

The QTS network architecture was implemented by establishing communication between the PU1 and the PU2, and then with the DAS. References 1.46 and 1.22 describe the NERVIA communication architecture implemented between the QTS and DAS.

The QTS included the operator panel to perform certain functions to be performed by operators in an application-specific installation, such as inhibition, periodic testing. However, in Reference 1.22, Rolls-Royce explained that these functions were not tested during EQ testing, as they are not safety functions. They were implemented in the QTS specimen so as to prove that these functions, which are commonly implemented on SPINLINE 3 systems, do not adversely affect the performance of the safety-related equipment during qualifications tests. Further in Reference 1.23, Rolls-Royce explained that the operator panel is a 1E component that is plant-specific that will be configured to match the cabinets components in the application. Therefore, the NRC staff did not evaluate the Operator panel in the SE. Licensees will need to verify that the configuration of the operator panel matches the requirements for the application specific design (see Section 5.2, Item 8).

3.6.1.2 The Test Software Application Program

The Rolls-Royce Document “Qualification Test Specimen and Data Acquisition System Specification” (Reference 1.46) describes the requirements for the design of the TSAP used for qualification testing.

The TSAP was a non-safety software application designed to support qualification testing while providing functionality representative of the functions to be performed by each module. EPRI TR-107330, Section 6.2.2, describes the requirements for the TSAP. The TSAP did not follow the Rolls-Royce software development process described in Section 3.4.4. Because the SPINLINE 3 platform described in the LTR did not identify a particular system architecture or

application, Rolls-Royce developed a TSAP to exercise the different boards included in the QTS, in a manner that could be capable of performing the signal processing necessary to implement the functions of a Rector Trip System (RTS) or an Engineering Safety Actuation System (ESFAS), and support response time loop.

The TSAP was based on a set of simulated control loops and program code to enable operability and prudency testing, as well as communication between two different PUs. The Rolls-Royce Qualification Test Specimen and Data Acquisition System Specification (Reference 1.46) describes the requirements for the design and configuration of the TSAP used for qualification testing. The TSAP included logic to perform the following functions:

- Read inputs associated with the operability and prudency tests, and qualification tests,
- Drive outputs required by the operability and prudency tests, and qualification tests,
- Provide logic for timer testing, and
- Read input for count rate.

For the EQ testing, Rolls-Royce developed two TSAPs, TSAP for PU1 (TS1) and TSAP for PU2 (TS2) (Reference 1.22). Specifically, TS1 was used to exercise the I/O in PU1 by receiving inputs, processing them (logic) according to the operating mode, and then generating the TSAP outputs. The configuration and logic used in TS1 varied with the operating mode according to the EQ test being performed. Also, TS1 included three tunable parameters to control time steps associated with specific analog output functions. The DAS selected the operating mode for TS1. TS2 was used to test the NERVIA network communication by sending data from PU2 to PU1 and then back and sending unidirectional data to the DAS. The configuration and logic used in TS2 did not vary with the operating mode. The detailed requirements, design description, and functionality of the TSAPs are provided in References 1.22 and 1.46.

3.6.1.3 The Data Acquisition System

Rolls-Royce used a DAS to simulate QTS inputs (including pulse inputs), acquisition of QTS outputs, network communication, and system status. The MCL (Reference 1.29) identifies all components and revision level of all test specimen and DAS software and firmware. The Rolls-Royce Document “Qualification Test Specimen and Data Acquisition System Specification” (Reference 1.46) describes the requirement specification, design, and configuration of the DAS.

The DAS generated analog and digital inputs to the QTS. This system was configured with a simulator application program which was used to create a variety of static and dynamic input signals used in the performance of qualification testing including pre- and post-qualification operational and prudency tests. The DAS provided simulated RTD signals to test the RTD input modules included in the QTS. Analog and digital outputs from the QTS were monitored with the PC-based DAS. The DAS also monitored analog and digital inputs to the QTS. To do this, Rolls-Royce used the PCI NERVIA+ (non-1E) board to communicate with the DAS using the NERVIA network. The TSAP sent information to the DAS regarding operation of the QTS, as

well as state of I/O signals and validity indicators for the NERVIA network. In Reference 1.22, Rolls-Royce explained that this non-1E board was not part of the qualification system and it was only used to communicate the DAS and the SPINLINE 3 platform during EQ testing. Therefore, the NRC staff did not evaluate the PCI NERVIA+ board. If the PCI NERVIA+ board is used in an application specific project, the licensees will need to verify that its use meets regulations; especially those described in DI&C-ISG-04 (see Section 5.2, Item 7).

Data was recorded by DAS and analyzed by Rolls-Royce during the various EQ tests to verify proper operation of individual input and output points. During each test, the TSAPs processed test signal supplied by the DAS. To detect any deviation in performance, responses of the test specimen during each qualification test were logged for comparison to the performance baseline established during prequalification testing.

3.6.2 Factory Acceptance Test

The integration of the system and factory acceptance test were performed after the SPINLINE 3 platform was manufactured to verify that the hardware, wiring, and communication cabling for the QTS and DAS had been properly installed and that communication had been established over each communication link. Rolls-Royce performed the Factory Acceptance Testing as part of qualification testing as discussed in Reference 1.77. Reference 1.80 describes the test procedure used for the FAT. The FAT included the following assessments:

- Functional tests to check correct operation of the QTS in every possible operating mode.
- Hardware failure tests to check that the DAS reports every failure that could occur in the QTS

As described before, Rolls-Royce performed EQ testing during several Campaigns. For the Campaigns 2010 and 2012, Rolls-Royce performed FAT. The results from Campaign 2012 reflect the configuration of the QTS that was used in the Campaigns 2010 and 2012. Due to modifications implemented in the QTS to address the failures observed during the Campaign 2011, Rolls-Royce performed FAT again to validate the solutions implemented. FAT was performed at the Rolls-Royce facilities in Grenoble, France.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	**Document Number**
FAT Test Procedure	3 010 783 A (Campaign 2010) 3 019 950 A (Campaign 2012)
System Specification QTS and DAS	3 006 404 E
FAT Test Report	3 010 783 B (Campaign 2010) 3 022 951 A (Campaign 2012)

Rolls-Royce reported the test results in Appendix A of the “Summary Equipment Qualification Test Report” (Reference 1.78). All FAT requirements were met during Campaigns 2010 and

2012. Based on this information, the NRC staff concluded that the FAT testing and the ensuing results meet the guidance presented in EPRI TR-107330, Section 5.

3.6.3 Pre-Qualification Testing

The pre-qualification testing was performed as described in EPRI-TR 107330 with the exception of burn-in testing. Reference 1.22 explained that the burn-in test was not performed because the Rolls-Royce SPINLINE 3 platform manufacturing routine includes routine burn-in of the hardware. Furthermore, Rolls-Royce performed FAT of the QTS, which was used to detect failures in the system, as well as performed functional tests. Thus, the time of QTS running during these tests provided sufficient burn-in time to eliminate those modules subject to early-life failures.

Rolls-Royce performed pre-qualification testing to (1) confirm that the SPINLINE 3 QTS was properly configured and operational, (2) provide baseline performance data for comparison with data obtained during and after qualification testing, and (3) validate the test procedures. Pre-qualification testing included the following assessments:

- The system setup and checkout test documented proper configuration and operation of the QTS and DAS, including hardware, software, input and output simulators; test and measurement equipment; and interconnecting cabling.
- The operability test to establish baseline performance included tests for analog module accuracy, system response time, operation of discrete inputs and outputs, performance of timer functions, failover tests (associated with the failure of redundant components), loss of power, detection of failure to complete a scan, power interruption, and power quality tolerance.
- Prudency testing demonstrated the ability of the QTS to operate within specifications under dynamic conditions. The prudency test included a burst of events test and an optic fiber connection failure test.

The pre-qualification testing was designed to follow the requirements of Section 5.2 of EPRI TR-107330 by establishing baseline conditions for the QTS and by verifying system configuration/setup and proper operation. This testing included operability testing and prudency testing as specified in EPRI TR-107330, Sections 5.3, 5.4, 5.5, and 6.4.3. The acceptance criteria for the pre-qualification test were defined in the System Setup and Checkout, Operability, and Prudency Procedures (References 1.84, 1.85, and 1.86). This test exposed the QTS to various normal and abnormal conditions of I/O operation and power source variations.

For the 2010 and 2012 Campaigns, Rolls-Royce performed pre-qualification testing. Due to modifications implemented in the QTS to address the failures observed during the Campaign 2011, Rolls-Royce performed pre-qualification testing again to validate the solutions implemented. Details of the testing can be found in the following Rolls-Royce documents:

Document Title	Document Number
System Setup & Checkout Test Procedure	3 010 294 E
Prudency Test Procedure	3 010 296 D
Operability Test Procedure	3 010 295 E
Pre-Qualification Acceptance Test Report	3 013 350 A (Campaign 2010) 3 020 950 A (Campaign 2012)

Rolls-Royce reported the test results in Appendix B of the "Summary Equipment Qualification Test Report" (Reference 1.78). The establishment of the baseline performance was acceptable and the results of the prudency testing showed the QTS was able to operate within specifications under dynamic conditions. Based on this information, the NRC staff concluded that the pre-qualification testing and the ensuing results meet the guidance presented in EPRI TR-107330, Section 5.

3.6.4 Radiation Withstand Testing

Radiation withstand testing of the SPINLINE 3 QTS was performed in accordance with the requirements of EPRI TR-107330, Section 4.3.6, and IEEE Std. 323-2003. Radiation exposure testing was performed during Campaigns 2010 and 2011. During the Campaign 2010, Rolls-Royce tested the QTS. This test was performed by Wyle Laboratory at the Southwest Research Institute in San Antonio, TX. During the Campaign 2011, Rolls-Royce tested the QTS spare parts. This test was performed by NTS at the University of Massachusetts Lowell Radiation Laboratory in Lowell, MA. Reference 1.81 describes the test procedure used to perform these tests.

The radiation test acceptance criteria are as given below based on Appendix C of the EQ Plan (Reference 1.77) and EPRI TR-107330, Section 4.3.6:

- The QTS shall not exhibit any exterior damage or degradation as a result of gamma radiation exposure based on visual examinations performed following Radiation Exposure Testing.
- The QTS shall pass the post radiation operability and prudency tests following the completion of radiation exposure testing.

The SPINLINE 3 QTS was not energized during Radiation Exposure Withstand Testing. The radiation test included the withstand capability of the QTS to a rapid dose of radiation that would be normally provided as a long term, dose level of 1100 radiation (plus 100 or minus 0 rad) gamma dose integrated over a 40 year period in a mild environment. Rolls-Royce performed this test to a level higher than the radiation requirement in EPRI TR-107330 to ensure that testing complied with the specific requirements of EPRI TR-107330, Section 4.3.6, and the general requirements of IEEE Std. 323-2003. Due to limitations of the source and the size of the overall test set, components were exposed separately. Each component in Campaigns 2010 and 2011 received the required dose plus margin.

Rolls-Royce described several events that occurred after the radiation exposure during the operability and prudency tests conducted in Campaigns 2010 and 2011. Rolls-Royce reported these events and its resolution in Rolls-Royce "Summary Equipment Qualification Test Report" (Reference 1.78) and "Investigations Results of 2011 NRC Qualification Tests" (Reference 1.79). The majority of these events required replacement of failed boards, fixing cable connections, or modifications to the DAS software. Failed boards were replaced and tested during the Campaign 2011. Some of these events were caused by bad cable connection, which were caused during transportation of the QTS. These events did not affect the results obtained during the radiation exposure test. Based on this information, the QTS met all applicable performance requirements after application of the radiation withstand test conditions.

Post testing inspection revealed no visible effects from the exposure. Rolls-Royce performed operability and prudency tests after radiation exposure withstand. Operability and prudency test results showed that exposure to the radiation test conditions had no adverse effect on the QTS.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	**Document Number**
Prudency Test Procedure	3 010 296 D
Operability Test Procedure	3 010 295 E
Radiation Exposure Test Procedure	3 010 286 B
Radiation Exposure Test Report	3 013 308 A (Campaign 2010) 3 018 588 A (Campaign 2011)

The level of exposure used during testing is consistent with installation in a mild environment, as specified in Section 4.3.6 of EPRI TR-107330. On the basis of these tests, the NRC staff concludes that the QTS hardware is qualified to the radiation exposure levels specified in the EPRI TR-107330. Applicants and licensees that reference this SE should also demonstrate that the maximum expected radiation at each SPINLINE 3 platform installation location will not exceed the maximum qualified radiation during normal plant operation, including anticipated operational occurrences (see Section 5.2, Item 16).

3.6.5 Temperature and Humidity Testing

Rolls-Royce performed environmental tests as identified in Section 4.3.6 and 6.3.3 of EPRI TR-107330 to demonstrate that the SPINLINE 3 platform equipment will not experience failures as a result of abnormal service conditions of temperature and humidity, as required by NRC RG 1.89 and IEEE 323-2003, subject to the enhancements and exceptions listed in Section C of NRC RG 1.209. Specifically, the SPINLINE 3 platform was required to operate under the environmental conditions defined in Section 4.3.6 of EPRI TR-107330. In addition, the acceptance criteria requires that detailed performance characteristics recorded during and after the environmental stress test must remain within acceptable tolerances compared with the performance baseline profile obtained during pre-qualification testing.

The environmental test acceptance criteria are as given below based on Appendix D of the EQ Plan (Reference 1.77), and EPRI TR-107330, Section 4.3.6:

- The QTS shall operate as intended during and after exposure to the environmental test conditions. Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) collected during testing shall demonstrate operation as intended.
- The QTS shall pass the Operability Test following at least 48 hours of operation at high temperature and humidity, following at least 8 hours of operation at low temperature and humidity and upon completion of the test.
- The QTS shall pass the Prudency Test following at least 48 hours of operation at high temperature and humidity.

Environmental testing was performed during Campaigns 2010 and 2011 in accordance with the environmental test procedure (Reference 1.82). During the Campaign 2010, Rolls-Royce could not complete this test due to problems at the test facility. Rolls-Royce decided not to use these results, and instead perform environmental testing during the Campaign 2011. The environmental testing was performed in NTS laboratories in Boxborough, MA.

The EPRI TR-107330 requires that the test PLC shall be powered with its TSAP operating during environmental testing, with one-half of the discrete and relay outputs ON and loaded to its rated current. In addition, all analog outputs shall be set to between one-half and two-thirds of full scale. Rolls-Royce powered its QTS during environmental testing as required in EPRI TR-107330. However, because the QTS only includes relay outputs, more than a half of the output points on each relay were constantly ON. In addition, analog outputs were operated continuously between 50 or 75 percent of full scale. The TSAP was loaded and operated in accordance with the operating mode for environmental testing described in Reference 1.46.

EPRI TR-107330, Section 4.3.6, requires that the test specimen meet its performance requirements during and following exposure to abnormal environmental conditions of 40°F to 120°F and 10 percent to 95 percent relative humidity (non-condensing). For the QTS, Rolls-Royce added additional margin to the required conditions and performed environmental tests from 35°F (2°C) to 140°F (60°C) and 5 percent to 95 percent relative humidity (non-condensing) in accordance with the test procedure defined in Reference 1.82. Rolls-Royce added this margin to ensure that testing complied with the specific requirements of EPRI TR-107330.

EPRI TR-107330, Section 6.3.3.1 requires to measure air temperature near the fan inlet if the power supply includes fans or at the bottom if the test specimen uses natural circulation. Because the QTS cabinet power supply does not include fans, Rolls-Royce installed cooling fans at the top of the cabinet, so it could create a natural circulation configuration by drawing air up through each component. Rolls-Royce monitored air temperature at the bottom of the QTS assembly. Rolls-Royce also monitored air temperature at the inlet of the QTS cabinet cooling fans during testing.

Note that due to limitations of the NTS environmental chamber, Rolls-Royce could not simultaneously test low temperature and humidity. Instead, Rolls-Royce ran a test at the lowest temperature (35°F) testing with a relative humidity of 12 percent, and the another test with a low relative humidity (5 percent) at 77°F. In Reference 1.22, Rolls-Royce explained how these test results sufficiently envelope the SPINLINE 3 platform susceptibility to synergetic effects for these service conditions. Further, EPRI TR-107330, Note 1 of Figure 4-4 allows decoupling the low temperature and low humidity test conditions, if the testing chamber cannot perform such conditions. The sequence of testing followed is described in Appendix D of Reference 1.78.

During environmental testing, operation of the QTS was continuously monitored and recorded by the DAS. The operating mode ran in the TSAP during this test is specified in the "System Specification of the QTS and DAS" (Reference 1.46). The QTS was configured to maximize internal heat generation, power supply loading, and module point loading during the tests. At least one point on each I/O module was monitored for proper operation during testing. Communications modules were exercised through the interface with external monitoring devices. Operability and prudency testing was repeated several times during testing and one time after testing to demonstrate that throughout the testing, the SPINLINE 3 was operating acceptably. Rolls-Royce did not submit the environmental qualification report for NRC staff review but its "Summary Equipment Qualification Test Report" (Reference 1.78) references the environmental qualification report and summarizes the test results. Although some problems were observed during EQ tests, following supplemental testing of the equipment with modifications or failure analysis, the "Summary Equipment Qualification Test Report" states that the environmental qualification performed on the SPINLINE 3 platform equipment met the technical requirements of the IEEE Std. 323-2003 as endorsed by RG 1.209.

Rolls-Royce performed operability testing during environmental tests, as defined in Reference 1.82, and prudency testing during high temperature and humidity tests. Rolls-Royce recorded several events that occurred during environmental testing affecting the QTS or the DAS. Rolls-Royce reported these events and its resolution in Rolls-Royce "Summary Equipment Qualification Test Report" (Reference 1.78) and "Investigations Results of 2011 NRC Qualification Tests" (Reference 1.79). Some of these events were most likely caused by bad cable connection, which were caused during transportation of the QTS to the test facility. Other events were caused by board failures; in these cases the boards were replaced with spare boards and the QTS was retested. Two events were caused by improper acceptance criteria values of the 48 VDC/24 VDC power converters. Rolls-Royce provided a detailed explanation of the test deficiencies and the analysis performed to resolve them in Reference 1.79; resolution required calculating new acceptance criteria values for the power converters to be used in the operability test procedure for Campaign 2012. Rolls-Royce confirmed that the values obtained during the Campaign 2011 met the new acceptance criteria (Reference 1.79). This became the new acceptance criteria for 48 VDC/24 VDC power converters. The new power converter installed in the QTS was Part Number 3 008 467.

In addition, during testing, Rolls-Royce observed a problem with unused digital inputs in the 16E.ANA board. To address this, Rolls-Royce reported in Reference 1.79 that after analyzing

the event and test results, they connected all unused inputs to ground (0 VDC) to avoid exceeding the tolerance limit. This event was detected because the DAS was collecting data from all inputs and compared them to a null input condition, which will not be the case when the SPINLINE 3 platform is used in application specific project. These events did not affect the results observed during environmental testing.

Details of environmental testing can be found in the following Rolls-Royce documents:

Document Title	**Document Number**
System Setup & Checkout Test Procedure	3 010 294 E
Prudency Test Procedure	3 010 296 D
Operability Test Procedure	3 010 295 E
Environmental Test Procedure	3 010 287 B
Environmental Test Report	3 013 309 A (Campaign 2010) 3 018 589 A (Campaign 2011)

After reviewing the information provided, the NRC staff determined that the manufacturer's temperature and humidity qualification conforms to the RG 1.209, Regulatory Position 4, and determined that the SPINLINE 3 platform met the requirements of EPRI TR-107330, Sections 4.3.6 and 6.3.3. An applicant or licensee that reference this SE should ensure that the temperature and humidity at the SPINLINE 3 platform installation location will not exceed the qualified temperature and humidity during normal plant operation, including anticipated operational occurrences (see Section 5.2, Item 15).

3.6.6 Seismic Testing

Seismic Testing was performed to demonstrate the suitability of the SPINLINE 3 platform for qualification as a Category 1 seismic device based on seismic withstand testing performed on the SPINLINE 3 QTS in accordance with RG 1.100 and IEEE Std. 344-1987. Section 4.3.9 of EPRI TR-107330 defines the recommended seismic test levels the test specimen is expected to withstand (i.e., the test specimen must continue to meet the manufacturer specified performance levels). These tests established the qualification envelope for SPINLINE 3 seismic withstand.

Due to the size of the QTS, Rolls-Royce could not mount all sub-assemblies on the lab's vibration table, so they had to separate the QTS components in the following two configurations and perform separate seismic tests.

- Configuration 1 – PU1 (QTS modules except RTD modules) and PU2 (QTS module with RTD) racks, hubs and converters assembly system (HCAS), and analog input output terminal block (AIOTB) and digital input terminal block (DITB).
- Configuration 2 – power supply rack type 1 (PS1 – 48 VDC/24 VDC) and type 2 (PS2 – 120 VAC/48 VDC), fan assembly, power supply assembly, periodic test assembly, and relay output terminal (ROTB) types 1 and 2.

Seismic testing was performed during Campaigns 2011 and 2012. During the Campaign 2011, Rolls-Royce encountered several problems that required reconfiguration and retesting of the QTS. Specifically, during the Campaign 2011, Rolls-Royce encountered failures in PU1 and HCAS due to mechanical problems with the test frame and cable connections. Rolls-Royce corrected these problems and during Campaign 2012, Rolls-Royce performed the necessary retesting of these components. The seismic tests were performed in NTS laboratories in Acton, MA. The Rolls-Royce Seismic Test Procedure (Reference 1.83) describes the test procedure for the Campaign 2011 and for the 2012. Rolls-Royce did not submit the seismic qualification report for NRC staff review but the manufacturer's "Summary Equipment Qualification Test Report" references the seismic qualification report and summarizes the test results.

During seismic testing, Rolls-Royce subjected Configuration 1 and Configuration 2 to a series of seismic simulation tests using a triaxial seismic simulator shake table. These tests included resonance search tests, as specified in IEEE Std. 344-1987, followed by five simulated Operating Basis Earthquakes (OBEs) and two simulated Safe Shutdown Earthquake (SSE).

The simulation vibrations are required to be applied triaxially (in three orthogonal directions), with random frequency content. The maximum SSE and OBE levels shown in Figure 4-5 of EPRI TR-107330 are (maximum acceleration) 14 g's and 9.75 g's respectively, based on 5 percent damping. However, Rolls-Royce used different SSE and OBE levels during seismic testing. These levels were based on testing previously performed in France. Thus, Rolls-Royce performed the five OBEs at 4.9 g and the SSE at 7 g. Specifically, Rolls-Royce performed the following tests in the 2011 Campaign:

- Resonance search as described in Section 7.1.4 of IEEE Std. 344-1987.
- Five triaxial Operating Basis Earthquake (OBEs) tests with a minimum Zero Period Acceleration (ZPA) of 4.9 g.
- One triaxial SSE test with a minimum ZPA of 7 g.

In the 2012 Campaign, Rolls-Royce performed the following additional tests to retest equipment that did not pass during the 2011 Campaign:

- Resonance search as described in Section 7.1.4 of IEEE Std. 344-1987.
- Five triaxial Operating Basis Earthquake (OBEs) tests with a minimum Zero Period Acceleration (ZPA) of 3.5 g.
- One triaxial SSE test with a minimum ZPA of 4.9 g.
- One triaxial SSE test with a minimum ZPA of 7 g.

The SPINLINE 3 QTS was mounted to the seismic test table in accordance with the Rolls-Royce Seismic Test Procedure (Reference 1.83) in order to simulate a typical 19-inch rack mount configuration using QTS SPINLINE 3 chassis mounting brackets and fastener hardware, and external termination assembly mounting plates. During seismic tests, the AC power supply to the QTS cabinet power supply was energized. Also, during testing Rolls-Royce de-energized

one of the two redundant 120 VAC power supply feeds to the QTS cabinet power supply assembly in order to place the full QTS load on only three of the six power converter groups. Note that EPRI TR-107330, Section 6.3.4.2, requires that seismic testing be performed with the power sources to the test PLC power supply modules set to operate at specified AC and DC source voltages and frequencies. Rolls-Royce did not test this requirement because the QTS does not include cabinet power supply modules fed from external DC sources. The TSAP was loaded and operating during seismic testing, exercising QTS components, and supporting automated test data collection in accordance with the operation mode described in Reference 1.46 for seismic testing.

Because the SPINLINE 3 platform does not include solid-state discrete outputs, the TSAP operated several of the relay output points to support measurement of time response during seismic testing. In particular, the QTS includes 16 Type 1 output relays and 16 Type 2 output relays, for a total of 32 output relays. In its RAI response (Reference 1.22), Rolls-Royce explained the circuits for the relays and related contacts were configured to monitor for chattering. Reference 1.46 shows the relay output circuit used during seismic testing. The output relay contacts were configured to operate at voltages of 24 VDC, 48 VDC, 125 VDC and 120 VAC. The output of these relays transitioned in such a manner that during the Seismic testing, approximately one-half of the output relays (16 or 14 of 32) were held ON and approximately one-half of the output relays (16 or 14 of 32) were held OFF. Also, every 5 seconds, one-quarter of the output relays (8 or 10 of 32) transitioned from OFF to ON, and one-quarter of the output relays (8 or 10 of 32) transitioned from ON to OFF.

The SPINLINE 3 QTS did not fully comply with the seismic requirements. The seismic table achieved the EPRI TR-107330 OBE and SSE Required Response Spectrum test levels throughout most of the required frequency range. The “Summary Equipment Qualification Test Report” shows OBE and SSE test results followed the RRS curve provided in Figure 4-5 in EPRI TR-107330 within the limits of the test facility seismic test table, with the exception that the minimum ZPA requirements are met. Results of the testing are described in the Summary Equipment Qualification Test Report, Reference 1.78. Below are brief descriptions of the events and failures reported during testing, as well as equipment limitations.

The maximum SSE and OBE acceleration levels for Campaign 2011 were 14 g maximum/ 7g ZPA and 9.75 maximum/4.9 g. ZPA respectively, based on 5 percent damping. Rolls-Royce recorded that the maximum SSE and OBE acceleration levels for the 2011 seismic testing exceeded the RRS curve given in Figure 4-5 in EPRI TR-107330. These results correspond to Configuration 1, except for the components tested during Campaign 2012, and Configuration 2. The maximum SSE and OBE acceleration levels for the components tested during Campaign 2012 were 14 g maximum / 7 g ZPA and 9.75 maximum / 3.5 g. ZPA respectively, based on a 5 percent damping.

