Regulatory Audit Report for the Review of the
Rolls-Royce SPINLINE 3 Digital Safety Instrumentation and Control Platform Licensing Topical Report
Grenoble, France

June 11-15, 2012

Summary of Audit Observations:

The U.S. Nuclear Regulatory Commission (NRC) staff conducted a regulatory audit at the Rolls-Royce facility in Grenoble, France from June 11 - 15, 2012. All audit objectives were satisfactorily met. The NRC staff focused the audit in the following areas:

- Requirements Threads: Rolls-Royce demonstrated that it maintains critical design basis information for the SPINLINE 3 Digital Safety Instrumentation and Control Platform (SPINLINE 3) hardware and software components in good order and in a readily retrievable state. The Rolls-Royce process tools greatly assists Rolls-Royce in the implementation of its processes.

- Independent Verification and Validation (IV&V): Rolls-Royce staff demonstrated a thorough knowledge of their roles and responsibilities. Review of past and current projects showed an active involvement of the V&V group consistent with Rolls-Royce processes.

- Configuration Management (CM): Rolls-Royce SPINLINE 3 configuration record keeping, documentation, management activities, and use of CM tools were demonstrated to be thorough and in accordance with their docketed processes.

- Commercial Grade Dedication (CGD): NRC staff reviewed Rolls-Royce items and processes referenced (but not docketed in detail) as part of their commercial grade dedication effort. Rolls-Royce demonstrated adherence to its processes, including a robust non-conformity reporting system.

- Secure Development: Rolls-Royce SPINLINE 3 development processes, configuration management, and test configurations support establishment of a secure development environment.

Background

The regulatory audit plan (Agencywide Documents Access and Management System (ADAMS) Accession No. ML12151A184) for the audit of the Rolls-Royce facility outside of Grenoble, France detailed the plans and expectations for the trip. The audit was in support of the NRC staff's review of the Rolls-Royce SPINLINE 3 Licensing Topical Report (LTR). The NRC staff's efforts on the audit are expected to support generation of a safety evaluation (SE) of the "generic" features of the SPINLINE 3 with regard to its potential use in safety related systems in domestic nuclear power plants. The work is being performed under Technical Assignment Control No. ME3600.

ENCLOSURE

Details of Regulatory Audit:

Major activities conducted on the audit are described below.

Summary of Entrance Meeting (Monday – June 11, 2012)

The NRC audit team, consisting of Tim Mossman, John Thorp, and Samir Darbali from the Office of Nuclear Reactor Regulation's Instrumentation and Control Branch, arrived at the Rolls-Royce facility outside of Grenoble, France on June 11, 2012. At the entrance meeting that morning, the audit team walked through their plan and objectives for the audit – consistent with what had been transmitted to Rolls-Royce in the regulatory audit plan. In addition, facility logistics and a more detailed audit schedule were discussed.

A number of Rolls-Royce staff members were introduced at the meeting, including Jean-Michel Palaric, who is the Director for Engineering Projects for Rolls-Royce's Instrumentation and Controls Group. Mr. Palaric provided a concise overview of Rolls-Royce's business sectors, with particular focus on their nuclear instrumentation and controls business.

At the conclusion of Mr. Palaric's overview, Philippe Paillat, Rolls-Royce's Head of Quality Management for the Instrumentation and Controls Group, provided an overview of the quality assurance organization and program. Rolls-Royce representatives provided a history of their incorporation of relevant quality assurance (QA) standards into its QA program, including IAEA 50-C-QA, ISO 9001, Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, Appendix B, and American Society of Mechanical Engineers (ASME) Nuclear Quality Assurance-1 (NQA-1). The Rolls-Royce Quality Management System (QMS) currently contains approximately 60 procedures, approximately 250 Work Instructions, and approximately 50 forms. The quality program focus is to maintain and execute the QMS, conduct audits of internal processes and suppliers, and assure certification of company management systems. Rolls-Royce staff member Hélène Jegou walked through the project software quality execution process – which had been submitted to the NRC as part of the LTR documentation. A large portion of the audit focused on Rolls-Royce's implementation of the tasks contained in the software process.

At the conclusion of the entrance meeting, a brief tour of the Rolls-Royce facility was conducted to orient the audit team to the facility. The audit team was able to view multiple generations of Rolls-Royce instrumentation and control components that have been used for nuclear plants and are still actively supported by Rolls-Royce.

Thread Audits

As described in Section B.3.2.2 of Branch Technical Position (BTP) 7-14 requirements, thread audits are an accepted method for checking the verification and validation (V&V) efforts of the applicant. BTP 7-14 also notes that requirements thread audits are effective in viewing the "actual development process".

Given the need for translation of certain documentation, the audit team cited several platform capabilities in the audit plan for which requirements thread audits would be performed. Those capabilities included:

- The fail-safe outputs following a failure as implemented by watchdog timer(s) internal to the analog output board (6SANA ISO). This feature was identified in the LTR as a "safety-oriented" feature for the SPINLINE 3 platform. This requirements thread audit reviewed the development process for a non-software (i.e., electronic hardware) capability of the platform.

- The fail-safe outputs following a failure as implemented by watchdog timer(s) internal to the digital output board (32ACT). This feature was identified in the LTR as a "safety-oriented" feature for the SPINLINE 3 platform. This requirements thread audit reviewed the development process for a field-programmable gate array (FPGA) implemented capability of the platform.

- The inconsistency checking of the control and data flows, which can initiate a central processing unit (CPU) stop and pre-defined output state. This feature was identified in the LTR as a "safety-oriented" feature for the SPINLINE 3 platform. This requirements thread audit reviewed the development process for the current Operational System Software (OSS) of the platform.

- The dual-port memory management function of the complex programmable logic device (CPLD) on the NERVIA+ daughter board. This feature is relevant to the potential use of digital communications between SPINLINE 3 units in a future application. This requirements thread audit reviewed the development process for CPLDs currently in use on the platform.

