



<b>Désignation du document</b> <i>Document name</i>	<b>SPINLINE 3 Secure Development and Operational Environment</b>	
<b>Affaire</b> <i>Product</i>	<input checked="" type="checkbox"/>	<b>SPINLINE 3 NRC Qualification</b>
<b>Equipement</b> <i>Equipment</i>	<input checked="" type="checkbox"/>	<b>SPINLINE 3 Digital Safety I&amp;C Platform</b>
<b>Sous-ensemble</b> <i>Subassembly</i>	<input type="checkbox"/>	
<b>Classé 1E ou équiv.</b> <i>Safety classification</i>	<input checked="" type="checkbox"/>	<b>1E</b>
<b>Document contractuel</b> (pour le client) <i>Contractual document (for customer)</i>	oui <input type="checkbox"/> non <input checked="" type="checkbox"/>	<b>Nbre de pages</b> <input type="text" value="44"/> <i>Number of pages</i>
<b>Code projet</b> <i>Project code</i>	<i>Niv1 / Level1</i> E.RE01	<i>Niv2 / Level2</i> 17.00
<b>Diffusion interne:</b> <i>Internal distribution</i>	ICC, QUA, KLI, LOG	
<b>Diffusion externe:</b> <i>External distribution</i>	NRC	
	Tampon archivage / <i>Archive stamp</i> <input type="checkbox"/>	
<b>Version française</b>		
<b>Rédigé par</b> <i>Written by</i>	<b>Vérifié par</b> <i>Checked by</i>	<b>Approuvé par</b> <i>Approved by</i>
<b>Nom :</b> <i>Name</i>	<b>Nom :</b> <i>Name</i>	<b>Nom :</b> <i>Name</i>
<b>Visa :</b> <i>Signature</i>	<b>Visa :</b> <i>Signature</i>	<b>Visa :</b> <i>Signature</i>
<b>Date :</b> <i>Date</i>	<b>Date :</b> <i>Date</i>	<b>Date :</b> <i>Date</i>
<b>English version</b>		
<b>Rédigé ou traduit par</b> <i>Written or translated by</i>	<b>Vérifié par</b> <i>Checked by</i>	<b>Approuvé par</b> <i>Approved by</i>
<b>Nom :</b> Peter Lobner <i>Name</i>	<b>Nom :</b> Hélène Tabouret <i>Name</i>	<b>Nom :</b> NP. DURAND <i>Name</i>
<b>Visa :</b> <i>Signature</i>	<b>Visa :</b> <i>Signature</i>	<b>Visa :</b> <i>Signature</i>
<b>Date :</b> 15 June 2011 <i>Date</i>	<b>Date :</b> 28/06/11 <i>Date</i>	<b>Date :</b> 28/06/11 <i>Date</i>



**TABLEAU DE MISE A JOUR**  
*Record of revisions*

<b>Indice /date</b> <b>Rédigé par</b> <i>Revision letter / date</i> <i>Written by</i>	<b>Pages modifiées</b> <i>Modified pages</i>	<b>Origine et désignation de la modification</b> <i>Origin and designation of the modification</i>
15 June 2011 P. Lobner		First issue

<b>Identification des moyens de production de ce document</b> <i>Identification of document production means</i>	
<b>Outils :</b> Microsoft Office Word  <i>Tools</i>	<b>Fichier :</b> Secure Dev and Op Environment_3 013 962A_NSR.doc  <i>File</i>



## TABLE DES MATIERES

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION</b> .....	<b>5</b>
1.1	Purpose .....	5
1.2	Constraints and assumptions .....	5
1.3	Definitions and abbreviations .....	6
1.3.1	<i>Definitions</i> .....	6
1.3.2	<i>Abbreviations</i> .....	6
1.4	Creation and update of this document.....	7
<b>2</b>	<b>REFERENCE DOCUMENTS</b> .....	<b>8</b>
2.1	NRC requirements and guidance documents .....	8
2.2	Rolls-Royce documents.....	8
2.2.1	<i>Physical and information technology (IT) security</i> .....	8
2.2.2	<i>Quality Management System (QMS)</i> .....	9
2.2.3	<i>Generic SPINLINE 3 platform software life cycle plans and related documents</i> .....	10
2.2.4	<i>Plant-specific SPINLINE 3 application software and system life cycle plans</i> .....	11
2.2.5	<i>Rolls-Royce supporting software processes</i> .....	12
<b>3</b>	<b>GENERIC SPINLINE 3 DESIGN AND SOFTWARE LIFE CYCLE PROCESS FEATURES THAT SUPPORT A SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT</b> .....	<b>14</b>
<b>4</b>	<b>SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT ACTIVITIES IN THE SPINLINE 3 LIFE CYCLE</b> ...	<b>16</b>
4.1	Concept phase.....	18
4.2	Basic design phase: Requirements specification .....	18
4.3	Basic design phase: System design.....	19
4.4	Detailed design phase .....	19
4.4.1	<i>Software Design</i> .....	20
4.4.2	<i>Coding</i> .....	20
4.4.3	<i>Software Integration</i> .....	21
4.4.4	<i>Software Validation</i> .....	21
4.5	Production phase.....	21
4.6	System integration and validation phase.....	22
4.7	Acceptance by customer and authorities phase.....	22
4.8	Operations and maintenance phases.....	23
4.9	Retirement phase .....	23
4.10	Transverse activities affecting all life cycle phases .....	23
4.10.1	<i>Quality Management System</i> .....	23
4.10.2	<i>Configuration Management System</i> .....	24
4.10.3	<i>Physical and IT Security</i> .....	24
<b>5</b>	<b>RESPONSIBILITIES</b> .....	<b>26</b>
<b>6</b>	<b>VULNERABILITY ASSESSMENT AND RISK MANAGEMENT</b> .....	<b>27</b>
6.1	Vulnerability assessment for the Rolls-Royce factory in Meylan, France .....	27
6.2	Vulnerability assessment for a plant-specific SPINLINE 3 system installed at a Licensee's facility .....	28
<b>7</b>	<b>REVIEWS AND AUDITS</b> .....	<b>29</b>
<b>8</b>	<b>TRAINING</b> .....	<b>30</b>
8.1	General training for Rolls-Royce employees.....	30
8.2	Specific training related to acceptable software life cycle processes.....	30
8.3	General training for contractors and external personnel .....	30
<b>9</b>	<b>RECORDS RETENTION AND HANDLING</b> .....	<b>31</b>