During the Campaign 2011, the QTS Configuration 1 showed two resonances frequencies below 100 HZ. Evaluation of this failure showed that the mounting configuration was not rigid enough for seismic testing. To address this, Rolls-Royce modified the test fixture and mounting

configuration and retested the QTS during the Campaign 2012. In 2012, Rolls-Royce did not observe resonances below 100HZ for Configuration 1. QTS Configuration 2 did not show resonances frequencies below 100 HZ. Most of the SPINLINE 3 equipment in Configuration 1 passed the 2011 Seismic Test except for the problems noted above. The two subassemblies of the SPINLINE 3 equipment in Configuration 1 were successfully retested in the 2012 test campaign.

Rolls-Royce recorded several events that occurred during seismic testing affecting the QTS or the DAS. Rolls-Royce reported these events and its resolution in Rolls-Royce "Summary Equipment Qualification Test Report" (Reference 1.78) and "Investigations Results of 2011 NRC Qualification Tests" (Reference 1.79). During seismic testing Rolls-Royce observed accuracy problems with the 6SANA modules. These problems were caused by not securing the potentiometers to the module. As part of the redesign of the mounting configuration, Rolls-Royce adjusted the potentiometers to be secured for the 6SANA modules, and then retested the module during the Campaign 2012. In addition, several modifications were made to the DAS and QTS before retesting the system, such as modifications to the assembly, cable configuration, and hub connections. In References 1.78 and 1.79, Rolls-Royce explains that the wiring and cabling requirements for the SPINLINE 3 platform are provided in its "Règles de Câblages dans les équipements type SPINLINE." Before using SPINLINE 3 system equipment in SR systems in a NPP, licensees must use this cable documentation for installation in order to determine that the plant-specific seismic requirements are enveloped by the capabilities of the system (see Section 5.2, Item 18).

Table 5-1 of EPRI TR-107330 requires that Operability and Prudency Testing be performed during SSE. Because the duration of each Operating Basis Earthquake/safe shutdown earthquake test (approximately 30 seconds) did not support full Operability or Prudency Testing, Rolls-Royce did not perform the Operability and Prudency Tests during the Seismic Tests. However, Rolls-Royce considers that the data collected during and after each OBE and SSE test demonstrated that the QTS operated as intended throughout the testing. In addition, Table 5-1 and Section 6.3.4.3 of EPRI TR-107330 require post-seismic Operability Testing to assess the impact of exposure to the OBE and SSE vibrations on the operability of the test specimen. Test results provided in the Summary EQ Test Report showed that exposure to the OBE and SSE vibrations had no adverse effects on the QTS performance.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	**Document Number**
Seismic Test Procedure	3 010 288 D
System Setup & Checkout Test Procedure	3 010 294 E
Prudency Test Procedure	3 010 296 D
Operability Test Procedure	3 010 295 E
Seismic Test Report	3 018 590 A (Campaign 2011) 3 020 948 A (Campaign 2012)

Based on the information provided, the NRC staff determined that the tested SPINLINE 3 QTS is qualified to the tested triaxial seismic simulator table limits, with the exceptions described above. For this reason the NRC staff finds that the SPINLINE 3 QTS system did not fully meet the requirements of EPRI TR-107330 for seismic requirements, and before using SPINLINE 3 platform in SR systems in a NPP, licensees must determine that the plant-specific seismic requirements are enveloped by the capabilities of the SPINLINE 3 system. This determination and the suitability of the SPINLINE 3 system for a particular plant and application is the responsibility of the licensee (see Section 5.2, Item 19).

3.6.7 Electromagnetic Interference / Radio Frequency Testing

EPRI TR-107330 includes EMC testing as part of the overall program to generically qualify a PLC for SR application in a NPP. Specific criteria for electromagnetic emissions, EMI susceptibility, electrostatic discharge withstand, power surge withstand, and isolation capability are given in Sections 4.3, “Hardware Requirements,” and 4.6, “Electrical,” of the guide while the qualification approach is specified in Section 6.3, “Qualification Tests and Analysis Requirements.”

Rolls-Royce performed EMI/RFI testing to demonstrate compliance with the applicable EMI/RFI emissions and susceptibility requirements of NRC RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” using additional guidance from EPRI TR-107330 as applicable. Rolls-Royce performed this test in accordance with its EMI/RFI test procedure (Reference 1.87). RG 1.180 endorses Military Standard (MIL-STD) 461E, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” and IEC 61000 series standards for the evaluation of the impact of EMI and RFI. The specific EMI/RFI tests performed included:

<u>EMI/RFI Emissions Tests</u>

- MIL-461E, CE101: Conducted Emissions, Low Frequency, AC and DC Power Leads
- MIL-461E, CE102: Conducted Emissions, High Frequency, AC and DC Power Leads
- MIL-461E, RE101: Radiated Emissions, Magnetic Field, QTS Surfaces and Leads
- MIL-461E, RE102: Radiated Emissions, Electric Field, Antenna Measurement

<u>EMI/RFI Susceptibility Tests</u>

- IEC 61000-4-6: Conducted Susceptibility, Induced RF Fields, Power/Signal Leads
- IEC 61000-4-13: Conducted Susceptibility, Harmonics/Interharmonics, Power Leads
- IEC 61000-4-16: Conducted Susceptibility, Common Mode Disturbance, Power/Signal Leads
- IEC 61000-4-8: Radiated Susceptibility, Magnetic Field, Helmholtz Coil Exposure
- IEC 61000-4-9: Radiated Susceptibility, Magnetic Field, Pulsed
- IEC 61000-4-10: Radiated Susceptibility, Magnetic Field, Damped Oscillatory
- IEC 61000-4-3: Radiated Susceptibility, High Frequency, Antenna Exposure

- MIL-STD-461 E: RS-103, Radiated Susceptibility, High Frequency, Antenna Exposure (from 1 to 8 GHz)

Note that Section 3 of USNRC RG 1.180, Revision 1, describes states that the qualifier can use either IEC or MIL-STD. series of test methods, and the series chosen must be applied in its entirety (no selective application or mixing of the MIL-STD. and IEC test methods). Rolls-Royce decided to use IEC 61000 series for the susceptibility tests, but mixing of methodology was necessary for the radiated susceptibility test, as IEC 61000-4-3 standard doesn't cover the radiated test up to 8 GHz. Therefore, Rolls-Royce performed radiated susceptibility test for the band 1-8 GHz using the MIL-STD. 461 E/RS103 methodology. Appendix O of the EQ Plan (Reference 1.77) describes the approach for this additional EMI/RFI test.

The EMI/RFI test acceptance criteria are as follows, based on Appendix F of the "Equipment Qualification Plan" (Reference 1.77), and EPRI TR-107330, Section 4.3.7:

- The QTS shall meet allowable equipment emission limits as specified in RG 1.180, Revision 1, for conducted and radiated emissions.
- The QTS shall operate as intended during and after application of the EMI/RFI test levels specified in RG 1.180 for conducted and radiated susceptibility.

In addition, evaluation of normal operating performance data (inputs, outputs, and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance criteria from Section 4.3.7 of EPRI TR-107330:

- The main processors and coprocessors shall continue to function
- The transfer of I/O data shall not be interrupted
- The emissions shall not cause the discrete I/O to change state
- Analog I/O levels shall not vary more than 3 percent

EMI/RFI testing was performed during Campaigns 2011 and 2012. During the Campaign 2011, Rolls-Royce encountered several problems during EMI/RFI and post EMI/RFI Proof testing that required reconfiguration and retesting of the QTS. Test documents included a brief explanation of the modifications made. Rolls-Royce corrected these problems and during Campaign 2012, Rolls-Royce performed the necessary retesting of the QTS. The EMI/RFI tests were performed in NTS facilities in Boxborough, MA. The Rolls-Royce EMI/RFI Test Procedure (Reference 1.87) describes the test procedure for the Campaign 2011 and for the 2012. In addition, Appendix O of the EQ Plan (Reference 1.77) describes the approach for additional EMI/RFI Testing of the Rolls-Royce SPINLINE 3 QTS performed in 2012. The specific EMI/RFI tests performed were:

- IEC 61000-4-16: Conducted Susceptibility, Common Mode Disturbance, Signal Leads - DC portion on Digital Inputs.

- MIL-STD. 461 E - RS103: Radiated Susceptibility, High Frequency, Antenna Exposure (from 1 GHz to 8 GHz).

In the Campaign 2011, the EMI/RFI testing was performed after completion of the ESD and EFT testing. In the Campaign 2012, the EMI/RFI testing was performed after the seismic testing. Rolls-Royce did not submit the EMI/RFI testing report for NRC staff review but the manufacturer's "Summary EQ Test Report" (Reference 1.78) references the EMI/RFI qualification report and summarizes the test results. The results described in the Summary EQ Test Report showed that the SPINLINE 3 platform does not fully comply with the allowable equipment emissions levels defined in RG 1.180, Revision 1. Specifically, Rolls-Royce chose not to perform the 61000-4-10 test (Radiated susceptibility, magnetic field) due to laboratory test limitations. RG 1.180, Revision 1, allows that equipment not intended to be installed in areas with strong sources of magnetic fields (e.g., cathode ray tubes, motors, cable bundles carrying high currents) can be exempt from this test. Rolls-Royce chose not to perform the RS103, Radiated Susceptibility test above 8 GHz, since that frequency range is reserved for satellite communication. Therefore, the SPINLINE 3 platform cannot be installed in areas with strong sources of magnetic fields and areas with radiated susceptibility above 8 GHz. Below is a description of the EMI/RFI testing performed, as well as events observed during these tests.

The SPINLINE 3 QTS was installed in the EMI/RFI test chamber mounted in metal frame instrument cabinets with all sides removed. Due to the size of the SPINLINE 3 QTS, the QTS could not meet the requirements to be mounted 6 ft. above the floor of the test chamber identified on EPRI TR-107330, Section 6.3.2.1. To prevent the EMI/RFI test results from being affected by beneficial ground paths that might exist through the test specimen mounting frame, the SPINLINE 3 QTS mounting frame(s) was mounted on non-conductive (i.e., wooden) supports approximately 4 inches above the floor of the test chamber. This was done to prevent the EMI/RFI test results from being affected by beneficial ground paths that might exist through the test specimen mounting frames. The test system power distribution was located inside the test chamber, even though this panel is not part of the QTS. Grounding and configuration of the power distribution panel was specified by Rolls-Royce. No additional components, cabinet or cable shielding was installed inside the chamber, and no additional noise filters or suppression devices were used on the I/O interfaces. The test system power supply circuits to the QTS cabinet power supply assembly were energized during testing. All test system power supply cables entering the EMI/RFI test chamber passed through filter capacitors located in the chamber walls.

During EMI/RFI, the QTS ran the TSAP, using the operating mode defined in Reference 1.46 for the EMI/RFI testing. In order to minimize transmission of outside EMI/RFI sources into the EMI/RFI test chamber, all power, signal, and communications cables entering the EMI/RFI test chamber were passed through filters located in the chamber walls. The DAS was installed outside the EMC chamber. In addition, to minimize the number of signal wire pass through filters, only signal wires from one circuit per I/O module was used during the test. All other signals were disconnected during testing.

EPRI TR-107330 requires that a portion of the Operability and Prudency tests be performed during the EMI/RFI testing. However, Rolls-Royce did not perform these tests because the configuration of the QTS inside the EMC chamber did not permit it. Instead, Rolls-Royce recorded data during the EMI/RFI test that demonstrated acceptable system performance during EMI/RFI. Note that the configuration of the QTS in the EMC chamber was maintained for the tests that followed EMI/RFI test (Surge Withstand and Class 1E to Non-1E Isolation).

Rolls-Royce recorded several events that occurred during EMI/RFI testing affecting the QTS or the DAS. Rolls-Royce reported these events and its resolution in Rolls-Royce "Summary Equipment Qualification Test Report" (Reference 1.78) and "Investigations Results of 2011 NRC Qualification Tests" (Reference 1.79). For example, while performing the DC portions of the IEC 610000-4-16 tests, Rolls-Royce noted a problem with the voltage injected to the equipment. Rolls-Royce analyzed this condition at its facilities and found the cause and solution to this event. Even though Rolls-Royce considered that the equipment passed the test, Rolls-Royce decided to retest the DC portions of the IEC 610000-4-16 the QTS during the Campaign 2012, which passed successfully. Appendix O of the EQ Plan explained the tests performed. Another event was that Rolls-Royce did not perform the test steps for CE101 and CE102 that required connection of the 120 VAC through LISN. Rolls-Royce explained in Reference 1.79 that this was not done because the QTS was configured differently than required in the EMI/RFI test procedure for this step. Lastly, Rolls-Royce performed MIL-STD-461E RE101 and RE102 on the area where worst case of emissions could be expected. For RE101, Rolls-Royce and NTS determined that the bottom face could not be tested due to space constraints. However, they determined what part of the bottom back face produced the higher level of emissions, which was the half where the cables came inside the cabinet, and afterwards Rolls-Royce performed the RE101 test. For RE102, Rolls-Royce and NTS determined that the worst case was the back face, since the front face is metallic, and afterwards Rolls-Royce performed the RE102 test. The QTS passed these tests successfully.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	**Document Number**
EMI/RFI Test Procedure	3 010 289 C
System Setup & Checkout Test Procedure	3 010 294 E
EMI/RFI Test Report	3 018 591 A (Campaign 2011) 3 020 951 B (Campaing 2012)

The NRC staff reviewed the "Summary EQ Test Report" and determined that the tested SPINLINE 3 platform met the EMI/RFI test acceptance criteria discussed above and is qualified up to the tested limits described above, with the exceptions of IEC 61000-4-10 testing levels and radiated susceptibility above 8 GHz. These limitations are consistent with RG 1.180, as long as the equipment is not installed in areas with source of strong magnetic fields or radiated emission sources above 8GHz.

Given the exceptions noted above, the NRC staff determined that the SPINLINE 3 platform did not fully meet the guidance of RG 1.180, Revision 1, for conducted or radiated emissions or susceptibility. Before using the SPINLINE 3 platform equipment in safety related systems in a nuclear power plant, licensees must determine that the plant-specific EMI requirements are enveloped by the capabilities of the SPINLINE 3 platform as approved in this SE. This determination and the suitability of the SPINLINE 3 platform for a particular plant and application is the responsibility of the licensee (see Section 5.2, Item 20).

3.6.8 Electrical Fast Transient Testing

EFT testing of the SPINLINE 3 QTS was performed as part of qualification testing to demonstrate compliance with the applicable EFT susceptibility requirements of NRC RG 1.180, Revision 1, using additional guidance from EPRI TR-107330, as applicable. The specific EFT test performed was IEC 61000-4-4, "Electromagnetic Compatibility (EMC), Part 4-4: Testing and Measurement Techniques, Electrical Fast Transient/Burst Immunity Test." This test established the qualification envelope for SPINLINE 3 for EFT susceptibility.

This test used the same SPINLINE 3 QTS configuration and test system setup described in the EMI/RFI Testing. The EFT testing was performed after completion of the ESD testing. The EFT testing was performed in the EMC chamber at the NTS facilities in Boxborough, MA.

During EFT, the QTS ran the TSAP operating mode defined in the QTS/DAS System Specification (Reference 1.46) for EFT testing. In particular, it cycled all but one of the output relay circuits on timed ON/OFF cycles. EFT testing was performed on a representative sample of I/O points.

EFT testing of the QTS is described in the "EFT Test Procedure" (Reference 1.88). This procedure states that the cabinet power supply assembly of a SPINLINE 3 platform is expected to be installed in Category B locations with EFT Low Exposure levels. So testing was performed to the corresponding EFT withstand level of 2 kV. Additionally, the signal circuits of the SPINLINE 3 platform are expected to be installed in Category B. So testing was performed to the corresponding EFT withstand level of 1 kV, with applied EFT test levels will be stepped up from 0.5 kV to the maximum specified test voltage in 0.5 kV increments.

The EFT test acceptance criteria were described in Appendix G of the Rolls-Royce EQ Plan, which was defined according to EPRI TR-107330, Section 4.3.7. Specifically, the QTS must withstand the applied EFT susceptibility test levels, and perform as follows:

- The QTS shall operate as intended during and after application of the IEC 61000-4-4 EFT test levels specified in Sections 4.2 and 5.3 of NRC RG 1.180, Rev. 1 for low exposure applications. Specifically:
    - IEC 61000-4-4: Power Leads, Level 3 Test Voltage Level: 2 kV max.
    - IEC 61000-4-4: Signal Leads, Level 3 Test Voltage Level: 1 kV max.

Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance from Section 4.3.7 of EPRI TR-107330:

- The main processors and coprocessors shall continue to function.
- The transfer of I/O data shall not be interrupted.
- The applied EFT disturbances shall not cause the discrete inputs/outputs to change state.
- Analog I/O levels shall not vary more than 3 percent (of full scale).

- Applying the EFT test voltages to the specified QTS interfaces will not damage any module or device in the QTS, or cause disruption of the operation of the BAP signals or any other data acquisition signals

As mentioned in the EMI/RFI testing, Rolls-Royce did not perform Operability and Prudency tests required in EPRI TR-107330 because the configuration of the QTS inside the EMC chamber did not permit it. Instead, Rolls-Royce recorded data during the test that demonstrated acceptable system performance during EFT. Note that the configuration of the QTS in the EMC chamber was maintained for the tests that followed EFT test (EMI/RFI, Surge Withstand, and Class 1E to Non-1E Isolation).

Rolls-Royce did not submit the EFT testing report for NRC staff review but Rolls-Royce "Summary EQ Test Report" (Reference 1.78) references the Surge Withstand qualification report and summarizes the test results. The Summary EQ Test Report states that the QTS passed the EFT testing.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	**Document Number**
EFT Test Procedure	3 010 290 B
EFT Test Report	3 018 592 A

The NRC staff reviewed the Summary EQ Test Report (Reference 1.78), and determined that the SPINLINE 3 platform exhibits acceptable performance against electrical fast transients as addressed in RG 1.180, Revision 1. Licensees must determine that the plant-specific EFT requirements are enveloped by the capabilities of the SPINLINE 3 system. This determination and the suitability of the SPINLINE 3 system for a particular plant and application is the responsibility of the licensee (see Section 5.2, Item 15).

3.6.9 Surge Withstand Testing

Rolls-Royce performed Surge Withstand testing on the SPINLINE 3 platform in accordance with RG 1.180, Revision 1. Specifically, the Surge Withstand Testing included:

- IEC 61000-4-5, “Electromagnetic Compatibility (EMC), Part 4-5: Testing and Measurement Techniques, Surge Immunity Test.”
- IEC 61000-4-12, “Electromagnetic Compatibility (EMC), Part 4-12: Testing and Measurement Techniques, Oscillatory Waves Immunity Test.”

This test used the same SPINLINE 3 QTS configuration and test system setup described in the EMI/RFI Testing. The Surge Withstand testing was performed after completion of the EMI/RFI testing. The Surge Withstand testing was performed in the EMC chamber at the NTS facilities in Boxborough, MA.

During Surge Withstand, the QTS ran the TSAP operating mode described in QTS/DAS System Specification (Reference 1.46) for surge withstand testing. In particular, it cycled all but one of the output relay circuits on timed ON/OFF cycles. Surge Withstand testing of the QTS is described in the “Surge Withstand Test Procedure” (Reference 1.89). This procedure states that the cabinet power supply assembly of a SPINLINE 3 platform is expected to be installed in Category B locations with surge waveform Low Exposure levels. So testing was performed to the corresponding ring wave surge withstand level of 2 kV and the corresponding combination wave surge withstand level of 2 kV open circuit and 1 kA short circuit. Additionally, the signal circuits of the SPINLINE 3 platform are expected to be installed in Low Exposure locations with Level 2 surge waveforms. So testing was performed to the corresponding ring wave surge withstand level of 1 kV and the corresponding combination wave surge withstand level of 1 kV open circuit and 0.5 kA short circuit.

The Surge Withstand test acceptance criteria were described in Appendix H of the Rolls-Royce EQ Plan (Reference 1.77), which was defined according to EPRI TR-107330, Section 4.6.2. Specifically, the QTS must withstand the surge withstand test levels, and perform as follows:

- Applying the Surge Withstand test voltages specified in Tables 15 and 22 of NRC RG 1.180, Revision 1 for low exposure applications to the specified QTS interfaces will not damage any module or device in the QTS, or cause disruption of the operation of the BAP signals or any data acquisition signals that could result in a loss of the ability to generate an trip.
- Evaluation of normal operating performance data (inputs, outputs, fault/diagnostic indicators and NERVIA communication links) shall demonstrate satisfactory operation of the QTS following application of the surge test voltages.
- Per Section 6.3.5 of EPRI TR-107330, failures of one or more redundant devices are acceptable as long as the failures do not result in the inability of the QTS to operate as intended. Faults or failures of redundant devices which occur during Surge Withstand testing will be evaluated for effect on the QTS operation.

As mentioned in the EMI/RFI testing, Rolls-Royce did not perform Operability and Prudency tests required in EPRI TR-107330 because the configuration of the QTS inside the EMC chamber did not permit it. Instead, Rolls-Royce recorded data during the test that demonstrated

acceptable system performance during Surge Withstand. Note that the configuration of the QTS in the EMC chamber was maintained for the tests that followed EMC test.

Rolls-Royce did not submit the Surge Withstand testing report for NRC staff review but the manufacturer's "Summary EQ Test Report" (Reference 1.78) references the Surge Withstand qualification report and summarizes the test results. The Summary EQ Test Report states that the QTS passed the Surge Withstand testing.

Rolls-Royce recorded several events that occurred during Surge Withstand testing affecting the DAS. Rolls-Royce reported these events and its resolution in Rolls-Royce "Summary Equipment Qualification Test Report" (Reference 1.78) and "Investigations Results of 2011 NRC Qualification Tests" (Reference 1.79). These events were identified by comparing data received by the DAS with the NERVIA data during testing. Rolls-Royce determined that these events did not affect the results recorded. Furthermore, Rolls-Royce modified the DAS to address these problems.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	**Document Number**
Surge Withstand Test Procedure	3 010 291 A
Surge Withstand Test Report	3 018 593 A

The NRC staff reviewed the Summary EQ Test Report (Reference 1.78), and determined that the SPINLINE 3 platform meets the surge withstand performance criteria in EPRI TR-107330and RG 1.180, Revision 1. Licensees must determine that the plant-specific surge requirements are enveloped by the capabilities of the SPINLINE 3 system. This determination and the suitability of the SPINLINE 3 system for a particular plant and application is the responsibility of the licensee (see Section 5.2, Item 15).

3.6.10 Electrostatic Discharge Withstand Testing

EPRI TR-107330, Section 4.3.8, requires that the test specimen under qualification be tested for immunity to the ESD test levels specified in EPRI TR-102323, Revision 1. Rolls-Royce performed ESD testing to demonstrate the suitability of the SPINLINE 3 platform for qualification as a SR device with respect to ESD withstand levels specified in EPRI TR-102323, Revision 1. Rolls-Royce performed the ESD test in accordance with IEC 61000-4-2 "Electromagnetic Compatibility, Part 4-2: Testing and Measurement Techniques, Electrostatic Discharge Immunity Test".

This test used the same SPINLINE 3 QTS configuration and test system setup described in the EMI/RFI Testing. The ESD testing was performed after completion of Seismic OBE testing. The ESD testing was performed in the EMC chamber at the NTS facilities in Boxborough, MA.

During ESD, the QTS ran the TSAP operating mode described in QTS/DAS System Specification (Reference 1.46) for ESD testing. In particular, it cycled all but one of the output relay circuits on timed ON/OFF cycles. ESD testing of the QTS is described in the "ESD Test Procedure" (Reference 1.90). This procedure identifies the selected points for application of electrostatic discharges to the QTS. In addition, electrostatic discharges were applied to horizontal and vertical edges of coupling planes setup in proximity to the QTS in accordance with Sections 8.3.3.2 and 8.3.3.3 of IEC 61000-4-2.

This procedure also states that Section 3.5 of EPRI TR-102323 recommends maximum ESD test levels of 15 kV for air discharges and 8 kV for contact discharges for SR instrumentation to be installed in a nuclear plant control room, which corresponds to IEC 61000-4-2 Level 4 installations. Rolls-Royce tested the QTS to maximum ESD test levels of 8 kV for air discharges and 6 kV for contact discharges, which correspond to IEC 61000-4-2 Level 3 installations. For Level 3 air discharges at 8 kV, the lower test levels include 4 kV and 2 kV. For Level 3 contact discharges at 6 kV, the lower test levels include 4 kV and 2 kV.

The ESD test acceptance criteria were described in Appendix I of the Rolls-Royce EQ Plan, which was defined according to EPRI TR-107330, Section 4.3.8. Specifically, the QTS must withstand the ESD test levels, and perform as follows:

- Applying the ESD test levels specified in Section 3.2 above to the specified QTS test points shall not damage any component in the QTS (see below for exception for redundant components), or cause disruption of the operation of the QTS BAP signals or any other data acquisition signals that could result in a loss of the ability to generate a trip.
  Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance from Section 4.3.7 of EPRI TR-107330:
  - The main processors and coprocessors shall continue to function.
  - The transfer of I/O data shall not be interrupted.
  - The applied ESD disturbances shall not cause the discrete inputs/outputs to change state.
  - Analog I/O levels shall not vary more than 3 percent (of full scale).

- Per Section 4.3.8 of EPRI TR-107330, failures of one or more redundant devices due to application of ESD test levels are acceptable as long as the failures do not result in the inability of the QTS to operate as intended. Faults or failures of redundant devices which occur during ESD testing will be evaluated for effect on the QTS operation. Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate intended operation of the QTS.

Rolls-Royce recorded several events that occurred during ESD testing affecting the DAS and QTS. Rolls-Royce reported these events and its resolution in Rolls-Royce "Summary

Equipment Qualification Test Report" (Reference 1.78) and "Investigations Results of 2011 NRC Qualification Tests" (Reference 1.79). Rolls-Royce determined that events related to the DAS did not affect the results recorded. During ESD testing, Rolls-Royce observed that the 3TP/2FL hub exhibited intermittent performance during ESD testing. To address this problem, Rolls-Royce added a requirement to use anti-static controls during maintenance of the SPINLINE 3 platform based system.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	Document Number
ESD Test Procedure	3 010 292 A
ESD Test Report	3 018 594 A

The NRC staff reviewed the "Summary Equipment Qualification Test Report" and determined that the tested SPINLINE 3 platform met the ESD test acceptance criteria discussed above and is qualified up to the tested limits described above, with the exception that during maintenance, plant personnel must use anti-static controls (see Section 5.2, Item 21).

Given the exception noted above, the NRC staff determined that the SPINLINE 3 platform did not fully meet the guidance of EPRI TR 102323, Revision 1, for ESD. Before using the SPINLINE 3 platform in SR systems in a nuclear power plant, licensees must determine that the plant-specific ESD requirements are enveloped by the capabilities of the SPINLINE 3 platform as approved in this SE. This determination and the suitability of the SPINLINE 3 platform for a particular plant and application is the responsibility of the licensee (see Section 5.2, Item 15).

