May 14, 2010

Mr. Sylvain Bazinette
Rolls-Royce
Civil Nuclear Business, Instrumentation & Controls
23, Chemin du Vieux Chêne
38246 Meylan-Cedex - France

SUBJECT: REQUEST FOR SUPPLEMENTAL INFORMATION RE: ROLLS ROYCE CIVIL NUCLEAR LICENSING TOPICAL REPORT, "SPINLINE 3 DIGITAL SAFETY I&C PLATFORM" (TAC NO. ME1736)

Dear Mr. Bazinette:

By letters dated July 1, 2009, December 23, 2009, January 8, 2010, and February 2, 2010 (available in the Agencywide Documents Access and Management System (ADAMS) under Accession Numbers ML092160018, ML093570361, ML100120087 and ML100330793, respectively), Rolls Royce Civil Nuclear - Société par Action Simplifiée (RRCN -SAS), the applicant, submitted a licensing topical report, "SPINLINE 3 Digital Safety I&C [Instrumentation and Control] Platform" (SPINLINE 3), for safety evaluation review by the U.S. Nuclear Regulatory Commission (NRC) staff.

The NRC staff is performing an acceptance review of the SPINLINE 3 application in accordance with Revision 3 of the Office Nuclear Reactor Regulation's Office Instruction, LIC 109, "Acceptance Review Procedures" (ADAMS Accession No. ML091810088). The NRC staff has determined that supplemental information is needed to complete the acceptance review.

On May 7, 2010, Mr. Peter Lobner, RRCN-SAS staff, and I agreed that the NRC staff will receive your response to the enclosed questions, which are significant issues, within two weeks of the date of this letter. If you have any questions regarding the enclosed questions, please contact me at 301-415-4053.

Sincerely,

/RA/

Jonathan Rowley, Project Manager
Licensing Processes Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 773

Enclosure: Supplemental Information questions

cc w/encl: See next page

Mr. Sylvain Bazinette
Rolls-Royce
Civil Nuclear Business, Instrumentation & Controls
23, Chemin du Vieux Chêne
38246 Meylan-Cedex - France

SUBJECT: REQUEST FOR SUPPLEMENTAL INFORMATION RE: ROLLS ROYCE CIVIL NUCLEAR LICENSING TOPICAL REPORT, "SPINLINE 3 DIGITAL SAFETY I&C PLATFORM" (TAC NO. ME1736)

Dear Mr. Bazinette:

By letters dated July 1, 2009, December 23, 2009, January 8, 2010, and February 2, 2010 (available in the Agencywide Documents Access and Management System (ADAMS) under Accession Numbers ML092160018, ML093570361, ML100120087 and ML100330793, respectively), Rolls Royce Civil Nuclear - Société par Action Simplifiée (RRCN -SAS), the applicant, submitted a licensing topical report, "SPINLINE 3 Digital Safety I&C [Instrumentation and Control] Platform" (SPINLINE 3), for safety evaluation review by the U.S. Nuclear Regulatory Commission (NRC) staff.

The NRC staff is performing an acceptance review of the SPINLINE 3 application in accordance with Revision 3 of the Office Nuclear Reactor Regulation's Office Instruction, LIC 109, "Acceptance Review Procedures" (ADAMS Accession No. ML091810088). The NRC staff has determined that supplemental information is needed to complete the acceptance review.

On May 7, 2010, Mr. Peter Lobner, RRCN-SAS staff, and I agreed that the NRC staff will receive your response to the enclosed questions, which are significant issues, within two weeks of the date of this letter. If you have any questions regarding the enclosed questions, please contact me at 301-415-4053.

Sincerely,
/RA/
Jonathan Rowley, Project Manager
Special Projects Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 773
Enclosure: Supplemental Information questions
cc w/encl: See next page

DISTRIBUTION:

PUBLIC	RidsNrrDpr		
PLPB Reading File	RidsNrrDprPlpb	RidsNrrLAEHylton	RidsAcrsAcnw_MailCenter
JRowley, NRR	RidsOgcMailCenter	RidsNrrDeEicb	

ADAMS ACCESSION NO.: ML101300192 **NRR-088**

OFFICE	PLPB/PM	PLPB/LA	PLPB/Acting BC	PLPB/PM
NAME	JRowley	EHylton	MMcCoppin	JRowley
DATE	5/12/10	5/12/10	5/14/10	5/14/10

