Rolls-Royce
5959 Shallowford Road, Suite 511
Chattanooga, Tennessee 37421
www.rolls-royce.com

August 3, 2012

U.S. Nuclear Regulatory Commission
Document Control Desk
11555 Rockville Pike
Rockville, MD 20852

ATTENTION: To whom it may concern

SUBJECT: Rolls-Royce Response to Request for Additional Information Re: Rolls-Royce Civil Nuclear "***SPINLINE 3*** Digital Safety Instrumentation and Control Platform" Topical Report (TAC NO. ME3600)

REFERENCES: (1) Project Number 0773: ***SPINLINE 3*** Digital Safety Instrumentation and Control Platform (TAC No. ME3600)
(2) Letter, Jonathan G. Rowley (NRC) to Mark Burzynski (Rolls-Royce),"Request for Additional Information (Set 2) Re: Rolls-Royce Civil Nuclear "***SPINLINE 3*** Digital Safety Instrumentation and Control Platform" Topical Report (TAC NO. ME3600)", July 18, 2012

NRC provided a request for additional information regarding the review of the Rolls-Royce ***SPINLINE 3*** Digital Safety Instrumentation and Control Platform Topical Report. The Rolls-Royce response to this request for additional information is provided by an enclosure to this letter.

Rolls-Royce hereby submits the following documents in connection with the referenced NRC project:

Document Title	Rolls-Royce Document Number	Versions: Proprietary (P), Non-proprietary (NP)	Notes
Response To Request For Additional Information - ***SPINLINE 3*** Digital Safety Instrumentation and Control Platform - Project No. 773	N/A	P	New document
Response To Request For Additional Information - ***SPINLINE 3*** Digital Safety Instrumentation and Control Platform - Project No. 773	N/A	NP	New document

Rolls-Royce considers some of the material contained in the response to be proprietary and requests that the proprietary documents be withheld from public disclosure. In accordance with 10 CFR 2.390, "Public inspections, exemptions, requests for

4601
NRR

withholding", an affidavit is enclosed identifying the specific portions of the above documents that are proprietary and the basis for making that determination. Proprietary and non-proprietary versions of the response to the request for additional information are provided.

All documents are submitted electronically and in hard copy.

If you have any questions related to this submittal, please contact me at 423-756-9730 extension 12 or by e-mail at mark.j.burzynski@ds-s.com.

Sincerely,

Mark J. Burzynski

Mark J. Burzynski
US I&C Licensing Manager
Rolls-Royce

Rolls-Royce Civil Nuclear US
5959 Shallowford Road, Suite 511
Chattanooga, Tennessee 37421
Tel: (423) 756-9730
www.rolls-royce.com

Affidavit

STATE OF TENNESSEE)

)

COUNTY OF HAMILTON)

1. In accordance with 10 CFR 2.390, "Public inspections, exemptions, requests for withholding", Rolls-Royce requests withholding from public disclosure of the documents listed in Table 1, which is attached to this affidavit.
2. I am familiar with the criteria applied by Rolls-Royce to determine whether certain Rolls-Royce information is proprietary. I am familiar with the policies established by Rolls-Royce to ensure the proper application of these criteria.
3. As required by 10 CFR 2.390, Rolls-Royce has included in Table 1 the following information:
   - Identity of the document or part sought to be withheld;
   - Declaration of the basis for proposing the information be withheld, encompassing considerations set forth in § 2.390(a);
   - Specific statement of the harm that would result if the information sought to be withheld is disclosed to the public; and
   - Locations in the documents of all information sought to be withheld.
4. As required in § 2.390(b)(4); Rolls-Royce wishes to note that the request for withholding from public disclosure applies to pages that contain commercially sensitive information that Rolls-Royce normally discloses only under a Non-Disclosure Agreement (NDA). This commercially sensitive information is not available in public sources and is the type of information customarily held in confidence by Rolls-Royce and our competitors.

5. Rolls-Royce is transmitting this information to NRC in confidence.

6. As noted in Table 1, release of this information in a public forum could cause harm to Rolls-Royce by revealing trade secrets and/or commercially sensitive design and operational details and technical processes related to designing, building, and/or operating a ***SPINLINE 3*** digital safety instrumentation and control system.

7. As Rolls-Royce US I&C Licensing Manager, I have been specifically delegated responsibility for reviewing the information sought to be withheld, and I am authorized to apply for its withholding on behalf of Rolls-Royce.

8. The foregoing statements are true and correct to the best of my knowledge, information, and belief.

Mark J. Burzynski

Mark J. Burzynski
US I&C Licensing Manager
Rolls-Royce

Sworn to and subscribed before me
this 1st day of August, 2012

Notary Public

My commission expires: 9-4-2013

Table 1. Documents requested for withholding from public disclosure

Document Title	Document Number	Part of document sought to be withheld from public disclosure	Basis for proposing the information be withheld, encompassing considerations set forth in § 2.390(a)	Specific statement of the harm that would result if the information sought to be withheld is disclosed to the public	Location(s) in the document of all information sought to be withheld (Notes 1 and 2)
Response To Request For Additional Information - ***SPINLINE 3*** Digital Safety Instrumentation and Control Platform - Project No. 773	N/A	Portions of response, as marked by brackets [[ ]].	Trade secrets and / or commercial information as per § 2.390(a)(4)	Rolls-Royce would be harmed by disclosure of aspects of the identified commercially sensitive information, which is of value to a competitor because it would enable them to make direct comparisons between the design features, equipment qualification processes, and commercial grade dedication methods for their ***SPINLINE 3*** safety I&C platform.	Some or all of the responses to questions 31, 32, 33, 36, 37, 38, 39, 47, 59, 63, 65, and 66 as marked by brackets [[ ]].

Notes:

(1) As required in NRC Information Notice (IN) 2009-07, documents containing proprietary information are marked with the word "Proprietary" at the top of the first page of the document and at the top of each page containing such information. In proprietary documents, brackets ("[[ ]]") denote proprietary information. In the proprietary document, the two brackets denoting the end of a proprietary segment of a report may appear one or more pages following the bracket indicating the start of the proprietary segment. In a nonproprietary edition of a proprietary document, the material within the brackets is removed.

(2) As noted in IN 2009-07, in instances in which a nonproprietary version would be of no value to the public because of the extent of the proprietary information, the agency does not expect a nonproprietary version to be submitted.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION ROLLS-ROYCE ***SPINLINE 3*** DIGITAL SAFETY INSTRUMENTATION AND CONTROL PLATFORM PROJECT NO. 773

The following request for additional information (RAI) questions address regulatory evaluation criteria for the Rolls-Royce ***SPINLINE 3*** Platform Licensing Topical Report (LTR). The topics covered in this set of RAI questions include: follow-up items requesting clarification of earlier RAI responses, Rolls-Royce's configuration management program, and Rolls-Royce's independent verification and validation (V&V) program.

Items for Additional Clarification

By letter dated November 7, 2011, the U.S. Nuclear Regulatory Commission (NRC) staff transmitted a set of RAI questions to Rolls-Royce (Agencywide Documents Access and Management System (ADAMS) Accession No. ML112900190). Rolls-Royce provided responses to these questions in a letter dated December 21, 2011 (ADAMS Accession No. ML12010A066). Based on the information provided, the NRC staff has the following follow-up questions.

RAI-31 (Follow-up question for RAI-1 and RAI-3) - RAI-1 and RAI-3 requested information about data communication from the input/output (I/O) boards to the UC25 N+ central processing unit (CPU) board and back.

The responses provided for these 2 RAI questions illustrate how the data is transferred through the backplane bus (BAP). Also, from the information provided, the NRC staff understands that the BAP is a Master/Slave parallel bus, controlled by the UC25 N+ CPU board, to address the I/O boards. This response states that the BAP uses a "Rolls-Royce proprietary secure protocol."

Further, the response to RAI-3 states: "The address of a given board, in a given position in the rack, is set during the design phase by a hardwired connection of specific pins on the backplane 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 operating system software (OSS) sets the relevant bits of the address bus. A board is then addressed when the bits on the address bus are equivalent to the address wired on the backplane panel."

Based on this information, the NRC staff reviewed additional documents submitted by Rolls-Royce, and found the following:

- Document No. 6 648 805 D describes the parallel bus interface and 68150 as follows: "When the microprocessor wants to access a board, it transmits the address of this board via the address bus and waits for an identifier to be returned. This identifier is part of the address corresponding to the position of the board in the addressable space. The TA signal (authorization to access the data bus) is then positioned by the peripheral component allowing the microprocessor to read the values transmitted by the addressed board on the data bus."

- Document No. 1 207 108 J explains that data acquired by the OSS is 'packed' or 'unpacked', so it can be used by the peripheral and/or application software.

Follow-up question: To support the NRC staff review, please provide the following:

a) A detailed description of data transmission through the BAP, including functions performed by the bus (describe how data is routed through the XF2 connector),

b) A description of how the communication between the CPU and I/O boards is performed through the XF1 connector,

c) A description and development of the proprietary secure protocol used in the BAP, and

d) A description of the 68150 component in the UC25 N+ CPU board.

Rolls-Royce Answer – The following response addresses the collective NRC question for ease of understanding rather than trying to address each subpart separately.

Additional Information about the 19" 6U Chassis

The 19'' 6U chassis includes:

- A metallic frame consisting of riveted and bolted parts, galvanized and chromate passivated, designed for electromagnetic protection and mechanical strength.
- Mounting rails for easy insertion and retrieval during maintenance.
- A backplane which provides two functions: [[

]]

The standard backplane with 21 slots is shown in Figure 1 below.