**Rolls-Royce**

10 REFERENCES.....32



## 1. INTRODUCTION

### 1.1 Purpose

The generic **SPINLINE 3** digital instrumentation and control (I&C) platform hardware and software and the associated life cycle processes described in the Licensing Topical Report (LTR, Ref. 1) have been developed by Rolls-Royce as the basis for building customized, high-integrity safety I&C systems for nuclear power plants. A plant-specific system built on this platform requires development of application software that is integrated with the generic platform software using well-defined software life cycle processes. A plant-specific system is integrated and factory tested in Rolls-Royce facilities before being delivered to a Licensee's site for installation, site acceptance testing, and operation.

Requirements for a secure development and operational environment for digital safety I&C systems are defined in Regulatory Guide 1.152 (Ref. 2), which includes a set of regulatory positions that describe a method that the NRC staff deems acceptable for complying with the Commission's regulations for promoting high functional reliability and design quality for the use of digital computers in safety systems of nuclear power plants. In Regulatory Guide 1.152, the NRC notes the following:

“...these regulatory positions are specifically concerned with the access controls and protective measures applied to the development of digital safety systems and with the ability of security features within the system to maintain system integrity and reliability in the event of inadvertent operator actions and undesirable behavior of connected equipment. This guide should not be used to address the ability of those security features to thwart malicious cyber attacks.”

This document describes how security features at the Rolls-Royce factories are employed along with quality and software life cycle processes to establish and maintain a secure development environment for the generic **SPINLINE 3** platform and for the future development of plant-specific **SPINLINE 3** systems. This document also identifies generic **SPINLINE 3** design and software life cycle process features that will support a Licensee in establishing a secure operational environment for a plant-specific system installed and operated at a nuclear power plant.

This is not intended as a stand-alone document. Instead, this document serves as a roadmap that makes liberal references to the **SPINLINE 3** LTR (Ref. 1) and other pertinent documents that contain the security, quality, and software life cycle process details that support the summary descriptions in this document of how compliance with specific Regulatory Guide 1.152 requirements is accomplished.

A summary Regulatory Guide 1.152 compliance matrix is provided in Appendix A. Vulnerability assessments of the secure development environments at the Rolls-Royce factories in France and in the US are provided separately in Rolls-Royce document 3 014 543 A (Ref. 3).

### 1.2 Constraints and assumptions

Regulatory Guide 1.152 (Ref. 2) includes regulatory positions 2.1 to 2.5 that provide specific guidance concerning security activities during the pre-operational phases of the life cycle of computer-based safety systems. “Security,” in the context of Regulatory Guide 1.152, refers to protective actions taken against a predictable set of nonmalicious acts that could challenge the integrity, reliability, or functionality of a digital safety system. For example, such protective actions include:

- Measures applied throughout the development life cycle of the system to prevent unauthorized, unintended, and unsafe modifications to the system, such as:
  - control of physical and logical access to the safety system and its data, and
  - controls to prevent inadvertent introduction of undocumented code or unwanted functions or applications
- The ability to maintain system integrity and reliability during operation and maintenance in the event of:
  - inadvertent operator actions, or
  - undesirable behavior of connected equipment.

This document does not address “cyber security”, which refers to those measures and controls taken in accordance with 10 CFR 73.54 (Ref. 4) to protect digital systems against the malicious acts of an intelligent



adversary. Cyber security is not addressed in Regulatory Guide 1.152 or in the Rolls-Royce licensing application for the generic **SPINLINE 3** digital safety I&C platform. As noted in Regulatory Guide 1.152, security controls applied to the latter phases of the lifecycle that occur at a Licensee's site (i.e., site installation, operation, maintenance, and retirement) are not part of the 10 CFR 50.55a (Ref. 5) licensing process and fall under the purview of other Licensee programs.

## 1.3 Definitions and abbreviations

### 1.3.1 Definitions

The following definitions are important for understanding the scope and applicability of this document and the associated vulnerability assessment (Ref. 3).

Computer	The term "computer" identifies a system that includes computer hardware, software, firmware, and interfaces (RG 1.152)
Computer security	Computer security includes the protection of digital computer-based systems throughout the development lifecycle of the system to prevent unauthorized, unintended and unsafe modifications to the system. Measures should be taken to protect safety systems during development, operation, and maintenance from inadvertent actions that may result in unintended consequences to the system. Computer security includes the protection of both physical and logical access to the safety system and its data such that controls should be provided to prevent unauthorized changes. Controls should address access via network connections and access via maintenance equipment. Additionally, the design of the plant data communication systems should ensure that the systems do not present an electronic path by which a person can make unauthorized changes to plant safety systems or display erroneous plant status information to the operators. (RG 1.152)
Cyber Security	Those measures and controls taken as part of compliance with 10 CFR 73.54 that protect digital systems against the malicious acts of an intelligent adversary (RG 1.152)
Nonmalicious act	Inadvertent operator actions or the undesirable behavior of connected systems. (RG 1.152)
Security	In the context of Regulatory Guide 1.152, refers to protective actions taken against a predictable set of nonmalicious acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system. (RG 1.152)

### 1.3.2 Abbreviations

The following abbreviations are used in this document.