The thread audits were conducted over several days during the audit week. The audit team also received detailed written and verbal explanations of the implementation of the requirements thread capabilities; however, for sake of protecting Rolls-Royce proprietary information, those design details are not contained in this audit report.

Watchdog timer capability on 6SANA ISO board

Rolls-Royce representatives Daniel Chaix and Abdellah Hadj-Rabah assisted the audit team in walking through the requirements, design, and test documentation related to the watchdog timer function(s) on the 6SANA ISO board. The audit team noted that this requirement was one that was implemented on the electronic board hardware and represented an example of the Rolls-Royce hardware development processes.

Rolls-Royce was able to provide a "master" document of module technical data, which identified critical controlled documents that constitute the design basis of the board. The document was controlled as Rolls-Royce Document No. 5100436664, Revision J (revision was dated December 21, 2011). The module technical data document also included a bill of materials (with appropriate identifying information) for all components that comprise the 6SANA ISO board.

The audit team walked through the following documents (that were identified in the module technical data document) with Rolls-Royce staff:

- The board Requirements Specification, Rolls-Royce Document No. 6 610 273, Revision B, dated September 28, 1987
- The board Detailed Design Schematic, Rolls-Royce Document No.1 479 050, Revision F, dated September 17, 1993
- The board Type Test Program, Rolls-Royce Document No. 1 479 167, Revision B, dated March 24, 1988
- The board Type Test Result, Rolls-Royce Document No. 1 479 873, Revision E, dated November 11, 2011
- The board User Manual, Rolls-Royce Document No. 1 479 165, Revision B, dated February 9, 1994

The audit team determined the requirements specification contains the requirement for the watchdog timer capability. The audit team noted that the requirements specification was from 1987, when the platform technology was being developed and maintained by Schneider Electric Company. Despite the change in ownership to Rolls-Royce and the passage of a quarter of a century, the requirements documentation was still recoverable and of reasonable quality to unambiguously identify board requirements. The audit team noted that no actual time was specified in the requirement specification for actuation of the watchdog timer protective function; however, the audit team's review of the detailed design schematic and type test program documentation identified sufficient information to determine the intended and acceptable response time for the watchdog timer(s) on the board.

The detailed design schematic of the electronic hardware board illustrated how the watchdog timer capability had been implemented on a global and local level within the board. The global watchdog protects against the output board receiving no communication for a period of time. The local watchdog capabilities are resident within each of the six possible output channels and protect against communications being lost with any of the channels used in a particular application. The "failed" states (i.e., actuated watchdog state) were defined (i.e., 15 Volts (V), 0 milliamperes (mA)) in the design schematic.

Sections 4.3 and 4.4 of the test program document specify the acceptance criteria for the watchdog capability and the board behavior if the watchdog is actuated. The acceptance criteria are consistent with the design documentation. Sections 2.8 and 2.9 of the test results document contain the data that confirms that the board met its acceptance criteria with respect to this requirement. The user document details how failures are indicated on the front of the board, including a watchdog actuation. The user manual also specifies the environmental conditions that the board should be operated within.

Overall, the audit team found that the documentation for this capability of the 6SANA ISO board constitutes good evidence of a well-documented design basis for the board. The documents were all signed by the appropriate Rolls-Royce personnel per Rolls-Royce processes. Rolls-Royce staff satisfactorily answered all the questions regarding their development processes, documentation, and design.

Watchdog timer on the 32ACT board

Rolls-Royce staff members Chaix and Hadj-Rabah also walked the audit team through the requirements, design, and test documentation related to the watchdog capability implemented on the 32ACT board. The 32ACT board makes use of a FPGA to implement its logic. For this requirements thread, the audit team walked through both the design documentation for the overall 32ACT board and the design documentation for the FPGA that is used on the board. Later in the audit, the audit team reviewed the Rolls-Royce FPGA/CPLD development process, its evolution and how it is nested with the overall Rolls-Royce board (hardware) development process.

The audit team reviewed "Master" documents for both the 32ACT board (Rolls-Royce Document No. 5100436357) and the 32ACT FPGA (Rolls-Royce Document No. 5100436534). The 32ACT master board document identified all the design documentation relevant to the board, as well as the bill of materials that comprise the board. The master document was revision D, dated July 21, 2008. The 32ACT FPGA master document identified the design documentation specific to the FPGA used on the board.

The board level documents were:

- The requirements specification, Rolls-Royce Document No. 5100436363, Revision A, dated April 2, 2011
- The detailed design schematic, Rolls-Royce Document No. 5100436360, Revision A, dated November 3, 2001
- Type test program, Rolls-Royce Document No. 5100436364, Revision A, dated January 22, 2002
- Type test result, Rolls-Royce Document No. 5100436365, Revision A, dated January 22, 2002
- The user manual, Rolls-Royce Document No. 5100436366, Revision A, dated September 24, 2001

Section 3.1 of the board requirements document identified the watchdog requirement for the board and the failsafe condition. Section 5.1.1 identified the time requirement on the watchdog function. The detailed board design schematic describes how the watchdog capability is implemented on the 32ACT FPGA.

The test specification document addressed testing of the watchdog capability – including the test of the output (Section 7.2.5), the time to actuate (Section 7.2.6), and the test of the failsafe position (Section 7.2.7). The audit team noted that the test acceptance criteria for the time to actuate to watchdog from the time last reset was actually more stringent in the test acceptance criteria than in the requirements specification. [Note: This simply demonstrated more accurate performance than specified.] Test data documented in Sections 7.2.5, 7.2.6, and 7.2.7 of the type test result confirmed that the board met the acceptance criteria of the test program specification.