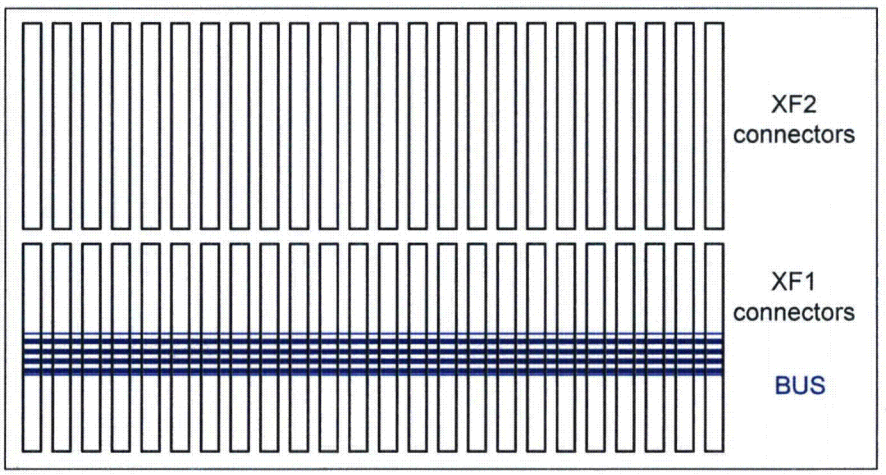

Figure 1: ***SPINLINE 3*** Backplane – Schematic Representation

As a mechanical optimization, applicable for racks which need only few boards, two smaller backplanes are available in a full separate packaging. These smaller backplanes are able to include respectively 10 and 11 slots. These smaller backplanes can be mounted in the same frame but are functionally fully independent. The advantage is to provide less mechanical chassis in a cabinet for some specific projects.

When used in a chassis, the two backplanes can be considered as equivalent to two half chassis, mechanically included in one single frame but built around two independent CPUs (i.e., one for each half rack). Such a configuration is shown in Figure 2 below.

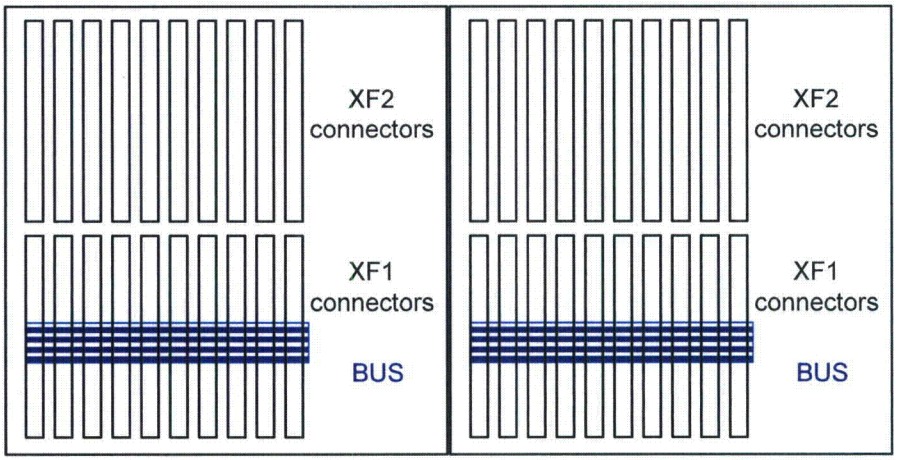

Figure 2: ***SPINLINE 3*** Backplane – Split Bus Configuration

The different power supply voltages are distributed to all the XF2 and XF1 connectors using the same pins for each specific voltage. [[

]]

The upper row connectors (XF2) are only pass-through connectors between the rear side and the front side for the external signals (e.g., inputs from sensors or outputs to actuators or signalization). [[

]]

The lower row connectors (XF1) do not provide any connection between the rear side and the front side. Only the functional front side boards are connected to the Parallel bus.

General Characteristics of the Boards

The main electronics boards are inserted on the front side of the chassis and the complementary boards known as "Interface boards" are inserted on the rear side. The main electronic boards, which are plugged in from the front of the chassis, provide the function (e.g., processing, analog or discrete acquisition, analog and discrete outputs). The Interface boards, which are plugged from the rear of the chassis, provide the connectors from sensors signals or to actuators control. Theses interfaces provide isolation and electrical adaptations between field signals and the main electronic boards. The boards can also support the following functions: protection (i.e., electromagnetic, overvoltage, and short circuit), test input connections, and safety position monitoring. Interface boards do not provide information directly to CPU through the bus. Instead, they are electrically in series between the sensors or actuators and the functional I/O digital boards.

Additional Information Regarding the Parallel Asynchronous Bus (BAP)

As a preliminary clarification, note that "backplane bus" refers to the functional data exchanges between the CPU and the I/O boards and is supported by a physical copper circuit made of parallel lines located on the "backplane panel".

Referring to licensing topical report (LTR) Section 4.3.2.2 and focusing on the parallel communication bus interconnecting the XF1 connectors, the functions of the backplane bus[1] are:
[[

]]

The Backplane Bus is a Master/Slave parallel bus with one Master board (the UC25 N+) and one or several Slave boards. The backplane bus (hardware) is a passive bus that provides interconnection between the processing board and the I/O boards. It was built as the first generation of asynchronous parallel communication bus. The parallel Bus is organized around three types of information: [[

[1] The "backplane bus" refers to the panel (the mechanical support of copper circuit for the power voltage distribution and on the other hand the copper circuit for the parallel communication bus) in the first paragraph of section 4.3.2.2, and to the electronic bus (the function as of a communication bus) in the second paragraph.

]]

One standard system control line is used:
[[

]]

The function of the bus consists of:
[[

]]

The bus data exchanges are shown temporally in Figures 3 and 4 for the read and write cycles, respectively.
[[

]]

Figure 3: ***SPINLINE 3*** BAP Data Exchange Control – Read Cycle

[[

]]

Figure 4: ***SPINLINE 3*** BAP Data Exchange Control – Write Cycle

[[

]]

The mapping of all components and peripherals accessible by the CPU has been predefined during the CPU board design. [[

]]

Example for the 32ETORTI for which the hardwired address on XF2 is "2"

The following information gives the information available at the predefined registers and related addresses (as given in the 32ETOR TI User Manual).
[[

]]

Secure Self-Tested Communication of BAP

The BAP bus interconnects the UC25 N+ CPU board to the different I/O boards. The UC25 N+ CPU board controls the BAP bus with the ***SPINLINE 3*** Operational System Software (OSS). The OSS checks that:

- The UC25 N+ CPU board can communicate with the I/O boards (that the bus address matches the address which is wired in the backplane and
- That any message is transmittable between UC25 N+ CPU board and I/O boards (that the bus data can take both 1 and 0 values on each strand).

The self test of the communication and the correct addressing of the boards is performed as follows. [[

]]

RAI 32 (Follow-up question for RAI-2) - RAI-2 asked Rolls-Royce to identify ***SPINLINE 3*** restrictions on hardware and physical architecture.

The RAI response provided does not clearly identify system restrictions or limitations. From the information provided, the NRC staff understood the following:

- The maximum number of transmitting stations in the NERVIA network is 20.
- A NERVIA+ daughter board can support one to three communication stations per unit.
- Only one UC25 N+ board can be installed in a backplane.
- One UC25 N+ CPU board is used per unit.
- One NERVIA+ daughter board can be mounted on the UC25 N+ CPU board to provide communication stations for the unit.

Based on this information, the NRC staff reviewed additional documents submitted by Rolls-Royce, and found the following:

- Document No. 1 207 108 J, Section 7.2, describes the maximum number of boards that can be run by the OSS.

As part of defining the scope of the LTR safety evaluation, the NRC staff needs to ensure that the limitations of the ***SPINLINE 3*** Platform are well understood and stated to both avoid artificially constraining applications that may be submitted and minimizing the potential for applications to be submitted that significantly exceed staff's generic understanding of how SPINLINE 3 may be configured.

Follow-up question: To support the NRC staff review, please confirm if our understanding of the system constraint is correct. Then, describe in detail the hardware constraints of the ***SPINLINE 3*** Platform (including number of communication stations and transceivers that the NERVIA+ daughter can support), and how this information relates to the information provided in Document No. 1 207 108 J, Section 7.2.

Rolls-Royce Answer – The NRC understanding of the system design constraints is partially correct. These parameters reflect two fundamental aspects of the ***SPINLINE 3*** system: one and only one processor can be installed on a backplane and that the [[
]] LTR Section 4.5.3 states that [[
]] can be supported. The other constraint regarding the NERVIA+ daughter board reflects the physical realities of the two boards: [[

]]

Rolls-Royce Document 1 207 108 J (Section 7.2) describes other hardware design constraints that must be considered in the design of a ***SPINLINE 3*** system, based on the following factors:

- maximum number of boards in a rack based on module size (i.e., pitch),
- load on Parallel Access Bus (i.e., Backplane Bus or BAP),
- heat dissipation, and
- power consumption.

---

[2] Note that this is a clarification of the information provided in the response to RAI 1.

The limitations on the number of module of each type that can be installed in a ***SPINLINE 3*** cabinet or on a NERVIA+ network is shown in Table 1 of Rolls-Royce Document 1 207 108 J. The design constraints for the ***SPINLINE 3*** chassis mounted boards within the scope of the LTR are as follows:
[[

]]

It should be noted that the ALIM 48V/5V-24V power supply board is not listed in Rolls-Royce Document 1 207 108 J (Section 7.2), since it set the constraints on power supply for a cabinet.
[[ ]]

The 8PT100 RTD conditioning board is not listed in Rolls-Royce Document 1 207 108 J (Section 7.2), since these boards are not connected to the BAP bus. As such, the boards are not discussed in the document in the context of configuration limitations of the Core System Software.

RAI-33 (Follow-up question for RAI-5) - Section 4.3 of the LTR states that the following components include electronic subcomponents, such as field programmable gate arrays (FPGAs), to process data. RAI-5 asked Rolls-Royce to provide detailed information on how these components were configured, how they operate, and how they will be dedicated for use in an Appendix B program.