Acronym	Definition
CM	Configuration Management
EEPROM	Electrically Erasable Programmable Read Only Memory
FAT	Factory Acceptance Test
FEPRM	Flash Erasable Programmable Read Only Memory
I/O	Input / output
IT	Information Technology
I&C	Instrumentation and Control



Acronym	Definition
LAN	Local Area Network
LAR	License Amendment Request
LDU	Local Display Unit
LTR	Licensing Topical Report
NPP	Nuclear Power Plants
OSS	Operational System Software
QMS	Quality Management System
SAT	Site Acceptance Test
SDD	Software Design Document
SRS	Software Requirement Specification
SSDE	System and Software Development Environment
V&V	Verification and Validation
SVVP	Software Verification and Validation Plan
SVTP	Software Validation Test Plan
SVTR	Software Validation Test Report
WAN	Wide Area Network

#### 1.4 Creation and update of this document

In this document, double brackets (“[[ ]]”) denote security-related sensitive information to be withheld from public disclosure pursuant to the guidance in NRC Regulatory Issue Summary 2005-31, “Control of Security-Related Sensitive Unclassified Non-safeguards Information Handled by Individuals, Firms, and Entities Subject to NRC Regulation of the Use of Source, Byproduct and Special Nuclear Material”, dated 22 December 2005. In the “secure” edition of this document, the two brackets denoting the end of segment containing security-related sensitive information may appear one or more pages following the bracket indicating the start of the segment containing security-related sensitive information. In the “public” edition of this document, the material within the brackets is removed.

The document is updated only when a change, which affects security, in the design of the generic **SPINLINE 3** digital safety I&C platform or the associated security, quality, or software life cycle processes affect compliance with Regulatory Guide 1.152 (Ref. 2), as documented herein.



## 2 REFERENCE DOCUMENTS

### 2.1 NRC requirements and guidance documents

Regulatory Guide 1.152 (Ref. 2) defines the NRC’s requirements for establishment of a secure development and operational environment for digital safety systems, including:

- Protection of the development environment against the inclusion of unwanted and undocumented code
- Protection of the digital safety system in the operational environment against:
  - Effects of undesirable behavior of connected systems
  - Inadvertent (non-malicious) access to the system

Regulatory Guide 1.152 Regulatory Positions 2.1 to 2.5 require that the digital safety system development process should identify and mitigate potential vulnerabilities in each phase of the digital safety system life cycle.

The description of the secure development and operational environment in the Rolls-Royce factories is organized based on the software life cycle phases for developing a plant-specific **SPINLINE 3** system. The generic **SPINLINE 3** platform software already has been developed and is in the maintenance phase of its life cycle. The associated vulnerability assessment (Ref. 3) also is organized based on the software life cycle phases for developing a plant-specific **SPINLINE 3** system

### 2.2 Rolls-Royce documents

This section identifies the Rolls-Royce security, quality, and software life cycle process documents that define the processes for establishing and maintaining a secure development environment in the Rolls-Royce factories.

#### 2.2.1 Physical and information technology (IT) security

Rolls-Royce factories are secure facilities. The two factories associated with delivery of a plant-specific **SPINLINE 3** system to a U.S. Licensee are the factories in Meylan, France and Huntsville, Alabama, USA.

- The factory in Meylan, France currently is the primary location for design and development of the generic **SPINLINE 3** platform hardware and software. This factory contains the **SPINLINE 3** software development environment. In addition, this factory is the primary location where a plant-specific **SPINLINE 3** system will be designed, developed, integrated, and factory tested.
- The factory in Huntsville, Alabama, USA also can be used for staging and factory testing a plant-specific **SPINLINE 3** system prior to delivery to the Licensee’s site for installation and site acceptance testing. Currently, there is no **SPINLINE 3** software development environment at the Huntsville factory.

Rolls-Royce documents governing physical and IT security are identified below:

#### Physical security

Document	Purpose
Physical Security, SMSPOL005, Revision 2	Establish the basic standards for physical security at a Rolls-Royce factory

#### IT security

II

<p><b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b></p>
---



**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]

**2.2.2 Quality Management System (QMS)**

As described in Chapter 1 of the LTR (Ref. 1), both the Meylan, France factory and the Huntsville, Alabama, USA factory operate under quality management systems that comply with the requirements of 10 CFR Part 50 Appendix B (Ref. 6). The applicable quality plans are listed below:

- For Meylan: Rolls-Royce SAS Quality Manual (Ref. 7)
- For Huntsville: Instrumentation & Controls US Quality Manual (Ref 8)

A mapping of these Rolls-Royce quality plans and associated quality procedures to 10 CFR Part 50 Appendix B is provided in Chapter 3 of the LTR.

These basic quality programs include many procedures that contribute to establishing a secure development environment in the respective factories. For example, in the Meylan factory, the following quality procedures apply to activities that have a direct bearing on the **SPINLINE 3** secure development environment.