3.6.11 Class 1E to Non-1E Isolation Testing

Rolls-Royce performed isolation testing on the SPINLINE 3 QTS in accordance with IEEE Std. 384-1981 and Section 6.3.6 of EPRI TR-107330. In particular, IEEE Std. 384-1981 requires that: (a) the isolation device prevents shorts, grounds, and open circuits on the Non-Class 1E side from unacceptably degrading the operation of the circuits on the Class 1E side and (b) the isolation device prevents application of the maximum credible voltage on the Non-Class 1E side from degrading unacceptably the operation of the circuits on the Class 1E side. The details of the tests are described in the "Class 1E to Non-1E Isolation Test Procedure" (Reference 1.91).

For this test, Rolls-Royce used the same SPINLINE 3 QTS configuration and test system setup described in the EMI/RFI Testing. The 1E to non-1E isolation testing was performed after completion of the last EMI/RFI Test. The 1E to non-1E isolation testing was performed at the NTS facilities in Acton, MA. Because of the problems observed during Seismic tests and the decision to perform additional testing in 2012, Rolls-Royce performed post EMI/RFI Operability and Prudency tests after the Class 1E to non-1E isolation testing.

The qualification of the SPINLINE 3 platform is based on a system design that permits Non-1E connections to the analog and mechanical output relay interfaces. Non-1E connections to the

SPINLINE 3 NERVIA network interfaces are also permitted through fiber optic cables. Accordingly, the following connections were tested: the 6SANA analog output module when interfaced with the Model I.6SANA Interface Board and SPINLINE 3 External Termination Panel (ETP), 32ACT discrete output module when interfaced with the Model I.32ACT Interface Board, Model MV16 Voting Module, Model 8SRELAY1 output relays terminal block, and Model 8SRELAY2 output relays terminal block. The NERVIA+ communication was not tested because this network uses fiber optic, which is incapable of transmitting electrical faults.

This test used the same SPINLINE 3 QTS configuration and test system setup described in the EMI/RFI Testing. During this test, the QTS ran the TSAP operating mode described in QTS/DAS System Specification (Reference 1.46) for Class 1E to non-1E testing. In particular, it cycled all but one of the output relay circuits on timed ON/OFF cycles. The TSAP also cycled a number of the analog output circuits through stair-stepping output values on repeating cycles, and exercised the NERVIA communication interface. The communication between the QTS and DAS was done using fiber optic cables.

Section 4.6.4 of EPRI TR-107330 requires that the test specimen modules under qualification provide electrical isolation capability of at least 600 VAC and 250 VDC applied for 30 seconds. Section 7.2.2.1 of IEEE Std. 384-1981, the highest voltage to which an isolation device Non-1E side is exposed shall determine the minimum voltage level that the device shall withstand across the Non-1E side terminals, and between the non-1E terminals and ground. Based on the system design for SPINLINE 3 platform, Rolls-Royce requires that cables connected to the SPINLINE 3 Platform analog output modules are routed separately from high voltage (greater than 120 VAC) cables, which establishes that a line-to-line short to a three conductor 120 VAC cable could result in a maximum possible voltage exposure of 240 VAC RMS. Therefore, Rolls-Royce tested the QTS analog output points for a maximum isolation capability of 250 VAC and 250 VDC applied for 30 seconds. The test voltages was applied across the line leads of the analog output module points (to simulate a line-to-line fault exposure), and across the line leads and AC ground (to simulate a line to ground fault). The applied current was limited to 10 amps. Higher fault currents would be expected to be automatically cleared by installed plant circuit protection devices.

The QTS output relay points were tested to the full EPRI TR-107330 voltage levels of 600 VAC and 250 VDC as listed above. The test voltages was applied across the line leads of the output relay points for both the ON and OFF states of the points, and across the line leads and AC ground of the output relay points for both the ON and OFF states of the points. The applied currents were limited to 25 amps (600 VAC) and 10 amps (250 VDC).

The Class 1E to Non-1E Isolation test acceptance criteria was described in Appendix J of the Rolls-Royce EQ Plan, which was defined according to EPRI TR-107330, Section 4.3.7 and 4.6.4. Specifically,

- Applying the Class 1E to Non-1E Isolation test voltages specified in Section 3.2 above for the required time to the specified QTS module points shall not disrupt the operation of any other module in the QTS, or cause disruption of the QTS BAP signals. Analog input and output levels shall not vary more than 3 percent (of full scale), except when the Class 1E to Non-1E Isolation test voltages are applied directly to the analog output module points. Evaluation of normal operating performance data (inputs, outputs, fault/diagnostic indicators and NERVIA+ communications) shall demonstrate satisfactory operation of the QTS during and after application of the Class 1E to Non-1E Isolation test voltages.
- Applying the Class 1E to Non-1E Isolation test voltages specified in Section 3.2 above for the required time to the specified QTS analog output module points shall not cause more than a 5 percent (of full scale) change to any other monitored analog output point on the same analog output module.
- Per Section 6.3.6 of EPRI TR-107330, failures of one or more redundant devices due to application of Class 1E to Non-1E Isolation test voltages are acceptable so long as the failures do not result in the inability of the QTS to operate as intended. Faults or failures of redundant devices which occur during Class 1E to Non-1E Isolation testing will be evaluated for effect on the QTS operation.
- Evaluation of normal operating performance data (inputs, outputs, fault/diagnostic indicators and NERVIA+ communications) will demonstrate intended operation of the QTS.

As mentioned in the EMI/RFI testing, Rolls-Royce did not perform Operability and Prudency tests required in EPRI TR-107330 after this test because the configuration of the QTS inside the EMC chamber did not permit it. Instead, Rolls-Royce recorded data during the test that demonstrated acceptable system performance during Class 1E to non-1E isolation tests.

Rolls-Royce did not submit the Class 1E to non-1E isolation testing report for NRC staff review but the manufacturer's "Summary EQ Test Report" (Reference 1.78) references the Class 1E to non-1E isolation qualification report and summarizes the test results. The Summary EQ Test Report states that the QTS passed the Class 1E t non-1E isolation testing.

Rolls-Royce recorded several events that occurred during Class 1E to non-1E isolation testing affecting the DAS. Rolls-Royce reported these events and its resolution in Rolls-Royce "Summary Equipment Qualification Test Report" (Reference 1.78) and "Investigations Results of 2011 NRC Qualification Tests" (Reference 1.79). Rolls-Royce analyzed these events to determine the cause and resolution. Rolls-Royce found that these events resulted from bad connections to the DAS, and thus these events did not affect the results recorded.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	**Document Number**
Class 1E to non-1E Isolation Test Procedure	3 010 293 A

Prudency Test Procedure	3 010 296 D
Operability Test Procedure	3 010 295 E
Class 1E to non-1E Isolation Test Report	3 018 595 A

The NRC staff reviewed the Summary EQ Test Report (Reference 1.78), and determined that the SPINLINE 3 platform met the criteria of IEEE Std. 384-1981 and Section 6.3.6 of EPRI TR-107330. It is the responsibility of the license to verify that the maximum test voltages cited above envelop the maximum credible voltages applied to 1E and Non-Class 1E interfaces (see Section 5.2, Item 22).

3.6.12 Performance Proof Testing

Rolls-Royce performed performance proof testing to demonstrate the continuing acceptable operation and performance of the SPINLINE 3 QTS following completion of all hardware qualification testing. EPRI TR-107330, Section 5.5 requires a final performance of the operability test procedure on completion of electrostatic discharge testing. Due to events observed during EQ testing, Rolls-Royce performed Operability and Prudency tests during Campaign 2011 after completion of Seismic SSE testing at the NTS facilities in Acton, MA, and during Campaign 2012 after completion of EMC testing at the NTS facilities in Boxborough, MA.

For this test, the QTS was configured similarly to the configuration expected when installed in a cabinet. The QTS was powered with the TSAP simulating I/O points as required to perform System Setup and Checkout, Operability and Prudency tests. In addition, the acceptance criteria for the Performance Proof testing are specified in the System Setup and Checkout, Operability and Prudency test procedures.

Rolls-Royce recorded several events that occurred during Performance Proof testing affecting the DAS and QTS. Rolls-Royce reported these events and its resolution in Rolls-Royce "Summary Equipment Qualification Test Report" (Reference 1.78) and "Investigations Results of 2011 NRC Qualification Tests" (Reference 1.79). After analyzing these events, Rolls-Royce modified the DAS to resolve them. The QTS was retested in Campaign 2012, and passed the tests satisfactorily.

During Performance Proof testing, the test specimen test shall demonstrate that the measured loop response times shall not vary more than ±10 percent from the baseline TUT loop response times. EPRI TR-107330, Section 4.2.1.A, requires an overall response time of 100 milliseconds or less. However, for the SPINLINE 3 platform, the cycle time is defined and configured during the design phase for each application (Reference 1.23). Therefore, for the TSAP ran during EQ testing, Rolls-Royce defined this cycle time in the "System Specification of the Qualification Test Specimen and Data Acquisition System" (Reference 1.46), which was set to 20 milliseconds. Note for an application specific project, Rolls-Royce will configure the cycle time to meet the plant requirements. Licensees using the SPINLINE 3 platform should confirm that the response time is configured and tested accordingly.

Details of the testing can be found in the following Rolls-Royce documents:

Document Title	Document Number
System Setup & Checkout Test Procedure	3 010 294 E
Prudency Test Procedure	3 010 296 D
Operability Test Procedure	3 010 295 E
Performance Proof Test Report	3 018 596 A (Campaign 2011) 3 018 949 A (Campaign 2012)

The NRC staff reviewed the Summary EQ Test Report (Reference 1.78), and determined that the test results of the Pre-Qualification, Prudency, and Operability Tests showed that the QTS performed in accordance with Rolls-Royce specifications and/or EPRI TR-107330 specifications before and after Qualification Tests, and no degradation in the performance of the QTS were identified.

3.6.13 Failure Mode and Effect Analysis

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

Section 5.2 of the LTR explains that Rolls-Royce performed reliability and safety analysis to each standardized board, and this scope does not represent a system to which the potential effects of failures can be analyzed. Instead, the results of these reliability and safety analysis are intended to be used as input data to support a system-level Failure Mode, Effects and Criticality Analysis (FMECA) and reliability analysis for SPINLINE 3 platform-based system. These analyses form part of a board's hardware design specification. Generic board/device-level FMECAs have been prepared in accordance with the guidance in IEC 60812. Rolls-Royce considers that these FMECAs are consistent the FMEA guidance of IEEE Std. 352-1987, Sections 4.1, 4.4, and 4.5.

The FMECA for each board identifies the effects of the failure modes of each function block in the device and define the potential malfunctions of the device. For each board/device-level malfunction, the FMECA assesses the ability to detect the malfunction. Table 3-4 groups the

SPINLINE 3 platform FMECA documentation into one table, and these documents contain the results of the FMECA for each board.

Table 3-4: SPINLINE 3 Platform FMECA and Reliability Information

Document Title	Rolls-Royce Document	Reference
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 RTD Conditioning Board: 8PT100 and I.8PT100 interface board	5 100 436 882 C	1.35
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Digital Isolated Input Board: 32ETOR TI SR and I.32ETOR TI interface board	5 100 435 707 C	1.36
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 32ETOR Input Terminal Block	3 008 991 B	1.37
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Analog Input Board: 16E.ANA ISO and I.16EANA interface board	5 100 436 348 C	1.38
Rolls-Royce Document, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Calibrated Pulse Acquisition Board: ICTO and I.ICTO interface board	1 479 513 C	1.39
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Actuator Drive Board: 32ACT and I.32ACT interface board	5 100 437 019 C	1.40
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Actuation Voting Module: MV16	5 100 436 936 C	1.41
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Output Relays Terminal Block: 8SRELAY1 & 8SRELAY2	5 100 436 935 C	1.42
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Analog Output Board: 6SANA ISO and I.6SANA interface board	3 008 651 B	1.43
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 NERVIA+ daughter board and I.NERVIA+ interface board	1 208 933 C	1.44
Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 ALIM 48V/5V-24V power supply board and I.ALIM 48 interface board	3 000 180 C	1.45

LTR, Section 5.2.1, and Reference 1.22 state that each application-specific SPINLINE 3 platform-based system will have a system-level FMECA, because the set of individual board-level analyses is not equivalent to a system-level analysis. Furthermore, Rolls-Royce noted that certain faults are only detectable at the system level. Therefore, determination of the reliability of a SPINLINE 3 platform-based safety system requires an application-specific system-level FMECA. The FMECA should demonstrate that single-failures, including those with the potential

to cause a non-safety system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions (see Section 5.2, Item 23). The combination of the SPINLINE 3 platform board-specific FMECAs and the system-level FMECA are required to demonstrate that there are neither any undetectable failures nor cascading failures that can contribute to a violation of the single failure criterion. These limitations are consistent with the LTR scope, which identifies application-specific FMEA document(s) that will address the topic of "FMEA" to fully satisfy the information content identified in DI&C-ISG-06 Section D.9.4.2.1.1.

The NRC staff reviewed the FMECA provided in the documents identified in Table 3-4 in consideration of the limited scope of the SPINLINE 3 platform FMECA as described within the LTR and the reliance upon an application-specific system functionality and architecture. These documents identify each component failure that affects the principle functions of the board and may not be detected and annunciated by SPINLINE 3 platform self-diagnostic features. These FMECAs can be used to support future demonstrations that the single-failure criterion can be satisfied for SPINLINE 3 platform-based systems.

Based on the information provided, a system-level FMECA should be performed to demonstrate that the application-specific use of the SPINLINE 3 platform identifies each potential failure mode and determines the effects of each. The FMECA should demonstrate that single-failures, including those with the potential to cause a non-safety system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot can adversely affect the protection functions.

3.6.14 Reliability Analysis

IEEE Std. 603-1991 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; however, as discussed within RG 1.152, Criteria for Use of Computers In Safety Systems of Nuclear Power Plants," and DI&C-ISG-06, the NRC's acceptance of the reliability of digital I&C systems is based on deterministic criteria for both hardware and programming, and the NRC does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for reliability of digital computers used in safety systems. Nevertheless, IEEE Std. 603-1991 further requires in Clause 5.15 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. IEEE Std. 603-1991 Clause 6.7 requires that when sense and command features are in maintenance bypass, the safety system shall remain capability of accomplishing its safety function while continuing to meet the single-failure criterion. Similarly, IEEE Std. 603-1991 Clause 7.5 requires that when one portion of a redundant safety system executes features is placed into a maintenance bypass condition, and then the remaining redundant portions should provide acceptable reliability. DI&C-ISG-06 states that the reliability and availability analysis 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 with further consideration of the effect of possible failures and the design features provided to prevent or limit its effects.

As mentioned before, Rolls-Royce submitted the reliability and safety analysis for each standardized board. Section 5.2.1.4 of the LTR describes the methods and approach used by Rolls-Royce to calculate the board level reliability. Rolls-Royce performed the FMECA in accordance with the guidance in IEC 60812, "Analysis techniques for system reliability – Procedure for FMEA." Rolls-Royce used the IEC 62380, "Reliability Data Handbook," for assessing component reliability and data for determining failure modes.

The documents listed in Table 3-4 (in the previous section) summarize the results of the board level reliability analyses; Section 4 defines analysis assumptions (e.g., environmental conditions) and its appendices include failure rates for all electronic components installed in the board. Rolls-Royce used RELEX reliability software to estimate the failure rates for each component. Each board's reliability analysis provides quantitative failure rate predictions expressed in units of 10^{-6} per hour. Table 5.2-1 in the LTR summarizes the predicted reliability for each board/device.

The NRC staff reviewed the reliability analysis summary, approach, and results provided in the documents listed in Table 3-4 and confirmed that these analyses identify the method used to predict the reliability of each board for installed hardware component failures. The reliability analyses clarify modeling assumptions and expectations associated with the predicted failure rates along with its use in modeling the expected reliability of SPINLINE 3 platform-based systems. The NRC staff could not determine full compliance to IEEE Std. 603-1991 Clauses 4.9, 5.15, 6.7, and 7.5, because these requirements are based on system-level reliability, which are established on a plant-specific and application-specific basis, and the analysis provided may not conform to the methods by which the applicant or licensee determines the reliability of its safety systems. Consequently, plant-specific actions should include the deterministic system-level evaluation of the degree of redundancy, diversity, testability, and quality provided in a SPINLINE 3 platform-based safety system to determine the degree provided is commensurate with the safety functions that must be performed. This plant-specific action item should consider the effect of possible failures, system-level design features provided to prevent or limit the failures' effects, and any application-specific inclusion of a maintenance bypass to support plant operations. Plant-specific actions should confirm that the SPINLINE 3 platform method for establishing reliability conforms to the method by which the applicant or licensee determined the reliability of the application-specific safety system or provides equivalent assurance. Plant-specific actions should also confirm that a resultant SPINLINE 3 platform-based system continues to satisfy any applicable reliability goals that the plant has established for this system (see Section 5.2, Item 24).

3.6.15 Data Supporting Setpoint Values

EPRI TR-107330, Section 4.2.4 recommends that the qualifier provide information about the qualified hardware to support an application-specific setpoint analysis. NRC RG 1.105, Revision 3 endorses International Society of Automation Recommended Practice 67.04, "Setpoints for Nuclear Safety-Related Instrumentation," with qualifications, as the basis for performing an application-specific setpoint analysis.

Rolls-Royce submitted Setpoint Analysis Support (Reference 1.92). This document provides a single, concise listing of the accuracy, drift, and other relevant specifications of the SPINLINE 3 digital safety I&C platform. The accuracy values summarized in this document were calculated over the full temperature and humidity ranges tested during EQ testing. The accuracy specifications are documented in accordance with Section 4.2.4 of EPRI TR-107330 and provide information required by EPRI TR-107330 to support an application specific setpoint analysis per ISA-S67.04-1994 standard. The Setpoint Analysis Support provides a single concise listing of the accuracy specifications of the SPINLINE 3 platform. The specifications documented are those typically used by nuclear industry users for calculating instrument measurement uncertainties and establishing critical control setpoints.

The SPINLINE 3 platform mapping of DI&C-ISG-06 (Reference 1.93) to provide information related to setpoint methodology identifies that Rolls-Royce provided supporting data for a plant-specific application to calculate the setpoints. Therefore, an application-specific design specification should provide the methodology and calculation as part of a referencing application or license amendment request (see Section 5.2, Item 25).

3.7 Platform Integrity Characteristics

SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," states that a special concern for digital computer-based systems is confirmation that the real time performance of the system is adequate to ensure completion of protective actions within the critical time periods identified within Clause 4.10 of IEEE Std. 603-1991. SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provides supplemental guidance to evaluate the real-time performance of digital systems and architectures, and discusses the identification of bounding real-time performance specifications and the verification of these specifications to demonstrate real-time performance. The establishment of predictable performance and behavior for a platform supports the future evaluation of a safety system that is based on the platform. The following subsections evaluate the Rolls-Royce SPINLINE 3 platform in terms of its response time characteristics, deterministic behavior, and fault management capabilities to support future evaluations of safety systems that are based on the SPINLINE 3 platform.

3.7.1 Response Time

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

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

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

Each licensee should provide its plant-specific and application-specific safety function response time design bases as response time performance requirements to be satisfied by a SPINLINE 3 platform-based system. The actual response time of an SPINLINE 3 platform-based system will be determined by its overall configuration; therefore, each licensee must determine that the SPINLINE 3 platform response time characteristics are suitable for its plant-specific application (see Section 5.2, Item10). Based on the information provided in the LTR and docketed documents, the NRC staff did not have sufficient information to evaluate and determine whether the SPINLINE 3 platform met the requirements in the GDCs. Therefore, the following information and description address the SPINLINE 3 platform response time characteristics and use of these characteristics in support of future plant-specific suitability determinations, because the SPINLINE 3 platform is a set of components to which response time budgets are allocated.

The SPINLINE 3 platform response time performance characteristics are described in general terms within the LTR, Sections 4.2. Also, the LTR identifies configuration settings that can affect response time performance (e.g., see LTR, Sections 4.2.4.1). For example, if the SPINLINE 3 platform-based system uses serial processing layers within a division, this can affect the overall system response time (e.g., more processors result in longer response times).

To satisfy a typical response time performance requirement, a SPINLINE 3 platform-based system must acquire and condition the input signal that represents the start of a response time performance requirement, transmit the signal through the BAP bus to the CPU, perform logic processing, generate an output signal, and transmit the output via the BAP bus to the output board, which represents the end of a response time performance requirement. These SPINLINE 3 platform response time components exclude 1) the earlier plant process delays through the sensor input to the platform and 2) the latter delays through a final actuating device to affect the

plant process; therefore, the licensee's plant-specific and application-specific safety function response time design bases should address these response time components separate from the response time performance requirements specified for the licensee's SPINLINE 3 platform-based system (see Section 5.2, Item 10).

As mentioned in Section 3.2.3.2 of this SE, Section 4.5.3 of the LTR and References 1.22 and 1.24, states that the Unit's 68040 processor and the Station's MPC860 processor (NERVIA+ board) operate independently of one another and only exchange data via the DPM that is dedicated to communications between the two processors. The exchange of data between these processors does not involve synchronization mechanisms (i.e., no handshaking), and thus a Unit works independently of the status of the Station or the network. So the cycle time for the Unit is different than the cycle time for the Station but both cycle time are predefined and fixed so that the minimum and maximum value of data processing can be guaranteed.

Section 4.2.6 of the LTR describes the deterministic behavior of the Unit in the SPINLINE 3 platform necessary to meet the response time requirements. In particular, Rolls-Royce explains that the Unit's cycle time is fixed and monitored, and this cycle time is continuously executed in the same order. This cycle time is defined during the design of the system using CLARISSE SSDE. During design, Rolls-Royce will configure the cycle time in accordance with customer requirements. This value considers hardware configuration (I/O boards), the OSS process time, and the functions/logics included in the application software, and then it is set to a larger value but close to the longest execution time of the system software. Rolls-Royce defines the boundaries for the Unit as:

- Minimum response time = the time for data acquisition + application processing + data output + input board minimum response time + output board minimum response time
- Maximum response time = the time for one cycle + the time for data acquisition + application processing + data output + input board maximum response time + output board maximum response time

Rolls-Royce will verify and validate this time during V&V activities for the SPINLINE 3 platform-based system. Rolls-Royce will also configure the minimum and maximum cycle time. During operation, plant operators can view these values through the LDU (Reference 1.30).

Section 3.4.2.1.2 of this SE and References 1.21, 1.22, and 1.30 explain that the cycle time for a plant-specific application is managed by the OSS's cycle time management basic module. This module acquires a time counter (located on the CPU) and compares it to the pre-defined cycle time. If the time measured is greater than the predefined time an error is produced and the CPU will stop. Section 3.4.2.3 of this SE describes the fault management for the SPINLINE 3 platform.

As mentioned before the system runs cyclically all its functions, including self-test routines; in this manner Rolls-Royce guarantees the CPU runs at 100 percent load in all cases. Because of

this, the SPINLINE 3 does not use real time processor control or interrupts to manage self-test programs running in the background. Also, References 1.22 and 1.23 explain that the speed of the CPU is not modified to run at 100 percent. Instead, the UC25 N+ CPU executes the code as fast as it can and the length of the code determines the cycle time. If in a cycle, time remains after all functions are performed, the OSS will verify the values acquired until the fixed cycle time is reached, in this manner the CPU is occupied 100 percent. In order to maintain the predefined cycle time, the OSS will perform certain self-tests (e.g., Data RAM address test, Code RAM checksum, etc.) over several cycles. Reference 1.24 explains that during design, Rolls-Royce designer can define the duration for these self-test to be performed during each cycle so the system can meet the cycle time requirements. Rolls-Royce constrained the overall time for all memory tests to not exceed 1 hour.

If the SPINLINE 3 platform-based system uses the NERVIA network to acquire data to be used by the application software, the response time of the system will need to consider the network cycle and data exchange in the DPM for data acquisition. Because the LTR does not define a specific system architecture for the SPINLINE 3 platform, the LTR description on response time does not consider data acquisition through the NERVIA network.

Section 4.5.2.1 of the LTR describes the network cycle time and the factors that are incorporated into its determination for a plant-specific application. In particular, this section explains that the network cycle time is defined during the design of the SPINLINE 3 platform, and that it will depend on the number of Stations in the network and the time allocated to each Station to transmit. The time allocated for transmission is called “time window”. The time window is defined based on preparation of the message, transmission of the message, and reception and processing of messages transmitted in the NERVIA network. One exception is for Receive-only stations (i.e., non-safety related, one-way communication), in this case the time window includes transmission of the message and reception and processing of messages transmitted in the NERVIA network. Receive-only Stations are not included in the calculation of the network cycle time because they are not transmitting messages. The network cycle time is the sum of all Stations in the network. In the LTR, Rolls-Royce noted that the network response time is bounded by the one network cycle time and the longest station time window.

During EQ testing, Rolls-Royce defined the QTS cycle time equal to 20 milliseconds (Reference 1.46). In addition, Rolls-Royce defined response time loops for analog inputs to analog outputs, analog inputs to discrete (Relay) outputs, and discrete inputs to discrete (relay) outputs. EPRI TR-107330, Section 5.3.B requires that Operability testing demonstrate that the test specimen response time does not vary by more than ± 20 percent from the value calculated using the manufacturer’s data during baseline testing, and that the test specimen response time does not vary by more than ± 10 percent from the measured baseline testing during qualification testing. In the Operability Procedure (Reference 1.85), Rolls-Royce explained that they could not meet this criterion and instead Rolls-Royce decided to demonstrate that the QTS response times will not exceed maximum expected response times, which were calculated based on the specific configuration of the QTS and the TSAP.

The QTS response time was specified during design of the QTS to be 20mS (Reference 1.22). During EQ testing, Rolls-Royce measured the response time of the QTS during Operability tests performed after each EQ test. The EQ Summary Report (Reference 1.78) shows that the QTS met the established criteria during Operability tests performed after each EQ test. This demonstrated that the response time of the QTS loaded with the TSAP (the time required for an output to be set in response to an input exceeding a trip condition) met Rolls-Royce response time specifications. Furthermore, this shows that the system performance (e.g., cycle time and processing load) are not affected by changes in environmental conditions. Because the configuration of the QTS does not represent a defined system architecture based on the SPINLINE 3 platform, the results of the cycle time tests are only valid for the QTS configuration.

Based on the information provided, the NRC staff has determined that the response time performance for a SR system based on the SPINLINE 3 platform requires a plant-specific action item to address system timing requirements and the timing budget among system components. Furthermore, the plant-specific action items should ensure that the SPINLINE 3 platform-based system satisfies its requirements in direct support of plant-specific and application-specific system response time of the accident analysis in Chapter 15 of the safety analysis report. Verification testing should also evaluate the test results against the expected minimum and maximum response times that were predicted for the equipment's performance to validate the response time analyses, and the response time requirements' traceability through the response time budgeting process and verification. The demonstration that actual SPINLINE 3 platform-based system response time performance falls between the predicted minimum and maximum response times should provide objective evidence of the determinism of the SPINLINE 3 platform and its components (see Section 5.2, Item 10).