The RAI response identifies descriptions provided in the LTR for FPGA and complex programmable logic device (CPLD) based components. Further, this response identifies development documents, as well as configuration management procedures used for the design and testing of these modules. The information provided in this response only referenced the procedure's names, so the NRC staff cannot evaluate how these procedures were established and used. Further, the NRC staff cannot evaluate the design and test program followed for these modules, and thus their robustness to be used in safety application.

Follow-up question: To support the NRC staff review, provide a detailed description on the design, testing, configuration management, communication with the BAP, operation, and dedication of these modules.

Rolls-Royce Answer – The response addresses the NRC question regarding additional clarification regarding the design, testing, and configuration management procedures used for the firmware development process.

Design and Testing

The design and testing processes for electronic boards with programmable components (i.e., FPGA or CPLD) are shown in Figures Q5-1 and Q5-2, which come from Rolls-Royce Procedure 8 303 687 A, Design Process for Programmable Components. This version was used for the original development of these boards.

The four phases (gray boxes) depicted on the left hand side of Figure Q5-1 are the four phases described in Rolls-Royce Procedure 8 303 349, Definition of the Electronic Design Process. See the response to RAI-6 for a description of this procedure.

The specific firmware development process steps are shown in the white box in Figure Q5-1 and in more detail in Q5-2.

Specification Phase

[[

]]

Design Phase

[[

]]

Test Definition Phase

[[

]]

Coding Phase

[[

]]

Simulation Phase

[[

]]

Synthesis, Placement and Routing Phase

[[

]]

In Situ Measurement and Testing

[[

]]

The archiving phase is used to save the data necessary to ensure the maintenance and sustainability of the component.

Configuration Management

Rolls-Royce Procedure 8 303 221 is used to ensure material is identified and marked in order to provide an unambiguous link with its specifications and allow control of production. It is also used to enable a technical analysis to be performed following the failure of an item which could impact the safety of a 1E function or have major quality implications, by:

- locating the item responsible for the failure and
- collecting any information useful to the analysis of the failure from tracing operations performed on the material, from quality documents associated with the manufacture and inspection of the material or from any other quality tracking document generated in the course of these operations.

Programmable components are identified by a number (set of alphanumeric characters), plus a version index (1 or 2 letters). The different ID elements are indicated on the a label affixed to the component. All markings are permanent, legible and applied in a way which does not impair the material's mechanical strength, protective surface treatment or functionality. Markings on the same component are always made in the same place.

Rolls-Royce Procedure 8 303 436 is used to specify the configuration management for a standard programmed component: revision level of the electronic board and revision level of the programmable device and firmware. For electronic boards with embedded software, the software configuration is managed through the software configuration management process (see LTR Section 6.2.6).

Rolls-Royce Procedure 8 303 711 is used for configuration management of the different deliverables (e.g., documents and schematics) during the design of a board. An open index is a provisional index used during the design phase. It is composed of a letter and a digit. The process works as follows:

- An index is open to the first amendment (e.g., A = > B1) for a new revision to a design. Multiple changes can be taken into account in this index over the evolution of the design. These changes are accumulated in the design folder.
- An open index is frozen as soon as all or part of the record is communicated to the outside. This ensures the traceability of the released material (index and content). When an open index is frozen, the records manager keeps a copy of all the elements of the record to the affected index.
- An open index can increment (e.g., B1 = > B2) when additional changes are made to a prototype.
- At the end of the industrialization phase and open index is closed (e.g., B1 = > B) and is composed of a single letter.

Rolls-Royce Procedure 8 303 675 defines the documentation that is required to be produced during each phase of the component development process.

RAI-34 (Follow-up question for RAI-5) - Please describe the process Rolls-Royce follows to perform modifications of modules containing electronic subcomponents (e.g., FPGAs, CPLDs), that have been previously commercial grade dedicated.

Rolls-Royce Answer – As described in the LTR Section 1.4.1, 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." Modification to the modules containing electronic subcomponents that have been previously commercial grade dedicated will be made using the current set of design procedures for electronic components. For example, Procedure 8 303 687 G, Design Process for Programmable Components, would be used for such modifications today. This version of the procedure was reviewed by NRC during the June 11-15, 2012 audit in Grenoble France.

RAI-35 (Follow-up question for RAI-6) - RAI-6 asked Rolls-Royce to describe the hardware development process followed for the ***SPINLINE 3*** Platform. The response provided identified Procedure Nos. 8 303 314 L, "Project Execution Definition," and 8 303 334 F, "Project Development Process (System Design)," as the documents defining the design process used for ***SPINLINE 3***. Copies of these procedures were provided in the attachments.

Follow-up question: After reviewing these procedures, the NRC staff has the following questions:

a) Section 4 of Procedure No. 8 303 314 identifies that for design engineering, Rolls-Royce would use the system design described in Procedure No. 8 303 334. However, it is not clear how these two procedures work together, since Procedure No. 8 303 334 describes the design process from the specification requirements until system acceptance by the client, which seems to overlap with the process described in Procedure No. 8 303 314. Please clarify how these documents are used and how they are cross referenced during the hardware development process.

b) Procedure No. 8 303 334 does not clarify what the design process would be used for existing modules that need to be updated or modified.

c) The response provided in the RAI states that "additional design process associated with firmware development is described in the response to RAI-5." As mentioned above, Rolls-Royce is asked to submit additional information for the NRC staff to evaluate the design process followed.

d) The response provided in the RAI identified that Procedure No. 8 307 032, "Principle for Control of Design (Safety System)," was submitted with the RAI response. However, this procedure was not included in the attachments of this RAI response. Please provide Procedure No. 8 307 032.

Rolls-Royce Answer to Part a – Rolls-Royce Procedure 8 303 314 defines a generic process to be used to fulfill contracts. This procedure describes the organizational structure and the basic principles applicable to the project execution process. The procedure outlines the management expectations for the project lifecycle phases and the formal project review meetings, which are shown on the top two lines of Figure Q6-1, ***SPINLINE 3*** Technology Development Process (taken from 8 303 314).

The procedure also specifies the set of subordinate procedures that are applied to project execution process. The procedures associated with the key sub-processes are noted on Figure Q6-1. Rolls-Royce Procedure 8 303 314 is one of them.

Rolls-Royce Answer to Part b - Rolls-Royce Procedure 8 303 314 specifies two procedures that are used to support the design (or modification) of electronic modules:

- Rolls-Royce Procedure 8 303 603, Equipment Design Process
- Rolls-Royce Procedure 8 303 349, Definition of the Electronic Design Process

Rolls-Royce Procedure 8 303 603 describes the stages involved in the design and manufacturing of equipment on projects and the sequence in which they are performed. It is a sub-process of the Project Execution Process (Procedure 8 303 314). It is designed to achieve the objectives of the Project Execution Process in terms of quality, completion times and design and realization costs. It describes the organizational structure and the basic principles applicable to the design of equipment meeting system specifications which is to be

manufactured and inspected for subsequent installation on site. Each item of equipment is designed by a multi-disciplinary group headed by an equipment design analyst who leads the team and is responsible for attaining the objectives associated with the design and manufacturing of the equipment. The Equipment Design Process consists of five phases: Analysis, Specification, Manufacturing, Qualification, and Site. The Analysis Phase involves planning, costing, and alignment with the System Requirements Specification. The Specification Phase involves defining equipment specifications, describing principles of operation, and detailing electrical functions. The Manufacturing Phase involves define equipment hardware structure, preparing mechanical drawings for racks and cabinets, and preparing equipment manufacturing files. The Qualification Phase includes preparation of the qualification test documents and design review to validate qualification documents. The Site (or Industrialization) Phase includes preparation of installation and packing instructions and archiving of equipment manufacturing files.

Rolls-Royce Procedure 8 303 349 describes the various stages of all design and design-related activities for an electronic circuit board. The process is iterative: in the event that goals are not met at the end of a phase or an activity, the process returns to an earlier stage. The design of each board is carried out by a cross-functional team with a development manager in charge who leads the participants and is responsible for the goals being reached. The Equipment Design Process consists of four phases: Specification, Definition, Qualification, and Industrialization. The Specification Phase (or Define the Specifications step) involves preliminary studies and preparing the specification. The Definition Phase (or Define the Board step) involves drawing the circuit diagrams (with simulation, as necessary), approve the component choices, devise the board testability, analyzing electromagnetic compatibility, perform safety studies, supply the components, design the printed circuit board, design the fittings, and provide the assembled printed circuit board. The Qualification Phase (or Qualify the Board step) involves defining the test methods, developing prototypes, designing the program and the test report, validating the prototype, and conducting the environmental qualification test. The Industrialization Phase (or Implement Large-Scale Production step) involves finalizing the industrial diagram, designing manufacturing methods, creating industrial files, manufacturing first batch test, incorporating improvements (as needed), and archiving final records.[3]

The contractual projects are managed through the Project Execution Process which is described in Rolls-Royce Procedure 8 303 314. The modules would be updated or modified through a different process which is called the New Offer Creation Process, described in Rolls-Royce Procedure 8 303 693. This process is used for any R&D project.

If, during the course of the execution of a contractual project, there is a need to update or to modify a module, then a change request is issued by the project; this change request will be managed through the New Offer Creation Process.

The Change Management Process (Rolls-Royce Procedure 8 303 197) ensures coordination between the R&D projects and the contractual projects, in order to guarantee that modifications and updates are taken into account by contractual projects and by including an impacts analysis.

The Rolls-Royce Procedure 8 303 314 procedure, section 1.2 shows the relationship between the Project Execution Process (PRA) and the New Offer Creation Process (PCO)

---

[3] The language used to describe the process used the phase names in earlier versions of the procedure and the step names in later versions.

The need for a new module, or any new electronic device would also be managed through the New Offer Creation Process (PCO), as described in section 10 of Rolls-Royce Procedure 8 303 334.