Document	Purpose
<ul style="list-style-type: none"> <li>• Principles for control of design (Safety Related systems only), 8 307 032 C</li> <li>• System Design (Safety Related systems only), 8 303 334 F</li> <li>• Control of Software Design (Safety Systems), 8 303 350 L</li> <li>• Quality Management System, 8 303 242 M</li> </ul>	Establish standard practices for control of design activities. This systematic process is intended to deliver consistent quality in design activities. The change management process manages changes to the design and establishes a barrier to unauthorized changes.



Document	Purpose
<ul style="list-style-type: none"> <li>Change Management process (technical changes), 8 303 197 L</li> <li>Software configuration management, 1 207 875 G</li> </ul>	<p>Establish change management processes, which define the reference configurations, known as the “baselines” for all configuration managed items, including software, software tools, and documents. The baseline is a measurement point that can be used to detect changes from an approved baseline.</p> <p>The CM system also establishes the framework for requirements traceability. This framework provides a means to detect unauthorized changes in requirements documents.</p>
<ul style="list-style-type: none"> <li>Control of Documents, 8 303 719 F</li> <li>Establishment of Technical documents, 8 303 198 Q</li> <li>Checking process for software documents, 1 207 947 E</li> </ul>	Establish consistent processes for managing quality documents. The configuration management process manages changes to these documents, and establishes a barrier to unauthorized changes.
<ul style="list-style-type: none"> <li>Control of Records, 8 303 320 M</li> </ul>	Establish practices for archiving records in a retrievable form.
<ul style="list-style-type: none"> <li>Nonconformity, 8 303 202 N</li> <li>Classified Nonconformities, 8 307 152 B</li> </ul>	Establish consistent processes for recording and handling nonconformities detected in work products.
<ul style="list-style-type: none"> <li>Audits, 8 303 239 N</li> </ul>	Establish a consistent process for auditing quality activities and confirming that quality processes are implemented as expected.
<ul style="list-style-type: none"> <li>Software quality control process, 8 303 634 D</li> <li>Software project management, 1 208 055 E</li> <li>Principles for control of design, safety systems, 8 307 032 C</li> <li>Control of Software Design (Safety Systems), 8 303 350 L</li> <li>Software impact analyses management, 8 307 034 C</li> </ul>	Establish standard practices for control of software design and development. This systematic process is intended to deliver consistent quality in the software products. The change management process manages changes to the software products and establishes a barrier to unauthorized changes.
<ul style="list-style-type: none"> <li>Checking upon receipt of external software, 8 303 671 B</li> <li>Requirements for software tools used for software development, 1 206 747 E</li> </ul>	Establish standard practices for inducting external software and tools for use on a software project. These processes protect against unauthorized changes to external software and tools.
<ul style="list-style-type: none"> <li>Training of Personnel, 8 303 321 J</li> <li>V&amp;V training plan, 1 208 210 C</li> </ul>	Establish requirements for quality system training for all employees and additional training for members of the independent V&V team

### 2.2.3 Generic **SPINLINE 3** platform software life cycle plans and related documents

The **SPINLINE 3** generic platform software was previously developed at the Rolls-Royce factory in Meylan, France and now is in the maintenance phase of its life cycle.

The documents listed below define the life cycle processes for the generic **SPINLINE 3** platform software. These processes supplement the basic QMS processes identified in Section 2.2.2. The **SPINLINE 3** software processes establish the development framework that is responsible for originally creating and maintaining the integrity of the generic **SPINLINE 3** platform software. These processes provide the means for detecting and correcting anomalies in the generic platform software, including anomalies resulting from unauthorized, unintended, and unsafe modifications.



Document	Purpose
<ul style="list-style-type: none"> <li>Software Quality Plan (SQP) - MC3, 8 303 429 E</li> <li>Software Modification Quality Plan, 1 208 686 B</li> <li>Software Quality Plan - SCADE Operator Library, 1 208 356 C</li> </ul>	Establish a consistent quality management processes tailored for the generic <b>SPINLINE 3</b> platform software and the associated SCADE library.
<ul style="list-style-type: none"> <li>Software Development Plan, 1 207 102 A</li> </ul>	Establish a consistent project management structure and process for the generic <b>SPINLINE 3</b> platform software and/or the associated SCADE library. For each new modification campaign, a new software development plan is written
<ul style="list-style-type: none"> <li>Software Configuration Management Plan for <b>SPINLINE 3</b> Software Sub-assemblies Managed by CM Tool, 1 208 878 E</li> </ul>	<p>Establish a consistent CM process for managing the generic <b>SPINLINE 3</b> platform software and/or the associated SCADE library. The current generic platform software baseline is a measurement point, which can be used to detect changes from an approved baseline.</p> <p>The CM system also establishes the framework for requirements traceability. This framework provides a means to detect unauthorized changes.</p>
<ul style="list-style-type: none"> <li>Rules for Verification and Validation of Software Components, 1 207 107 D</li> <li>(OSS) Software Validation Test Plan, 1 207 146 F</li> <li>(CD_LDU) Software Validation Test Plan 1 207 175 E</li> </ul>	Establish a consistent V&V process for the next modification campaign for the generic <b>SPINLINE 3</b> platform software and/or the associated SCADE library. The V&V records are part of the baseline for the current generic platform software. These V&V records support the ability to detect changes from an approved baseline.
<ul style="list-style-type: none"> <li>(OSS) Software Integration Test Plan and Report, 1 207 204 D</li> <li>(CD_LDU) Software Integration Test Plan and Report, 1 207 239 A</li> </ul>	Establish a consistent process for performing and reporting the results of software integration tests for the generic <b>SPINLINE 3</b> platform software. The integration test results are part of the baseline for the current generic platform software. These test records support the ability to detect changes from an approved baseline.