In addition to the board level documentation, the audit team was able to review the 32ACT FPGA-specific documentation. [Note: the FPGA/CPLD development process has its own

specific development activities that more closely aligned with software development processes and are “nested” within the overall electronic board (hardware) design processes.] The “master” document for the FPGA was Rolls-Royce Document No. 5100436534, Revision B, which identified all the relevant design basis documents for the FPGA. The 32ACT FPGA documents reviewed included:

- The requirements specification, Rolls-Royce Document No. 5100436536, Revision A, dated June 15, 2001
- The design document, Rolls-Royce Document No. 5100436537, Revision A, dated October 4, 2001
- The design report, Rolls-Royce Document No. 5100436538, Revision A, dated March 6, 2002
- The test specification, Rolls-Royce Document No. 5100436539, Revision A, dated October 4, 2001
- The test report, Rolls-Royce Document No. 5100436540, Revision A, dated March 6, 2002
- The programming specification / instruction, Rolls-Royce Document No. 5100436541, Revision B, dated October 30, 2002

The audit team observed that the FPGA requirements specification contained requirements consistent with the board requirements for the watchdog timer, including detailed descriptions of each of the two registers. Sections 5.5.3 and 5.5.4 of the specification prescribe how the watchdog is to function and the time to actuate (with tolerance) from last communication.

Section 6.3.5 of the design document addresses in detail how the watchdog is to be implemented. In addition, Section 6.3.5.5 describes the design of the counter (i.e., clock) used to determine when a watchdog should be actuated. The design report described physical constraints on the FPGA chip, as well as defined each of the pin positions.

The test specification described the test set-up and architecture of the test bench. The test tool and all the files to be used in the test were defined. The audit team inquired about how the tool was used. Rolls-Royce indicated that the tester defines the inputs and expected outputs for all the tests and that the tool executes the tests and produces the test evidence. The audit team also noted that since the FPGA development is “nested” within the overall electronic board design, that the FPGA is tested at both the FPGA-level and again at the board level (integrated on the overall board). Section 5.5.1 of the test report indicated that the tests were passed. The test report also contained the log file of the test as test evidence.

The audit team also reviewed the programming instruction. The audit team noted that a 32bit CRC was used to ensure the integrity of the FPGA executable files.

Again, the audit team found that the documentation for this capability of the 32ACT board constitutes good evidence of a well-documented design basis for the board. The audit team found that the documentation for both the overall board and the FPGA demonstrates good adherence to Rolls-Royce processes for hardware and FPGA development. The documents were all signed by the appropriate Rolls-Royce personnel per Rolls-Royce processes.

Rolls-Royce staff was readily able to answer all the questions regarding their development processes, documentation, and design.

OSS inconsistency checking of the control and data flows

Sylvain Bazinette from Rolls-Royce walked the audit team through the requirements and design documentation related to the OSS checking of control and data flows. The detection of any inconsistencies is to result in the CPU entering a stop condition, with a pre-defined state for each output. This capability is implemented in the OSS, which will be resident on all SPINLINE 3 systems.

Five types of tests or checks are defined in the Rolls-Royce documentation for the OSS to perform. These tests address checks on the microprocessor (i.e., UC25) board, the "intelligent" and non-intelligent boards, NERVIA network stations NERVIA network communication status and other specific tests.

Documentation reviewed included:

- The software requirements specification, Rolls-Royce Document No. 1 207 108J (previously submitted on docket – ADAMS Ascension No. ML100330819)
- The preliminary design document, Rolls-Royce Document No. 1 207 141H (previously submitted on docket – ADAMS Ascension No. ML100330838)
- The software validation test plan, Rolls-Royce Document No. 1 207 146G (previously submitted on docket – ADAMS Ascension No. ML100330844)
- The software validation report, Rolls-Royce Document No. 1 207 232F (previously submitted on docket – ADAMS Ascension No. ML100330814)

With much of the relevant documentation on this thread already having been submitted on the docket, the audit team focused on observing how Rolls-Royce used its software tools to control and maintain design basis information relevant to this capability.

The audit team was able to witness that all this documentation was maintained in the Rolls-Royce Dimensions tool. [Expanded discussion of the Dimensions tool is contained in the Configuration Management section of this audit report.]

The audit team reviewed and discussed the following items:

- The original code walk-through (contained in the Dimensions tool) from 1995. The code walk-through indicated that the code met SRS requirements, as well as Rolls-Royce coding standards. The walk-through document was signed by a representative of the V&V organization.

- The test script for the requirements verification test.

- The various tools that were used to perform static tests on the code (e.g., software coding rules checking). The read-out from these tools were contained in Dimension.

Since much of the requirement and test information was already docketed, the audit team took the opportunity to view other supporting developmental documentation to help confirm that Rolls-Royce executes its processes as detailed in its plans. The audit team determined the documentation contained in the Dimensions tool demonstrates good adherence to Rolls-Royce processes for software development. The documents were all signed by the appropriate Rolls-Royce personnel per Rolls-Royce processes. Rolls-Royce staff readily answered all the questions regarding their development processes (including test tools and equipment), documentation ,and design.

CPLD memory management on the NERVIA+ board

Rolls-Royce technical representatives Chaix and Hadj-Rabah walked the audit team through the requirements, design, and test documentation related to the dual-port memory management capability implemented on a CPLD within the NERVIA+ board. The CPLD function serves to arbitrate access to the dual-port memory on the NERVIA+ board to preclude errors associated with simultaneous reading and writing to a specific memory location. Similar to the FPGA-related capability thread detailed above, documentation from both the CPLD and NERVIA+ board development were reviewed. The audit team also reviewed the Rolls-Royce FPGA/CPLD development process, its evolution and how it is nested with the overall Rolls-Royce board (hardware) development process.