Rolls-Royce Answer to Part c - See response to RAI-5 above.

Rolls-Royce Answer to Part d - A copy of the procedure was provided in Rolls-Royce letter dated March 14, 2012.

RAI-36 (Follow-up question for RAI-7) - LTR Section 4.3.4.4 states the accuracy and the response time of the ICTO board can be adjusted according to the needs. RAI-7 asked Rolls-Royce to explain how these can be adjusted and how these will be evaluated and decided for a plant-specific application.

The NRC staff reviewed the response provided for this answer, in particular the description provided in the third paragraph on how these parameters are defined and adjusted. Further, the NRC staff reviewed Document No. 1 479 513 C to understand how the ICTO board works. This document states: "The ICTO board and the associated I.ICTO interface board comprise two separate identical channels, each forming the interface between the acquisition system and the processing unit. Each channel has two operating modes which are handled automatically by the hardware."

Follow-up question: To support the NRC staff review, respond to the following requests.

a) Please describe in detail how the ICTO parameters are configured in the software embedded in the ICTO microcontroller.

b) Please explain, when the ICTO board is in operation, how these parameters are transferred from the ICTO channels to the acquisition system and the processing unit. This description should include how the data is exchanged through the 16 kB shared memory of the BAP.

Rolls-Royce Answer to Part a – [[

]] (refer to the figure included in our previous answer to RAI7 and extracted from the System Specification 3 006 404 E). [[

]] During the initialization phase of the CPU rack (described in document 1 207 108 J, section 5.2), the intelligent peripherals, such as the ICTO board are initialized. This process is described in section 5.2.2 of document 1 207 108 J:

> The parameters supplies by the 68040 µp during the initialization process are:
> - values for defining the microcontroller's operating functions,
> - initial variable values for handling the communication protocol during the normal operation phase.

The values for defining the microcontrollers operating functions include parameters like the ones of the ICTO board.

Rolls-Royce Answer to Part b - The parameters are [[

]]

RAI-37 (Follow-up question for RAI-8) - RAI-8 requested information about the Local Display Unit (LDU) and the Operator Panel. Specifically, the NRC staff is requesting clarification about units that can interface with the system. Section 4 of the LTR identifies the following units as those that can interface with the system:

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

Follow-up question: To support the NRC staff review, please respond to the following requests.

a) Please identify the interface unit that Rolls-Royce is asking the NRC to review and approve.

b) Please identify for each interface unit whether it is safety (1E) or non-safety related (non-1E).

c) The description provided about communication between UC25 N+ and LDU states this is an asynchronous link, only used during maintenance. Please provide additional information about this communication and how it meets the requirements of Interim Staff Guidance 4. Specifically the protocol used to communicate parameters changed to the ***SPINLINE 3*** Operating System.

d) In the RAI response, Rolls-Royce explained that when the LDU is not connected, the interface function is idle. What measures does Rolls-Royce impose to restrict access to the front panel RJ45 connector when the LDU is not connected?

e) Regarding the Operator Panel, in the RAI response it seems that the information can be related to the information provided for the ATU in LTR Section 4.6.9 or to the MMU in LTR Section 4.6.10. Please clarify if the Operator Panel is the ATU and/or the MMU. If not, please clarify the description provided in the RAI and to what interface it belongs.

f) Please provide a clear description of the ATU and MMU. In particular, describe how the ***SPINLINE 3*** platform communicates with these interfaces. Also, clarify if either interface will be qualified during the qualification of the ***SPINLINE 3*** platform.

Rolls-Royce Answer to Part a - Rolls-Royce is asking for the approval of the ***SPINLINE 3*** safety platform with the following understanding of standard interfaces:

- The LDU is periodically connected to the ***SPINLINE 3*** safety processors to support parameter changes as described in LTR Sections 4.4.3.5.5 and 4.4.4.3 and the response to RAI 8.
- The Operator Panel is the ***SPINLINE 3*** platform human interface feature used to support periodic testing and local maintenance activities. The Operator Panel provides the plant maintenance staff with the necessary connectors, lamps, and pushbuttons to support local monitoring and control for the output inhibition function. The Operator Panel is not used during normal operation of the ***SPINLINE 3*** equipment. The Operator Panel is a plant-specific and is customized to match cabinet contents and meet customer requirements. The Operator Panel is designed and manufactured using typical components qualified for 1E applications.
- The ATU is periodically connected to the ***SPINLINE 3*** safety processors to support periodic testing and maintenance activities as described in LTR Section 4.6.9 and the response to RAI 8.

- The MMU is permanently connected to the ***SPINLINE 3*** network to support periodic testing and maintenance activities as described in LTR Section 4.6.10 and the response to RAI 23.

Rolls-Royce believes that these interfaces fall within the scope of the NRC review; however, the non-1E functionality of these devices is not within the scope of NRC review.

Rolls-Royce Answer to Part b - The interface subsystems have the following safety classifications:

- The LDU is a non-1E device as noted in LTR Table 3.8-1 line item 5.4.2.
- The Operator Panel is designed and manufactured as a 1E device. As noted in the response to RAI 30, the operator interface functions performed by the operator panel are not safety functions.
- The ATU is a non-1E device as noted in LTR Section 4.6.9.
- The MMU is a non-1E device as noted in LTR Section 4.6.10.

Rolls-Royce Answer to Part c - The interface subsystems comply with ISG-4 in the following manner:

- The Local Display Unit (LDU) meets criterion 1.10, as noted in LTR Table 3.7-1. The Local Display Unit provides a means of interacting with the UC25 N+ processor via a Human-Machine Interface to display selected values and change selected parameters.
- The Operator Panel is not covered by ISG-4 criterion 3.1, since the guidance does not apply to conventional hardwired control and indicating devices.
- The ATU is not covered by ISG-4, since it is not permanently connected to the ***SPINLINE 3*** safety system and does not alter the safety processor.
- The MMU meets criteria 1.3 and 1.8, as noted in LTR Table 3.7-1.

Within the Operational System Software (OSS), the Core System Software (CSS) uses the LDU driver program[4] for dialogue with the LDU. The purpose of the CD_LDU program is to provide the interface between the LDU and the CSS. [[

[4] The LDU driver program is referred to by the acronym LDU CPU in the LTR and the software module name CD_LDU in the development documents.

]]

The LDU is described in more detail in LTR Sections 4.1.3, 4.3.4.7, 4.4.2, 4.4.3.2, 4.4.3.4, 4.4.3.5, 4.4.3.5.1, 4.4.3.5.5, 4.4.4.3, and 4.6.3. The development of the CD_LDU software is described in LTR Sections 6.2 and 6.3.

The CSS and CD_LDU interface is described in more detail in Rolls-Royce Document 1 207 108 J, ***SPINLINE 3*** / *OSS / Software Requirement Specification*, in Sections 2.1.3, 2.3, 2.5.2, 5.2.1, 5.2.7, 5.3.1, 5.3.4, 5.9, and 5.10.

Rolls-Royce Answer to Part d - The LDU interface is located inside the cabinet housing the ***SPINLINE 3*** safety equipment. Access is controlled as described in LTR Table 3.8-2 item 5.9 and Section 3 of Rolls-Royce document 3 013 962 A, ***SPINLINE 3*** *Secure Development and Operational Environment.* The generic platform includes hardware contacts for open door detection. It provides a signal to enable an alarm and remote indication in case of open door.

Rolls-Royce Answer to Part e - The Operator Panel is a permanent hardware feature located in the ***SPINLINE 3*** equipment cabinets. It is system and application specific. It is typically used for local order or display of inhibition, inhibition locking, and tester connection signaling. It is not the ATU nor is it the MMU. The ATU is a test device that is temporarily connected to the ***SPINLINE 3*** system to perform periodic testing. The ATU plugs into the Operator Panel to perform periodic testing. The MMU is permanently connected to the ***SPINLINE 3*** network, as described in LTR Section 4.5.7 and is used to monitor test state status for testing performed by the ATU. The MMU does not connect Operator Panel or the ATU.

Rolls-Royce Answer to Part f - The ATU is described in LTR Section 4.6.9. The ATU generates input signals with generators, analog or discrete outputs for simulating and testing the units receiving signals from sensors. These signals are input via the Operator Panel interface. For the units receiving their input data on networks, the ATUs are [[

]]

The MMU is described in LTR Section 4.6.10. The MMU communicates with a NERVIA+ network through a PCI NERVIA+ board installed in the MMU through an gateway interface described in LTR Section 4.5.7 using the NERVIA communication protocol described in LTR Section 4.5.

The UC25 N+ safety processor communicates with the LDU through the LDU driver (LDU CPU), which is described in several places throughout LTR Section 4. The LDU driver software is part of the Class 1E Operational System Software, which was developed using the development lifecycle process described in LTR Section 6.2.

None of the interfaces are qualified during the testing.

RAI-38 (Follow question for RAI-14) - RAI-14 asked Rolls-Royce to define the cycle time for the test specimen application program to be run in the Qualification Test Specimen.

The response provided information about the cycle time and CPU load for the Qualification test Specimen. Based on the information, the NRC staff reviewed information provided in the LTR, as well as other documents submitted to the NRC. Of particular interest is the information provided about the OSS in the LTR. In particular, LTR Section 4.4.3.1 explained that the OSS and the application software are the executable code in the system. Further, this code is executed sequentially, periodically and deterministically. The NRC staff understands that the cycle time for the ***SPINLINE 3*** Platform would depend on the application for a plant-specific project.