#### 2.2.4 Plant-specific SPINLINE 3 application software and system life cycle plans

The documents listed below define the life cycle processes for the development of plant-specific application software and the integrated system, through the site acceptance test (SAT) phase of the life cycle. These references are generic templates that will be completed as plant-specific software and system Plans that will be submitted to NRC as part of the Licensee’s License Amendment Request (LAR).

These processes establish the development framework that will be responsible for originally creating the plant-specific application software and integrating it with the generic **SPINLINE 3** platform software and the plant-specific hardware. These processes provide the means for detecting and correcting anomalies in plant specific software, including anomalies resulting from unauthorized, unintended, and unsafe modifications to the application software or the plant-specific configuration of the Operational System Software (OSS), which is part of the generic **SPINLINE 3** platform software.

The following documents define the life cycle processes for the plant-specific application software and the integrated system

Document	Purpose
<ul style="list-style-type: none"> <li><b>SPINLINE 3</b> Software Quality Assurance Plan – SQAP (generic template), 8 307 208 B</li> </ul>	Establishes a consistent quality management process tailored for development of plant-specific <b>SPINLINE 3</b> application software and configuration of the OSS.



Document	Purpose
<ul style="list-style-type: none"> <li><b>SPINLINE 3</b> Software Development Plan – SDP (generic template), 8 307 211 B</li> </ul>	Establish a consistent project management structure and process for development of plant-specific <b>SPINLINE 3</b> application software and configuration of the OSS.
<ul style="list-style-type: none"> <li><b>SPINLINE 3</b> Software Configuration Management Plan – SCMP (generic template), 8 307 209 B</li> </ul>	<p>Establish a consistent CM process for development of plant-specific <b>SPINLINE 3</b> application software and configuration of the OSS. The software baseline established by the CM system is a measurement point, which can be used to detect changes from an approved baseline.</p> <p>The CM system also establishes the framework for requirements traceability. This framework provides a means to detect unauthorized changes.</p>
<ul style="list-style-type: none"> <li><b>SPINLINE 3</b> Software Validation &amp; Verification Plan – SVVP (generic template), 8 307 210B</li> </ul>	Establish a consistent V&V process for development of plant-specific <b>SPINLINE 3</b> application software and configuration of the OSS. This V&V process provide an independent means to ensure the complete and correct implementation of the intended design and to detect anomalies in the software prior system acceptance by the Licensee.
<ul style="list-style-type: none"> <li>System Integration and Factory Test Plan (generic template), 8 307 245 A</li> <li>System Installation and Site Test Plan (generic template), 8 307 243 A</li> </ul>	Establish factory acceptance test (FAT) and site acceptance test (SAT) processes for a plant-specific <b>SPINLINE 3</b> system. These tests provide a means to detect anomalies in the integrated system prior to acceptance by the Licensee.
<ul style="list-style-type: none"> <li>System Training Plan (generic template), 8 307 242 A</li> </ul>	Establish training requirements for the Licensee’s staff, including training on security-related features of the plant-specific <b>SPINLINE 3</b> system. This training is intended to prepare the Licensee for maintaining a secure operational environment following system installation and acceptance at the Licensee’s facility.
<ul style="list-style-type: none"> <li>System Operations &amp; Maintenance Plan (generic template), 8 307 244 A</li> </ul>	Establish the operations and maintenance practices to be implemented by Licensee’s staff, including operation and maintenance security-related features of the plant-specific <b>SPINLINE 3</b> system. This standardized operations and maintenance processes will assist the Licensee in maintaining a secure operational environment following system installation and acceptance at the Licensee’s facility.

**2.2.5 Rolls-Royce supporting software processes**

The documents listed below establish a variety of standard processes that contribute to the integrity of the **SPINLINE 3** software, associated documentation, and software tools.

Document	Purpose
<ul style="list-style-type: none"> <li>Software Guideline: C programming rules, 1 205 955 D</li> <li>Software Guideline: C programming rules: synthesis [IL_Prog_C], 1 208 954 C</li> <li>Defensive programming application rules [IL_Prog_Def], 1 208 605 C</li> <li>Definition of algorithm description language, 1 206 623 B</li> <li>Software Guideline: SCADE Design Rules, 1 208 250 F</li> </ul>	Establish standards for doing programming and using software tools in connection with modifying the generic <b>SPINLINE 3</b> platform software or developing plant-specific application software. These standards contribute to the integrity of the respective software products. In addition, peer reviewers and V&V staff know what to expect in the software products and are better able to detect anomalies that do not confirm to the standard software practices.