3.7.2 Determinism

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

EPRI TR-107330 provides specifications and guidance intended to achieve a deterministic execution cycle with deterministic behavior that ensures an application and its constituent tasks will be completed within specified time limits. In particular, EPRI TR-107330, Section 4.4.1.3, "Program Flow Requirements," specifies that, where scanning of the inputs and application program execution are performed in parallel, methods should assure that the input scan and application program execution are completed each cycle.

The following subsections describe the deterministic characteristics of the SPINLINE 3 platform and architecture and evaluate these characteristics.

3.7.2.1 Deterministic and Known Real Time Performance (Deterministic Computation)

Section 4.2.6 of the LTR describes the deterministic behavior of the SPINLINE 3 platform. This section explains how this behavior will support the response time requirements for the system. Section 3.7.1 of this SE discusses the establishment and confirmation of response time performance requirements for a SPINLINE 3 platform-based system so that the real time performance is known.

As described in Section 3.4.2.1, the SPINLINE 3 platform's OSS performs specific functions during each cycle. These functions are executed cyclically in the same order and in a fixed amount time. The cycle time is fixed during the design phase of the system. A plant specific action item was identified in Section 3.4.2.1 to address system timing requirements and the timing budget among system components.

The SPINLINE 3 platform includes a cycle time management basic module, which manages the cycle time for a plant-specific application (see Section 3.4.2.1). This module will regulate the cycle time to meet the pre-defined value. If the cycle time is longer, the CPU will be stopped and indication will be generated to alert operators.

In Reference 1.24, Rolls-Royce explained that the SPINLINE 3 platform only uses interrupts when the system fails to drive the outputs to a predefined safe state. Specifically, the interrupts will be used when an exceptional internal condition occurs (e.g., instruction errors). In addition, the interrupts will have to be configured in the OSS through an interrupt vector table, which is triggered by the exceptional condition. Rolls-Royce also confirmed that the system does not use interrupt-driven tasks or to manage OSS functions.

In addition, operation of the Unit's 68040 processor and Station's MPC860 processor are independent from each other. In particular, the processing section of the Unit's 68040 processor executes the OSS and application software, and the Station's MPC860 processor controls the NERVIA communications. These processors only exchange data via DPM. Section 3.2.3.2 of this SE describes how access to the DPM operates. Furthermore, a failure of the Station does not affect the NERVIA network and the operation of the Unit (See LTR, Section 4.5.4.2). This failure will be communicated to the Unit to be processed as defined in the system requirements (see Section 3.4.2.3).

The NRC staff determined that the SPINLINE 3 platform supports deterministic and known real time performance through deterministic computation. Section 3.7.1 in this SE describes the allocation of time delays to elements of the platform and architecture. A thorough timing analysis and validation testing, as identified in the plant-specific action items, should be performed to provide assurance that the application is appropriately sized to maintain the capability for deterministic execution of the safety function.

3.7.2.2 Deterministic Digital Communication for Safety Signals

As described in Section 3.2.3 of this SE, the SPINLINE 3 platform uses the BAP bus for communication between the CPU and I/O boards, and the NERVIA network to implement communication inside and among divisions.

Section 3.2.3.1 describes operation of the BAP bus. In particular, the Unit uses BAP bus in each chassis for data exchange between the CPU and I/O boards. The BAP bus uses predefined configurations for this data exchange. The OSS ensures that communication between the CPU and I/O boards occurs within its timing budget, and each SPINLINE 3 platform board that responds to BAP bus requests contains monitoring logic to ensure that it continues to be successfully accessed. If a failure occurs during this communication exchange, the system will generate an error to alert operators to the system's condition when any of the BAP bus transaction time, board access time, or frame time is not satisfied, so that corrective actions can be taken.

Communications independence between the BAP bus and NERVIA network is provided because (1) the OSS uses the BAP bus for communication with the I/O boards, (2) the OSS controls the BAP bus, and (3) the Unit's and Station's processors operate independently.

Section 3.2.3.2 of this SE describes the NERVIA network. In particular, the NERVIA network uses a time-based token bus protocol that broadcast data to all Stations in the network. A Station is allowed to transmit its data on the network only during its specified time window (i.e., when it has the token). When a Station is transmitting, the message is received by all other Stations. The cycle time of each network is fixed and monitored. The network stations always transmit in the same order. The network design establishes the sequence of transmitting stations and assigns the pre-defined time window to each of these stations. The NERVIA network configuration (e.g., data and time frame to transmit data) is defined during the development process for a plant-specific application (see Section 5.2, Item 5).

As mentioned in the previous section, Station and Units have independent cyclical processing time. Further, exchanges between a Unit and an associated Station are not synchronized, and they only occur through DPM according to a dedicated protocol, which is managed by [
].

The NRC staff determined that the SPINLINE 3 platform supports deterministic digital communication for safety systems. Section 3.7.1 in this SE describes the allocation of time delays to elements of NERVIA communication. A thorough timing analysis and validation testing, as identified in the plant-specific action items, should be performed to provide assurance that the NERVIA network is appropriately configured to maintain the capability for deterministic execution of the system safety functions.

3.7.3 Self-Diagnostics and Test and Calibration Capabilities

IEEE Std. 603-1991 Clause 5.7 states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability be provided during power operation, and shall duplicate, as closely as practicable, performance of the safety function. IEEE Std. 603-1991 Clause 5.7 allows exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station; however, appropriate justification must be provided; acceptable reliability of equipment operation must be demonstrated; and the capability shall be provided while the generating station is shut down. IEEE Std. 603-1991 Clause 5.7 references IEEE Std. 338-1987, “Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems” for the testing of Class 1E systems, and RG 1.118, “Periodic Testing of Electric Power and Protection Systems,” endorses with exceptions IEEE Std. 338-1987 as a method acceptable to the NRC staff for satisfying the Commission's regulations with respect to periodic testing of electric power and protection systems. Furthermore, RG 1.22, “Periodic Testing of Protection Actuation Functions,” describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.

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

SRP BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” states that automatic diagnostics and self-test features should preserve channel independence, maintain system integrity, and meet the single-failure criterion during testing. Additionally, the benefits of diagnostics and self-test features should not be compromised by additional complexity that may result from the implementation of diagnostics and self-test features. In particular, the scope and extent of interfaces between safety software and diagnostic software such as self-test routines should be designed to minimize the complexity of the integrated software.

EPRI TR-107330 provides guidance and requirements applicable to PLC-based system’s diagnostics and test capability so that the combination of self-diagnostics and surveillance testing will detect all failures that could prevent a PLC from performing its intended safety function. The range of conditions for which diagnostics or test capabilities are to be provided includes processor stall, executive program error, application program error, variable memory error, module communications error, module loss of configuration, excess scan time detection,

application not executing, and field device (e.g., sensor, actuator) degradation or fault. The means of detection include watchdog timer, checksum for firmware and program integrity, read/write memory tests, communications monitoring, configuration validation, heartbeat, and self-diagnostics or surveillance test support features. EPRI TR-107330 identifies diagnostics that are executed upon power-up and diagnostics that run continuously thereafter.

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

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

Section 4.6 of the LTR describes the diagnostics and maintenance features provided in the SPINLINE 3 platform. In particular, the SPINLINE 3 platform performs tests and self-test diagnostics of the system (including I/O boards) and communication. Rolls-Royce considers that a combination of self-tests, periodic testing, and surveillance are necessary to successfully detect failures and reduce maintenance or trouble shooting of the system. Specifically, periodic tests and surveillance are performed to detect failures or problems that are not detectable by self-diagnostic tests. Maintenance activities, including periodic testing and surveillance, will be defined based on the system requirements and the plant-specific application. In addition, how failures are managed will be defined in the failure management for a plant-specific application (see Section 5.2, Item 6).

Section 4.6.5 of the LTR, Sections 3.4.2.1.3 and 3.4.2.3 of this SE, and Reference 1.30 and 1.31 describe self-diagnostic tests performed by the SPINLINE 3 platform. The OSS performs several tests to detect software, hardware, and/or network failures. Self-tests are performed during initialization of the system and during operation of the system. Even though the tests performed are identical, the actions taken during these two phases are different. During initialization, the OSS will perform self-tests to detect any problem with initiation functions. In this phase, if an error is detected, most likely the CPU will stop operating. During operation, if a

failure is detected, this can cause the system to operate in partially degraded condition (see Section 3.4.2.2) or totally degraded.

Self-diagnostic tests are performed during each cycle, except for certain memory self-test (e.g., EEPROM parameter degradation test) that require longer time, and therefore are performed over several cycles. Section 4.6.5 of the LTR and Reference 1.24 explain that during design, Rolls-Royce designer will define the duration for these self-test to be performed during each cycle so the system can meet the cycle time requirements (see Section 3.7.1 for information on response time).

Self-tests are performed by the TESTS module in the OSS. Specifically, this module will perform:

- CPU board test and self-test. This function will activate the watchdog and run the self-tests included in Category 1 (see Section 3.4.2.1.3).
- Addressing tests on peripherals (I/O boards) and stations. This function verifies modules and Stations in the system by calling the addressing in the Hardware tables and confirming that they are present in the rack. This function runs the self-tests included in Category 2.
- Activity tests on intelligent peripherals. This function performs activities required to monitor operation of intelligent peripherals, such as board clock tests and watchdog tests. This function runs the self-tests included in Category 2 and 5.
- Communication status test. This function confirms that the communication chain between Stations on the network is operating correctly. This function runs the self-tests included in Category 3 and 4.

Section 4.6.8 of the LTR describes the typical failure mode for software self-diagnostics implemented in the SPINLINE 3 platform. These tests are performed in conjunction with hardware self-tests (described above) to verify the correct operation of the SPINLINE 3 platform components. These tests will evaluate the CPU board, intelligent peripherals, and NERVIA network. Configuration of these tests is a plant-specific application.

Rolls-Royce has also implemented self-diagnostic tests associated with the NERVIA network. These tests are described in Section 4.5.6 of the LTR. Specifically:

- Station self-tests to detect failures on the hardware components of the NERVIA+ board.
- CPU self-tests to detect communication failures with the Station. Note that the OSS already Category 3 self-tests to determine the status of the NERVIA+ board (intelligent peripheral) and communication status (i.e., data located in the DPM).
- Message/Data tests to detect errors (e.g., corrupted data) in the message received/transmitted in the network by verifying the consistency blocks. Note that the OSS performs Category 4 self-tests to detect errors in data or messages.

When failures are detected the OSS will perform pre-defined actions or functions in accordance with the failure management for the plant-specific application (see Section 3.4.2.3). For example, if a board activity test or self-test in Category 2 results in an operating error, the function is halted, the board enters its error status, which is defined in the failure management (e.g., modify validity indicator), and indication (i.e., internal indicators) is sent to the CPU to invalidate data from the board, and indication is sent to the MMU (external indicators) (see Section 3.4.2.3). The message sent to the MMU will help maintenance operators identify the error and required corrective actions. The diagnostic functions in the MMU will be configured for a plant-specific application.

During software integration and validation of the OSS (References 1.49 and 1.51), Rolls-Royce performed several tests to verify and validate operation of the SPINLINE 3 tests and self-tests implemented in the OSS and the NERVIA network. For example, a test was performed to verify that the system would stop if the FLASH EEPROM detected a parameter modified after initialization. In this case the system halted and displayed an error code. This was the result expected for this validation test. The tests identified in these references showed that Rolls-Royce successfully validated this aspect of the OSS and NERVIA communication. Section 3.5 of this SE discusses how the results from these tests were used as part of the CGD of the SPINLINE 3 platform.

In addition to diagnostics and self-tests, Section 4.6 of the LTR describes the Rolls-Royce proposed strategy for testing the SPINLINE 3 platform-based system. As stated before, because the LTR does not define a particular system or application, testing and surveillance will be defined for a plant-specific application. Therefore the following description just summarizes the platform attributes for testing and surveillance.

During periodic testing, operators will verify accuracy, calibration, setpoint values, and response time. Maintenance operators will use the ATU to perform testing and surveillance. To perform periodic testing, the maintenance operator will place SPINLINE 3 platform in bypass mode to avoid any spurious actuation. Based on the plant-specific application, Rolls-Royce will configure the automatic tests to be performed by the ATU. The ATU will generate input signals and send them to the system, and then receive the output signals to compare the results obtained and verify operation of the system. Table 4.6-1 of the LTR lists tests to be performed on the main type of boards.

Rolls-Royce will define the periods between periodic tests and surveillance after performing a dependability analysis, which will take into account the efficiency of self-diagnostic tests and surveillance functions. A detailed coverage of self-test, periodic tests, and surveillance will depend on the plant-specific application and system requirements.

The NRC staff has reviewed the diagnostics and self-test capabilities for the SPINLINE 3 platform, and finds them to be suitable for a digital system used in SR applications in nuclear power plants. The diagnostics capabilities are found to be adequate. However, the licensee should establish surveillance program, which in combination self-tests and periodic tests, will

provide the detection capabilities claimed in the failure modes and effects analysis (see Section 5.2, Item 27). The NRC staff has determined that the diagnostics and self-test capabilities comply with the guidance of EPRI TR-107330 overall. In addition, the NRC staff agrees with Rolls-Royce position that surveillance and periodic testing are necessary, in addition to the diagnostics and self-test capabilities of the SPINLINE 3 platform, to detect all failures.

3.8 Diversity and Defense-in-Depth

The regulation at 10 CFR 50.55a(h), "Protection and safety systems," requires compliance with IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995.

The regulation at 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants," requires in part various diverse methods of responding to an ATWS; 10 CFR Part 50, Appendix A, GDC 21, Protection Systems Reliability and Testability, requires in part that "no single failure results in the loss of the protection system;" GDC 22, Protection System Independence, requires in part "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions ... not result in loss of the protection function ... Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function;" GDC 24, Separation of Protection and Control Systems, requires in part that "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired;" and GDC 29, Protection Against Anticipated Operational Occurrences, requires in part defense against anticipated operational transients "to assure an extremely high probability of accomplishing ... safety functions."

The NRC staff Requirements Memorandum on SECY 93-087, dated July 21, 1993, describes the NRC position on D3 requirements to compensate for potential common-cause programming failure.

Guidance on the evaluation of diversity and defense-in-depth (D3) is provided in SRP BTP 7-19. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 31, 1994, summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses.

Diversity and defense-in-depth is a strategy that is applied to the overall I&C system architecture in the context of a specific plant design. In the LTR, Rolls-Royce stated that diversity and defense-in-depth should be addressed in the context of an NPP's suite of safety and non-safety I&C systems. Furthermore, the LTR does not propose a specific I&C system for a specific plant application; therefore this SE cannot determine the adequacy of the SPINLINE 3 platform against the guidance in BTP 7-19. Thus, the performance of a plant-specific D3

analysis is a plant-specific action for SR applications of the SPINLINE 3 platform (see Section 5.2, Item 28). The analysis determinations will be evaluated as part of a plant-specific review. BTP 7-19's D3 evaluation should demonstrate that plant vulnerabilities to CCFs have been adequately addressed in the context of an overall suite of I&C systems. Furthermore, the four-point position within BTP 7-19 was developed in recognition that programming design errors are credible sources of CCFs that apply to nuclear power plants that incorporate digital protection systems, which includes RTS and ESFAS.

3.9 Review of System Communication and DI&C-ISG-04

The NRC Task Working Group 4, "Highly Integrated Control Rooms-Communications Issues," developed interim NRC staff guidance on the review of communications issues applicable to digital safety systems. DI&C-ISG-04 contains NRC staff positions on three areas of interest: (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations. Section 4.5 of the LTR describes SPINLINE 3 digital communications implemented using the NERVIA digital communication network. Section 3.2.3.2 of this SE describes the NERVIA communication process. Table 3.7.1 in Appendix A of the LTR contains Rolls-Royce's assessment regarding SPINLINE 3 conformance to the provisions of DI&C-ISG-04, Revision 1.

Evaluation of a safety system against this guidance is an application-specific activity that requires an assessment of a full system design. Since Rolls-Royce's SPINLINE 3 LTR (Reference 1.4) does not address specific applications or establish a definitive safety system design, the evaluation against this guidance is limited to consideration of the means provided within the platform to address issues related to interactions among safety divisions and between SR equipment and equipment that is not SR. A full safety system design, which is based on the SPINLINE 3 platform, will require further evaluation against this guidance. Regardless, the following subsections provide an evaluation of each SPINLINE 3 platform communication method against the applicable points for that position. A single general plant-specific action item has been created to address full compliance to each DI&C-ISG-04 clause (see Section 5.2, Item 29).

3.9.1 DI&C-ISG-04, Staff Position 1 - Interdivisional Communications

Staff Position 1 of DI&C-ISG-04 provides guidance on the review of communications, which includes transmission of data and information among components in different electrical safety divisions (or channels) and communications between a safety division and equipment that is not SR. This ISG does not apply to communications within a single division or channel. This NRC staff position states that bidirectional communications among safety divisions and between safety and non-safety equipment may be acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. It also states that systems which include communications among safety divisions and/or bidirectional communications between a safety division and non-safety equipment should adhere to the 20 points described below. The methods by which the SPINLINE 3 platform either meets these points or provides

an acceptable alternative method of complying with NRC regulations are discussed below. In several instances, full compliance with these points cannot be determined without a specific application system. For those points, this evaluation will highlight any features of the SPINLINE 3 platform that would support compliance with the point and provide any applicable pointers to future SPINLINE 3 system reviewers as to specific items for review.

3.9.1.1 Staff Position 1, Point 1

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

The LTR described a generic SPINLINE 3 platform, which did not define a specific communication architecture for a safety channel. Section 4.2.4.1 of the LTR describes a "representative" safety channel using the NERVIA network. However, without a specific system with a specific application, the NRC staff cannot reach a conclusion on this point.
The SPINLINE 3 platform described in the LTR includes capabilities to comply with the guidance provided this Staff Position 1, Point 1. For example, the UC25 N+ CPU board (Unit)'s 68040 processor operates asynchronously from the communication section and all data is transferred through a dual ported memory, enable through [ ]. The UC25 N+ CPU board is also continuously informed of the status of each communication interface so that it retains the ability to perform its safety function without reliance on data from outside of the 68040 processor.

The NRC staff recognizes that the SPINLINE 3 platform provides allowances for implementation of system features that could comply with the guidance provided by Staff Position 1, Point 1. However, evaluation of this point would require plant-specific analysis to verify compliance with this staff position.

3.9.1.2 Staff Position 1, Point 2

Staff Position 1, Point 2, states that 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.

Section 4.5.7 of the LTR states that the NERVIA network can be configured as one-way communication (typically from safety related components to non-safety related components). In particular, Rolls-Royce states that isolation would be enforced using two methods:

- The non-safety related component would be configured as a “non-transmitting station” on the NERVIA network, such that it would not be set-up to attempt to transmit data over the network. The component would only be configured to “listen” to network communications.
- Data isolation would be further enhanced by use of a one-way data barrier that would preclude any attempted transmission from the non-safety related component onto the NERVIA network. However, at this time, no details have been provided on the exact one-way data barrier that would be used.

The specific device used to provide data isolation was not specified in the LTR, and, therefore, would be subject to application specific review.

In addition, as described in Section 3.2.3.2 of this SE and Section 4.5.4.2 of the LTR, the NERVIA+ board provides the interface between the Unit’s 68040 processor and the Station’s MPC860 processor, so that safety channels can be protected from adverse influences caused by information or signals originating at the opposite side of the data link. The features included are:

- Use of the DPM to transfer information
- Perform 32 bit cyclic redundancy checks (CRC) on received messages and CB checksum on data within received messages
- Flag of erroneous data
- Detect absence of data updates (i.e., identify “stale” data)
- Continuous monitoring of communications link status
- Detection of communications link failure

Furthermore, the LTR Section 4.5.4.2 states that a failure of the Station does not affect the NERVIA network and the operation of the Unit. This failure will be communicated to the Unit to be processed as defined in the system requirements.

As stated in Staff Position 1, Point 1, the LTR described a generic SPINLINE 3 platform and a “representative” safety channel using the NERVIA network. But enough information was not provided for the NRC staff to reach a conclusion on this point. The NRC staff recognizes that the SPINLINE 3 platform provides allowances for implementation of system features that could comply with the guidance provided by Staff Position 1, Point 2. However, evaluation of this point will require plant-specific analysis to verify compliance with this staff position. This point will need to be reviewed as an Application Specific Action Item.

3.9.1.3 Staff Position 1, Point 3

Staff Position 1, Point 3, states that a safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. 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 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 (e.g., 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.

As stated in Staff Position 1, Point 1, the LTR described a generic SPINLINE 3 platform and a “representative” safety channel using the NERVIA network. But enough information was not provided for the NRC staff to determine if communications from outside a single division that do not support the safety function will be included.

The NRC staff recognizes that the SPINLINE 3 platform provides allowances for implementation of system features that could affect compliance with this position. These cases would require plant-specific analysis to verify compliance with this staff position. Thus, without a specific system architecture, the NRC staff cannot reach a final determination on compliance with this point. This point will need to be reviewed as an Application Specific Action Item.

3.9.1.4 Staff Position 1, Point 4

Staff Position 1, Point 4, states that 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. The function processor, the

communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be SR, and must be designed, qualified, fabricated, etc., in accordance with 10 CFR Part 50, Appendices A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure 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.

Section 4.5.3 of the LTR and References 1.22 and 1.24, states that the Unit's 68040 processor and the Station's MPC860 processor (NERVIA+ board) operate independently of one another and only exchange data via DPM that is dedicated to communications between the two processors. Section 3.2.3.2 of this SE describes how access to the DPM operates.

Section 4.5.4.3 of the LTR and Reference 1.24 provide detailed description on data management and conflict resolution. Further, the CPLD memory management function was chosen as one of the "requirement threads" to be evaluated during the NRC staff's regulatory audit (Reference 2.5) at the Rolls-Royce facility in Grenoble, France. The NRC staff reviewed objective evidence during the audit that demonstrated that the capability was properly implemented and rigorously tested.

Neither the safety or communications processors, nor any of its supporting circuitry, were developed under an Appendix B program. However, all of these components were subject to CGD. An evaluation of Rolls-Royce's CGD effort is contained in Section 3.5 of this SE.

The LTR Section 4.5.4.2 describes how the SPINLINE 3 platform the failure mechanisms implemented in the SPINLINE 3 platform. For example, if Unit's 68040 processor cannot access data stored on the DPM, it would continue to operate. Performance of required safety functions of the system within the required cycle time would then depend on the application being written in a way that the system defaults to a safe state when the DPM data cannot be accessed. The treatment of these failures will be defined in the system requirement specification for a plant-specific application.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes that the SPINLINE 3 platform provides allowances for implementation of system features to comply with the guidance provided by Staff Position 1, Point 4 (i.e. the platform uses separate processors that operate asynchronously).

3.9.1.5 Staff Position 1, Point 5

Staff Position 1, Point 5, states that 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.

Section 4.5.2.1 of the LTR describes the network cycle time and the factors that are incorporated into its determination for a plant-specific application. In particular, this section explains that the network cycle time is defined during the design of the SPINLINE 3 platform, and that it will consider the number of Stations in the network, when a Station can transmit, and how long it will take to send its message. In Table 3.7-1, Rolls-Royce noted that the longest possible delay can occur when concurrency of access to a byte. In this case, this delay will be equal to the time to read or write access to the DPM by the Station's MPC860 processor.

In addition, Section 4.2.6 of the LTR describes the response time for the Unit. In this section, Rolls-Royce explains that cycle time is fixed and monitored. This cycle time is defined during the design of the system. Furthermore, References 1.21, 1.22, and 1.30 explain that the cycle time for a plant-specific application is defined and managed by the OSS's cycle time management basic module. This module guarantees that the CPU executes the OSS and application software within defined time and thus the CPU runs at 100 percent load in all cases. During EQ testing, Rolls-Royce loaded the QTS with the TSAP to demonstrate this characteristic. The EQ Summary Report shows that the specified QTS cycle time was met during Proof testing.

Staff Position 1, Point 5 must be evaluated as an application specific review for a plant-specific application because this time will depend on the I/O boards and the application software configured. When implementing a SPINLINE 3 safety system the licensee must review Rolls-Royce's timing analyses and validation tests for the application specific SPINLINE 3 system in order to verify that it satisfies its plant-specific requirements for system response and display response time presented in the accident analysis in Chapter 15 of the safety analysis report.

3.9.1.6 Staff Position 1, Point 6

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

Section 3.2.3.2 of this SE describes the interactions that take place between the Unit's 68040 processor and Station's MPC860 processor. While the processing section of the Unit's 68040

processor executes the OSS and application software, the Station's MPC860 processor section controls the NERVIA communications.

Section 3.4 and References 1.30 and 1.32 describe the software architecture for the SPINLINE 3 platform. In particular, the OSS consists of several modules, which are organized and prioritized depending on its functions. The execution of these modules is performed in order during every cycle for the pre-defined system cycle time. The cycle time management basic module will monitor and manage the cycle time. References 1.23, 1.24 and 1.30 explain that certain self-tests can be spread over several cycles to maintain the defined cycle time for the system. Execution of these modules is not event driven or controlled by interrupts (Reference 1.24). In addition, the Unit control program does not perform communication handshaking when accessing data from the DPM.

The BAP communication satisfies Point 6, because this communication bus does not include handshaking or interrupts. The communication between the CPU board and the I/O boards is deterministic. The communication section is an event-driven interrupt system, however, the criteria of DI&C-ISG-04 Position 6 only apply to the safety function processor which corresponds to the processing section of the Unit's 68040 processor.

The NRC staff review determined that communications protocols associated with the NERVIA network include the use of a time-based token protocol, but no handshaking is done by the communications section of the Station's MPC860 processor. The safety function processor contained within the Unit's 68040 processor communicates externally using only the DPM, and this process does not use handshaking or interrupts. The NRC staff therefore determined that the SPINLINE 3 platform complies with Staff Position 1, Point 6.

3.9.1.7 Staff Position 1, Point 7

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

Section 3.2.3.2 of this SE, Section 4.5.4.3 and Table 3.7-1 of the LTR, and References 1.22 and 1.30 explain that the data is organized in CBs so they can be transmitted in one frame by the NERVIA network. This message is defined during design of the system for a plant-specific application. Further the size of the message to be transmitted by each Station in the network is also defined during design of the system for a plant-specific application. The allocation of DPM memory is static and does not change during program execution.