Follow-up question: To support the NRC staff review, respond to the following requests.

a) Describe the relationship between CPU speed and code execution.

b) Since the OSS does not change for a plant-specific project, the OSS will have support for I/O modules not installed in the system. Please explain how these functions will affect the speed of the CPU and code execution to guarantee full use of the CPU.

c) LTR Sections 4.4.3.2 and 4.4.3.5.3 state that the cycle time management maintains the fixed cycle time, which is checked at each cycle. Document No. 1 207 110 J, "Interface Specifications," Section 3.2.1, describes the variables that the OSS uses to set the cycle time. However this document does not describe how this is done, only where this information is stored for the cycle time management. Then Section 3.4 of Document No. 1 207 110 J lists a variable to indicate if the cycle time is monitored or regulated. How is the pre-defined cycle time specified, monitored, and regulated?

d) Does the number of procedures and/or functions used by the application software change the size of the OSS code?

Rolls-Royce Answer to Part a - The speed of the CPU is not modified to always run at 100%. The ***SPINLINE 3*** Operational System Software (OSS) and Application Software operates sequentially in a continuous loop after initialization without the use of interrupts or multi-tasking, as described in LTR Section 4.4.3.2. [[

]]

Rolls-Royce Answer to Part b - The complete set of I/O board drivers for the ***SPINLINE 3*** I/O modules are contained in the Basic Functions (BF) part of the OSS. [[

]] The Application Software portion of the software embedded on the UC25 N+ processor calls the data stored by the OSS

from the specific I/O configuration of the plant-specific system. [[

]]

Rolls-Royce Answer to Part c - The cycle time is specified during the design phase according to the overall customer requirement and the optimal distribution over the units constituting the global architecture. [[

]] The effective execution time of the software (within the allocated cycle time) is verified and validated during the test and validation phase.

[[

]]

Rolls-Royce Answer to Part d - No. The OSS size and content is fixed. Only the size of the Application Software changes for each system design.

RAI-39 (Follow-up question for RAI-28) - RAI-28 requested clarification on how valid/invalid data will be treated and recorded by the data acquisition system (DAS) during environmental qualification testing.

The response provided in this question identified these possible treatments on data transferred in the NERVIA network:

- Nominal treatment
- Not nominal conditions and expected behaviors

According to the information provided in this response, during each cycle TSAP1 uses a signed 32 bit counter to transfer data to TSAP2 and DAS. A 32 signed bit counter is also used when data is being sent to TSAP1. Also, when data is exchanged from TSAP1 and TSAP2, a global validity indicator is used to indicate if the data is valid or not. Then the response explains how data is treated during not nominal conditions and expected behaviors. This section does not explain when such treatment is used or even what triggers such treatment. Further this section uses terms (e.g., TSAP1 counter) that are not clearly related to the previous validity management scheme. Because of the unclear information provided, the NRC staff reviewed additional documents to understand how data will be treated and transferred on the NERVIA networks.

LTR Section 4.5.2 indicates that invalid or corrupt data are processed by receiving stations until a valid message is received. LTR Section 4.5.4.2 states that erroneous data is flagged as invalid and handled in accordance with the engineering fault management, which is built into the application software. Then Section 4.5.5.2 states that if there is an error the data is invalidated by the receiving unit OSS, and the application software processes the data as invalid.

LTR Section 4.5.6 states: "The refreshment indicator is incremented by the emitting Unit each time it transmits the CB [consistency block]. The receiving Unit checks that the refreshment indicator has been updated. This ensures that the information available in the CB has been refreshed by the emitting unit since its last processing by the receiving unit."

Document No. 1 207 108 J, "OSS Software Requirement Specification," Section 4.2, describes the 'validite_associe' flag used to identify valid/invalid data transferred on the NERVIA network. So when data is invalid, this flag is set to invalid. Then LTR Section 5.8.48 states that a validity indicator needs to be associated with each CB.

Thus it is not clear if the referenced documents are referring to the same validity management scheme described in your response, or whether the terms used are related.

Follow up question: To support the NRC staff review, respond to the following requests.

a) Explain what "not nominal conditions and expected behaviors" are and when and how they occur.

b) Provide detailed explanation on how data will be treated and transferred on the NERVIA network, using the terminology provided in the LTR and other Rolls-Royce documents, and cross reference with the treatments described in the RAI response, since a clear connection could not be made. For example, it is not clear if the global indicator described in the RAI response is the same validity indicator described in Document No. 1 207 108 J (i.e., 'validite_associe' flag).

c) Describe the variables associated with data transmission and validity that are described in the LTR and Document No. 1 207 108 J.

Rolls-Royce Answer to Part a - The terms "not nominal conditions and expected behaviors" are used in a generic way in the Software Requirements Specifications, in order to describe the software behavior in all situations in a deterministic way. Said another way, the method of handling valid data (expected condition) and invalid data (not nominal condition). In the TSAP1 case, the software defines the behavior for when the TSAP1 counter reaches its maximum value or if the counter value it receives from TSAP2 is invalid. These are not pre-determined behaviors and need to be defined and set in the application software.

Rolls-Royce Answer to Part b - The answer provided by RR for RAI 28 contained several descriptions:
[[

]]

Regarding our answer to RAI 28, the following answer should be corrected, in order to be less ambiguous:
[[

]]

Rolls-Royce Answer to Part c – The following variables are explained:
[[

]]

RAIs regarding Rolls-Royce SPINLINE 3 Configuration Management

The following questions relate to the Rolls-Royce Software Configuration Management Plan (SCMP).

RAI-40 - SCMP Section 2.7.1, "Archival of the environment managed by the configuration management tool," reads: "An archive baseline contains every version of every managed element regardless of its state. The archival method is described in [Train_CMtool]. The archive baseline is archived according to the rules set out in [Rules_IT]."

a) Please explain what it's meant by the term "state". Also, clarify if this term is related to whether an element has been "checked out" or "checked in."

b) Please state if you have submitted documents [Train_CMtool] and [Rules_IT] for NRC staff review. If you have submitted them, please provide the date of the letter.

Rolls-Royce Answer to Part a –Each configuration item has a life cycle defined in the configuration Management Tool (Dimensions CM), as defined in Section 2.2 of Rolls-Royce document 1 208 878 E. 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.).

Rolls-Royce Answer to Part b – Neither of these documents have been submitted to NRC. Both documents were made available to NRC during the audit held on June 11-15, 2012. Rules_IT is Rolls-Royce Instruction 1 204 971. Train_CMtool is a presentation package used for internal training.

RAI-41 - SCMP Section 2.5, "The various levels of checks," reads: "All the intermediate states of items are managed in configuration, whatever their life cycle."

This sentence is unclear and does not describe the checks perform at different levels. Please provide a better description of what is meant by this statement.

Rolls-Royce Answer – All versions of configuration items (i.e., document or source code) are managed in the configuration management tool (Dimensions CM), whether they are in progress, for verification, or for testing. The different life cycles are described in the Section 2.2 of Rolls-Royce document 1 208 878 E.

RAI-42 - The terms "classified software," "safety classified software," "standard software," and "not classified" are used in Sections 2.6.2 and 2.4 of the SCMP. Please explain what is meant by these terms.

Rolls-Royce Answer – "Safety classified software" means the same thing as "classified software"; which is Class 1E or safety-related software in US terminology. "Not classified" means the same thing as "non-safety software" in US terminology. "Standard software", as used in Section 2.6 of Rolls-Royce document 1 208 878 E refers to "not classified" software (or "non safety software").

RAI-43 - SCMP Section 2.8, "Change Management," reads: "Change management is carried out in accordance with the standard procedures outside of the CM [configuration management] tool and is not affected by the implementation of the CM tool. Only traceability elements are added to the CM tool so as to ensure links with these standard procedures."

Please explain what these "standard procedures" are and what document contains them. If the document that contains these standard procedures has been submitted for staff review, please provide the date of the letter.

Rolls-Royce Answer – The change control process is described in Section 7.3 of Rolls-Royce document 1 207 875 G. This document was submitted to NRC on December 23, 2010.

There are two types of change requests:

- Change Requests as such, 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.

The following tools are used to manage change requests:

- 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 – Non-conformities*.
- Dimensions CM: tool specific to the Rolls-Royce Software group used for change management (including change request management and software configuration management).

Rolls-Royce documents 8 303 197 and 8 303 202 were made available to NRC during the audit held on June 11-15, 2012.

The following questions relate to the Rolls-Royce CM tool.

RAI-44 - Please state if the CM tool is running on one computer, or on a server. If the CM tool is running on a server, please explain what the process is for using the tool from multiple computers simultaneously.

Rolls-Royce Answer – The CM tool (Dimensions CM) is running on a server. One of its purposes is to manage the different access to the items. When a document or safety software source file is checked-out, the file is locked and no one else can check-out the file. When the parallel check out is allowed (i.e., non-safety software source files), the tool gives an alert at the check-in when the item has been checked-out by different users. A merge can be performed by the integrator with a merge tool provided by Dimensions CM.

RAI-45 - Please give details regarding what the operating system is for the computer(s) that runs the CM tool (e.g., Windows, Linux, UNIX).

Rolls-Royce Answer – The Dimensions CM server runs on Windows. The users use the Desktop client, which also runs on Windows.

RAI-46 - Please explain if the Work Area used to modify items is located on a local or shared drive.

Rolls-Royce Answer – The work area could be located on a local or a shared drive. The choice made by the users. If they choose to use the local drive, they have to check-in in Dimensions every day.

RAI-47 - Please state if the computer(s) that runs the CM tool is/are connected to the internet. If they are not intended to be connected to the internet, please explain what measures are taken to prevent a connection, if any.

Rolls-Royce Answer – [[

]]

RAI-48 – Please explain who has authorization to access the CM tool and how the CM tool is protected from unauthorized access.

Rolls-Royce Answer – In Dimensions CM, each project is managed in a specific Product environment. Only project team members have access to a product. The access is given by the Software Methods and Means Manager, after they have received project-specific configuration management training.

RAI-49 - Please explain how the change control process prevents unauthorized changes to the software.

Rolls-Royce Answer – The software used by the Verification and Validation (V&V) team for the validation is a reference version in Dimensions, locked by a baseline in the tool. The configuration items cannot be deleted nor modified when they are in a baseline.