The audit team, along with Rolls-Royce staff, walked through the following CPLD-level documentation:

- The “master” CPLD document, Rolls-Royce Document No. 5100436207, Revision B, dated June 14, 2002
- The CPLD requirements specification, Rolls-Royce Document No. 5100436611, Revision B, dated February 12, 2002
- The CPLD design specification, Rolls-Royce Document No. 5100436612, Revision B, dated February 12, 2002
- The CPLD detailed design report, Rolls-Royce Document No. 5100436613, Revision B, dated February 13, 2002
- The CPLD test specification, Rolls-Royce Document No. 5100436614, Revision B, dated February 12, 2002
- The CPLD test report, Rolls-Royce Document No. 5100436615, Revision B, dated February 12, 2002

Similar to the other requirements audited, the master CPLD document identified all the documents relevant to the CPLD design basis, many of which are listed above.

The requirements specification contained the requirements for the three major functions implemented on the CPLD, including the memory management function. Sections 6.6 and 6.7 contained the requirements for communications to both the UC25 (i.e., CPU) and NERVIA+ processor related to dual-port memory management. The requirements were clearly specified.

The design specification contained the VHDL (very-high-speed integrated circuits (VHSIC) hardware description language) code for the three CPLD functions. The audit team reviewed

the code and noted the relative brevity and simplicity of the VHDL code for the functions. The design report specified the specific CPLD component to be used, as well as the pin assignments for the CPLD. The document identified the version of the tool used in creating the CPLD. The CPLD clock speed is also addressed in the design report, specifically describing how it will meet design requirements.

The CPLD test specification describes the test configuration, tools, and specific test to be executed for the memory management function. Section 5.5 of the test report contains the record of the (successful) test that was executed, as well as the data captured from the simulation tool.

Once the CPLD is integrated on the NERVIA+ board, it is subject to board level tests. The audit team reviewed the following NERVIA+ board level test documentation:

- The type test specification document, Rolls-Royce Document No. 5100436204, Revision A, dated January 18, 2002
- The test report, Rolls-Royce Document No. 5100436205, Revision C, dated February 22, 2011

Section 5 of the test specification described the configuration for the board level tests, and Section 7.3.5 described a very specific shared memory test designed to verify the board's capability (as supported by the CPLD) to control conflict along with acceptance criteria. A specially designed test was deemed necessary, as a "random" memory access conflict is expected to be a rare event. The test report contains the record and data from the board level test.

The documents reviewed during this thread audit were all signed by the appropriate Rolls-Royce personnel per Rolls-Royce processes. Rolls-Royce staff satisfactorily answered all the questions regarding their development processes, documentation, and design.

As with the other requirements threads audited, the audit team found that the documentation for this capability of the NERVIA+ board, as implemented on a CPLD, constitutes acceptable evidence of a well-documented design basis for the board and associated CPLD. The audit team determined that the documentation for both the overall board and the CPLD demonstrates good adherence to Rolls-Royce processes for hardware and CPLD development.

Independent Verification and Validation (IV&V)

The IV&V portion of the audit focusing on IV&V was intended to confirm that the Rolls-Royce V&V processes are implemented per their documentation, with a focus on record keeping, documentation, and management activities. The audit team requested to see records related to the most recent examples(s) of SPINLINE 3 software development.

Pierre Monteil and Eric Morlot from the V&V group were the primary Rolls-Royce participants in this portion of the audit.

IV&V Organization and Processes

The IV&V portion of the audit started with a thorough discussion of the V&V processes for both OSS development and SPINLINE 3 application development. The differences identified between these two processes are attributable to the OSS being developed as part of a traditional software development effort and the SPINLINE 3 application being developed using tools specifically designed for SPINLINE 3 applications (e.g., the CLARISSE tool). The audit team had an extensive question and answer session with Rolls-Royce V&V personnel about the software development processes, V&V involvement and the V&V organization. The audit team made the following observations:

- The V&V staff are extremely knowledgeable of their roles in OSS and SPINLINE 3 application development.

- While V&V staff could not point to any examples of serious conflict between the V&V organization and a software development project organization, they were able to clearly articulate how disagreements would be escalated through the QA organization, should any arise.

- In light of the growth of Rolls-Royce's instrumentation and control business in recent years, the audit team questioned Rolls-Royce V&V representatives on the level of resources needed to address the increased volume of work. Rolls-Royce indicated that it is confident in the size of their organization and their ability to hire new staff and/or access contract staff as needed. Rolls-Royce V&V personnel noted that they had added four V&V personnel in the past year.

- When asked about the relative experience level of the V&V organization, Rolls-Royce staff indicated that their least experienced V&V engineer had over a decade of relevant experience.

- V&V staff also provided examples of various internal and external training sessions their personnel had attended recently in order to maintain technical proficiency.

- Rolls-Royce V&V staff confirmed that no matrixing of Rolls-Royce staff is used for V&V on Class 1E projects – which is consistent with their planning documents

- Rolls-Royce V&V personnel indicated their test application for OSS upgrades and modifications is customized depending on the OSS features being tested and the test application is developed following Rolls-Royce's application software development processes

V&V Test Bench

The audit team visited the "test bench," which is an isolated test configuration used by the V&V staff for testing of OSS and application software. The audit team conducted a question and answer session with the previously identified V&V staff, as well as another V&V technician

working at the bench, regarding configuration and operation of the test bench. The audit team observed that:

- The test bench was isolated (from a network connectivity standpoint) from the other Rolls-Royce networks. [Note: isolation of test equipment supports establishment of a secure development environment.]

- Test scripts and test data were reviewed from tests that were being performed at the time. V&V personnel confirmed that they author the test scripts and that the scripts and all test results are maintained in the Dimensions tool.

- The CMU report documents the hardware configuration of the unit used in test.

- Cyclic redundancy checks (CRC) are performed on data (i.e., code) in EPROM and Flash memory to ensure that the correct modules are being tested. Data generated demonstrated this check.

- For OSS development testing, V&V staff indicated that test applications are customized for the features of the OSS to be tested. These test applications are developed following Rolls-Royce SPINLINE 3 application processes.

- For application code, the applicable OSS version is used on the test bench.

- Again, Rolls-Royce staff demonstrated they are well versed in their own processes and use of tools that support process implementation.