Stations check CBs to determine if data has been corrupted or stale. Section 4.5.4.2 of the LTR describes the typical failure mechanisms to detect corrupted data. In particular, the receiving Station in the NERVIA network will check the 32 bit CRC, the refresh indicator, and the identification data of the CB to verify that data was not corrupted during transfer. Corrupted or stale data will be flagged by the Unit, and it won't be used. The system requirement specification will identify how the system for a plant-specific application will handle this data. The CB is transmitted in the NERVIA in an Ethernet frame. Further information on how the Ethernet frame is configured is provide din Section 4.5.4.3 of the LTR. The NERVIA network will continuously transmit this message, and the message will change when the data changes.

Based upon the above discussion on the SPINLINE 3 system's use of predefined data sets with a pre-determined format via the respective communications processors, the NRC staff concludes that the SPINLINE 3 platform complies with Staff Position 1, Point 7. Note that how corrupted or stale data is managed after being flagged will be defined for a plant-specific application.

3.9.1.8 Staff Position 1, Point 8

Staff Position 1, Point 8, states that 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.

The Rolls-Royce SPINLINE 3 NERVIA+ board contains one to three microprocessors (i.e., MPC860) dedicated to digital communications for a given safety processor. Data exchanges between safety processors (i.e., MP68040) within the same division, safety processors in other divisions, and between safety processors and non-safety processors are handled by the dedicated communication microprocessors (i.e., MPC860). As described in Section 4.5.2.6 of the LTR and Section 3.2.3.2 of this SE, the NERVIA+ board microprocessor and UC25 N+ board microprocessor operate independently.

The microprocessor(s) on the NERVIA+ board only exchange information with the UC25 N+ board SR processors performing safety functions (i.e., MP68040) via DPM located on the NERVIA+ board. A given communications processor will place received data into the DPM, which the associated safety processor will read each application cycle. Outgoing data is written to the DPM by the safety processor, which is then read each communication cycle by the communication processor prior to transmission. In this manner, the safety processor has no direct involvement in the digital communications that may be performed by a SPINLINE 3-based system.

Section 4.5.4.3 of the LTR, Section 3.2.3.2 of this SE, and Reference 1.24 describe management of the DPM on the NERVIA+ board in the exchange of data. A CPLD manages access to the DPM to ensure that the two processors do not simultaneously attempt to read and

write to the same memory location. The NRC staff evaluated the CPLD requirement for memory management as part of the regulatory audit (Reference 2.5) and found that the Rolls-Royce documentation supports a finding of reasonable assurance that this capability has been adequately defined and tested.

As described in Staff Position 1, Point 2, Section 4.5.7 of the LTR states the NERVIA network can be configured as one-way communication (typically from safety related components to non-safety related components). This feature was not described in enough detail for the NRC staff to evaluate how one-way communication is implemented.

The NRC staff has determined that the data exchange between safety divisions complies with Staff Position 1, Point 8. However, because the LTR does not define a specific configuration of the SPINLINE 3 system and that the one-way data barrier is also not defined, conformance to Staff Position 1, Point 8 is an application specific action item. An applicant referencing this SE should confirm that data exchanged between safety and non-safety division does not adversely affect the safety functions.

3.9.1.9 Staff Position 1, Point 9

Staff Position 1, Point 9, states that 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.

As noted above in the evaluation of Point 8, Section 4.5.2.6 of the LTR and Section 3.2.3.2 of this SE state that the NERVIA+ board processor and UC25 N+ board microprocessor operate independently. Further, Section 4.5.3 of the LTR identifies that the 32 kilobytes DPM on the NERVIA+ board is used to exchange data between the MPC860 communications microprocessor on the NERVIA+ board and the MP68040 safety processor on the UC25 N+ board. Section 4.5.4.3 and Reference 1.24 of the LTR describes how the DPM is managed to ensure data consistency. During the regulatory audit in Grenoble, France (Reference 2.5), the NRC staff reviewed a requirement thread that was central to management of access to the DPM and interviewed Rolls-Royce staff regarding the use of “consistency blocks” in the transport of data. The NRC staff found that Rolls-Royce’s documentation and NRC staff explanations were consistent with a finding that data is transmitted through the dual-ported memory in a fashion that is consistent with DI&C-ISG-04, Staff Position 1, Point 9. Table 3.7-1 in Appendix B of the LTR clearly states that message data is stored in fixed predetermined locations in the dual-ported memory.

The NRC staff has determined that the data exchange within SPINLINE 3 platform based systems complies with Staff Position 1, Point 9.

3.9.1.10 Staff Position 1, Point 10

Staff Position 1, Point 10, states that 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. 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 a key lock 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.

Table 3.7-1 in the LTR specifically states that software is installed in read-only flash memories. Upon start-up, software is loaded into dedicated RAM, which is write-locked while in operation. Certain designated modifiable parameters may be changed via the Local Display Unit (non-safety) while the channel is inoperable. Reference 1.24 describes that during a parameter change (via LDU) the application remains functional, but the EEPROM won't be accessible while the change is being performed. After the data is copied to the EEPROM, the OSS will copy the data to the RAM. Section 3.2.3.2 of Reference 1.31 provides a detailed description how variable parameters are copied to the EEPROM and how the application software is notified of such changes.

Section 4.4.3.5.5 of the LTR states that the Local Display Unit is "not permanently installed." As mentioned in Section 3.2.1.5 of this SE, Rolls-Royce did not request approval of the Local Display Unit. Furthermore, the LTR does not explain how configuration of a one-way communication is implemented (see Staff Position 1, Point 2). An applicant or licensee referencing this SE should confirm that data exchanged between safety and non-safety division adversely affect the safety function. Further, given that the LTR does not define a specific configuration of a system based on the SPINLINE 3 platform is not defined, conformance to Staff Position 1, Point 10 is an application specific action item.

3.9.1.11 Staff Position 1, Point 11

Staff Position 1, Point 11, states that provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless

all safety functions associated with that processor are either bypassed or otherwise 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.

At this time, The NRC staff would not expect any message data relayed through the NERVIA DPM to the processor to affect the execution of application software. Rolls-Royce provided a description on how the SPINLINE 3 platform complies with this point in Table 3.7-1 of the LTR. However, since there is no specific system architectures defined in the LTR, it is unknown whether any interdivisional communication will be designed into a future application and/or what messages may be crafted. An applicant or licensee referencing this SE should confirm that either no interdivisional communications are used in safety system using the Rolls-Royce SPINLINE 3 platform or, if interdivisional communications are proposed, that the communications conform to the provisions of this point.

3.9.1.12 Staff Position 1, Point 12

Staff Position 1, Point 12, states that 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. This Section provides 12 examples of credible communication faults, but cautions that the possible communication faults are not limited to the list of 12.

Section 4.5.2.1 of the LTR describes the communication operations within a NERVIA network. Section 4.5.4.2 of the LTR describes the failure mechanisms to detect typical failures. These checks include:

- Verification of message integrity via CRC32 check at the message level.
- Verification of consistency block (i.e., the data within the message) integrity via CB checksum at the consistency block level.
- Verification that data is not “stale” (e.g., due to a NERVIA station failing and not transmitting a message, a failure in the transmission medium, continuous transmission of a NERVIA station which will cause the hub to block the signal).

The NRC staff notes that although the NERVIA board is capable of detecting these errors, the engineered fault management features for the error will be application-specific.

In addition, Section 4.5.6 of the LTR describes self-tests performed by the NERVIA+ board. These self-tests include checking watchdog timer activation for the NERVIA+ board, evaluating the CRC of the executable code in RAM (to ensure that the executable code has not corrupted), and tables prescribing the configuration of the network, station and messages. Results of self-

tests are reported to the UC25 N+ board processor. Any errors detected are made available to the OSS. Treatment of the errors would need to be determined on an application specific basis.

Section 4.5.6 of the LTR also describes tests performed by the UC25 N+ board processor on data that it reads from the DPM on the NERVIA+ board. The UC25 N+ will do its own CB checksum on the consistency block data to ensure that it has not been corrupted. The UC25 N+ also checks an indicator associated with each consistency block to determine whether it has been updated since the last time it was processed by the UC25 N+ processor. Any errors detected are made available to the OSS. The design and operation of the SPINLINE 3 platform is intended to prevent communication faults from adversely affecting the application program or its ability to perform its assigned safety functions. Treatment of the errors would need to be determined on an application specific basis.

In Table 3.7-1 of the LTR, Rolls-Royce provided explanations for how the SPINLINE 3 platform would respond to each of the 12 faults listed in DI&C-ISG-04 Position 1, Point 12. For each of these cases, specific design features of the SPINLINE 3 platform that have been evaluated by the NRC staff in this SE were credited for ensuring that the integrity of the safety functions would be maintained. However, treatment of communication failures would need to be determined on an application specific basis.

The NRC staff also reviewed the NERVIA+ board reliability analysis (Reference 1.33). This document notes although “software faults are not considered” as part of the hardware reliability and failure modes analyses, the failure mode analyses (Appendix 2 of the document) addresses failure modes for the NERVIA transceiver, microprocessor (i.e., MPC860), dual-port (shared) memory, and CPLD. These components are central to the receipt, transmission and processing of digital communications on the NERVIA+ board. For each of the failures modes considered that identified an effect on the system, a means of detection was identified. Table 6.1 of the document summarizes self-tests that address specific failure modes for network communication and dual-port (shared) memory.

The NRC staff has determined that the Rolls-Royce SPINLINE 3 components have built-in capabilities to detect and handle a variety of communication errors. The NRC staff evaluated the 12 example communication faults listed under Point 12 and found that they will not adversely affect the performance of the required safety functions, and that the SPINLINE 3 platform complies with Staff Position 1, Point 12. An applicant or licensee should review the treatment of communication failures and data errors for a plant-specific application.

3.9.1.13 Staff Position 1, Point 13

Staff Position 1, Point 13, states that vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. 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.

In the LTR, Rolls-Royce did not describe any error correction that will be attempted by the operating system software of the SPINLINE 3 platform. When errors are detected the systems are designed to flag data as failed and to enter into a state that would not compromise the safety functions of the system. As noted above in Point 12, the Rolls-Royce SPINLINE 3 components perform multiple checks of received data. In addition, consistency blocks that are not updated due to variety of causes will be identifiable as “stale” data. Section 4.5.4.2 of the LTR describes the typical failure mechanisms to detect stale or corrupted data (See Point 7). The specific course of action that an application built on a SPINLINE 3 platform takes in response to having an error condition made available to it will need to be evaluated on an application specific basis.

The NRC staff determined that the Rolls-Royce SPINLINE 3 platform has the ability to comply with Staff Position 1, Point 13; however, specific treatment of errors by an application would need to be review on an application-specific basis. Any proposed use of error correction methods incorporated into a specific system or application software would need to be evaluation on an application-specific basis.

3.9.1.14 Staff Position 1, Point 14

Staff Position 1, Point 14, states that 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. Implementation of other communication strategies should provide the same reliability and should be justified.

Messages sent over the NERVIA network are broadcast to all Stations on the network. These messages would be relayed through a passive Ethernet hub. Two Ethernet hubs (i.e., 10 Megabytes per second Ethernet Hub: 4TP and 10 Megabytes per second Ethernet Hub: 3TP/2FL) are included among the equipment being commercial grade dedicated as described in the LTR, Section 4.5.3. Furthermore communication to the NERVIA network is only through the NERVIA+ boards.

The NERVIA network is a time based token bus. The network physical topology is a star made of passive hubs, achieving a point to point configuration from the transmitting Station to the receiving Stations. The NRC staff would not anticipate that a SPINLINE 3 system would use equipment outside of a safety division for transmission of data. However, without defined communication architecture to review, the NRC staff cannot reach a final conclusion on this point. An applicant referencing this SE should confirm that no equipment outside of the safety

division is used in the transmission of messages within a NERVIA network. If an alternate strategy is used, it should be justified per Point 14.

3.9.1.15 Staff Position 1, Point 15

Staff Position 1, Point 15, states that communications 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.

The evaluation of SPINLINE 3 platform against Staff Position 1, Point 7, determined that a fixed data format of the data sets used by the Station was established. As a result, these data sets are predefined and its format and sequence are pre-determined.

As described in Section 4.5.2.1 of the LTR and Section 3.2.3.2 of this SE, the data transmission cycle time and the amount of data transferred during a cycle is determined by application-specific design. Reference 1.24 explains that each Station is configured to operate in a coordinated manner within the sequenced emission of all Stations in the overall cycle. The data transmitted and the frequency of transmission remains fixed for any given configuration while the system is operable. The SPINLINE 3 platform also has provisions for identifying data as being updated even if it has not changed in value since the previous update or for identifying stale data.

The NRC staff determined that the SPINLINE 3 platform complies with Staff Position 1, Point 15.

3.9.1.16 Staff Position 1, Point 16

Staff Position 1, Point 16, states that network connectivity, liveliness, and real-time properties essential to the safety application should be verified in the protocol. Liveliness, in particular, is taken to mean that no connection to any network outside the division can cause a RTS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 CFR Part 50, Appendix A, GDC 24, which states, “interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired,” and (2) IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” (Source: NUREG/CR-6082, Section 3.4.3).)

In the LTR, Rolls-Royce states that the SPINLINE 3 platform can utilize network based communications for the exchange of data between divisions. The protocols used for the NERVIA network include provisions for identifying a loss of connectivity. The protocol can also detect and flag corrupted or stale messages. Also, the NERVIA network performs several self-diagnostic tests (LTR Section 4.5.6 and Reference 1.24). Specific treatment of errors by an application would need to be review on an application-specific basis.

As described in previous points, the processing section of the Unit functions independently from the Station (NERVIA+ board) and is designed to accomplish all safety related function tasks independently of the communications processor. Even if the communications processor were to stall, there would be no loss of system safety functionality.

However, without a defined communication architecture to review, the NRC staff cannot reach a final conclusion on this point. An applicant or licensee referencing this SE should confirm that no equipment outside of the safety division is used in the transmission of messages within a NERVIA network. If an alternate strategy is used, it should be justified per Point 16.

3.9.1.17 Staff Position 1, Point 17

Staff Position 1, Point 17, states that pursuant to 10 CFR 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

Communications for the SPINLINE 3 system are performed over the NERVIA network. The components of this interface are described in Section 3.2.1.3.5 of this SE and Point 14. The fiber optic cabling provides electrical isolation between safety divisions as well as EMI/RFI protection for the remaining system components. The NERVIA+ board and the Fiber Optic Modems were subject to environmental qualifications as discussed in Section 3.6 of this SE. The generic qualification of the SPINLINE 3 platform encompasses both the hardware and the software used in the system. The SPINLINE 3 platform was qualified in accordance with the EPRI TR-102323 criteria. As noted in Section 3.6 of this SE, the qualification of the SPINLINE 3 platform does not include the fiber optic cables used to connect the PU1 and PU2. Therefore, an application specific evaluation will be required for plant-specific applications of a SPINLINE 3 platform that utilizes fiber optic cables to connect NERVIA+ modules between safety divisions.

The NRC staff has determined that the SPINLINE 3 platform meets the guidance provided by Staff Position 1, Point 17. However, as noted above, fiber optic cables used to implement the NERVIA communications for a system in safety applications will require application specific review and approval to verify these cables are qualified for the environment in which they will be used, in accordance with 10 CFR 50.49 as applicable. Furthermore, safety applications using the SPINLINE 3 platform will require application specific review to confirm that the plant-specific environment is consistent with the qualification envelope defined in Section 3.6 of this SE.

3.9.1.18 Staff Position 1, Point 18

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

Section 3.9.1.12 describes how SPINLINE 3 platform detects communication faults. In addition, this point mentions that the NRC staff reviewed the NERVIA+ board reliability analysis (Reference 1.33), and found that the hardware reliability and failure modes analyses performed considered means of detection for each failure. Rolls-Royce only performed a FMECA for the board. In the LTR, Rolls-Royce noted that a FMECA should be performed for a plant-specific application. In addition, in Table 3.7-1, Rolls-Royce states that a plant-specific communication analysis is recommended if third party systems are included.

In addition, the NERVIA+ board manages and handles all NERVIA communication, including the NERVIA protocol. The UC25 N+ CPU board is not burdened or interrupted by the NERVIA communication. Communication errors and malfunctions do not interfere with the execution of the safety function.

The NRC staff determined that for the SPINLINE 3 platform, the requirement to perform failure modes and effects analyses for a plant-specific application meets the intent of the guidance provided in Staff Position 1, Point 18.

3.9.1.19 Staff Position 1, Point 19

Staff Position 1, Point 19, states that the communications data rates be such that they will not exceed the capacity of a communications link or the ability of nodes to handle traffic, and that all links and nodes have sufficient capacity to support all functions. To do this, 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 and that communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

As described in the discussion for DI&C-ISG-04 Staff Position 1, Point 7, above, the communication rates for the NERVIA network are defined during the design of the system. In addition, the volume of data transmitted through the NERVIA network remains constant as the safety function processor performs its safety functions. Actual data transmission rates and data volume are application specific parameters which cannot be assessed in a generic platform perspective. The number of Stations in the NERVIA network that can transmit is fixed during the system design process. Data scan rates are also set during the system design phase and are based on a constant cycle time. Furthermore, the response time of the system is set during the design phase of the SPINLINE 3 platform-based system.

Since these parameters are constant for a given application an initial confirmation that parameter limits are not exceeded should be performed once the true data rates have been identified. Implementation of SPINLINE 3 platform safety system applications will require application specific review to verify conformance to the guidance of Staff Position 1, Point 19.

3.9.1.20 Staff Position 1, Point 20

Staff Position 1, Point 20, states that 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.

A discussion of the SPINLINE 3 platform response time is provided in Section 3.7.1 of this SE. Also, Section 3.9.1.5 states that Section 4.5.2.1 of the LTR describes the network cycle time and the factors that are incorporated into its determination for a plant-specific application, and Section 4.2.6 of the LTR describes the response time for the Unit. Both sections explain that the network and processor cycle times are defined during the design of the SPINLINE 3 platform.

To ensure that the SPINLINE 3 platform meets its application system response time requirements, the execution time for all of the systems tasks is calculated and measured during system development. This calculation includes terms to address the response time of the memory processing and associated circuits.

Staff Position 1, Point 20, cannot be assessed for the SPINLINE 3 platform and must be evaluated as an application specific review for a plant-specific application because this time will depend on the I/O boards, application software, and NERVIA network. When implementing a SPINLINE 3 safety system the licensee must review Rolls-Royce's timing analyses and validation tests for the SPINLINE 3 system in order to verify that it satisfies its plant-specific requirements for system response and display response time presented in the accident analysis in Chapter 15 of the safety analysis report.

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

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function block, which receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device.

The design of field device interfaces and the determination of means for command prioritization were not provided in the LTR for SPINLINE 3 platform. If a SPINLINE 3 platform based design is used for the development of a command prioritization system then an additional evaluation of that system against the criteria of DI&C-ISG-04 Section 2 should be performed. Since the LTR for the SPINLINE 3 platform does not address a specific application involving command prioritization, no evaluation against this staff position could be performed.

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

Section 3 of DI&C-ISG-04 provides guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from

sources in more than one safety division, and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

In Table 3.7-1 of the LTR, Rolls-Royce provided a brief description on how the SPINLINE 3 platform can comply with Section 3. However, the NRC staff did not evaluate this information because the design of multidivisional control and display stations was not provided in the SPINLINE 3 platform LTR. Furthermore, Rolls-Royce did not request review and approval of the operator displays described in Section 3.2.1.5 of this SE.

If a SPINLINE 3 platform based design is used for the development of a multidivisional station, then an additional evaluation of that system against the criteria of DI&C-ISG-04 Section 3 should be performed. Since the SPINLINE 3 platform LTR does not address a specific application involving a multidivisional control or display station, no evaluation against this staff position could be performed.

3.10 Compliance to IEEE Std. 603-1991 Requirements

For nuclear power generating stations, the regulation at 10 CFR 50.55a(h) requires that safety systems must meet the requirements stated in IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" and the correction sheet dated January 30, 1995. The NRC staff's evaluation is based on the guidance contained in SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," which provides acceptance criteria for this standard. This NRC staff evaluation also addresses the RG 1.153, "Criteria for Safety Systems," endorsement of IEEE Std. 603-1991.

Table 3.8-2 of the LTR provides a cross-reference between clauses of IEEE Std. 603-1991 to sections within the LTR. Each section identified in this table contain corresponding plant-specific action items to demonstrate that the plant and application-specific design basis for a safety system has been appropriately bounded within the scope of the LTR; otherwise, additional plant-specific equipment efforts should be performed.

The subsections below document the evaluation of the SPINLINE 3 platform against those regulatory requirements. This evaluation supports conclusions regarding adherence of the SPINLINE 3 platform relevant regulatory requirements. Since Rolls-Royce's SPINLINE 3 LTR (Reference 1.4) does not address specific applications or establish a definitive safety system design, the evaluation against this guidance is limited to consideration of the means provided within the platform to address issues related to interactions among safety divisions and between SR equipment and equipment that is not SR. Because the NRC staff evaluation is largely limited to a determination regarding whether the SPINLINE 3 platform supports satisfying the various clauses of IEEE Std. 603-1991, a single general plant-specific action item has been created to address full compliance to each IEEE Std.603-1991 clause, which applies to each plant-specific and application-specific use of the SPINLINE 3 platform (see Section 5.2, Item 30).

3.10.1 IEEE Std. 603-1991 Clause 4, “Safety System Designation”

Clause 4 of IEEE Std. 603-1991 states that a specific basis shall be established for the design of each safety system of the nuclear power generating station. SRP Chapter 7, Appendix 7.1-C, Section 4, “Safety System Designation” provides acceptance criteria for these requirements.

The determination and documentation of the design basis for a safety system is an application-specific activity that is dependent on the plant design. Since the LTR does not address a specific application of the platform, the design basis for a safety system is not available for review and no evaluation of the SPINLINE 3 platform against these regulatory requirements could be performed. Nevertheless, Table 3.8-2 provides a cross-reference of IEEE Std. 603-1991 Section 4 and information in the LTR to address these items. Specifically,

- Clauses 4.7 and 4.8 EQ, Section 5.1
- Clause 4.9 Reliability and Availability Analysis, Section 5.2

3.10.2 IEEE Std. 603-1991 Clause 5, “Safety System Criteria”

Clause 5 of IEEE Std. 603-1991 requires that safety systems maintain plant parameters, with precision and reliability, within acceptable limits established for each design basis event. The power, I&C portions of each safety system are required to be comprised of more than one safety group of which any one safety group can accomplish the safety function.

The establishment of safety groups that can accomplish a given safety function is a plant-specific and application-specific activity and the topical report scope does not include specific applications. Therefore, the following evaluations against the requirements of IEEE Std. 603-1991 Section 5 are limited to capabilities and characteristics of the SPINLINE 3 platform that are relevant to satisfy each requirement.

The following clauses were not evaluated because addressing compliance with this guidance is an application-specific activity that depends on the system design. Therefore, NRC staff determinations are not provided for these clauses.

- Clause 5.2, Completion of Protective Action
- Clause 5.9, Control of access
- Clause 5.10, Repair
- Clause 5.11, Identification
- Clause 5.12, Auxiliary features
- Clause 5.13, Multi-unit stations
- Clause 5.14, Human Factor considerations

3.10.2.1 IEEE Std. 603-1991 Clause 5.1, “Single Failure Criterion”

This clause requires that the safety system be able to perform its safety function required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

Determination that no single failure within the safety system can prevent required protective actions at the system level is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those features and capabilities that support adherence to the single failure criterion by a system design based on the platform. Since the LTR does not address a specific application for approval, the evaluation against this requirement is limited to consideration of the means provided within the platform to address failures. The NRC staff evaluation of the capabilities and characteristics of the SPINLINE 3 platform that are relevant to the Single-Failure Criterion are documented in Section 3.7.3, Self-Diagnostics and Test and Calibration Capabilities, and Section 3.6.13, Failure Mode and Effects Analysis.

3.10.2.2 IEEE Std. 603-1991 Clause 5.3, “Quality”

Clause 5.3 of IEEE Std. 603-1991 states that the components and modules within the safety system must 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 QA program. SRP Chapter 7, Appendix 7.1-C, Section 5.3, “Quality,” provides acceptance criteria for the quality requirement. This acceptance criteria states that the QA provisions of 10 CFR Part 50, Appendix B, apply to a safety system.

Rolls-Royce developed the SPINLINE 3 platform following a commercial process, rather than specifically for use in SR systems in nuclear power plants. As a result, the design process that led to the SPINLINE 3 platform was not governed by Appendix B of 10 CFR Part 50. The SPINLINE 3 platform has undergone CGD and been subjected to Class 1E EQ. Section 3.5 of this SE provides the NRC staff evaluation of the CGD. The platform is now maintained under a QA program intended to satisfy the requirements of Appendix B in all aspects of the product life cycle going forward with the treatment of the SPINLINE 3 platform, including the design control process, purchasing, fabricating, handling, shipping, storing, building, inspecting, testing, operating, maintaining, repairing, and modifying of the generic platform. However, application software and its specific life cycle processes are outside the scope of this review and will be treated in plant-specific reviews.

Based on the review of the SPINLINE 3 platform development process, operating experience, life cycle design output documentation, and testing and review activities, the NRC staff finds the dedication evidence of the SPINLINE 3 platform to be acceptable for demonstrating built-in

quality, and thus the SPINLINE 3 hardware and OSS show sufficient quality to be suitable for use in SR applications.

3.10.2.3 IEEE Std. 603-1991 Clause 5.4, “Equipment Qualification”

This clause contains the EQ requirements. SRP Chapter 7, Appendix 7.1-C, Section 5.4, “Equipment Qualification” provides acceptance criteria for IEEE Std. 603-1991 Clause 5.4.

The qualification of the SPINLINE 3 platform under the generic service conditions required in EPRI TR-107330 were used to demonstrate the capability of a safety system based on the platform to satisfy this requirement. The evaluation of the environmental qualification for the SPINLINE 3 platform is contained in Section 3.6 of this SE. This section also identifies plant-specific actions to demonstrate that the SPINLINE 3 platform performance as bounded by its EQ satisfies the requirements of the plant-specific installation environment for the plant-specific and application-specific safety functions.

The NRC staff evaluation provided in Section 3.6 determined that the SPINLINE 3 platform EQ provided a type test and supporting analyses to establish a documented set of platform safety functions, range of installation conditions, and installation limitations for the SPINLINE 3 platform that is suitable for reference by licensees and conforms to RG 1.209’s endorsement of IEEE Std. 323-2003 for qualification of SR computer-based I&C systems installed in mild environment locations. The NRC staff further determined that the SPINLINE 3 platform EQ is capable of satisfying IEEE Std. 603-1991, Clause 5.4, for the plant-specific use as long as a referencing applicant or licensee confirms that the application and installation have been bounded by the SPINLINE 3 platform EQ including each boundary/interface condition and installation limitation. This is covered by Application Specific Action items 15, 16, 19, 20, 21, and 22, described in Section 5.2 of this SE.