OFFICIAL RECORD COPY

REQUEST FOR SUPPLEMENTAL INFORMATION

BY THE OFFICE OF NUCLEAR REACTOR REGULATION

SPINLINE 3 DIGITAL SAFETY I&C PLATFORM

ROLLS ROYCE CIVIL NUCLEAR

PROJECT NO. 773

By letters dated July 1, 2009, December 23, 2009, January 8, 2010, and February 2, 2010, Rolls Royce Civil Nuclear submitted licensing topical report, “SPINLINE 3 Digital Safety I&C Platform,” for safety evaluation review by the U.S. Nuclear Regulatory Commission (NRC) staff. The NRC staff is performing an acceptance review of the submittal and has the following questions:

1. NRC Regulatory Guide (RG) 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, endorses Institute of Electrical and Electronic Engineers (IEEE) Standard (Std) 1012-1998, "IEEE Standard for Software Verification and Validation," for meeting the regulatory guidance for software verification and validation. The Interim Staff Guidance (ISG)-06 compliance matrix (ADAMS Accession No. ML100640485) indicated that the "SPINLINE 3 Software Validation Test Plan" (SVTP), Doc. No. 1 207 146 G (ADAMS Accession No. ML100330844), is the software verification and validation plan (SVVP) for the platform. However, the SVTP does not address all of the topics that are supposed to be addressed by an SVVP. For example, IEEE 1012 states that an SVVP should address: verification and validation (V&V) overview, V&V processes (only one of which might be testing, as not all attributes are testable), V&V administrative requirements and V&V documentation requirements. The SVTP addresses analysis of software functions, test resources, analysis of tests, coverage of tests, regression tests, and tests on upgrades, as would be expected in a test plan. However, the SVTP does not address V&V overview, V&V processes (other than testing), V&V administrative requirements and V&V documentation requirements. For example:

   a) Clause 7.4, "V&V Overview," of IEEE 1012 states: "The SVVP shall describe the organization, schedule, software integrity level scheme, resources, responsibilities, tools, techniques, and methods necessary to perform the software V&V." Clause 7.4.1, "(SVVP Section 4.1) Organization," of IEEE 1012 further states: "The SVVP shall describe the organization of the V&V effort, including the degree of independence required (See Annex C of this standard). The SVVP shall describe the relationship of the V&V processes to other processes such as development, project management, quality assurance, and configuration management. The SVVP shall describe the lines of communication within the V&V effort, the authority for resolving issues raised by V&V tasks, and the authority for approving V&V products. Annex F provides an example organizational relationship chart"; whereas, the STVP, being focused on testing, does not address these topics.

   b) Clause 7.5, "(SVVP Section 5) V&V Processes," of IEEE 1012 states: "The SVVP shall identify V&V activities and tasks to be performed for each of the V&V processes described in Clause 5 of this standard, and shall document those V&V activities and

ENCLOSURE

tasks. The SVVP shall contain an overview of the V&V activities and tasks for all software life cycle processes."

Clause 5 of IEEE 1012 states: "V&V processes support the management process (5.1), acquisition process (5.2), supply process (5.3), development process (5.4), operation process (5.5), and maintenance process (5.6). The minimum V&V activities and tasks supporting the above processes are referenced in the following subclauses and defined in Table 1. This clause's subtitles are the same as subtitles in Table 1 to correlate the requirements of the following subclauses with Table 1 tasks."

Clause 7.5.1, "(SVVP Sections 5.1 through 5.6) Software life cycle," further states:

> "The SVVP shall include sections 5.1 through 5.6 for V&V activities and tasks as shown in SVVP Outline (boxed text). The SVVP shall address the following eight topics for each V&V activity:
>
> 1) *V&V Tasks.* The SVVP shall identify the V&V tasks to be performed. Table 1 describes the minimum V&V tasks, task criteria, and required inputs and outputs. Table 2 specifies the minimum V&V tasks that shall be performed for each software integrity level.
>
> 2) *Methods and Procedures.* The SVVP shall describe the methods and procedures for each task, including on-line access, and conditions for observation/evaluation of development processes. The SVVP shall define the criteria for evaluating the task results.
>
> 3) *Inputs.* The SVVP shall identify the required inputs for each V&V task. The SVVP shall specify the source and format of each input. The inputs required for the minimum V&V tasks are identified in Table 1. Other inputs may be used. For any V&V activity and task, all of the required inputs from preceding activities and tasks may be used but for conciseness, only the primary inputs are listed in Table 1.
>
> 4) *Outputs.* The SVVP shall identify the required outputs from each V&V task. The SVVP shall specify the purpose, format, and recipients of each output. The required outputs from each of the V&V tasks are identified in Table 1. Other outputs may be produced. The outputs of the Management of V&V and of the V&V tasks shall become inputs to subsequent processes and activities, as appropriate.
>
> 5) *Schedule.* The SVVP shall describe the schedule for the V&V tasks. The SVVP shall establish specific milestones for initiating and completing each task, for the receipt and criteria of each input, and for the delivery of each output.
>
> 6) *Resources.* The SVVP shall identify the resources for the performance of the V&V tasks. The SVVP shall specify resources by category (e.g., staffing, equipment, facilities, travel and training).
>
> 7) *Risks and Assumptions.* The SVVP shall identify the risks (e.g., schedule, resources, or technical approach) and assumptions associated with the V&V tasks. The SVVP shall provide recommendations to eliminate, reduce, or mitigate risks.

8) *Roles and Responsibilities.* The SVVP shall identify the organizational elements or individuals responsible for performing the V&V tasks;"

whereas, the SVTP does not address all of these topics, and for those it generally addresses (e.g., methods and procedures), they are addressed in a limited manner as they concern only testing. Similarly, under V&V reporting requirements (Clause 7.6), V&V administrative requirements (Clause 7.7) and V&V documentation requirements (Clause 7.8), IEEE 1012 contains extensive detailed guidance that it states shall be in an SVVP; whereas, the STVP does not address these topics for all V&V activities.

2. RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," as providing an approach acceptable to the staff, for meeting the regulatory requirements and guidance as they apply to development processes for safety system software.

   a) The platform software development plan (platform SDP), "Software Development Plan," Doc. No. 1 207 102 A (ADAMS Accession No. ML 093620283), is mainly a structural plan prescribing who does what and when, as called for by IEEE 1074, but with much less detail. It implies that the details are contained in a document called [CCGL_MC3]. Please provide documentation that includes a level of detail comparable to that in IEEE 1074.

   b) The platform SDP contains detail regarding the development process, responsibility distribution and risk analysis. However, there are some things called for by IEEE 1074 that are missing. For example: metric development and analysis and resource estimation. Also omitted was a discussion of quality, except for a reference to a document called [PAQL_MC3]. Please provide information on how documents to be used in future platform software development cover the omitted topics.

3. Risk Management is not addressed. Please provide risk management information.

   a) RG 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." IEEE 7-4.3.2 Clause 5.3.6, "Software Project Risk Management," calls for software risk management. However, the platform software quality plan (platform SQP), Doc. No. 8 303 429 E (ADAMS Accession No. ML093620244), contains no provision for risk analysis or control. Please provide risk analysis/management information or explain how this was accomplished during platform software development.

   b) IEEE 1012, Table I, Clause 5.6.1, Item 8, states: "Review and update risk analysis using prior task reports. Provide recommendations to eliminate reduce or mitigate the risks." The Software Modification Quality Plan (SMQP), Doc No. 1 208 686 B (ML093620234), Section 5.2.1, discusses "impact on existing systems" under "General Impact Assessment," but there is no indication of a detailed risk analysis or mitigation plan. Please provide documentation that includes a detailed risk analysis or mitigation plan.

4. RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 828-1998, "IEEE Standard for Software Configuration Management Plans," for software configuration management plans. The platform software configuration management plan (platform SCMP) is "Software Configuration Management Plan for SPINLINE 3 Software Sub-assemblies Managed by CM

Tool," Doc. No. 1 208 878 D (ADAMS Accession No. ML093620238). The technical process in this document is described in detail, but virtually all of the management pieces are missing completely. Please provide documentation that includes the management pieces.

The platform SCMP was very difficult to follow. The translation into English from French is challenging to comprehend. Configuration management software was apparently used for some of it, but not all. There is no detail at all regarding V&V, except for mentioning that V&V is done before changes are approved. There is no mention of the parties responsible for management of the various pieces of the process. IEEE 828 calls for processes for interface control, resources or V&V and none of these is addressed in this document. There was no reference to external documents for those processes.