V&V of Current OSS Upgrade

At the time of the audit, Rolls-Royce was in the midst of a development effort (i.e., VD3 project) to update portions of the OSS. The audit team was able to use this opportunity to examine objective evidence regarding Rolls-Royce's application of the current V&V processes to the development. For this part of the audit, Rolls-Royce used the Dimensions tool in real time to find all the requested documentation related to the on-going development.

The audit team reviewed the following items:

- Specification Phase: Rolls-Royce staff accessed the verification form for requirements specification (Rolls-Royce Document No. SPL3_FV_481) used by the V&V staff to record their review of the Software Requirements Specification (SRS) for the development. The audit team noted that Rolls-Royce's V&V staff made numerous comments against the SRS. One specific comment related to an inconsistency between the OSS specification and the hardware specification. The audit team considered this positive objective evidence that the V&V reviewer had a broad knowledge of SPINLINE 3 documentation and thoroughly verified the SRS against other system documentation. The documentation also contained resolutions for all comments made. [In the case of the inconsistency comment, the resolution was to complete an update to the hardware specification, as the software specification reviewed was actually correct.]

- Specification Phase: The V&V review of the specification (Rolls-Royce Document No. SPL_FV_443) documented 13 comments and the "refused" version 3 of the specification. Comments were given major or minor designations by the V&V reviewer. The audit team considered this information to be objective evidence the V&V organization was thorough in their review and had the authority to hold development until documentation met with their approval.

- Specification Phase: The software verification test plan (Rolls-Royce Document No. 1 207 406H) had been written by the V&V team, per Rolls-Royce processes for OSS development. The document was to be confirmed by the development team and approved by the QA organization; however, given that the VD3 project was still on-going, the document had not yet been finalized. The audit team determined the plan at this stage of the process is objective evidence of Rolls-Royce properly implementing its development processes.

- Design Phase: Rolls-Royce V&V staff generated three comments on the FDB driver design specification (Rolls-Royce Document No. SPL3_FL_97). Two of the comments were accepted and one was rejected by the design team with justification.

- Design Phase: The FDB driver detailed design document (Rolls-Royce Document No. SPL3_FV_429) was also reviewed. The audit team noted that Rolls-Royce V&V personnel had performed a review and signed the document.

- Coding (Implementation) Phase: During this phase, a static code review is performed (per Rolls-Royce development plans) using the QA_C tool. The tool is run by the development team to evaluate the code against Rolls-Royce coding rules and it generates various metrics for the code. The V&V team verifies the report prior to the development progressing further. The audit team was shown the results of the QA_C run for the FDB driver code and noted the metrics generated at the bottom of the report. The report, as well as all of the other development documentation, was found in the Dimensions tool.

- The audit team noted the various approved design and development documentation had been formally signed by a Rolls-Royce V&V staff member. The audit team also noted there were at least three different V&V signatures on the various documents, which demonstrated depth to the reviews conducted by the V&V organization (i.e., Rolls-Royce did not rely solely on one individual for V&V).

  [Note: the VD3 project was still in development at the time of the audit, so evidence from the integration and verification phase was not yet available.]

Configuration Management

The Configuration Management (CM) portion of the audit focused on Rolls-Royce's record keeping, documentation, management activities, and use of CM tools. The NRC audit team reviewed plans, procedures, guides, and training documentation used for CM and observed how

Rolls-Royce staff used tools to control and manage software and documentation, as well as track non-conformities within their processes.

Use of CM Tools

Rolls-Royce makes use of several CM tools throughout various stages of software development and product manufacturing. These tools include the Dimensions CM tool, GEVOL, ORIENT, and a tool incorporated within CLARISSE.

The Serena Dimensions CM tool is the main CM tool used by Rolls-Royce. The audit team received a presentation on this tool and observed its use throughout various parts of the audit. Before procuring and implementing the Dimensions CM tool in its processes, Rolls-Royce used an Excel file to manage item configuration. This Excel file is still being kept by Rolls-Royce and it is used when working on older software products.

The Dimensions CM tool is used by Rolls-Royce at the software development level to manage technical documents, source files (those that are not managed by CLARISSE), executable files, test files, and software QA reports. Each of these types of items has its own dedicated lifecycle.

Changes in the Dimensions CM tool are managed with 'requests' which would include a verification form, non conformity, or a change request (depending on the item type). Links are created between requests and items, and baseline reference configurations are created. For making changes to items, Rolls-Royce typically uses the Windows version of the CM tool which runs on its servers. Although the Web version of the tool is rarely used, it would only be used by Rolls-Royce for entering change requests.

The Dimensions CM tool requires a login ID and password. Access is granted to select projects and requires multiples approvals. Although the tool can be used from multiple computers at the same time, Rolls-Royce makes use of item check out and lock features. For example, when a document is locked, it cannot be edited by another user. The NRC observed files in the Dimensions tool that were checked out and locked.

In the case where there are multiple developers working on the source code, parallel check out is used and implemented with the 'Merge' function. A person who is not one of the developers performs the integration of changes into the code. However, for OSS development, there is only one developer and the parallel check out process is not used. Also, parallel check out cannot be used for document changes.

Rolls-Royce uses its shared project directory as the Work Area. The Work Area is used to check out documents for editing. Training on the use of the tool stipulates that if a local C drive is used as the Work Area, a backup copy has to be made daily on the shared project directory.

Training on the PC and Web client versions of the Dimensions CM tool is provided on the Rolls-Royce internal website. Advanced training on the tool is also available to Rolls-Royce staff. The training progress is tracked and after completion, access to the tool is granted. For new projects, training is provided again at the beginning of the project to everyone involved, as well as quality training on item identification, management, and baselines (including naming of baselines and project requirements). A software quality manager is present during the training.

CLARISSE includes software engineering tools that facilitate CM, document generation, and project administration, so the Dimensions CM tool is not used to manage CLARISSE files.