3.10.2.4 IEEE Std. 603-1991 Clause 5.5, “System Integrity”

This clause states 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. SRP Chapter 7, Appendix 7.1-C, Section 5.5, “System Integrity,” provides acceptance criteria for system integrity.

Determination of system integrity is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those characteristics that can support fulfillment of this requirement by a system design based on the platform. Since the LTR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the integrity demonstrated by the platform and its features to assure a safe state can be achieved in the presence of failures. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.5.

3.10.2.5 IEEE Std. 603-1991 Clause 5.6, “Independence”

This clause contains the requirements for physical, electrical, and communications independence. SRP Chapter 7, Appendix 7.1-C, Section 5.6, “Independence” provides acceptance criteria for system integrity.

The LTR states that specific redundancy needed for an SPINLINE 3 platform-based system is intended to be defined at the system level during the actual plant implementation. Therefore, the determination of independence is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those characteristics that can support fulfillment of this requirement by a system design based on the platform. The platform’s evaluation against this requirement is limited to consideration of the digital communications described in Section 3.2.3 and evaluated in Section 3.9 this SE, because the LTR does not address a specific application or establish a definitive safety system design. Although the system seems suitable to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.6.

The NRC staff has determined that conformance with IEEE Std. 603-1991 Clause 5.6 remains an application-specific activity that should take into consideration the full system design, any use of a shared component, the equipment’s installation, and the power distribution architecture. When considering the use of a shared component or the power distribution architecture, the application-specific activities of the full system design should take into further consideration the digital communications evaluation in Section 3.9 of this SE.

3.10.2.5.1 IEEE Std. 603-1991 Clause 5.6.1, “Between Redundant Portions of a Safety System”

This clause states that the safety systems be designed such that there is sufficient independence between redundant portions of a safety system such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.

The LTR states that specific redundancy needed for a SPINLINE 3 platform-based system is intended to be defined at the system level during the actual plant implementation to accomplish the safety function during and following any design basis event requiring that safety function.

3.10.2.5.2 IEEE Std. 603-1991 Clause 5.6.2, “Between Safety Systems and Effects of Design Basis Event”

This clause states that the safety systems required to mitigate the consequences of a specific design basis event must be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of

this standard. Clause 5.6.2 further states that EQ in accordance with 5.4 is one method that can be used to meet this requirement.

Determining the effects of design basis events and establishing the physical separation of the safety system from the effects of those events are application-specific activities. However, the qualification of the SPINLINE 3 platform under the generic service conditions required in EPRI TR-107330 can be used to demonstrate the capability of a safety system based on the platform to satisfy this requirement. The evaluation of the environmental qualification for the SPINLINE 3 platform is contained in Section 3.6 of this SE. This section also identifies plant-specific actions to demonstrate that the SPINLINE 3 platform performance as bounded by its EQ satisfies the requirements of the plant-specific installation environment for the plant-specific and application-specific safety functions.

Based upon the installation of SPINLINE 3 platform equipment in a mild environment that is bounded by the EQ that is discussed and evaluated in Section 3.6 of this SE, the NRC staff determined that the SPINLINE 3 platform supports satisfying IEEE Std. 603-1991 Clause 5.6.2 after a referencing applicant or licensee adequately addresses the plant-specific actions associated with confirming the application and installation have been bounded by the SPINLINE 3 platform EQ including each boundary/interface condition and installation limitation.

3.10.2.5.3 IEEE Std. 603-1991 Clause 5.6.3, “Between Safety Systems and Other Systems”

This clause states that the safety systems be designed such that credible failures in and consequential actions by other systems will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a single random failure. The three subsections below document the evaluation of interconnected equipment, equipment in proximity, and the effects of a single random failure separately.

Evaluation of this Clause requires identification of credible failures in and consequential actions by other systems as documented in the applicant’s or licensee’s plant-specific design basis. The SPINLINE 3 platform provides digital communication design features that can support independence between an SPINLINE 3 platform-based safety system and other interfacing systems, which are discussed and evaluated in Section 3.2.3.2 of this SE. The SPINLINE 3 platform can also support classification of interconnected equipment; however, the LTR did not provide sufficient information for the NRC staff to review communication from 1E to non-1E system. Therefore, demonstration that adequately qualified isolation devices are used where required should be performed as part of the plant-specific application of the SPINLINE 3 platform.

3.10.2.5.4 IEEE Std. 603-1991 Clause 5.6.4, “Detailed Criteria”

This clause does not contain any requirements; therefore no evaluation against this part is required.

3.10.2.6 IEEE Std. 603-1991 Clause 5.7, “Compatibility for Testing and Calibration”

This clause contains testing and calibration requirements. Determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements (e.g., accuracy) that apply. In addition, the establishment of the types of surveillance necessary for the safety system to ensure detection of identifiable single failures that are only announced through testing is an application-specific activity. Since the LTR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to enable testing and calibration for a redundant portion of a safety system (i.e., channel). Section 3.7.3 of this SE discusses the SPINLINE 3 platform’s ability to support satisfying IEEE Std. 603-1991 Clause 5.7, and identifies plant-specific actions to ensure that IEEE Std. 603-1991 Clause 5.7 will be satisfied.

3.10.2.7 IEEE Std. 603-1991 Clause 5.8, “Information Display”

This guidance states that the information displays for manually controlled actions should include confirmation that displays will be functional, and that safety system bypass and inoperable status indication should conform to the guidance of RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems.”

The design of information displays and operator workstations is an application-specific activity. Since the LTR does not address a specific application nor requested an evaluation of display devices within the scope of the platform, the NRC staff did not evaluate this item.

3.10.2.8 IEEE Std. 603-1991 Clause 5.15, “Reliability”

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

Table 5.1-2 of the LTR summarizes the reliability calculation for the SPINLINE 3 platform’s components. Each board’s reliability analysis includes individual hardware component failures and excludes consideration of software failures. The LTR does not provide specific configuration details for any application to establish a definitive safety system configuration; furthermore, safety system reliability goals are established on a plant-specific and application-specific basis.

The evaluation against this requirement is limited to consideration of the reliability characteristics of the platform and its components. The NRC staff's review SPINLINE 3 platform reliability is addressed Section 3.6.14 of this SE. This review identifies a plant-specific action item (see Section 5.2, Item 24).

3.10.3 IEEE Std. 603-1991 Clause 6, "Sense and Command Features – Functional and Design Requirements"

The requirements of this clause, in addition to the requirements of Clause 5, apply to the Sense and Command Features of a safety system.

The functional and design requirements for the sense and command features of a safety system are dependent solely on the specific application. Since the LTR does not address a specific application of the platform, include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the SPINLINE 3 platform against these regulatory requirements could be performed. Specifically, the following requirements were not evaluated:

- Clause 6.1 Automatic Control
- Clause 6.2 Manual Control
- Clause 6.3 Interaction between Sense and Command Features and other Systems
- Clause 6.4 Deviation of System Inputs
- Clause 6.6 Operating Bypass
- Clause 6.7 Maintenance Bypass

3.10.3.1 IEEE Std. 603-1991 Clause 6.5, "Capability for Testing and Calibration"

Clause 6.5 of IEEE Std. 603-1991 assures the availability of sense and command feature input sensors.

The LTR states that the applicability of this clause will be evaluated on a plant-specific basis. Nevertheless, Table 3.8-2 of the LTR states that the SPINLINE 3 platform will support a plant's existing methods to check operational availability of the system through the self-diagnostic and periodic testing described in Section 4.6 of the LTR. The NRC staff's review of these design features is provided in Section 3.7.3 of this SE.

3.10.3.2 IEEE Std. 603-1991 Clause 6.8, "Setpoints"

This clause is related to determination of sense and command feature setpoints.

This requirement for setpoints primarily addresses factors beyond the scope of a digital platform (e.g., plant design basis limits, modes of operation, and sensor accuracy). The LTR does not address a specific application or establish a definitive safety system, which is necessary to

demonstrate the adequacy of setpoints that are associated with IEEE Std. 603-1991 Clause 4.4. Therefore, the setpoint uncertainty must be addressed in an application-specific analysis. Section 5.2.3 of the LTR describes the approach Rolls-Royce used to prepare the setpoint analysis support documentation for the SPINLINE 3 digital safety I&C platform. The NRC staff's review of this approach is provided in Section 3.6.15 of this SE.

3.10.4 IEEE Std. 603-1991 Clause 7, "Execute features – functional and design requirements"

Section 7 of IEEE Std. 603-1991 contains five clauses that only apply to execute features of safety systems. Execute features are the electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling.

Since the LTR does not address a specific application of the platform, include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the SPINLINE 3 platform against these regulatory requirements could be performed. Specifically, the following requirements were not evaluated:

- Clause 7.1 Automatic Control
- Clause 7.2 Manual Control
- Clause 7.3 Completion of Protective Action
- Clause 7.4 Operating Bypass
- Clause 7.5 Maintenance Bypass

3.10.5 IEEE Std. 603-1991 Clause 8, "Power Source Requirements"

Clause 8 of IEEE Std. 603-1991 states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems, and that specific criteria unique to the Class 1E power systems can be found in IEEE Std. 308-1980. SRP Chapter 7, Appendix 7.1-C, Section 8, does not provide acceptance criteria for IEEE Std. 603-1991 Clause 8.

Section 4.3.4.9 of the LTR describes the power supplies for the SPINLINE 3 platform. In particular the LTR states that each chassis of the SPINLINE 3 platform will include an ALIM 48V/5-24 V board. However, determination of the power sources to be provided to a safety system is an application-specific activity.

3.11 Conformance with IEEE Std. 7-4.3.2-2003

RG 1.152, Revision 2, "IEEE Standard Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," states that conformance with the requirements of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," is a method that the NRC staff has deemed acceptable for satisfying the Commission's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," contains guidance for the evaluation of the application of the requirements of IEEE Std. 7-4.3.2-2003.

With the consideration that the LTR for SPINLINE 3 platform scope does not propose to satisfy all clauses of IEEE Std. 7-4.3.2-2003 via its components–similar to the clauses IEEE Std. 603-1991–the NRC staff's evaluation of each clause has a limited scope that does not provide a SE of SPINLINE 3 platform against the full clause. Furthermore, Table 3.8-1 of the LTR provides Rolls-Royce assessment for compliance of the SPINLINE 3 platform with IEEE Std. 7-4.3.2-2003.

The Regulatory Position in RG 1.152 provides guidance that establishment of a secure environment be addressed in the development process. SRP acceptance criteria for this guidance can be found in SRP Chapter 7, Appendix 7.1-D, Section 9 and DI&C-ISG-01. The evaluation of the SPINLINE 3 platform against this guidance is contained in Section 3.12 of this SE. Because the NRC staff evaluation is largely limited to the determination of the degree that the SPNLINE 3 platform and its development processes support satisfying the various clauses of IEEE Std. 7-4.3.2-2003, a single general plant-specific action item has been created to address full compliance to each IEEE Std. 7-4.3.2-2003 clause, which applies to each plant-specific and application-specific use of the SPINLINE 3 platform (see Section 5.2, Item 31).

The requirements of IEEE Std. 7-4.3.2-2003 supplement the requirements of IEEE Std. 603-1991 by specifying criteria that address hardware, software, firmware, and interfaces of computer-based safety systems. Consequently, the structure of IEEE Std. 7-4.3.2-2003 parallels that of IEEE Std. 603-1991. For those clauses where IEEE Std. 7-4.3.2-2003 contains no requirements beyond those found in IEEE Std. 603-1991 and SRP Chapter 7, Appendix 7.1-D contains no additional guidance, no review for compliance with IEEE Std. 7-4.3.2-2003 is required. Specifically, Clauses 4, 6, 7, and 8 were not reviewed. Thus, the subsections below are limited to those clauses where further evaluation is warranted. The review against the driving clauses of IEEE Std. 603-1991 is documented in the corresponding subsections of Section 3.10 of this SE.

3.11.1 IEEE Std. 7-4.3.2-2003 Section 4 – Safety System Design Basis

Section 4 of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Section 4 of IEEE Std. 603-1991 are necessary.

The NRC staff's review of the SPINLINE 3 platform against the requirements found in Section 4 of IEEE Std. 603-1991 is addressed in Section 3.10.1 of this SE.

3.11.2 IEEE Std. 7-4.3.2-2003 Clause 5, "Safety System Criteria"

Clause 5 of IEEE Std. 7-4.3.2-2003 contains requirements beyond those in IEEE Std. 603-1991 Clause 5. In addition, SRP Chapter 7, Appendix 7.1-D, Section 5 contains specific acceptance criteria for IEEE Std. 7-4.3.2-2003 Clause 5.

The implementation of a computer-based safety system is an application-specific activity. Since the LTR does not address a specific application, the evaluation against the following requirements addresses the capabilities and characteristics of the SPINLINE 3 platform that are relevant for adherence to each requirement.

Note that the following clauses were not evaluated because they do not identify requirements beyond those identified in IEEE Std. 603-1991.

- Clause 5.10, "Repair"
- Clause 5.12, "Auxiliary features"
- Clause 5.13, "Multi-unit stations"
- Clause 5.14, "Human factors consideration"

3.11.2.1 IEEE Std. 7-4.3.2-2003 Clause 5.1, "Single Failure Criterion"

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

The LTR states that an SPINLINE 3 platform-based safety system supports an application-specific design that will satisfy the single-failure criterion of Clause 5.1 of IEEE Std. 603-1991. The NRC staff's review of the SPINLINE 3 platform against the requirements found in Clause 5.1 of IEEE Std. 603-1991 is addressed in Section 3.10.2.1 of this SE.

3.11.2.2 IEEE Std. 7-4.3.2-2003 Clause 5.2, "Completion of Protective Action"

Clause 5.2 of IEEE Std. 7-4.3.2-2003 states that no requirements beyond those found in Clause 5.2 of IEEE Std. 603 are necessary.

The NRC staff's review of the SPINLINE 3 platform against the requirements found in Clause 5.2 of IEEE Std. 603-1991 is addressed in this SE.

3.11.2.3 IEEE Std. 7-4.3.2-2003 Clause 5.3, “Quality”

Clause 5.3 of IEEE Std. 7-4.3.2-2003 states that hardware quality is addressed in IEEE Std. 603-1991, and that software quality is addressed in IEEE/EIA Std. 12207.0-1996 and supporting standards. Clause 5.3 further requires that the digital computer development process include the development activities for both computer hardware and software, the integration of the hardware and software, and the integration of the computer with the safety system. Clause 5.3 includes six sub-clauses to identify activities beyond the requirements of IEEE Std. 603-1991 that are necessary to meet quality criterion for digital computer-based systems including its software. Each sub-clause under Clause 5.3 addresses one of these six activities.

As described in Section 3.10.2.2 of this SE, the SPINLINE 3 platform was developed following a commercial process. Rolls-Royce I&C France dedicated the commercial grade SPINLINE 3 platform, and it is now maintained under a QA program intended to satisfy the requirements of Appendix B, 10 CFR Part 50.

For the development of the application software, Rolls-Royce will follow development process established to satisfy the requirements of Appendix B, 10 CFR Part 50. However, review of the development process for the application software will be part of a plant-specific application (see Section 5.2, Item 9).

3.11.2.3.1 IEEE Std. 7-4.3.2-2003 Clause 5.3.1, “Software Development”

Clause 5.3.1 of IEEE Std. 7-4.3.2-2003 requires an approved QA plan consistent with the requirements of IEEE/EIA 12207.0-1996 for all software that is resident at runtime.

EPRI TR-106439, as accepted by the NRC SE dated July 17, 1997, and EPRI TR-107330, as accepted by the NRC SE dated July 30, 1998 provide guidance for the evaluation of existing commercial computers and software.

As described in Section 3.4.2, the operating software of the SPINLINE 3 platform and software embedded in certain I/O and communication boards were originally developed for non-US nuclear applications, in accordance with European standards for nuclear applications. Specifically, the software development process for the OSS was part of the MC3 project (Reference 1.72). In Section 6.2.2.8 of the LTR, Rolls-Royce explains the maintenance and modification processes for the SPINLINE 3 platform. These processes are part of the I&C France Quality Management. The OSS developed for MC3 project has gone through several modifications, as described in Section 2 of the LTR. Rolls-Royce submitted Software Modification Quality Plan (Reference 1.74) to describe the modifications made after the MC3 project. This quality plan establishes the process to manage evolution of software included in the SPINLINE 3 platform (e.g., OSS, NERVIA+ board software, CLARISSE, etc.). In particular, this plan describes the process to modify SPINLINE 3 software. This process takes into

consideration that a change to a software component (e.g NERVIA+ board) would affect other components.

To support description of SPINLINE 3 platform software development, Rolls-Royce submitted a Design Analysis Report (Reference 1.58). This report summarizes the assessment performed by MPR Associates on Rolls-Royce quality assurance program and development process for the SPINLINE 3 platform. Regarding the process for software development, this report concluded that the processes were adequate for software development for safety applications. This conclusion was based on the review of software life cycle processes, documentation and testing performed on the SPINLINE 3 software.

Section 3.5 of this SE discusses the CGD activities and evidence development undertaken by Rolls-Royce to dedicate the OSS. The CGD activities included source code inspection, application object testing, component testing, module prototype testing, functional testing, reconstitution of software documentation, and product operating history assessment.

The NRC staff also reviewed the quality of the propose SPINLINE 3 software development process of the Application software. Specifically, the NRC staff reviewed the software planning documentation and its compliance with BTP 7-14 (see Section 3.4.4). However, application software and its specific life cycle processes are outside the scope of this review and will be treated in plant-specific reviews.

Based on the evaluation of the CGD evidence and the process in place to preserve the dedication of the OSS, the NRC staff determined that the OSS of the SPINLINE 3 platform is suitable to support SR applications in nuclear power plants and meets this regulatory requirement. However, a plant-specific evaluation of the quality of application software is necessary for future applications.

- IEEE Std. 7-4.3.2-2003 Clause 5.3.1.1, “Software Quality Metrics”

Clause 5.3.1.1 of IEEE Std. 7-4.3.2-2003 states that the use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met.

Since the pre-developed operating software was dedicated rather than developed under the current Rolls-Royce software QA program, this requirement does not apply within the context of the scope of the TR. Note that Reference 1.72 identifies the metrics followed for the development of the MC3 project.

An evaluation of metric usage for the application software development will be conducted as part of a plant-specific review for any system based on the SPINLINE 3 platform. It is noted that the responsibilities for the QA manager to develop measurable data relating to the effectiveness

of the Rolls-Royce software QA program is included in the software quality assurance plan for the development of the application software.

3.11.2.3.2 IEEE Std. 7-4.3.2-2003 Clause 5.3.2, “Software Tools”

Clause 5.3.2 of IEEE Std. 7-4.3.2-2003 states that software tools used to support software development processes and V&V processes shall be controlled under configuration management, and that the tools shall either be developed to a similar standard as the safety relate software, or that 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.

Section 6.1 of the LTR describes the software development history for the SPINLINE 3 platform OSS. In particular, the OSS was developed in accordance with IEC 880-1986. Rolls-Royce has used the OSS since it was developed for the N4 project in the 1980’s and then used for the MC3 project. Rolls-Royce developed the OSS using ANSI C high level programming language (see Section 6.2.2.4 of the LTR). Reference 1.72 describes the software quality plan followed for the development of the generic SPINLINE 3 platform software for the MC3 project. This Reference also describes the tools used for the MC3 project. Section 3.5 describes the CGD process and the NRC staff’s evaluation of the development process and documentation for the OSS. In addition, the NRC staff reviewed several documents associated with the OSS development process during the regulatory audit as part of the thread audit for the OSS inconsistency checking of the control and data flows (Reference 2.5).

Rolls-Royce submitted its Requirements for Software Development Tools (Reference 1.94), which describes the measures imposed for software tools used for software development, so software quality can be ensured. The Rolls-Royce staff has to follow the steps described in this document to identify and develop software tools for software development, as well as the process to qualify commercially-available tools. This process was used for maintenance and management of evolution of software present in SPINLINE 3 platform, as described in Software Modification Quality Plan (Reference 1.74). In this manner, Rolls-Royce identifies the software classification level and the tools required for the modification.

Rolls-Royce uses the CLARISSE SSDE and SCADE for the development of SPINLINE 3 platform-based I&C systems. This tool is used to define the system architecture, hardware architecture, design the application software, and generate the executable code for a plant-specific application. As mentioned previously, CLARISSE SSDE and SCADE are only used and dedicated to the development of SPINLINE 3 platform-based I&C systems for nuclear applications. Section 6.2.7 of the LTR describes the development and validation of software tools for the SPINLINE 3 platform. In particular, this section states that Rolls-Royce developed the non-Class 1E CLARISSE SSDE and SCADE software tool in accordance with the guidance for software tools in IEC 880-1986. Further, this section states that software tools are controlled under the I&C France Configuration Management Program, which is also identified in Software Modification Quality Plan (Reference 1.74). In addition, the Design Analysis Report (Reference

1.58) assessed the development, validation and use of these software tools, and found that the usage of the tools is acceptable for the development of class 1E safety software.

For the development of the application software, Rolls-Royce will use the SCADE tool to define I&C functions for a plant-specific application, and CLARISSE to assemble all software components, hardware configuration, compiling of the file, and creation of the executable code for a plant-specific application. Rolls-Royce developed proprietary libraries in the SCADE tool, which are used to create application software that will be incorporated into the executable SPINLINE 3 software. Rolls-Royce considered these libraries part of the CGD of the SPINLINE 3 platform.

The NRC staff has reviewed the dedication process for the OSS of the SPINLINE 3 platform and the verification evidence for the software tools in this section and in Section 3.5 of this SE. Based on the information provided and the dedication effort, the NRC staff has determined that the output of the software development tools for SPINLINE 3 platform software was subject to V&V activities that would detect any defects or errors caused by the usage of the tools. Consequently, the use of these tools in the development of the platform software is consistent with this regulatory criterion and is, therefore, acceptable.

3.11.2.3.3 IEEE Std. 7-4.3.2-2003 Clause 5.3.3, “Verification and Validation”

Clause 5.3.3 of IEEE Std. 7-4.3.2-2003 states that a V&V program exists throughout the system life cycle, and states that the software V&V effort be performed in accordance with IEEE Std. 1012-1998.

As noted, the operating software of the SPINLINE 3 platform was pre-developed before the Rolls-Royce Appendix B, 10 CFR Part 50 compliant QA program was established. Consequently, the OSS was commercially dedicated and did not always have the current V&V program in place. However, Rolls-Royce developed the OSS in accordance with IEC 880, which requires rigorous establishment of software development plans and V&V activities to develop software for use in nuclear power plants (e.g., software quality assurance plan). Section 6.32 and Reference 1.72 of the LTR describes the OSS development process followed for the OSS. These references described the V&V activities, documentation prepared and tests performed. In Section 6.2.5 of the LTR, Rolls-Royce describes that procedures were prepared for V&V activities in accordance with the requirements in IEC 880.

RG 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std. 829-1983, “IEEE Standard for Software Test Documentation,” subject to the provisions and exceptions identified in the RG, identifies an acceptable method for satisfying test documentation requirements.

RG 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std. 1008-1987, “IEEE Standard for Software Unit

Testing," subject to the provisions and exceptions identified in the RG, identifies an acceptable method for satisfying software unit testing requirements.

As noted, the operating software of the SPINLINE 3 platform was pre-developed before the Rolls-Royce software QA program was established, and thus the OSS was commercially dedicated. Rolls-Royce submitted Software Integration Test Plan, Software Validation Plan, and Software Validation Report (References 1.49, 1.50, and 1.51, respectively). These documents describe the validation test plan, test cases, and test results. Furthermore, during the regulatory audit (Reference 2.5), the NRC staff observed the test bench used by the V&V team for testing the SPINLINE 3 platform software. Also, the NRC staff examined the development process to update portions of the OSS. The NRC staff observed how Rolls-Royce implemented the V&V processes.

Based on evaluation of V&V documentation, the dedication process and testing for the OSS conducted as part of the CGD process, and observations during the regulatory audit, the NRC staff concludes that the software testing of the OSS of the SPINLINE 3 platform is consistent with the guidance and is, therefore, acceptable to meet this regulatory criterion.

3.11.2.3.4 IEEE Std. 7-4.3.2-2003 Clause 5.3.4, "Independent V&V Requirements"

Clause 5.3.4 of IEEE Std. 7-4.3.2-2003 defines the levels of independence required for the V&V effort, in terms of technical independence, managerial independence, and financial independence.

The independence provided by the V&V activities and QA organization for the Rolls-Royce software QA program is described in Section 6.2.5 of the LTR, Reference 1.72, and regulatory audit (Reference 2.5). Specifically, Rolls-Royce uses a V&V team to perform V&V activities of 1E safety class software. This team is independent from the design team, and is responsible for testing and documenting evaluation of the safety class code. During the regulatory audit, the NRC staff observed that approved design and development documentation were formally signed by the Rolls-Royce V&V team member.

Based on these reviews and information, the NRC staff finds that the independence of V&V applied to the development of the OSS for the SPINLINE 3 platform meet this regulatory criterion.

3.11.2.3.5 IEEE Std. 7-4.3.2-2003 Clause 5.3.5, "Software Configuration Management"

Clause 5.3.5 of IEEE Std. 7-4.3.2-2003 states that SCM shall be performed in accordance with IEEE Std. 1042-1987, and that IEEE Std. 828-1998 provides guidance for the development of software configuration management plans. IEEE Std. 828-1990 and IEEE Std. 1042-1987 are endorsed by RG 1.169.

Section 6.2.6 of the LTR, Reference 1.72, and regulatory audit (Reference 2.5) describe software configuration management activities performed for the development of the OSS. For the MC3 project, Rolls-Royce did not use a separate Configuration Management Plan to describe these activities. Instead, Rolls-Royce describe these activities in the Software Quality Plan for the MC3 project. Section 6.2.6 of the LTR identifies the SCM reports prepared for the generic software of the SPINLINE 3 platform. After the Software Modification Quality Plan (Reference 1.74) was established, Rolls-Royce prepared Software Configuration Management Report for each software modification. Section 6.2.2.8 of the LTR lists the SCM reports prepared for the OSS. In particular, SCM for the SPINLINE 3 platform is currently established by the SCMP, Rolls-Royce document 1 208 878 E (Reference 1.76) and the Configuration Management Process, Rolls-Royce document 1 207 875 G (Reference 1.75). These documents define the SCM roles and responsibilities for internal organizations and staff, identify the SCM tools, and describe the processes for SCM including item identification, configuration control activities, change control authority and request mechanisms, and change/error tracking and reporting.