Document	Purpose
<ul style="list-style-type: none"> <li>• Identification rules and self supervision for programming hardware components, 1 203 540 D</li> <li>•</li> </ul>	
<ul style="list-style-type: none"> <li>• Establishment and application of engineering documents, 8 303 198 Q</li> <li>• Establishment of manufacturing and test documents, 8 303 217 M</li> <li>• Establishment of test &amp; factory reports, 8 303 228 J</li> <li>• Software Guideline - Documentation Guidelines, 1 207 853 E</li> <li>• Software Guideline - SRS Documentation Guideline, 1 207 854 C</li> <li>• Guide for writing a SDD - SW Design Description, 1 207 855 B</li> <li>• Guide for writing a SW Development File, 1 208 607 B</li> <li>• SW Integration Test File - Documentation Guideline, 1 207 857 C</li> <li>• Guide for writing a SVTP, 1 207 858 B</li> <li>• Guide for writing a SVTR, 1 207 859 B</li> <li>• Guide for writing a SVTPR, 1 208 535 A</li> <li>• Guide for writing a SMF GI - SW Manufacturing File - Generation Instruction, 1 207 860 C</li> <li>• Guide for writing a SMF PI - SW Manufacturing File - Programming Instruction, 1 207 861 B</li> <li>• Guide for writing a SUD - SW User Documentation, 1 207 862 B</li> <li>• Guide for writing a SCMR - SW Configuration Management Report, 1 207 863 C</li> <li>• Guide for writing a LSD - List of SW Document, 1 207 864 B</li> <li>• Guide for writing a LTLUS - List of Tools and Library Used for SW, 1 207 865 B</li> <li>• Software Document Evaluation Process, 1 207 947 E</li> </ul>	<p>Establish standards for originally preparing documentation for the generic <b>SPINLINE 3</b> platform software or plant-specific application software. These standards contribute to the integrity of the respective documentation. In addition, peer reviewers and V&amp;V staff know what to expect in the documentation and are better able to detect anomalies that do not confirm to the standard documentation practices.</p>
<ul style="list-style-type: none"> <li>• Software Guideline: Requirements on tools used for software development, 1 206 747 8</li> <li>• Checking upon receipt of external software, 8 303 671 B</li> </ul>	<p>Establish standards for inducting tools and commercial software into the factory for use in the secure development environment. These practices protect against the unauthorized introduction of tools, including tools that may contain malware.</p>
<ul style="list-style-type: none"> <li>• Source code static analysis process using QA-C, 8 307 104 B</li> </ul>	<p>Establish standard practices for performing static code analysis, which has the capability to detect anomalies in the code. This helps ensure the effectiveness of the static analysis.</p>



### 3 GENERIC *SPINLINE 3* DESIGN AND SOFTWARE LIFE CYCLE PROCESS FEATURES THAT SUPPORT A SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT

The generic *SPINLINE 3* platform has been designed as the foundation for plant-specific digital safety I&C systems that will implement nuclear safety functions. The design of the generic *SPINLINE 3* platform and the application software life cycle processes applied through the factory test phase also establish a secure development and operational environment that strengthens security functions by:

- providing protection against unauthorized, unintended, and unsafe modifications to the system, and
- implementing design requirements that promote integrity and reliability during operation and maintenance in the event of inadvertent operator actions or undesirable behavior of connected equipment.

The main *SPINLINE 3* features that support a secure development and operational environment are summarized below.

- The generic *SPINLINE 3* hardware platform is a highly-reliable foundation for a digital safety I&C system.
  - Board / device-level failure mode and effects analyses and reliability analyses predict high reliability. Refer to LTR Section 5.2 (Ref. 1) for details.
  - Operational experience demonstrates high reliability from installed *SPINLINE 3* systems and earlier generations of Rolls-Royce digital safety I&C systems.
- Software life cycle processes are in place at the Rolls-Royce factory to ensure production of high-integrity, high-reliability software for *SPINLINE 3* systems.
  - Refer to LTR Section 6.2 for a description of the life cycle processes that apply to the generic platform software and to LTR Section 6.4 for the corresponding life cycle processes for the plant-specific application software.
  - Strict software design control processes are in place.
  - Writing guides for software life cycle documentation ensure the systematic production of the comprehensive documentation for safety system software.
  - Configuration management (CM) system and records provide the framework for implementing requirements traceability. Together, the CM and requirements traceability processes define the approved software baseline and provide the means to detect authorized and unauthorized modifications to that baseline.
  - V&V activities provide an independent capability to detect unauthorized modification of software components and baselines.
  - Testing activities provide the means to demonstrate that design requirements, including security requirements, have been implemented in the plant-specific system.
- *SPINLINE 3* software does not include unwanted functions.
  - The Operational System Software (OSS) performs only limited functions; primarily those associated with initialization, self-diagnostic tests, and management of interfaces with input/output (I/O) boards and networks and the application software. The OSS is configured for a plant-specific application, but does not require any change to the OSS baseline. See LTR Section 4.4.3 for details.
  - The plant-specific application software is a simple software module that receives data, performs specific calculations, and returns results to the OSS. See LTR Section 4.4.5 for details.
- The integrity of the production code in a *SPINLINE 3* system is checked upon initialization and at the beginning of each processing cycle.
  - The *SPINLINE 3* platform software and application software is loaded on flash memory chips as executable code on the UC25+ processor boards.
  - At initialization after manual reset by an operator and then at beginning of each processing cycle, the checksum is calculated and regularly checked by the OSS, which verifies that the checksum generated for the executable code in memory is correct. This covers the application specific code, the OSS code, and the configuration parameters.



- The production code cannot be changed in the field without replacing the flash memory chips holding the code.
  - Updating this software requires replacing the flash memory chips.
  - A UC25+ processor board must be removed from its rack to replace the flash memory chip on the board. The processor boards are not hot-swappable, so the rack must be powered off.
  - Access to **SPINLINE 3** systems to remove a UC25+ processor board is limited to one channel at a time by administrative controls. Access to a cabinet (i.e., door open) is alarmed by the **SPINLINE 3** system.
  