Configuration management within CLARISSE is based on the 'Part' concept, which includes: System Architecture, Unit, Network, etc. A Part is a set of consistent elements such as definition data, documentation, a table, or generated code. There is a hierarchical dependency between hardware configuration, application description, system application interface, and processing unit. Based on these dependencies, CLARISSE checks for consistency between Parts and will detect inconsistencies if different versions are used in the project.

CLARISSE creates the following three directories: 'Production' (development area, used by the designer), 'Control' (V&V area used by the verifier), and 'Reference.' CLARISSE will create a reference of the Part in the Reference area. From this reference, five files are produced (including a report file) that are controlled in the Dimensions CM tool and are placed in the Project/Archive directory. CLARISSE creates a Checksum number that is included in the report.

The audit team observed an example of Parts management on the CLARISSE tool for the Neutron Parameters Processing Unit (NPPU) project, which included the process of opening the CLARISSE CM tool menu, and selecting a Part from the list. The OSS 'Application Interface' Part was selected and the audit team observed the Reference Version, Child Parts, Used Parts, and Used Tools identified for this Part.

Change Requests for CLARISSE are handled with the Dimensions CM tool, even though there is an option for it in the CLARISSE tool.

Rolls-Royce uses the GEVOL system change management tool to track change requests at the company level. These change requests can come from within Rolls-Royce or from a customer. The audit team was shown the 'Definition of Change Management Process' procedure (Rolls-Royce Document No. 8 303 197), which lists the different categories defined in GEVOL, such as: request, analysis, responsibilities, Class 1E or non Class 1E, deferred modifications, verify evolution, and apply. Access to this tool requires a login ID and password.

The audit team was also shown the 'Change Notice Form' template (Rolls-Royce Document No. 8 303 051 K) used to close out a change request from GEVOL. This form identifies any change(s) made to a software version and indicates the destination organization.

For tracking non-conformity claims at the company (manufacturing) level, Rolls-Royce uses the ORIENT tool. These non-conformity claims can either come from Rolls-Royce of from a customer.

A software change that is made due to a non-conformity claim will also be managed with the Dimensions CM tool. Software non-conformities were tracked on an Excel file before Rolls-Royce implemented the use of the Dimensions CM tool.

ORIENT allows sorting of non-conformities based on owner and status, but not on type of non-conformity. The audit team requested, and Rolls-Royce demonstrated various searches for non-conformities to show its ability to conduct review and analysis for process and product

quality corrective and preventive actions. Access to this tool also requires a login ID and password.

The audit team was shown the 'Non-conformity Report' document guide (Rolls-Royce Document No. 1 207 870 C) which provides instructions for placing a request on the Dimensions tool including instructions on naming and recording the non-conformity. This guide also provides a link to a template used to track old projects that were developed before the use of the Dimensions CM tool.

The audit team reviewed the 'Non-conformities' procedure (Rolls-Royce Document No. 8 303 202), which is a quality procedure used to identify and manage safety-related non-conformities at the company level. This procedure directs the reader to the 'CM Process' (Rolls-Royce Document No. 1 207 875). There cannot be a project delivered without closing all non-conformities on a safety system.

Management and Control of the Software

The NRC staff requested Rolls-Royce to provide the following CM documents for review. These documents address different aspects of the Rolls-Royce implementation of CM activities.

The audit team was shown the software configuration management plan (SCMP) for the Safety-Critical Application Development Environment (SCADE) Libraries (Rolls-Royce Document No. 3 013 037 A) which serves as the CM plan for all SCADE libraries used in SPINLINE 3. The plan addresses CM activities such as item identification, responsible organizations, reference configurations, control of changes, and configuration audits and review, amongst others. Rolls-Royce uses the Dimensions CM tool to manage the SCADE libraries.

The audit team reviewed the 'List of Software Documents' (LSD) for the Mochovce 3-4 NPPU project (Rolls-Royce Document No. 3 015 828 A). The LSD is the point of entry for the software development and evolves along with the developed software. It is signed after the documentation audit. The document name, reference, and revision are kept in the Dimensions tool from the Software Detail Design phase to the completion of the Software Component Test Description and Reports.

The audit team examined the 'List of Tools and Libraries Used for the Software Development' (LTLUS) documentation guide (Rolls-Royce Document No. 1 207 865 B), which provides guidance for the software developer and the software auditor and includes a list of common tools, development tools, V&V tools, libraries, and instructions on how to create an archive disc.

The audit team looked at the LTLUS for the Mochovce 3-4 project (Rolls-Royce Document No. 3 307 285 B) which lists the tools used by SPINLINE 3 and the PC. The audit team also reviewed a newer version of the LTLUS template (Rolls-Royce Document No. 8 307 285 B).

The audit team reviewed the 'Software Tracking Configuration Management Report File' documentation guide (Rolls-Royce Document No. 1 207 863 C) which provides a history of the software development. This document tracks the changes made in the different versions, the Dimensions tool baselines, addressed non-conformances, non-conformances to be addressed in a future revision, etc. The purpose of this guide is to provide software modification

traceability and to identify key lifecycle configuration states. There is a version of this document for the units (software products) and one for the system (global). The audit team viewed the global version of this guide for the Mochovce 3-4 project (Rolls-Royce Document No. 3 016 899 A).

The audit team reviewed the SCMPs for the 'System Workshop' (AS) (Rolls-Royce Document No. 1 208 868 B) and the 'Monitoring and Maintenance Unit' (PdM) (Rolls-Royce Document No. 3 000 342 B). The life cycle development of these systems was performed in accordance with non class 1E development processes. Document and source code files for the AS and the PdM are managed with the Microsoft Visual Source Safe (VSS) CM tool. For the next project, Rolls-Royce will use the Dimensions CM tool for configuration management of the AS, and a new SCMP will be generated that will require application specific action items.