The executables are available for production in a repository named "Archirep" available on the company network.

This repository is managed by the Information Technology (IT) group. 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 executables in the Archirep repository. When the files are available, the V&V team verifies with the checksum the integrity and conformity of the executables they have validated.

The manufacturing team uses the executables in Archirep for programming the components being delivered.

RAI-50 - Please explain if Streams or Projects are used when managing files with the CM tool. Please explain if there is a Rolls-Royce document that provides instructions as to what method to use to manage files.

Rolls-Royce Answer – Only Projects are used for classified (i.e., safety-related) software. The streams are used for non-classified (i.e., non-safety related) software if more than one developer works on the development for the same software. A Guide for the use of streams is currently being written (reference Rolls-Royce document number 3 018 219) but has not been issued yet.

RAI-51 - Please explain if files developed and controlled with the CM tool can be modified in parallel (i.e., two or more people can check the same file out and work on it separately). If so, please explain what controls the CM tool uses to manage the process of checking the file back in.

Rolls-Royce Answer – Parallel check-out is not allowed in the CM tool for the documents or for the safety software source files. When the parallel check out is allowed (i.e., non-safety software source files), the tool gives an alert at the check-in when the item has been checked-out by different users. A merge can be performed by the integrator with a merge tool provided by Dimensions CM.

RAI-52 - Please explain how the 'Request' feature of the CM tool is used to authorize and control changes.

Rolls-Royce Answer – The requests in CM Tool have a life cycle with different statuses: to be analyzed, to be done, differed, rejected, closed. A request is taken into account when it is in the status "to be done". This status is given by the Software Project Leader, with the agreement of the project leader, if needed.

RAI-53 - Please explain what type of 'Client' is used to run the CM tool (i.e., Desktop, Web, Windows Explorer Integration, or Command Line).

Rolls-Royce Answer – The CM tool used by the software team is the Desktop. The web client is only used by users who are external to the software team and only for managing requests or for viewing documents.

The following questions relate to the Rolls-Royce CM Process [SI_Conf_Mngt].

RAI-54 - The CM Process [SI_Conf_Mngt] lists GEVOL and ORIENT as system change and non- conformity management tools used throughout the company, whereas Dimensions CM is the change management tool specific for the software group.

a) Please state if there is a situation or event in the software development and/or CM processes that requires the use of GEVOL or ORIENT. Please explain if in such an event, the same change is also tracked independently with the Dimensions CM tool.

b) Please explain if and how the GEVOL and ORIENT tools interact or exchange information with the Dimensions CM tool.

c) Please state if the Dimensions CM tool shares the same work area as GEVOL and ORIENT.

d) Please state if any of the files controlled by the Dimensions CM tool is also controlled by GEVOL or ORIENT.

Rolls-Royce Answer to Part a - GEVOL and Orient tools are tools used at the company level. These tools are used for requests coming from outside the software team or for requests which have an effect on the software used by the manufacturing in order to inform them of the change. A request is then systematically created in Dimensions CM, and it references the GEVOL or Orient number.

Rolls-Royce Answer to Part b - There is no link between either GEVOL or Orient and Dimensions CM. The Dimensions CM request references the GEVOL or Orient number.

Rolls-Royce Answer to Part c - GEVOL and Orient are only change requests tools. There is no Work area for these tools.

Rolls-Royce Answer to Part d – None of the files controlled by the Dimensions CM tool are controlled by GEVOL or ORIENT, since these tools do not have work areas..

RAI-55 - The CM Process [SI_Conf_Mngt], Section 7.3.1, "Record", reads: "Records are recorded in: ... in Dimensions CM in accordance with the procedure indicated in [SI_GD_NC]."

Please explain if [SI_GD_NC] has been submitted for NRC staff review. If it has been submitted for NRC staff review, please provide the date of the letter.

Rolls-Royce Answer – Rolls-Royce document 1 207 870, *Documentation Guide: Non-conformity Report*, has not been submitted to NRC. This document was made available to NRC during the audit held on June 11-15, 2012.

RAI-56 - Please explain how the List of Tools and Libraries used for Software Development and List of Software Documents are used with the CM tool for tracking purposes (i.e., are these lists accessed/edited from the CM tool?).

Rolls-Royce Answer – The LTLUS and LSD are word documents managed in Dimensions CM. The LSD is created with a list extracted from Dimensions. This list is modified and integrated in the word document.

RAI-57 - Please provide a description of your corrective action program and how it is applied in the CM and software development processes.

Rolls-Royce Answer – When a non conformity is identified on 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.

RAI-58 - Please explain if any documents controlled in CM are maintained in hard copy. If so, please explain how access to these documents is controlled and how is the change management process applied to them.

Rolls-Royce Answer – Rolls-Royce Procedure 8 303 320, *Control of Records,* defines the requirements for the control of records, including hard copy records. The types of documents listed in this procedure are:

- Technical documents, including qualification reports, as specified in the procedure for drafting and applying technical documents, as defined in Rolls-Royce document 8 303 198, *Establishment and Application of Engineering Documents.*
- Quality management system documents,
- Inspection log-books of classified procured item for Transmitters and Probes,
- End of manufacturing reports,
- Site job reports,
- Documents originated from outside the company relating to outsourced design and/or the provision of a service associated with the product specifications. They are considered as part of the technical documents category and comply with the procedure for establishment and application of engineering documents, as defined in Rolls-Royce document 8 303 198.

Documents subject to this archiving method are held in appropriate locations with controlled access (hard copy of the most recent revision index applicable). These documents are microfilmed each time they are amended.

Any person writing or issuing a document which has to be recorded is responsible for recording the document according to this procedure.

RAIs regarding Rolls-Royce *SPINLINE 3* Independent Verification and Validation

Section 3.3.12 of the Rolls-Royce ***SPINLINE 3*** Platform LTR does not make an explicit commitment to comply with Regulatory Guide (RG) 1.168 or Institute of Electrical and Electronic Engineers (IEEE) Standard (Std.) 1012-1998 for future development or enhancements to the ***SPINLINE 3*** platform. As an alternate approach, Rolls-Royce states that the ***SPINLINE 3*** verification and validation (V&V) process was established in accordance with International Electrotechnical Commission (IEC) 880-1986. In order for the NRC staff to establish that Rolls-Royce's approach provides for V&V equivalent to NRC regulatory positions and endorsed standards, the following additional information is requested.

RAI-59 - RG 1.168, Section C.1, states "Software used in nuclear power plant safety systems should be assigned integrity level 4 or equivalent, as demonstrated by a mapping between the applicant or licensee approach and integrity level 4 as defined in IEEE Std. 1012-1998." The NRC staff does note that Rolls-Royce's V&V approach is described throughout a number of documents, rather than a single document. The LTR provides a mapping between the provisions in Section 7 of IEEE Std. 1012-1998 and Rolls-Royce documentation. However, the mapping does not go to the level of detail of identifying how Rolls-Royce activities map to the software integrity level 4 activities identified in the IEEE Standard. In order to facilitate the NRC staff making a finding of equivalency between Rolls-Royce's existing procedures for future work on the SPINLINE 3 Platform and NRC endorsed methods for V&V of safety related software systems, additional information is requested.

Per the RG quotation above, please provide a mapping of the specific Rolls-Royce V&V activities that Rolls-Royce considers being the equivalent of the software integrity level 4 tasks identified in IEEE Std. 1012-1998. Please use the information provided in Tables 1 through 3 of the IEEE Std. for this mapping. In particular, Table 2 of IEEE Std. 1012-1998 identifies tasks appropriate for integrity level 4 systems. Table 1 of IEEE Std. 1012-1998 provides an elaboration of those tasks along with inputs and outputs to each task. In addition, Section C.7 of RG 1.168 states that Table 3 of IEEE Std. 1012-1998 contains additional tasks appropriate for software integrity level 4 systems.

Should there be tasks or activities in IEEE Std. 1012-1998 or RG 1.168 for which there is no equivalent Rolls-Royce activity, please provide Rolls-Royce rationale for not having provisions to perform those tasks for future development on the Rolls-Royce SPINLINE 3 Platform.

Rolls-Royce Answer – IEEE Std 1012-1998 notes in Section 1.6 that:

> Not all V&V efforts are initiated at the start of the life cycle process of acquisition and continued through the maintenance process. If a project uses only selected life cycle processes, then compliance with this standard is achieved if the minimum V&V tasks are implemented for the associated life cycle processes selected for the project. ... For life cycle processes that are not used by the project, the V&V requirements and tasks for those life cycle processes are optional V&V tasks invoked as needed at the discretion of the project.

For ***SPINLINE 3*** the lifecycle processes used were: Requirements V&V (Section 5.4.2), Design V&V (Section 5.4.3), Implementation V&V (Section 5.4.4), and Test V&V (Section 5.4.5).

IEEE Std 1012-1998 also notes in Section 1.6 that:

> Specific software development methods and technologies (such as automated code generation from detailed design) may eliminate development steps or

> combine several development steps into one. Therefore, a corresponding adaptation of the minimum V&V tasks is permitted.

For ***SPINLINE 3*** the development steps were adapted to reflect the modular nature of the Operating System software, the use of the CLARISSE engineering workshop to configure the system and develop the Application Software, and the Rolls-Royce software validation test equipment.

IEEE Std 1012-1998 also notes in Section 1.6 that:

> When this standard is invoked for existing software and the required V&V inputs are not available, then V&V tasks may use other available project input sources or may reconstruct the needed inputs to achieve compliance with this standard.

For ***SPINLINE 3*** use of the legacy software design and V&V document was used as described in the commercial grade dedication documents.

Similarly, IEEE Std 1012-1998 notes in Section 5 that:

> Not all software projects include each of the life cycle processes listed above. To be in compliance with this standard, the V&V processes shall address all those life cycle processes used by the software project.