- There are no provisions for remote access to a **SPINLINE 3** system:
  - The NERVIA digital communications network is used to implement data communication within the safety system and with other systems outside the safety system. It implements a proprietary protocol, which does not allow for any dynamic modification of the communication scheme established and validated during design.
  - NERVIA software can enforce one-way communication via fiber optic cabling to other divisions or external systems. One-way communications will be implemented with a hardware solution. These features are major contributors in making the system secure and preventing external systems from influencing the behavior of a **SPINLINE 3** safety system.
  
- Only local access is available for maintenance and testing of a **SPINLINE 3** system.
  - The front-panel CPU 25 serial links used for maintenance and testing by means of the Local Display Unit (LDU) implement proprietary protocols and require physical access to the SPINLINE 3 cabinets.
  - The potential for operator error during maintenance and testing is reduced by limiting the allowable actions that can be taken locally and including controls over those actions. For example:
    - Setpoints that can be modified on site by the operator and the allowable range for such modifications are defined during the design of the I&C system. Allowable setpoint changes will be made using the **SPINLINE 3** LDU.
    - Access to **SPINLINE 3** systems to make setpoint changes is limited to one channel at a time by administrative controls. Access to a cabinet (i.e., door open) is alarmed by the **SPINLINE 3** system.
    - Access to setpoints modification using the **SPINLINE 3** LDU is protected by a password stored in the UC25+ parameter EEPROM.
    - Setpoint values are checked to be within a predefined range defined during the design of the I&C system.
  
- Access to the Rolls-Royce development environment in Meylan, France is protected.
  - Access to the factory, the factory LAN, the development environment, quality records, and the configuration management system are restricted in accordance with internal procedures (see Section 2.2).
  - This development environment is connected to the factory LAN and is protected in accordance with Rolls-Royce IT procedures.



#### 4 SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT ACTIVITIES IN THE *SPINLINE 3* LIFE CYCLE

Regulatory Guide 1.152 (Ref. 2) defines a set of life cycle phases for a digital safety I&C system. The similar life cycle process used by Rolls-Royce for development of a plant-specific *SPINLINE 3* system is described in the quality procedure entitled “Principles for Control of Design (safety systems)” and illustrated in Figure 4-1