The audit team asked Rolls-Royce staff about its use of a Change Control Board (CCB). Rolls-Royce explained that the CCB is used for more complex software associated with changes that affect the product provided to the customer. The audit team examined the CCB forms associated with a specific project. These forms track and document the requested, reviewed and implemented changes. The CCB is comprised of the Project Leader, the Software Project Leader, the Software Quality Leader, and the V&V Tech Leader.

For SPINLINE 3, the software affecting the development of the product, for example a change needed for the OSS, CLARISSE, or the NERVIA network, would be reviewed within the project process steps. All changes or responses to the Non-Conformances would be addressed in configuration control internal audits at the start of the project, at the phase reviews and prior to delivery. A report of all changes and non-conformances is produced in the Dimensions tool, extracted to an Excel file and then addressed. Rolls-Royce V&V staff ensures there is an effective impact analysis of each change.

Secure Development Environment, Record Keeping, and Document Control

Only the IT department has the rights to move files from the Dimensions tool into the Projects directory and into the archive locations. V&V staff check that these are the correct files and a Checksum is used to ensure the file is uncorrupted.

The audit team reviewed the 'IT Logistics Support Rules' document (Rolls-Royce Document No. 1 204 971 G), which lays out the rules for archiving executable files. These files are copied from the Dimensions tool by IT and stored in a read-only directory so they can be accessed by those required to use them, but who have not been involved in the development process. V&V staff signs the logistics support rules document after the files in the directory have been verified.

Rolls-Royce also maintains hard copy versions of its documents and software. After each project has been completed, an 'Archive' is created and given an identification number which goes into the Software Configuration Management Report (SCMR). The SCMR for each project includes all the new baselines for the project.

At the End of Phase Review, a hardcopy version (latest revision) and a microfiche copy (latest and older revisions) are placed in their respective archives. Rolls-Royce's IT Manager, Vincent Ferrari, provided the audit team a tour of the archives where the document hardcopies are

stored. Forms are used to obtain and control access to these documents. The audit team reviewed Rolls-Royce Procedure No. 8 303 320 M, Section 6.1, 'Records of documents held in permanent archives,' which dictates that microfiche are never to be destroyed (unless there is a specific request for it). Documents are converted into microfiche every time they are amended and the microfiche are kept offsite in a fire and flood protected storage area.

Controlled versions of code are copied into CDs and kept in an access controlled (locked) vault. The company servers are backed up daily and the data is stored in 1.6TB hard drives which are also stored in an access controlled (locked) vault. Once a week, these drives are taken to an outside facility for storage. After a specified period of time, the older drives will be reused.

Design input/output records with requirements for legibility, traceability and portability are considered "lifetime" records and are kept for the life of the given systems.

Commercial Grade Dedication

The Commercial Grade Dedication (CGD) portion of the audit was focused on three particular topics – the internal Rolls-Royce QA audit of their processes and platform characteristics in support of CGD, the Rolls-Royce implementation of follow-up activities on non-conformity reports received from fielded SPINLINE 3 systems and the Rolls-Royce activities relative to CGD of CPLD/FPGA components.

CGD Internal Audit

The Rolls-Royce CGD report (Rolls-Royce Document No. 3 010 795A) noted that an internal audit was performed of SPINLINE 3 processes and characteristics to support the CGD effort. The audit team met with a supervisor in the Rolls-Royce QA organization to review the results of the internal audit. This supervisor had performed the audit, which was documented in Rolls-Royce Document No. MPD.11.5256, dated June 15, 2011.

The audit team observed the following from the review:

- The audit was performed over two months in the spring of 2011. A total of 16 discrepancies were noted, with follow-up actions and responsible Rolls-Royce parties identified for resolution.
- A spreadsheet of the discrepancies was maintained, documenting actions taken to resolve them. Most of the items were addressed via corrective action. A few items were either deferred or accepted (if the safety impact was deemed negligible).
- The audit team reviewed item D.1, which addressed a missing record from the design phase. The corrective action performed was to track down the record.
- The audit team also reviewed item D.7, which dealt with a configuration management issue related to the ICTO pulse board software prior to implementation of the Dimensions tool. The corrective action was identified, but implementation was deferred until the next revision.
- The Rolls-Royce QA Supervisor indicated that Revision B of the CGD Report will have a complete version of the discrepancies table, with identification of actions taken.

Operating History

One of several methods that can be used in CGD involves establishing an operating history for the item that is favorable to performing its intended use in the future. To assist in evaluating the SPINLINE 3 platform operating history, the audit team examined how Rolls-Royce implemented its non-conformity report system. The audit team's review of Rolls-Royce's performance in addressing and documenting non-conformities confirmed Rolls-Royce understands the operating experience of its platforms, takes measures to correct any issues that are attributable to the platform, and has effectively documented this experience.

Joël Schindler, from the Rolls-Royce QA department, explained Rolls-Royce non-conformity reporting using several examples. Rolls-Royce uses a tool, ORIENT, to document and track all non-conformities.

The audit team observed the following:

- The first non-conformity reviewed was identified as item AA-11-1188. This example was not for a SPINLINE 3 system, but it was illustrative of the non-conformity process. The non-conformity was opened on April 20, 2011. The audit team reviewed the main form. Rolls-Royce staff noted that it was the "older" form, as the standard reporting form has been updated to reflect 10 CFR 21 requirements. The documentation indicated that the resolution team was comprised of the QA manager and two technical managers. The specific non-conformity involved a reported capacitor supplier defect. The safety significance of the issue was identified. Customers had been notified of the non-conformity and records of the communication to customers were recorded in ORIENT, as well as any re-communication attempts in the event that no response was received from the original notification.

- A SPINLINE 3 non-conformity – identified as item 12-1468 – dated April 12, 2012 was also reviewed. The issue involved a soldering concern. The issue was entered into the ORIENT database on the newer reporting form that reflected 10 CFR 21. The root cause evaluation was still in process; however, potentially affected parts had been "quarantined."