Rolls-Royce uses the Serena Dimensions CM tool for SCM. This tool manages all configuration items (e.g., technical documents, source files, etc.), except CLARISSE files. The CLARISSE SSDE includes tools that facilitate software configuration management. In addition, the Rolls-Royce proprietary libraries in the SCADE tool have its own configuration management plan which is described in Rolls-Royce document 3 013 037, which was reviewed during the regulatory audit (Reference 2.5). The audit report (Reference 2.5) describes configuration management within CLARISSE. Furthermore, during the regulatory audit, the NRC staff observed Rolls-Royce process for record keeping and configuration management. The NRC staff noted that Rolls-Royce has maintained records of all design basis documentation for the generic SPINLINE 3 platform. Reference 2.5 describes the Configuration Management tools used by Rolls-Royce.

Based on this review, the NRC staff determined that the SCMP of the Rolls-Royce software QA program, as applied to the control and maintenance of the OSS of the SPINLINE 3 platform, complies with this regulatory criterion and is, therefore, acceptable.

3.11.2.3.6 IEEE Std. 7-4.3.2-2003 Clause 5.3.6, “Software Project Risk Management”

Clause 5.3.6 of IEEE Std. 7-4.3.2-2003 defines the risk management (RM) required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.3.6, “Software Project Risk Management” provides acceptance criteria for software project RM. This section states that software project RM is a tool for problem prevention, and be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. It also states that software project risks may include technical, schedule, or resource related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety related functions. Additional guidance on the topic of RM is provided in IEEE/EIA Std. 12207.0-1996, “IEEE Standard for Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology –

Software Life Cycle Processes," and IEEE Std. 1540-2001, "IEEE Standard for Life Cycle Processes B Risk Management."

Table 3.8-1 of the LTR identifies that this is a requirement for a plant-specific application. Therefore, the NRC staff could not evaluate this criterion. Development of future applications should use a software risk management program to assist in the identification and resolution of potential problems.

3.11.2.4 IEEE Std. 7-4.3.2-2003 Clause 5.4, "Equipment Qualification"

Clause 5.4 of IEEE Std. 7-4.3.2-2003 defines the computer EQ required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.4, "Equipment Qualification," provides acceptance criteria for computer EQ. This section of Appendix 7.1-D states that in addition to the EQ criteria provided by IEEE Std. 603-1991 and Section 5.4 of SRP Chapter 7, Appendix 7.1-C, additional criteria, as defined in Sections 5.4.1 and 5.4.2, are necessary to qualify digital computers for use in safety systems. These sections are discussed below.

3.11.2.4.1 IEEE Std. 7-4.3.2-2003 Clause 5.4.1, "Computer System Testing"

Clause 5.4.1 of IEEE Std. 7-4.3.2-2003 discusses the software that should be operational on the computer system while qualification testing is being performed. SRP Chapter 7, Appendix 7.1-D, Section 5.4.1, "Computer System Testing," provides acceptance criteria for computer EQ testing. This section states that computer EQ testing should be performed while the computer is functioning, with software and diagnostics that are representative of those used in actual operation.

Section 3.6 of this SE discusses the evaluation of the environmental qualification program for the SPINLINE 3 platform. In particular, Rolls-Royce complied with the guidance of EPRI TR-107330 for the generic qualification of a PLC platform, with the exceptions identified in Section 3.6. Section 3.6.13.6.1.2 of this SE discusses the TSAP developed by Rolls-Royce for its generic qualification program. The TSAP was specifically designed to support qualification testing of the SPINLINE 3 platform while providing generic functionality of the SPINLINE 3 platform.

Based on the evaluation in Section 3.6 of this SE and review of the design documents for the TSAP (References 1.46) as well as qualification test plans and results (References 1.77 and 1.78, respectively), the NRC staff concludes that the Rolls-Royce qualification program met the requirement for computer testing of the SPINLINE 3 platform.

3.11.2.4.2 IEEE Std. 7-4.3.2-2003 Clause 5.4.2, "Qualification of Existing Commercial Computers"

Clause 5.4.2 of IEEE Std. 7-4.3.2-2003 defines the Qualification of Existing Commercial Computers for use in SR applications in nuclear power plants. SRP Chapter 7, Appendix 7.1-D, Section 5.4.2, "Qualification of Existing Commercial Computers," provides acceptance criteria for computer EQ. This section states that EPRI TR-106439 and EPRI TR-107330 provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

As mentioned previously, Rolls-Royce developed the OSS and certain software components in accordance with European standards, not compliant with the requirements in 10 CFR Part 50, Appendix B. Rolls-Royce commercially dedicated the pre-developed operating software of the platform under the guidance of EPRI TR-106439 and generically qualified the SPINLINE 3 platform in accordance with the guidance of EPRI TR-107330. The evaluation of the evidence from each of these activities is contained in Sections 3.5.

Note the LDU and MMU, described in Section 4.6.10 of the LTR, are commercial products. However, the NRC staff did not evaluate these items because they were not part of the scope for evaluation of the SPINLINE 3 platform.

Based on the findings of this review, the NRC staff finds that the generic qualification program of the SPINLINE 3 platform complies with the guidance of both EPRI TR-106430 and EPRI TR-107330, subject to satisfactory resolution of the generic open items in Section 5.0 of this SE.

- IEEE Std. 7-4.3.2-2003 Clause 5.4.2.1, "Preliminary Phase of the COTS Dedication Process"

This clause of IEEE Std. 7-4.3.2-2003 specifies that the risks and hazards of the dedication process are to be evaluated, the safety functions identified, configuration management established, and the safety category of the system determined. Most of these requirements are satisfied generically by the approved guidance in EPRI TR-107330, which addressed the risks and hazards in the development of the guide and selected the safety functions and system safety categories that are covered by the scope of the guidance.

The configuration management of the COTS item (i.e., the OSS of the SPINLINE 3 platform) is described in Section 3.5.4.2 of this SE. Based on the prior acceptance of the EPRI TR-107330 guidance and the review of the Rolls-Royce SCMP, the NRC staff finds that the Rolls-Royce qualification program met the requirements of this clause (and its sub-clauses on risks and hazards evaluation, safety function identification, and configuration management controls) for the computer qualification of the SPINLINE 3 platform.

- IEEE Std. 7-4.3.2-2003 Clause 5.4.2.2, "Detailed Phase of the COTS Dedication Process"

This clause of IEEE Std. 7-4.3.2-2003 involves evaluation of the commercial grade item for acceptability based on detailed acceptance criteria. In particular, critical characteristics of the COTS item are to be evaluated and verified. The characteristics are identified in terms of physical, performance, and development process attributes. This requirement is addressed by the guidance in EPRI TR-106439. Specifically, a critical design review is specified to identify physical, performance, and dependability (i.e., development process) characteristics, which are then verified by one or more of the fours methods identified in the guide.

Section 3.5 of this SE contains the evaluation of the COTS dedication process executed by Rolls-Royce for the OSS of the SPINLINE 3 platform. As discussed, a commercial grade software evaluation was performed by Rolls-Royce to identify critical characteristics. A survey of the QA processes in place during the development of the legacy software was coupled with testing to verify that the critical characteristics are acceptably demonstrated by the SPINLINE 3 platform. Based on the review of the dedication process and the testing results, the NRC staff determined that the Rolls-Royce qualification program satisfies this clause for the generic qualification and CGD of the SPINLINE 3 platform.

- IEEE Std. 7-4.3.2-2003 Clause 5.4.2.3, “Maintenance of Commercial Dedication”

This clause of IEEE Std. 7-4.3.2-2003 specifies that documentation supporting CGD of a computer-based system or equipment is to be maintained as a configuration control item. In addition, modifications to dedicated computer hardware, software, or firmware are to be traceable through formal documentation.

The Rolls-Royce qualification program has generated and maintained evidence of CGD and qualification for the SPINLINE 3 platform. Section 3.5 of this SE discusses Rolls-Royce’s approach to configuration control under its SCMP. Section 3.5.4.2 of this SE describes the plans and procedures for treating SR application software under the Rolls-Royce software QA program. In addition, Reference 1.74 describes the modification process for SPINLINE 3 software. This plan identifies SCMP (Reference 1.76) to describe the Software Configuration Management Plan to control configuration management activities. Furthermore, Section 6.2.2.8 and 6.2.6 of the LTR identifies the SCM reports prepared for all revisions of the OSS.

Based on the review of the Rolls-Royce software QA program for its suitability to preserve the dedication of the OS under maintenance modification, the NRC staff finds that the Rolls-Royce software QA program meets this requirement as applied to maintenance of the OSS of the SPINLINE 3 platform.

3.11.2.5 IEEE Std. 7-4.3.2-2003 Clause 5.5, “System Integrity”

Clause 5.5 of IEEE Std. 7-4.3.2-2003 states that in addition to the system integrity criteria provided by IEEE Std. 603-1991, the digital system shall be designed for computer integrity, test

and calibration, and fault detection and self-diagnostics activities. These attributes are further defined in Clause 5.5.1, “Design for computer integrity,” Clause 5.5.2, “Design for test and calibration,” and Clause 5.5.3, “Fault detection and self-diagnostics.” There are no specific acceptance criteria shown in SRP Chapter 7, Appendix 7.1-D, Section 5.5, “System Integrity.”

3.11.2.5.1 IEEE Std. 7-4.3.2-2003 Clause 5.5.1, “Design for Computer Integrity.”

Clause 5.5.1 of IEEE Std. 7-4.3.2-2003 states that the computer must be designed to perform its safety function when subjected to conditions, either external or internal, that have significant potential for defeating the safety function.

The SPINLINE 3 platform includes features to provide fault tolerant capabilities. In addition, the SPINLINE 3 platform includes diagnostics and self-testing (see Section 3.7.3) that can facilitate a high-level of computer integrity. However, Rolls-Royce did not define a system architecture or application for the SPINLINE 3 platform. Instead, Rolls-Royce defined a generic platform that can be used in a wide range of applications or configurations. Therefore, the NRC staff only evaluated the features provided in the generic platform, as described in Sections 3.7 of this SE. This evaluation should be used to support future evaluations of plant-specific applications that are based on the SPINLINE 3 platform.

Furthermore, the SPINLINE 3 platform qualification activities documented by Rolls-Royce, which are discussed in Sections 3.6 of this SE, provide suitable evidence that the SPINLINE 3 platform is capable of handling environmental conditions, external or internal, that have the potential to defeat implemented safety functions.

Based on the information provided, the NRC staff has determined that the features provided on the SPINLINE 3 platform can allow the system performing its safety functions. However, determination of compliance with this criterion requires a plant-specific action item to address system integrity for a plant-specific application (see Section 5.2, Item 31).

3.11.2.5.2 IEEE Std. 7-4.3.2-2003 Clause 5.5.2, “Design for Test and Calibration”

Clause 5.5.2 of IEEE Std. 7-4.3.2-2003 states that test and calibration functions shall not adversely affect the ability of the computer to perform its safety function, and that it shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change. The clause further states that V&V, configuration management, and QA be required for test and calibration functions on separate computers such as test and calibration computers that provide the sole verification of test and calibration data, but that V&V, configuration management, and QA is not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

As stated in Section 3.7.3, maintenance activities, including periodic testing and surveillance, will be defined based on the system requirements and the plant-specific application. Online

diagnostics and self-tests are provided in the SPINLINE3 platform to support test and calibration requirements in general. These are described in Section 3.10.3.1. The qualification tests performed for the SPINLINE3 platform were conducted with diagnostics executing in conjunction with the TSAP performing basic functions (see Section 3.6 of this SE). The performance of these tests demonstrated that the diagnostics and self-tests did not adversely affect the ability of the system to perform its simulated functions. Therefore, the NRC staff concludes that the diagnostic and self-test capabilities provided by the SPINLINE 3 platform conform to this requirement. However, determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements that apply and establishment of the types of surveillance necessary for the safety system to ensure that the identifiable single failures only announced through testing are detected are application-specific activities (see Section 5.2, Item 31).

3.11.2.5.3 IEEE Std. 7-4.3.2-2003 Clause 5.5.3, “Fault Detection and Self-Diagnostics”

Clause 5.5.3 of IEEE Std. 7-4.3.2-2003 discusses fault detection and self-diagnostics, and stated that if reliability requirements warrant self-diagnostics, then computer programs should contain functions to detect and report computer system faults and failures in a timely manner, and that these self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function.

Sections 3.4.2.1.3 and 3.4.2.3 of this SE describe the diagnostics and self-test capabilities provided in the SPINLINE 3 platform. These tests and diagnostics offer extensive and thorough coverage to detect failures in the system hardware , as well as to detect identified failure modes from the FMEA performed by Rolls-Royce (see Sections 3.6.13 of this SE for discussions the FMEA). If errors are encountered during self-tests or a test during one of this category, the OSS will perform pre-defined actions for a plant-specific application (see Section 3.4.2.3). Rolls-Royce will define these actions in the application specific Failure Analysis for a plant-specific application.

The hardware-based diagnostic features of the SPINLINE 3 platform satisfy this requirement and, along with the software-based diagnostics, the SPINLINE 3 platform is acceptable for providing fault detection in support of SR applications. However, because Rolls-Royce did not define the actions to be taken when faults are detected, as well as identifying that a combination of self-tests, periodic testing, and surveillance are necessary to successfully detect failures (see Section 3.7.3), there may be additional fault-detection and diagnostic capabilities implemented as part of the application or system design to provide more comprehensive coverage of identified failures with automatic tests and diagnostics. Therefore, a plant-specific evaluation is necessary to establish full conformance with Clause 5.5.3.

3.11.2.6 IEEE Std. 7-4.3.2-2003 Clause 5.6, “Independence”

Clause 5.6 of IEEE Std. 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std. 603-1991, data communications between safety channels or between safety and non-safety

systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence," provides acceptance criteria for computer EQ. This section states that the regulation at 10 CFR Part 50, Appendix A, GDC 24, "Separation of protection and control systems," requires the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Establishment of communications among redundant portions of a safety system or between the safety system and other non-safety systems in a plant is an application-specific activity. The base platform architecture identified in the LTR does not specify any direct connections or bi-directional communications between the SPINLINE 3 platform and any other system. Since the LTR does not address a specific application or provide a definitive safety system design, the evaluation of the SPINLINE 3 platform against the communications independence aspect of this regulatory requirement is limited to features and capabilities of its communication networks. Section 3.2.3 of this SE discusses communications interconnects within the scope of the SPINLINE 3 platform while Section 3.9 contains the evaluation of the SPINLINE 3 communications capabilities with respect to the guidance in DI&C-ISG-04.

Based on the evaluation described in this section and the other referenced sections, the NRC staff finds that the communications capabilities of the SPINLINE 3 platform provide acceptable design features to enable communications independence when appropriately configured. However, the specific interconnections defined for an application must be determined and evaluated in a plant-specific review.

3.11.2.7 IEEE Std. 7-4.3.2-2003 Clause 5.7, "Capability for Test and Calibration"

Clause 5.7 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. SRP Chapter 7, Appendix 7.1-D, Section 5.7, "Capability for Test and Calibration," provides no acceptance criteria for IEEE Std. 7-4.3.2-2003 Clause 5.7.

As described in Sections 3.4.2.1.3, 3.4.2.3, 3.7.3, 3.10.2.6, and 3.10.3.1 of this SE, the SPINLINE 3 platform provides on-line diagnostics and self-tests to detect failures within the platform. Further, Table 3.8-1 of the LTR identifies that there are no requirements beyond those identified in IEEE Std. 603 (see Sections 3.10.2.6 and 3.10.3.1).

The NRC staff finds that the SPINLINE 3 platform complies with this clause. However, as noted in Section 3.4.2.1.3, it is an Application Specific Action Item to identify that the diagnostics and self-tests do address the failure modes of the specific application and that appropriate display mechanisms are provided.

3.11.2.8 IEEE Std. 7-4.3.2-2003 Clause 5.8, “Information Displays”

Clause 5.8 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. However, SRP Chapter 7, Appendix 7.1-D, Section 5.8, “Information Displays,” noted that, in the past, information displays only provided a display function and, therefore, required no two way communication. More modern display systems may also have included control functions and, therefore, the NRC staff reviews the capacity for information displays to ensure that incorrect functioning of the information displays does not prevent the safety function from being performed when necessary.

Since the LTR does not address a specific application nor include display devices within its scope, no evaluation of the SPINLINE 3 platform against this clause could be performed. Further, Table 3.8-1 of the LTR identifies that there are no requirements beyond those identified in IEEE Std. 603-1991 (see Section 3.10.2.7).

3.11.2.9 IEEE Std. 7-4.3.2-2003 Clause 5.9, “Control of Access”

Clause 5.9 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. For this reason, there is no additional guidance beyond that found in Section 5.9 of SRP Chapter 7, Appendix 7.1-C and RG 1.152, Revision 2.

The regulatory position section in RG 1.152, Revision 2, provides guidance on security regarding electronic access to a safety system. SRP acceptance criteria for this guidance can be found in SRP Chapter 7, Appendix 7.1-D, Section, Section 9 and DI&C-ISG-01. The evaluation of the SPINLINE 3 platform against this guidance is contained in Section 3.12 of this SE.

3.11.2.10 IEEE Std. 7-4.3.2-2003 Clause 5.11, “Identification”

Clause 5.11 of IEEE Std. 7-4.3.2-2003 states that (1) identification requirements specific to software systems (i.e., firmware and software identification) shall be used to assure the correct software is installed in the correct hardware component, (2) means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools, and (3) physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std. 603-1991 Clause 5.11. SRP Chapter 7, Appendix 7.1-D, Section 5.11, “Identification” provides acceptance criteria and adds that the identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation that identifies the changes made by that revision for computer EQ.

Establishing software/firmware identification requirements and providing the means for retrieving that identification information are directly related to the Rolls-Royce QA Program. Section 3.5.3.2.1.3 contains the evaluation of the Rolls-Royce SCMP as it applies to maintaining OSS. The Rolls-Royce SCMP for application software is outside of the scope of this review.

SPINLINE 3 source code is an identified SCM component so version management and change control mechanisms are applied. The platform software components for the SPINLINE 3 are controlled based on assigned part numbers. The configuration information of each software component is securely maintained as part of the Rolls-Royce system configuration management records and can be referenced by part number against for a plant-specific project. Software versions for the assemblage of software components are defined in terms of a formally released, configuration controlled software project. The source code for each software version is copied into CDs and stored in an access-controlled vault. Rolls-Royce uses the Serena Dimension Tools during software development to manage source files and executable files. In addition, Rolls-Royce uses the software engineering tool included in CLARISSE for configuration management of CLARISSE files. The NRC staff observed how these tools are used during the regulatory audit (Reference 2.5).

The complied system software for each processor contains embedded information with build date, firmware type, and an internal checksum. This compiled software is then downloaded to a programmer (CLARISSE) to generate the FLASH EEPROM installed in the UC25 N+ CPU board using access-controlled equipment as part of the manufacture and assembly activities. No mechanism is provided by Rolls-Royce for altering the system software of a module in the field other than replacement of the flash memories on the CPU board.

Identification of the system software can be checked at the factory using Rolls-Royce tools (i.e., CLARISSE SSDE). Also, software identification can also be verified using the LDU for a plant-specific application. Further, the SPINLINE 3 platform will include a label to identify the processing unit name and release on each chip used to store the application software. The process for confirming the identification of installed firmware was observed by NRC staff during the regulatory audits conducted at the Rolls-Royce facility. Table 3.8-2 of the LTR states that the SPINLINE 3 platform hardware and software for a plant-specific application will be individually identified to enable the correct configuration and installation in accordance with the plant's identification scheme.

Based on the process observed during the regulatory audit for SPINLINE software identification, the NRC staff determined that the SPINLINE 3 platform complies with the guidance of IEEE Std. 7-4.3.2-2003 Clause 5.11 for its system software. However, assurance that proper hardware and software configuration is installed for a plant-specific application should be verified for each application.

3.11.2.11 IEEE Std. 7-4.3.2-2003 Clause 5.15, "Reliability"

Clause 5.15 of IEEE Std. 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std. 603-1991, when reliability goals are identified, the proof of meeting the goals shall include the software. Guidance is provided in SRP Chapter 7, Appendix 7.1-C, Section 5.15.

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

Determination of the reliability of a digital safety system is an application-specific activity that requires an assessment of a full system design, its application and system software, and the software life cycle processes. Since the LTR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures, the evaluation against this requirement is limited to consideration of the reliability characteristics of the digital platform and the quality of its system software. While the evaluation indicates the platform satisfies this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.15. Evaluation of the hardware reliability for the SPINLINE 3 platform is given in Section 3.6.14 of this SE.

Rolls-Royce performed a quantitative reliability and availability analysis for modules of the SPINLINE 3 platform (see Section 3.6.14 of this SE) as specified by EPRI TR-107330. According to EPRI TR-107330, software failures are generally not determined quantitatively because they "are caused by design errors and; therefore, do not follow the random failure behavior used for hardware reliability analysis." Thus, the reliability and availability analysis results are not sufficient as a sole means for evaluating reliability of digital safety systems based on the SPINLINE 3 platform.

A qualitative evaluation of software reliability for a safety system involves consideration of the quality of the software as demonstrated through its life cycle processes, testing, and operating experience. Application software and its specific life cycle processes are outside the scope of this review and will be treated in an application-specific review. The platform software for the SPINLINE 3 has undergone CGD as pre-developed software and the associated development history, operating experience, life cycle documentation, and testing and review activities have been reviewed (see Section 3.5 of this SE).

The demonstrated qualitative evidence of the OSS reliability for the SPINLINE 3 platform shows that the OSS provides suitable reliability and meets this requirement. However, demonstration of the hardware and software reliability of the implemented system is necessary to fully comply with this clause for digital safety system reliability. Specifically, an evaluation of system reliability, including the contribution of application software, will be treated in a plant-specific review.

3.12 Secure Development and Operational Environment

RG 1.152, Revision 3, describes a method that the NRC considers acceptable to comply with the regulatory criteria to promote high functional reliability, design quality, and establish a secure development and operational environments for the use of digital computers in SR

systems at nuclear power plants. The guidance for secure development and operational environments states that potential vulnerabilities should be addressed in each phase of the digital safety system life-cycle. The overall guidance provides the basis for physical and logical access controls to be established throughout the digital system development process to address the susceptibility of a digital safety system to inadvertent access and modification.

A secure development environment must be established to ensure that unneeded, unwanted and undocumented code is not introduced into a digital safety system – either the OSS or the application software. Regulatory positions 2.2 – 2.5 of RG 1.152, Revision 3 specifically identify controls that an applicant should implement during the development activities for safety related digital systems. Section 4.7 of the LTR addresses RG 1.152, Revision 3 (draft), and provides a description of the secure development activities performed for the development of the SPINLINE 3 platform. The manufacturer further describes compliance with RG 1.152 in Rolls-Royce document 3 013 962, “Secure Development and Operational Environment” (Reference 1.95).

The manufacturer’s secure development environment process addresses the V&V activities used to detect and prevent the use of unintended code, and the control and monitoring of access to the development environment. These measures and the design review and configuration management activities that are detailed in other Rolls-Royce procedures and plans provide protection against the introduction of unintended functionality into the platform.

The generic SPINLINE 3 platform software and plant-specific application software for a SPINLINE 3 system are developed in-house by Rolls-Royce. The primary location for the development of the generic SPINLINE 3 platform hardware and software is the Rolls-Royce facility in Meylan, France. This facility is also where a plant specific SPINLINE 3 system will be designed, developed, integrated, and factory tested. Rolls-Royce has another facility in Huntsville, Alabama, USA that also can be used for staging and factory testing a plant specific SPINLINE 3 system prior to delivery to a licensee. Currently, there is no SPINLINE 3 software development environment at the Huntsville factory. For an application specific review, the licensee should confirm that the application software is developed under a secure development environment (see Section 5.2, Item 32).

The manufacturer developed the SPINLINE 3 platform under a secure environment which controls the access to the facility, the facility Local Area Network (LAN), the development environment, quality records, and the configuration management system. The SPINLINE 3 software configuration management process is described in Section 3.5.4.2 of this SE.

Rolls-Royce performed a Vulnerability Assessment of the secure development environment at the Meylan, France facility. The Rolls-Royce document “Secure Development and Operational Environment Vulnerability Assessment” (Reference 1.96), identifies vulnerabilities within the safety system life cycle. The assessment identifies several vulnerabilities considered that could affect the safety system design, including: unauthorized access to the development environment, introduction of errors in the software manufacturing file, and introduction in the

generic platform software of undocumented code or other unwanted and undocumented functions or applications. The Vulnerability Assessment provides the measures used to mitigate these vulnerabilities and prevent the introduction of undocumented or unwanted code. Mitigation approaches address potential vulnerabilities to both internal and external threats that could otherwise challenge the confidentiality or integrity of the design. The Vulnerability Assessment addresses both physical and logical security control of the development environment and design products.

The Vulnerability Assessment states that unauthorized modification of software components and baselines is detected by V&V activities. An unauthorized change to the software can be detected by a comparison with a copy of the approved software baseline that is stored offsite and not subject to change by the same person. The V&V team uses a reference version of the software for validation. This reference version is locked by a baseline in the configuration management tool, and so, it cannot be deleted or modified. In the configuration management tool, each project is managed in a specific product environment and only project team members have access to a product. Access to the product environment is given by the Software Methods and Means Manager, after the team member has received project-specific configuration management training.

Executable files are available for production in a repository available on the company network. This repository is managed by the Information Technology (IT) group. Although all users (e.g., software team, manufacturing team, etc.) have read access on this repository, only the IT group has write access. When the software has been validated by the V&V team, the development team asks the IT Group to put the executable files into the repository. The V&V team then verifies with the checksum the integrity and conformity of the executable files they have validated. The manufacturing team uses the executable files in the repository for programming the components being delivered.

Whereas the manufacturer uses the term “dead” code when referring to the inadvertent introduction of undocumented, unwanted or unauthorized code; it uses the term “deactivated” code when referring to code that is purposely included, but may not be used in a plant specific application. Section 4.4.3.1 of the LTR states that the OSS supports all configurations of hardware and therefore, will have support for I/O modules that may not be installed in a plant specific application. Section 6.3 of the Software Preliminary Design (Reference 1.31) further discusses the use of deactivated code. For an application specific review, the licensee should confirm that the correct I/O modules are installed and that the deactivated code for boards not installed does not adversely affect the safety functions to be implemented in the SPINLINE 3 system (see Section 5.2, Item 2).

Without a specific operational environment to assess, the NRC staff cannot reach a determination on a plant-specific SPINLINE 3-based system’s ability to withstand undesirable behavior of connected systems and preclude inadvertent access. However, the SPINLINE 3 platform does include design attributes and features that a licensee could apply and credit to demonstrate protection against undesirable behavior of connected systems and the prevention

of inadvertent access. Section 3 of Reference 1.95 provides a list of such features. Nevertheless, the final determination on protection against undesirable behavior from connected systems and inadvertent access in the operational environment is a plant-specific activity (see Section 5.2, Item 32).