For ***SPINLINE 3*** the V&V activities align with the following lifecycle processes: Requirements V&V (Section 5.4.2), Design V&V (Section 5.4.3), Implementation V&V (Section 5.4.4), and Test V&V (Section 5.4.5).

And finally, IEEE Std 1012-1998 notes in Section 5 that:

> Some V&V activities and tasks include analysis, evaluations, and tests that may be performed by multiple organizations (e.g., software development, project management, quality assurance, V&V). For example, risk analysis and hazard analysis are performed by project management, the development organization, and the V&V effort. The V&V effort performs these tasks to develop the supporting basis of evidence showing whether the software product satisfies its requirements. These V&V analyses are complementary to other analyses and do not eliminate or replace the analyses performed by other organizations.

For some V&V activities and tasks the legacy ***SPINLINE 3*** software design and V&V document was used to demonstrate compliance, as described in the LTR and commercial grade dedication documents.

For ***SPINLINE 3*** some of the V&V activities and tasks listed in IEEE Std 1012-1998 are performed by groups other than the V&V organization, as noted in the matrix below.

The ***SPINLINE 3*** development V&V activities align with the IEEE Std 1012-1998 V&V tasks in the following manner:

5.4.2 Activity: Requirements V&V	***SPINLINE 3***
1) Task: Traceability Analysis	[[ ]]
2) Task: Software Requirements Evaluation	[[ ]]

3) Task: Interface Analysis	[[ ]]
4) Task: Criticality Analysis	[[AI]]
5) Task: System V&V Test Plan Generation and Verification	[[
6) Task: Acceptance V&V Test Plan Generation and Verification	]]
7) Task: Configuration Management Assessment	Accomplished by approval of the Software Configuration Management Plan for ***SPINLINE 3*** software and Software Quality Assurance Manager review.
8) Task: Hazard Analysis	[[ ]]
9) Task: Risk Analysis	[[ ]]
5.4.3 Activity: Design V&V	***SPINLINE 3***
1) Task: Traceability Analysis	[[ ]]
2) Task: Software Design Evaluation	[[ ]]
3) Task: Interface Analysis	[[ ]]
4) Task: Criticality Analysis	[[ ]]

5) Task: *Component* V&V Test Plan Generation and Verification	[[ ]]
6) Task: Integration V&V Test Plan Generation and Verification	[[ ]]
7) Task: V&V Test Design Generation and Verification	[[ ]]
8) Task: Hazard Analysis	[[ ]]
9) Task: Risk Analysis	[[ ]]
5.4.4 Activity: Implementation V&V	***SPINLINE 3***
1) Task: Traceability Analysis	[[ ]]
2) Task: Source Code and Source Code Documentation Evaluation	[[ ]]
3) Task: Interface Analysis	[[ ]]
4) Task: Criticality Analysis	[[ ]]
5) Task: V&V Test Case Generation and Verification	[[ ]]
6) Task: V&V Test Procedure Generation and Verification	

7) Task: Component V&V Test Execution and Verification	[[ ]]
8) Task: Hazard Analysis	[[ ]]
9) Task: Risk Analysis	[[ ]]
5.4.5 Activity: Test V&V	***SPINLINE 3***
1) Task: Traceability Analysis	[[ ]]
2) Task: Acceptance V&V Test Procedure Generation and Verification	[[ ]]
3) Task: Integration V&V Test Execution and Verification	[[
4) Task: System V&V Test Execution and Verification	
5) Task: Acceptance V&V Test Execution and Verification	]]
6) Task: Hazard Analysis	[[ ]]

7) Task: Risk Analysis	[[ ]]

In Section C.7 of Regulatory Guide 1.168, Revision 1, NRC states that:

> The following tasks are considered by the NRC staff to be part of the minimum set of V&V activities for critical software unless they are (1) incorporated into other V&V tasks in the software verification and validation plan (SVVP) or (2) performed outside the software V&V organization as part or all of the duties of some other organization.

The ***SPINLINE 3*** development V&V activities align with the Regulatory Guide 1.168 V&V tasks in the following manner:

Regulatory Guide 1.168 Activity	***SPINLINE 3***
7.1 Audits	Performed by the Software Quality Assurance Manager. See Section 11 of Rolls-Royce document 1 208 686 B, *Software Modification Quality Plan for* ***SPINLINE 3 S****oftware*, Section 4.4 of Rolls-Royce document 8 308 209 B, *Software Configuration Management Plan*, and Section 6 of Rolls-Royce document 8 307 208 B, *Software Quality Assurance Plan – US Template.*
7.2 Regression Analysis and Testing	The analysis of changes is performed in accordance with Rolls-Royce documents Change management 8 303 197, *Change Management,* Sections 4.11 and 6.2 of 8 307 210 B, *Software Verification and Validation Plan – US Template.* Regression testing is also addressed in LTR, sections 6.2.2.5, 6.2.2.7, 6.2.2.8, and 6.4.4. ***SPINLINE 3*** regression tests are documented in 1 207 146 G, *OSS Software Validation Test Plan.*
7.3 Security Assessment	Accomplished in Rolls-Royce documents 3 013 962 A, ***SPINLINE 3*** *Secure Development and Operational Environment*, and 3 014 543 A, ***SPINLINE 3*** *Secure Development and Operational Environment Vulnerability Assessment.*

7.4 Test Evaluation	Accomplished for technical adequacy by the Software Development Team review of the Software Validation Test Plans and Software Validation Test Reports. Accomplished for consistency with quality assurance requirements by the Software Quality Assurance Manager review and approval.
7.5 Evaluation of User Documentation	User documents are prepared in accordance with Rolls-Royce documents 8 307 244 A, *System Operations and Maintenance Plan – US Template,* and 8 307 273 A *Software User Manual Template.*. These documents are prepared, reviewed, and approved by the design organization in accordance with the requirements defined in Rolls-Royce document 8 303 198, *Establishment and Application of Engineering Documents.*

In order to reach a conclusion regarding appropriate independence of V&V activities (RG 1.168, Section C.3), the NRC staff requests that Rolls-Royce provide the following supplemental information regarding Procedure No. 8 303 350 L, "Quality Procedure – Control of Software Design (safety systems).

RAI-60 - In Section 3.2 of Procedure No. 8 303 350 L, a special staffing case is noted for V&V staffing for Class B or C2 software.

a) Please define Class B and Class C2 software.

b) If Class B and C2 software would be used for safety class systems in U.S. plants:

- Please explain why a staffing exception is taken for these "safety class" software developments.

- Please explain why it is acceptable for members of the development team, who still report to the software project manager, to perform V&V and still maintain independence to perform their V&V role.

Rolls-Royce Answer to Part a) - Class B software is defined in IEC 61226:

> **5.3.3 Category B**
>
> Category B denotes functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, especially the functions required to operate after the non-hazardous stable state has been achieved, to prevent design basis events (DBE) from leading to unacceptable consequences, or mitigate the consequences of DBE. The operation of a category B function may avoid the need to initiate a category A function. Category B functions may improve or complement the execution of a category A function in mitigating the consequences of a DBE, so that plant or equipment damage or activity release may be avoided or minimized.
>
> Category B also denotes functions whose failure could initiate a DBE or worsen the severity of a DBE. Because of the presence of a category A function to provide the ultimate prevention of or mitigation of the consequences of a DBE, the safety requirements for the category B function need not be as high as those for the category A function. This allows, if necessary, the category B functions to be of higher functionality than category A functions in their method of detecting a need to act or in their subsequent actions.

Class C2 is the French Standard RCC-E equivalent of IEC 61226 Category B software.

Class C software is also defined in IEC 61226:

> **5.3.4 Category C**
>
> Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Category C includes functions that have some safety significance, but are not category A or B. They can be part of the total response to DBA but not be directly involved in mitigating the physical consequences of the accident, or be functions necessary for beyond design basis accidents.

Rolls-Royce Answer to Part b) - According to IEC 61226, ***SPINLINE 3*** System Software is classified as Category A or NC (non-classified). There is no Category B or C ***SPINLINE 3*** System Software.

IEC 61226 Category A is equivalent to a US classification of safety-related (Class 1E). IEC 61226 Category NC is quite similar to a US classification of non-safety related (Non Class 1E).

The development process for Category A software is specified in IEC 60880. It specifies independent V&V to the same degree as Revision 1 of Regulatory Guide 1.168 does for safety-related software.

The development process for Category B software is specified in IEC 62138. It specifies independent V&V to the same degree as 10 CFR Part 50 Appendix B does for safety-related design in Criterion III (Design Control). That is, The V&V process is performed by individuals or groups other than those who performed the original design, but who may be from the same organization.

The development process for Category C software is specified in IEC 62138. It specifies normal industrial design practices.

As described in LTR Section 4.4, the ***SPINLINE 3*** Class 1E software consists of the following:

a. Operational System Software (OSS), including:
    - Core system software
    - Basic Functions (BF)
    - Local Display Unit driver (LDU CPU)
b. Application-oriented library of re-usable software components (SCADE Function Blocks)
c. Software embedded in the NERVIA+ board
d. Software embedded in the ICTO Pulse Input board
- Application Software (for safety-related projects)

The non-Class 1E ***SPINLINE 3*** software includes the following:

- "CLARISSE" workshop software
- Animation software
- PC local display unit software
- Test bench

RAI-61 - In Section 6.2.1 of Procedure No. 8 303 350 L, the typical project organization chart depicts the Software V&V Manager (SVVM) reporting to the Project Manager (PM) who is in charge of both hardware and software. Per Section 6.2.2, the PM has responsibilities related to cost and schedule for the overall project.

Please clarify how Rolls-Royce's internal processes and procedures provide the appropriate authority and organizational freedom to perform the V&V activities, when combined with the organizational structure presented in Section 6.2.1, to be consistent with accepted NRC staff regulatory positions and standards on independence of V&V.