The platform software has already been developed, and as such, would not necessarily be expected to claim compliance with newer process documents. However, it is difficult to reach a conclusion about the quality of the platform development process. Please provide documents that show the process is in compliance with NRC endorsed standards. Some of these omissions are addressed in software modification quality plan (SMQP), but those sections are not referenced in this document. For example:

a) IEEE 828, Clause 4.2.1, states: "The organizational context, both technical and managerial, within which the planned SCM activities are to be implemented, shall be described." However, the platform SCMP does not describe the organizational, management or authority context for configuration management. This is very significant, because without structured oversight of the process, there is little hope of proper implementation of the process.

b) IEEE 828, Clause 4.3.2.1, states: "The plan shall specify procedures for requesting a change to a baselined CI [configuration item] and the information to be documented for the request." However, the platform SCMP does not specify the procedures for requesting a change to a baselined CI. This is significant, because without a detailed process for change requests, it is impossible to be sure sufficient information is available to do proper risk analysis, scheduling, and V&V planning.

c) IEEE 828, Clause 4.3.4, states: "The plan shall identify the configuration audits and reviews to be held for the project." However, the platform SCMP does not specify an audit or review process. This is important because configuration reviews are important management tools for establishing a baseline.

d) IEEE 828, Clause 4.3.4, states: "The Plan shall identify the external items to which the project software interfaces." However, the platform SCMP has no provisions to ensure that external interfaces are identified. This is important because the effects of external hardware or support software on a given CI might not be properly analyzed.

e) IEEE 828, Clause 4.3.4, states, in part, that for each type of SCM [software configuration management] the plan shall specify which tools, techniques, equipment, personnel and training are needed and how each resource will be provided or obtained. However, the platform SCMP, Section 3, contains descriptions of the tools and processes to be used for configuration management, but there is no provision to ensure that personnel are made available or adequately trained to execute those processes.

f) IEEE 828, Clause 4.3.4, states: "SCM plan maintenance information identifies the activities and responsibilities necessary to ensure continued SCM planning during the

life cycle of the project." However, the SCMP does not specify how the SCM process will be monitored and maintained or the organizations responsible for those functions. This is important because SCM processes may need to evolve to adapt to other internal or external changes to the project or its external interfaces.

In view of these discrepancies, please explain how these provisions of IEEE 828 were met in the development of the platform software. For example, for IEEE 828 provisions omitted from the SCMP that are addressed elsewhere, please indicate where and how the software development program directed software developers and V&V personnel to those other references.

5. The "SPINLINE 3 Software Verification and Validation Plan-SVVP," Doc. No. 8 307 210 B (ADAMS Accession No. ML092160055), a template SVVP for future U.S. projects (application SVVP), generally follows the format of IEEE 1012, but has some discrepancies (see No. 6 below). However, in general, the level of detail in the application SVVP is less than that of IEEE 1012. This presents a challenge to the review in that it will be difficult to verify that regulatory requirements and guidance are met when the application SVVP does not specify the process in as much detail as the guidance for preparing it. Please provide application V&V documentation that includes a level of detail comparable to that in IEEE 1012.

6. The application SVVP is inconsistent with IEEE 1012. For example: IEEE 1012, Table 1, Clause 5.4.4, Item No. 2.3, prescribing traceability activities calls for "consistency" between the software requirements specification (SRS) and the system specifications. It defines consistency as agreement between the level of detail in the SRS and the systems specifications. However, in Section 4.3.1, "Software Requirement Specification Evaluation and Traceability Analysis," of the application SVVP, there is no mention of consistency in the specified traceability activities. Please explain how this provision of IEEE 1012 is to be assured, or justify why no consistency analysis is necessary.

7. Item 2.3 in IEEE 1012, Table 1, Clause 5.4.4, calls for verification of the completeness of source code implementation for particular source code components, for example, exception handling and testability. However, in the application SVVP, Section 4.5.1, "Source Code Evaluation," while tasks are specified for verifying that the source code implements the specified design elements, there is no reference to verification of the completeness of that implementation. Please explain how this provision of IEEE 1012 is to be met.

8. The "SPINLINE 3 Software Quality Assurance Plan-SQAP," Doc. No. 8 307 208 B (ADAMS Accession No. ML092160054), the U.S. template for application SQAPs, states that IEEE Std 730-1998 is "applicable." Does this mean that the platform SQAP is purported to comply with the standard?

9. Please clarify whether documents that state that certain references are "applicable," are purported to comply with those references.