During the June, 2012 Regulatory Audit (Reference 2.5), the NRC staff observed Rolls-Royce's implementation of secure development environment activities at the Meylan, France, facility, including the use of tools to control access to documents and software files. The NRC staff was able to confirm that access to the facility, the facility LAN, the development environment, quality records, and the CM system are restricted in accordance with Rolls-Royce procedures. The NRC staff's observations during the audit support a finding of reasonable assurance that appropriate secure development environment activities are being performed.

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

4.0 SUMMARY

The NRC staff determined that the SPINLINE 3 platform standardized circuit boards described in the LTR, their design features, the generic software (i.e., library of software functions, the NERVIA newtork communication software, the operational system software, and software embedded in electronic boards with electronic components), and the processes used to produce them are sufficient to support compliance with the applicable regulatory requirements for plant-specific and application-specific use within SR I&C systems when each plant-specific and application-specific use satisfies the limitations and conditions delineated in Section 5.0 of this SE, and the system is properly installed and used. The NRC staff determined that the SPINLINE 3 platform can be used in SR systems to provide reasonable assurance of adequate protection of public health, safety and security based on the technical evaluation provided in Section 3.0 of this SE. On this basis, the NRC staff determined that the SPINLINE 3 platform is acceptable for use in SR I&C systems.

5.0 LIMITATIONS AND CONDITIONS

For each generic open item and plant-specific action item that applies to the applicant's or licensee's use of the SPINLINE 3 platform, an applicant or licensee referencing this SE should demonstrate that it has satisfactorily addressed the applicable items. The set of applicable items provide limitations and conditions for the SPINLINE 3 platform's use, as reviewed by the NRC staff and documented within this SE.

5.1 Generic Open Items

Beyond the plant-specific action items that follow, the NRC staff identified no generic open items to be addressed by an applicant or licensee referencing this SE for installation of a SR system based on the SPINLINE 3 platform.

5.2 Plant-Specific Action Items

The following plant-specific actions should be performed by an applicant or licensee referencing this SE for a SR system based on the SPINLINE 3 platform.

1. SRP – The licensee must establish full compliance with the design criteria and regulatory requirements identified in SRP Chapter 7, Table 7.1, that are relevant to the specific application(s) of the SPINLINE 3 platform as a SR digital I&C system in a nuclear power plant (see Section 2.0 of this SE).

2. System configuration – An applicant referencing this SE should demonstrate that the SPINLINE 3 platform used to implement the plant-specific system is unchanged from the generic platform addressed in this SE. Otherwise, the licensee should clearly and completely identify any modification or addition to the generic SPINLINE 3 platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes. In addition, the applicant must verify that modules, features, and or functions that require configuration (e.g., inhibition function on MV16, MV16 voting scheme, parameters for ICTO board, etc.) are properly configured and tested to meet system requirements. Furthermore, a V&V activity must confirm that the hardware tables for I/O boards not used in the system are deactivated.

3. System architecture – An applicant or licensee referencing this SE must verify that the system architecture for the application supports the system requirements, and it addresses the regulatory requirements in IEEE Std. 603-1991, Clause 4.

4. System communication architecture – An applicant or licensee referring this SE must evaluate the communication network architecture for the application.

5. Network configuration – An applicant or licensee referring this SE should evaluate configuration of the NERVIA network for the system application. In addition, a V&V

activity must confirm the type and number of stations transmitting on the network, station parameters and tables, amount of data transmitted by each station, time frame (time window) for each Station to transmit data, configuration of the DPM, Station sequence number, and the overall network cycle time for the system. The communication network should comply with NRC staff position for interdivisional communications, which includes data communications between different safety divisions and data communications between a safety division and equipment that is not SR.

6. Error and failure detection and management – An applicant or licensee referencing this SE must review the actions defined to be taken when failures and errors are detected during tests and self-tests, and ensure that these actions are consistent with system requirements. In addition, the applicant should review how errors and failures are indicated and managed after they are detected. The applicant should confirm that this information is provided in the single failure analysis for the plant-specific application.

7. Safety to non-safety communication – An applicant or licensee referencing this SE should verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety to non-safety systems.

8. Operator display – An applicant or licensee referencing this SE and uses an operator display must ensure that the supporting SPINLINE 3 platform components and the operator display instrumentation will be functional during all conditions within the plants design basis and that the operator display instrumentation will not adversely affect the system's ability to perform its safety functions. In addition, the applicant should evaluate that the operator displays demonstrate conformance with DI&C-ISG-04 positions.

9. System development and process implementation – An applicant or licensee referencing this SE should demonstrate that the development of its application software followed a development process that is equivalent to the one described in Section 3.4.4.1 of this SE and the LTR.

10. System cycle time – The applicant or licensee referencing this SE must demonstrate that the cycle time allocated to the application software, and consequential processor loading, permits execution of the safety function at least once in the available task execution cycle and is consistent with the plant-specific response time requirements. In addition, the licensee must perform timing analyses and functional testing for the particular application implementation and system configuration to demonstrate that the response time performance and reliability of a safety related system based on the SPINLINE 3 platform satisfies application specific requirements established in Chapter 15 of the safety analysis report for the plant.

The licensee must perform timing analyses and functional testing for a particular application implementation and system configuration to demonstrate acceptability for satisfying regulatory requirements.

11. Development of application software and use of development tools – An applicant referencing this SE should confirm that the implementation of the software development processes is conducted in accordance with the processes described for the application software in the LTR. In addition, an applicant or licensee referencing this SE should confirm that the CLARISSE SSDE is used as described in Sections 3.4.1 and 3.4.4.1 for designing and implementing the system architecture and configuration of the I/O boards and NERVIA network. The applicant should also confirm that the CLARISSE tools used for testing and validation of the application software were in accordance with Section 3.4.4 of this SE and the project specific V&V plan.

12. Life cycle planning documentation of application software – An applicant referencing this SE should confirm that specific life cycle planning documentation for application software has been developed in accordance with the software templates described in Section 3.4.4.1.1 of this SE and should evaluate conformance to the guidance criteria provided by industry standards and practices endorsed by the NRC, as referenced in SRP BTP 7-14.

13. Not Used.

14. Inclusion in NUPIC list – An applicant or licensee referencing this SE must confirm that Rolls-Royce is currently on the NUPIC list, or confirm that Rolls-Royce quality processes conform to the applicant's 10 CFR Part 50, Appendix b complaint program (i.e., Rolls-Royce is included in the applicant's Approved Vendor List).

15. Equipment Qualification - The licensee must demonstrate that the generic qualification envelope for the SPINLINE 3 platform bounds the corresponding plant-specific conditions (i.e., temperature, humidity, seismic, and EMC) for the location(s) in which the equipment is to be installed. In addition, an applicant or licensee referencing this SE should address its conformance to or deviations from the manufacturer identified boundary/interface conditions and installation limitations within the Summary EQ Report (see Reference 1.78). An applicant or licensee referencing this SE should identify the applicability of each condition and limitation. For each applicable condition or limitation, the applicant or licensee should either demonstrate its conformance or provide justification for any deviation. For any deviation, an applicant or licensee should demonstrate that the deviation does not invalidate the SPINLINE 3 platform qualification in a manner that is adverse to the reliable performance of a safety function. Such demonstrations that deviations are justified should consider performance of supplemental testing, supplemental analysis, or both.

16. Radiation and location – The applicant or licensee must demonstrate that the generically qualified radiation withstand capability of the SPINLINE 3 platform bounds the expected radiation exposure for the location(s) in which the equipment will be installed.

17. Passive hub and TP/FL converters assembly – An applicant or licensee referencing this SE and uses hubs and TP/FL converters assembly different than the one used in the QTS, then the applicant must confirm that the hub or other network device used on the NERVIA network is truly passive and does not use an embedded microprocessor.

18. Cabling requirements – An applicant or licensee referencing this SE must confirm that the wiring and cabling associated with the SPINLINE 3 platform are installed in accordance with Rolls-Royce document “Regles de Cablages dans les equipements type SPINLINE.”

19. Seismic limitations - An applicant or licensee referencing this SE must demonstrate that the qualified seismic withstand capability of the SPINLINE 3 platform bounds the plant-specific seismic withstand requirements. See Section 3.6.6 of this SE for boundary conditions established for the SPINLINE 3 platform during Seismic testing.

20. EMI/RFI limitations – An applicant or licensee referencing this SE must demonstrate that the SPINLINE 3 platform is not installed in areas of strong magnetic field and in areas susceptible to radiation above 8 GHz. Furthermore, the applicant must demonstrate that the qualified EMI/RFI capability of the SPINLINE 3 platform bounds the plant-specific EMI/RFI requirements.

21. ESD limitations – An applicant or licensee referencing this SE must confirm that the operation and maintenance procedure for the SPINLINE 3 platform-based system includes a requirement for technicians to use anti-static controls during maintenance.

22. Voltage tested for 1E to Non-1E – If a specific application requires Class 1E to non-Class 1E isolation to be provided, the licensee must demonstrate that the generic qualification envelope for the specific module(s) employed to provide electrical isolation bounds the maximum credible voltages applied to the interconnected non-Class 1E equipment. Furthermore, the licensee must demonstrate that the execution of the safety function implemented using the SPINLINE 3 platform will be unaffected by loss of any of those modules due to damage while providing electrical isolation.

23. FMECA – An applicant or licensee referencing this SE must perform a system-level FMECA to demonstrate that the application-specific use of the SPINLINE 3 platform identifies each potential failure mode and determines the effects of each. The FMECA should demonstrate that single-failures, including those with the potential to cause a non-safety system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot can adversely affect the protection functions, as applicable.

24. Reliability – An applicant or licensee referencing this SE must perform a deterministic system-level evaluation of the degree of redundancy, diversity, testability, and quality provided in a SPINLINE 3 platform-based safety system to determine if the degrees provided are commensurate with the safety functions being performed. An applicant or licensee should confirm that a resultant SPINLINE 3 platform-based system continues to satisfy any applicable reliability goals that the plant has established for the system. This plant-specific action should consider the effect of possible failures, system-level design features provided to prevent or limit the failures' effects, and any application-specific inclusion of a maintenance bypass to support plant operations. An applicant or licensee should demonstrate that the SPINLINE 3 platform reliability analysis method provides an equivalent level of assurance to the applicant's or licensee's reliability analysis method. The licensee must demonstrate that any plant-specific claims regarding quantification of reliability and availability address the impact of surveillance intervals on mean time to repair as part of the analysis. Furthermore, the licensee must demonstrate that any reliability and availability analysis addresses the impact of hardware CCF on availability.

25. Setpoint – An applicant must perform an analysis of accuracy, repeatability, thermal effects and other necessary data for use in determining the contribution of the SPINLINE 3 platform to instrumentation uncertainty in support of setpoint calculations.

26. Not Used.

27. Testing and surveillance – Since Rolls-Royce stated that a combination of surveillance, software diagnostics and automatic self-tests are necessary to provide comprehensive coverage of all platform failures, the applicant must establish the additional periodic surveillance testing that is necessary to detect system failures for which automatic detection is not provided and define appropriate surveillance intervals to provide acceptable comprehensive coverage of identifiable system failure modes. Also, the licensee must determine those physical configuration and plant-specific installation conditions that impact safety system maintenance and define any necessary diagnostic, testing, or surveillance functions to be implemented in application software to support maintenance and repair.

28. D3 analysis – An applicant or licensee referencing this SE must perform a plant-specific D3 analysis for SR applications of the SPINLINE 3 platform.

29. DI&C ISG-04 – although the NRC staff determined that the SPINLINE 3 platform includes features to support satisfying various sections and clauses of DI&C ISG-04, an applicant or licensee referencing this SE must evaluate the SPINLINE 3 platform based-system for full compliance against this guidance. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with its direct and indirect consequences.

30. IEEE Std. 603 – Although the NRC staff determined that the SPINLINE 3 platform supports satisfying various sections and clauses of IEEE Std.603-1991, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std.603-1991. Because this SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with its direct and indirect consequences, an applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 603-1991 clause to its application-specific SPINLINE 3 platform-based safety system or component. In addition, the applicant or licensee must demonstrate that the plant-specific and application-specific use of the SPINLINE 3 platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

31. IEEE Std. 7-4.3.2 – Even though the NRC staff determined that the SPINLINE 3 platform supports satisfying various sections and clauses of IEEE Std. 7-4.3.2-2003, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std. 7-4.3.2-2003. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with its direct and indirect consequences. The applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 7-4.3.2-2003 clause to its application-specific SPINLINE 3 platform-based safety system or component. Further, the applicant or licensee must demonstrate that the plant-specific and application-specific use of the SPINLINE 3 platform satisfies the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.

32. Secure Development Operational Environment – An applicant or licensee referencing this SE for a SR plant-specific application should ensure that a secure operational environment has been established for its plant-specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152.

6.0 REFERENCES

1. Rolls-Royce Documents

1.1. Rolls-Royce submittal letter dated July 8, 2009 (ADAMS No. ML092160018).
1.2. Rolls-Royce submittal letter dated January 31, 2011 (ADAMS No. ML110310577).
1.3. Rolls-Royce submittal letter dated December 18, 2012 (ADAMS No. ML13003A319).
1.4. Rolls-Royce Document 3 008 503 D, Proprietary Licensing Topical Report for SPINLINE 3 Digital Safety I&C Platform (ADAMS Accession No. ML13003A323 and ML13003A318).

1.5. Rolls-Royce Document 3 008 503 D-NP, Non-Proprietary Licensing Topical Report for "SPINLINE 3 Digital Safety I&C Platform (ADAMS Accession No. ML13003A321).
1.6. Rolls-Royce submittal letter dated December 23, 2009 (ADAMS Accession No. ML093570361).
1.7. Rolls-Royce submittal letter dated January 8, 2010 (ADAMS Accession No. ML100120087).
1.8. Rolls-Royce submittal letter dated February 2, 2010 (ADAMS Accession No. ML100330793).
1.9. Rolls-Royce submittal letter dated March 5, 2010 (ADAMS Accession No. ML101480946).
1.10. Rolls-Royce submittal letter dated May 28, 2010 (ADAMS Accession No. ML101480946).
1.11. Rolls-Royce submittal letter dated June 15, 2010 (ADAMS Accession No. ML101670080).
1.12. Rolls-Royce submittal letter dated December 23, 2010 (ADAMS Accession No. ML103610005).
1.13. Rolls-Royce submittal letter dated February 25, 2011 (ADAMS Accession No. ML110560422).
1.14. Rolls-Royce submittal letter dated March 31, 2011 (ADAMS Accession No. ML110910424).
1.15. Rolls-Royce submittal letter dated June 30, 2011 (ADAMS Accession No. ML111820015).
1.16. Rolls-Royce submittal letter dated July 6, 2011 (ADAMS Accession No. ML111870540).
1.17. Rolls-Royce submittal letter dated November 18, 2011 (ADAMS Accession No. ML11339A035).
1.18. Rolls-Royce submittal letter dated March 14, 2012 (ADAMS Accession No. ML120740394).
1.19. Rolls-Royce submittal letter dated May 31, 2012 (ADAMS Accession No. ML12188A036).
1.20. Rolls-Royce submittal letter dated July 19, 2012 (ADAMS Accession No. ML12201A090).
1.21. Rolls-Royce submittal letter dated September 21, 2012 (ADAMS Accession No. ML12271A452).
1.22. Rolls-Royce submittal letter dated December 21, 2011 (ADAMS Accession No. ML12010A066).
1.23. Rolls-Royce submittal letter dated August 3, 2012 (ADAMS Accession No. ML12220A022).
1.24. Rolls-Royce submittal letter dated April 4, 2013 (ADAMS Accession No. ML13102A042).
1.25. Rolls-Royce letter dated September 15, 2011 (ADAMS Accession No. ML1125900362).
1.26. Rolls-Royce Document 8 303 186, Civil Nuclear SAS Quality Manual (ADAMS Accession No. ML092160045).
1.27. Rolls-Royce Document 500-9600000-10, ICQ-005C, Instrumentation and Controls US Quality Manual (ADAMS Accession No. ML092160024).
1.28. Not Used.

1.29. Rolls-Royce Document 3 010 612 G, Master Configuration List (ADAMS Accession No. ML12201A091).
1.30. Rolls-Royce Document 1 207 108 J, Software Requirement Specification – Operational System Software (ADAMS Accession No. ML100330819).
1.31. Rolls-Royce Document 1 207 141 H, Software Preliminary Design – Core System Software (ADAMS Accession No. ML100330838).
1.32. Rolls-Royce Document 1 207 110 J, Interface Specifications – Operation System Software and application software (ADAMS Accession No. ML100330830).
1.33. Rolls-Royce Document 6 648 805 D, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 UC25 N+ CPU Board (ADAMS Accession No. ML093570382).
1.34. Rolls-Royce Document 1 207 228 G, SPINLINE 3 Safety of Processing Unit Software (ADAMS Accession No. ML093620225).
1.35. Rolls-Royce Document 5 100 436 882 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 RTD Conditioning Board: 8PT100 and I.8PT100 interface board (ADAMS Accession No. ML093570367).
1.36. Rolls-Royce Document 5 100 435 707 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Digital Isolated Input Board: 32ETOR TI SR and I.32ETOR TI interface board (ADAMS Accession No. ML093570375).
1.37. Rolls-Royce Document 3 008 991 B, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 32ETOR Input Terminal Block (ADAMS Accession No. ML093570366).
1.38. Rolls-Royce Document 5 100 436 348 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Analog Input Board: 16E.ANA ISO and I.16EANA interface board (ADAMS Accession No. ML093570370).
1.39. Rolls-Royce Document 1 479 513 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Calibrated Pulse Acquisition Board: ICTO and I.ICTO interface board (ADAMS Accession No. ML093570378).
1.40. Rolls-Royce Document 5 100 437 019 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Actuator Drive Board: 32ACT and I.32ACT interface board (ADAMS Accession No. ML0935703711).
1.41. Rolls-Royce Document 5 100 436 936 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Actuation Voting Module: MV16 (ADAMS Accession No. ML093570379).
1.42. Rolls-Royce Document 5 100 436 935 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Output Relays Terminal Block: 8SRELAY1 & 8SRELAY2 (ADAMS Accession No. ML093570377).
1.43. Rolls-Royce Document 3 008 651 B, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 Analog Output Board: 6SANA ISO and I.6SANA interface board (ADAMS Accession No. ML093570365).
1.44. Rolls-Royce Document 1 208 933 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 NERVIA+ daughter board and I.NERVIA+ interface board (ADAMS Accession No. ML093570380).

1.45. Rolls-Royce Document 3 000 180 C, Reliability Analysis and Predictive Safety Analysis of the SPINLINE 3 ALIM 48V/5V-24V power supply board and I.ALIM 48 interface board (ADAMS Accession No. ML093570376).
1.46. Rolls-Royce Document 3 006 404 E, System Specification of the Qualification Test Specimen and Data Acquisition System (ADAMS Accession No. ML101670096).
1.47. Rolls-Royce Document 8 307 288 A, Quality Procedure – Commercial Dedication, (ADAMS Accession No. ML100120120).
1.48. Not used.
1.49. Rolls-Royce Document 1 207 204 E, Software Integration Test Plan and Report (SITR) – SCC (Core System Software) (ADAMS Accession No. ML100330808).
1.50. Rolls-Royce Document 1 207 146 G, Software Validation Test Plan (SVTP) – Operation System Software for Safety Class Units (ADAMS Accession No. ML100330844).
1.51. Rolls-Royce Document 1 207 232 F, Software Validation Test Report (SVTR_ Operational System Software for Safety Class Units (ADAMS Accession No. ML100330814).
1.52. Rolls-Royce Document 8 303 314 L, Project Execution Process (ADAMS Accession No. ML12010A068).
1.53. Rolls-Royce Document 8 303 334 F, Project Development Process – System Design (ADAMS Accession No. ML12010A069).
1.54. Rolls-Royce Document 8 307 032 C, Principle for Control of Design (Safety Systems) (ADAMS Accession No. ML120740402).
1.55. Rolls-Royce Drawing 3 008 630A (ADAMS Accession No. ML13135A037).
1.56. Rolls-Royce Document 8 303 350 L, Safety Software Design Process (ADAMS Accession No. ML103610009).
1.57. Rolls-Royce Document 8 307 209 B, SPINLINE 3 Software Configuration Management (ADAMS Accession No. ML092160049).
1.58. Rolls-Royce Document MPR-3337 Rev1, SPINLINE 3 Design Analysis Report (ADAMS Accession No. ML092160044).
1.59. Rolls-Royce Document 1 208 356 B, Software Quality Plan – SCADE Operator Library (ADAMS Accession No. ML093620232).
1.60. Rolls-Royce Document 8 307 208 B, SPINLINE 3 Software Quality Assurance Plan (ADAMS Accession No ML092160054).
1.61. Rolls-Royce Document 8 307 210 B, SPINLINE 3 Software Verification and Validation Plan (ADAMS Accession No. ML092160055).
1.62. Rolls-Royce Document 8 307 211 B, SPINLINE 3 Software Development Plan (ADAMS Accession No. ML092160050).
1.63. Rolls-Royce Document 8 307 245 A, System Integration and Factory Test Plan (ADAMS Accession No. ML092160052).
1.64. Rolls-Royce Document 8 307 243 A, System Installation and Site Test Plan (ADAMS Accession No. ML092160027).
1.65. Rolls-Royce Document 8 307 244 A, System Operations and Maintenance Plan (ADAMS Accession No. ML92160053).
1.66. Rolls-Royce Document 8 307 242 A, System Training Plan (ADAMS Accession No. ML092160022).

1.67. Global Quality Assurance Audit Report (ADAMS Accession No. ML111870545).
1.68. Rolls-Royce Document 3 010 794 A, Dedication Plan for the Generic SPINLINE 3 Digital Safety I&C Platform (ADAMS Accession No. ML100120134).
1.69. Rolls-Royce Document 3 010 795 B, Dedication Report for the Generic SPINLINE 3 Digital Safety I&C Platform (ADAMS Accession No. ML13003A326).
1.70. Rolls-Royce Document 3 018 281 B, EPRI TR-16439 Critical Characteristics and EPRI TR-107330 Compliance Matrix Assessment Report (ADAMS Accession No. ML13003A325).
1.71. Rolls-Royce Document 1 207 102 A, Software Development Plan (ADAMS Accession No. ML093620283).
1.72. Rolls-Royce Document 8 303 429 A, Software Quality Plan (SQP) – MC3 (ADAMS Accession No. ML093620244).
1.73. Rolls-Royce Document 1 207 107 D, Rules for Verification and Validation of Software Components (ADAMS Accession No. ML103610007).
1.74. Rolls-Royce Document 1 208 686 A, Software Modification Quality Plan (ADAMS Accession No. ML093620234).
1.75. Rolls-Royce Document 1 207 875 G, Software Configuration Management Process (ADAMS Accession No. 103610008).
1.76. Rolls-Royce Document 1 208 878 E, Software Configuration Management Plan for SPINLINE 3 Software Sub-assemblies Managed by CM Tool (ADAMS Accession No. ML110310589).
1.77. Rolls-Royce Document 3 006 501 E, Equipment Qualification Plan (ADAMS Accession No. ML12188A041).
1.78. Rolls-Royce Document No. 3 014 545 C, Summary Equipment Qualification Test Report (ADAMS Accession No. ML13003A324).
1.79. Rolls-Royce Document No. 3 018 630 A, Investigations Results of 2011 NRC Qualification Tests (ADAMS Accession No. ML12188A046).
1.80. Rolls-Royce Document 3 010 783 B, Factory Acceptance Test Procedure for QTS and DAS (ADAMS Accession No. ML12188A0404).
1.81. Rolls-Royce Document 3 010 286 B, Radiation Exposure Test Procedure (ADAMS Accession No. ML101670117).
1.82. Rolls-Royce Document 3 010 287 B, Environmental Test Procedure (ADAMS Accession No. ML101670121).
1.83. Rolls-Royce Document 3 010 288 D, Seismic Test Procedure (ADAMS Accession No. ML12188A043).
1.84. Rolls-Royce Document 3 010 294 E, System Setup and Checkout Test Procedure (ADAMS Accession No. ML12271A453).
1.85. Rolls-Royce Document 3 010 295 E, Operability Test Procedure (ADAMS Accession No. ML12271A453).
1.86. Rolls-Royce Document 3 010 296 D, Prudency Test Procedure (ADAMS Accession No. ML12271A453).
1.87. Rolls-Royce Document 3 010 289 C, EMI/RFI Test Procedure (ADAMS Accession No. ML12271A453).

1.88. Rolls-Royce Document 3 010 290 B, Electrical Fast Transient Test Procedure (ADAMS Accession No. ML110910433).
1.89. Rolls-Royce Document 3 010 291 A, Surge Withstand Test Procedure (ADAMS Accession No. ML110910451).
1.90. Rolls-Royce Document 3 010 292 A, Electrostatic Discharge Test Procedure (ADAMS Accession No. ML110910453).
1.91. Rolls-Royce Document 3 010 293 A, Class 1E to Non-Class 1E Test Procedure (ADAMS Accession No. ML110910456).
1.92. Rolls-Royce Document 3 009 397 B, Setpoint Analysis Support (ADAMS Accession No. ML13003A327).
1.93. Rolls-Royce Document 3 011 552 B, Mapping of Generic SPINLINE 3 Licensing Documents to the ISG-06 Submittal Guidance (ADAMS Accession No. ML110910426).
1.94. Rolls-Royce Document 1 206 747 D, Requirements for Software Development Tools (ADAMS Accession No. ML093620258).
1.95. Rolls-Royce Document 3 013 962 A, Secure Development and Operational Environment (ADAMS Accession No. ML111820022).
1.96. Rolls-Royce Document 3 014 543 A, Secure Development and Operational Environment – Vulnerability Assessment (ADAMS Accession No. ML13017A270).

2. NRC Staff Documentation

2.1. NRC requests the supplemental information dated May 14, 2010 (ADAMS Accession No. ML101300192).
2.2. NRC acceptance letter dated December 1, 2010 (ADAMS Accession no. ML103350490).
2.3. NRC Requests for Additional Information dated November 7, 2011(ADAMS Accession No. ML112900190).
2.4. NRC Requests for Additional Information dated July 18, 2011 (ADAMS Accession No. ML12167A416).
2.5. NRC Requests for Additional Information dated March 28, 2013 (ADAMS Accession No. ML13037A493).
2.6. NRC Audit Report Regarding The Rolls-Royce SPINLINE 3 Digital Safety Instrumentation and Control Platform Licensing Topical Report (TAC NO. ME3600) (ADAMS Accession No. ML12243A459).