Rolls-Royce Answer - Section 6.2.1 outlines the Project Manager responsibility to report to the corporate organization status on project costs, schedule, and quality performance. This reporting function must be understood in the context of other relevant and important parts of the same procedure.

Section 3.1 identifies the general principles applicable to the development of safety class software. It states:

- A software development team is formed. The team consists of two groups:
  - one, headed by the Software Project Manager (SPM), is responsible for development activities,
  - the other, headed by the Software Verification and Validation Manager (SVVM), is responsible for verification and validation activities.

This section outlines the separation of software development activities from the verification and validation activities.

Section 6.2.3 specifies that the Software Project Manager is responsible to:

- attain the objectives set for the software project (costs, deadlines and quality)

The Software Project Manager is to meet the budget and schedule set for the project.

Section 6.2.4 specifies that the Software Verification and Validation Manager is responsible for

- meeting commitments on costs and completion times for V&V work,

The choice of language in Section 6.2.4 is important. The Software Verification and Validation Manager is responsible for meeting the budget and schedule commitments made to the project by the V&V group. This reflects the financial independence that the V&V group has for the project. It is in contrast with the lesser financial independence the Software Project Manager has in meeting objective set for the Software Development team. The reporting of the V&V team performance by the Project Manager as required by Section 6.2.1 is to the commitments made by the V&V group.

Section 6.6 outlines the project management process applied to the project, including estimation, organization, and initial planning for development. It specifically notes that "this process is under the responsibility of the SPM for development activities and under the responsibility of the SVVM for V&V activities." These requirements ensure that the separation of software development activities from the verification and validation activities specified in Section 3.1 extends to the financial independence required by Regulatory Guide 1.188, Revision 1.

RAI-62 - Section 6.2.11 of Procedure No. 8 303 350 L states that in the event of disagreement between the development team and the V&V team, the Software Group Manager's decision shall be binding. The section also notes that a mediation process is available via the Software Quality Assurance Manager, with potential escalation of issues to the Engineering Department Manager and the Quality & Infrastructure Department Manager.

Please clarify the organizational relationship between the Software Group Manager, Software Quality Assurance Manager, Engineering Department Manager, and the Quality & Infrastructure Department Manager. Specifically, please explain how they sit in the overall organizational chart.

Rolls-Royce Answer - Section 6.2.11 reflects several important points that apply to the question of dispute resolution. First, the V&V team performs the verification and validation (review functions) with the requisite independence. The V&V team is free to identify and report errors, discrepancies, and potential problems. Second, the Software Development Group, and the 10 CFR Part 50 Appendix B design authority, is responsible for the final design. They have the responsibility to address and resolve the V&V team findings in a technically responsible manner. They cannot delegate the design responsibility to the V&V group nor can the V&V group assume design responsibility for resolution of problems. Either approach diminishes the independence of the development process. The information cited in the NRC question reflects these first two points on fundamental organizational responsibilities.

The independent review process has an inherent amount of tension and the potential for conflict. Constructive tension associated with a strong questioning attitude is good for the development process. Tension that strays from legitimate technical issues to other points of conflict can have a detrimental effect on the development process. The remainder of the discussion in Section 6.2.11 addresses the controls Rolls-Royce has put in place to address unresolved conflicts between the V&V group and the Software Development team. It states (in full):

> ***6.2.11 Dispute resolution procedure***
>
> In the event of disagreement between the development team and the V&V team, the **Software Group Manager**'s decision shall be binding. The close involvement and independence of the SQAM ensures that the mediation of the Software Group Manager is consistent with the project Quality objectives.
>
> In the event of disagreement between the Software Group Manager and the SQAM, the decision shall be taken at a higher level by the Engineering Department Manager and the Quality & Infrastructure Department Manager.

The last point of discussion addresses how Quality Assurance organization monitors for these unresolved disputes and processes and escalation process to resolve disagreements in a manner consistent with overall quality objectives.

Rolls-Royce believes that the approach outlined in Section 6.2.11 satisfies the separation of the design and review functions required by 10 CFR Part 50 Appendix B Criterion III with sufficient independence, as in Regulatory Guide 1.168, revision 1. These activities are performed within a quality structure that reflects Rolls-Royce's commitment to a strong safety culture.

Additional questions related to Rolls-Royce V&V.

RAI-63 - RG 1.168, Section C.6, discusses the use of tools. In addition, IEEE Std. 7-4.3.2 – 2003, Section 5.3.2, which is endorsed by RG 1.152, Revision 3, also discusses the use of tools. The NRC staff did note Rolls-Royce discussion of the tools used to support the Rolls-Royce V&V processes in the docketed materials. For example:

- Document No. 1 208 686 B references use of VERIF_COMP
- Document No. 1 207 107 D references use of VERIF_COMP_UNIX

Please clarify how the tools referenced above are used to support V&V activities. Specifically, the NRC staff is looking to ensure that the tools are not used in lieu of personnel to confirm system characteristics and performance.

Rolls-Royce Answer – The [[
]] that is reviewed as part of the source code verification activity. [[

]]

RAI-64 - RG 1.168, Section C.3, quotes the following from Title 10 of the *Code of Federal Regulations* Part 50, Appendix B: "the program must provide for indoctrination and training of personnel performing activities affecting quality as necessary to ensure that suitable proficiency is achieved and maintained." The NRC staff noted descriptions of the organization(s) involved in docketed Rolls-Royce materials; however, the NRC staff did not identify any specific descriptions regarding how V&V personnel were selected and/or trained.

Please provide information to demonstrate that V&V personnel are sufficiently proficient in software engineering.

Rolls-Royce Answer – Rolls-Royce uses a formal procedure (1 208 210 D, *Software V&V Team Training Plan*) to ensure that V&V personnel are sufficiently proficient in software engineering and V&V techniques. The program requires initial training or experience in industrial computing for the languages used for ***SPINLINE 3*** projects. It also provides specific

training for the specific ***SPINLINE 3*** programming rules. A comprehensive training program is specified for the various methods and tools used for ***SPINLINE 3*** V&V activities.

RAI-65 - Document No. 1 208 686 B, "Software Modification Quality Plan," Section 8.2.5, describes the 'software integration tests' for software modification. Document No. 8 303 350 L, "Project Execution Process: Software," Section 8.5, which also describes integration, notes that the tests performed are not recorded. Please clarify how the V&V organization and/or Rolls-Royce V&V processes are used during integration testing and how test documentation is recorded and maintained.

Rolls-Royce Answer – As a way of background, the ***SPINLINE 3*** software validation testing is performed on a [[

]] Integration Testing in the context of IEEE Std 1012-1998 is accomplished at two points in the validation process for ***SPINLINE 3*** technology using this test apparatus.

[[

]]

The discussion of interface testing in the two documents mentioned in the RAI is not in the same context as IEEE Std 1012-1998 Integration Testing.

This IEEE Std 1012-1998 Integration Testing is documented in the Software Validation Test Plan and Software Validation Test Report documentations produced by V&V for the OSS and Application Software.

RAI-66 - Document No. 8 303 350 L, "Project Execution Process: Software," Section 8.4, notes that 'manual coding' is verified and subject to unit tests by the V&V team. Please explain how automatic code generation is treated under the Rolls-Royce V&V processes. Section 4.4.4.1 of the LTR addresses the use of CLARISSE in automatic code generation.

Rolls-Royce Answer – CLARISSE is used to produce the executable code for each ***SPINLINE 3*** Processing Unit. CLARISSE is a comprehensive tool which is used to:

- define the system architecture (i.e., processing units, networks)
- describe the data exchanged and the time constraints concerning the networks
- describe the hardware architecture (i.e., cards, I/O)
- design the application software by means of SCADE
- automatically link the system I/O and the SCADE application I/O
- generate the executable code of each Processing Unit

The Application Software code is generated from Library Functions (C code), SCADE Generated Code (C code), and Hand Written External Functions (C code).

The various inputs to CLARISSE (e.g., software requirements specification, network diagrams, and equipment functional diagrams) are all verified by the V&V organization.

[[

]]

RAI-67 (Follow question for RAI-11(b)) - In the Rolls-Royce response to RAI-11(b) regarding commercial grade dedication, the statement is made: "Rolls-Royce concluded that the ***SPINLINE 3*** software and firmware development processes (including the original validation testing) were of acceptable [sic] based on the rigor of the development processes, quality of the development documentation, and the validity of the results obtained. The software validation tests were accepted by Method 2 and are described in LTR Sections 6.2 and 6.3."

As was noted earlier in this set of RAIs at the start of the V&V section of questions (i.e., RAI-59 – RAI- 67), the NRC staff understands that ***SPINLINE 3*** was not developed under a program specifically tailored to IEEE Std. 1012. However, in order to substantiate that the software V&V processes were of sufficient rigor for purposes of commercial grade dedication – when taken in context with other activities performed and credited under Method 1 and Method 4 per EPRI-106439 – please provide a mapping of the original V&V activities (associated with the "original validation testing" noted above) to the software integrity level 4 tasks identified in IEEE

Std. 1012-1998. [Note: this request is similar to RAI 59, but is focused on the original V&V processes used in ***SPINLINE 3*** development, rather than the current processes that would be used for future platform development.]

Rolls-Royce Answer – The original development process for SPINLINE 3 software maps to the IEEE Std 1012-1998 V&V tasks in the same manner as shown in the response to RAI 59. The changes that have occurred since the original development only affected how tasks were performed rather than what tasks were performed. The newer software documentation has a more explicit method of identifying requirements to facilitate requirements traceability. The Test Bench was developed to support software validation testing. These changes were described and demonstrated to NRC during the June 11-15, 2012 audit in Grenoble France.

Also, see LTR Table 3.8-9, Mapping **SPINLINE 3** SQP MC3 and Other Content to IEEE 1012-1998 SVVP Content Guidance, for additional information.