- An additional non-conformity (item RP-11-110) was reviewed later in the audit involving a SPINLINE 3 system. The report originated with a Rolls-Royce customer on April 26, 2011. All documentation related to the notification from the customer was contained in the ORIENT database – including the part serial number. Per the documentation in ORIENT, the investigation continued until September 5, 2011, and involved an independent failure analysis at a third-party laboratory. The formal test report from the third party laboratory was contained in the ORIENT database. The follow-up correspondence to the customer, which contained the third-party laboratory report and conclusions, was also contained in the database.

- The ORIENT tool can be used to produce "statistics" on the non-conformities (e.g., by cause). The biggest "category" of non-conformities was identified as "continuous improvement."

CPLD / FPGA development

Per audit team request, Rolls-Royce walked through its CPLD/FPGA development process – both their original process and the current (revised) process. The original process is documented in Rolls-Royce Document No. 8 303 687A. The current process is documented in Rolls-Royce Document No. 8 303 687G and was revised to conform to IEC 62566 (which specifically addresses standards for CPLD/FPGA development).

Rolls-Royce explained that CPLD/FPGA development is a subset of board development. Board requirements that are implemented by a CPLD/FPGA flow down into a CPLD/FPGA requirement document. The CPLD/FPGA development process defined the steps and "checks" in place to appropriately define requirements, then to design, implement, and test the CPLD/FPGA. This process includes steps that appear equivalent to those used in software development.

Once CPLD/FPGA development is complete, the CPLD/FPGA is integrated back into the board development process. The CPLD/FPGA is then tested again along with the board. This process was examined in two of the thread audits.

Rolls-Royce staff walked the audit team through the development records for the ACCG4 FPGA. The development plan (Rolls-Royce Document No. 3 017 052A) defined the reviews, documents to be produced (including the authors, verifiers, and approvers) and development roles (with specific names). The minimum requirement for testing the FPGA was specified. Section 5.5 of the plan addressed configuration control, including critical elements such as VHDL code, coding tools, test tools, scripts, and records. QA review meeting minutes are documented (As noted in an example reviewed by the audit team from a January 10, 2012, meeting).

The audit team also reviewed a NERVIA FPGA development. The initialization review was performed on May 31, 2011. The specification review was performed on October 18, 2011. The document (Rolls-Royce Document No. 3 015 407A) was verified and the verification form was attached (and populated by the verifier). Comments are identified by the verifier as major, minor, or question. Software QA personnel also signed the specification. The test report was documented in Rolls-Royce Document No. 3 018 292A. Tests were performed in a simulated environment. [Note: final testing is performed with the FPGA integrated into the electronic board.] The annex of the test report contained the test scripts.

Handling of Parts Suppliers

Although not part of the original audit plan, the audit team examined Rolls-Royce's processes with respect to handling of incoming parts and management of parts suppliers. The audit team toured the parts receipt area of the Rolls-Royce facility and observed parts receipt and acceptance activities. The audit team also made numerous inquiries to Rolls-Royce staff regarding their processes.

The audit team observed the following items:

- Rolls-Royce has a dedicated technical management group that focuses on obsolescence management.

- Rolls-Royce has performed routine audits on its suppliers. Rolls-Royce staff reviewed the approved supplier list (spreadsheet) with the audit team. The spreadsheet showed all the Rolls-Royce parts suppliers, along with parts supplied, audit type, audit date and record of audit report. Each year suppliers are "graded" by Rolls-Royce's procurement department. Action plans are developed for any "problem" suppliers.

- Rolls-Royce representatives guided the audit team through the parts receipt inspection area. In the receipt inspection area, the audit team observed:
    - Rolls-Royce has five employees routinely working in receipt inspection – two focused on mechanical components, two on electrical components, and one skilled in multiple disciplines.
    - The audit team observed receipt of a detector (mechanical) component.
        - The package was inspected and opened.
        - A drawing for the component was readily available and used to support visual inspection.
        - The component drawing version was verified against the supplier specification.
        - A checklist specific to the component was used to conduct the inspection.
        - The checklist contained a list of documents to be provided by the supplier and level of control for the part.
        - The audit team witnessed the checklist being populated – including verification of the supplier provided certificate of performance.
        - "Smart" sampling of parts is performed – with sampling guidelines provided at the receipt inspection workstation.
    - The audit team observed receipt of a 10-slot backplane board used in the SPINLINE 3 system
        - The inspector performed a visual check of the quality of soldering and positioning of components.
        - Tools to facilitate inspection are readily available at the inspection workstation.
        - Documentation – with visual examples – of acceptance and unacceptable attributes of parts is also readily available at the workstation.
    - Any non-conformities found during receipt inspection are recorded in the ORIENT database. Non-conforming parts are affixed with a red label and placed in a non-conforming parts quarantine area that is locked. The audit team witnessed this non-conforming parts area.

Equipment Qualification

While not part of the planned audit scope, the audit team was afforded the opportunity to view the SPINLINE 3 test specimen that is intended for use in completing their Equipment Qualification (EQ) tests. EQ testing is required as part of the CGD effort. The initial EQ tests performed on a Rolls-Royce SPINLINE 3 test specimen identified a few items for further

investigation. The audit team observed the changes in the new SPINLINE 3 test specimen that had been previously communicated as the appropriate corrective actions for the items discovered.

Secure Development

As noted earlier in this audit report, the audit team observed the following:

- The requirements threads audited by the audit team demonstrated that Rolls-Royce maintains good traceability from requirements through test during development.
- The Dimensions tool helps maintain configuration control of all critical development documentation, code, and test resources.
- The test bench environment used for V&V activities is isolated from other networks within the Rolls-Royce facility.

Summary of Exit Meeting

The exit meeting was held on June 15, 2012. The audit team lead indicated that all audit objectives were satisfactorily met. No open items or concerns were identified.