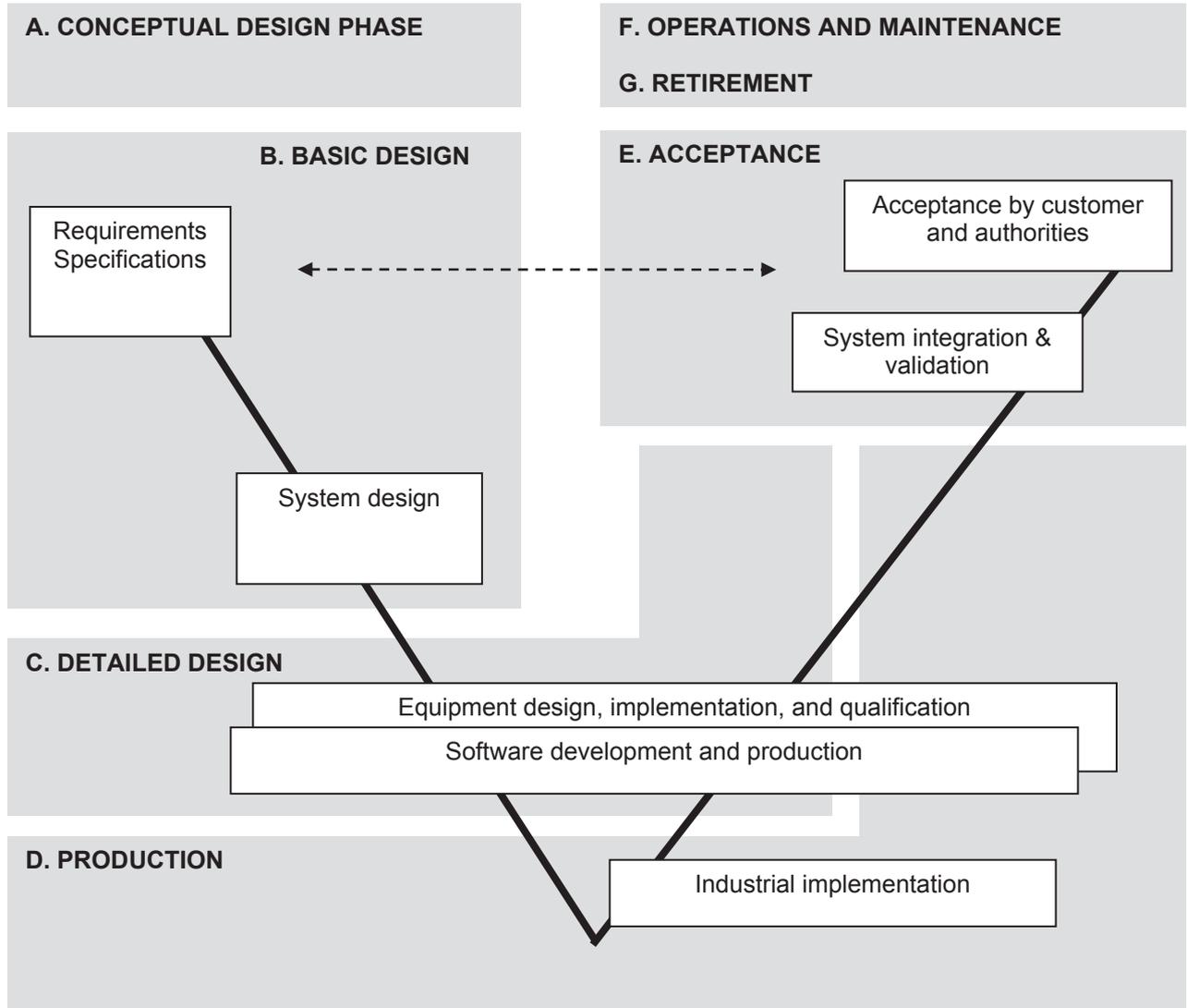
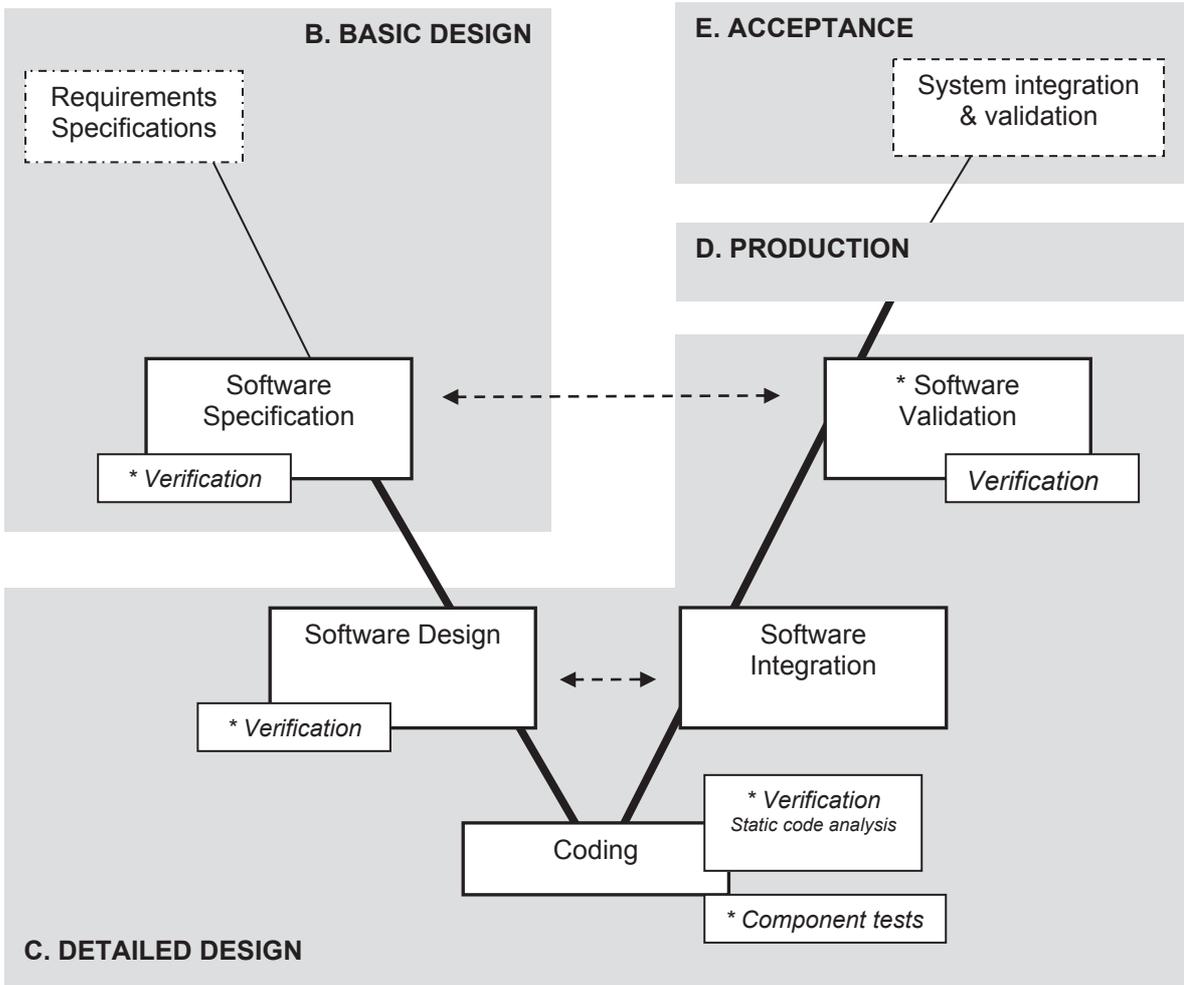


Figure 4-1 - Rolls-Royce System Life Cycle Process

The quality procedure “Principles for Control of Design (safety systems)” further links the system life cycle process with the software life cycle process, as shown in Figure 4-2. Tasks identified by (\*) are conducted by an independent verification & validation (V&V) team. This software life cycle process for a plant-specific *SPINLINE 3* system is further detailed in the Software Quality Assurance Plan (generic template) that is intended to be used to produce the plant-specific SQAP.



**Figure 4-2 - Rolls-Royce Software Life Cycle Process and Link to the System Life Cycle Process**

The alignment between the **SPINLINE 3** system and software life cycle phases with the life cycle phases identified in Regulatory Guide 1.152 (Ref. 2) is shown in Table 4-1.



**Table 4-1 - Alignment between *SPINLINE 3* system and software life cycle phases and life cycle phases in Regulatory Guide 1.152**

Rolls-Royce Application System Life Cycle Phases (Refer to Figure 4-1)	Rolls-Royce Application SW Life Cycle Phases (Refer to Figure 4-2)	Responsibility	Reg. Guide 1.152 Life Cycle Phases
Concept		Licensee with possible involvement of Rolls-Royce	Concepts
Basic Design: Requirements Specification	Basic Design: Software Specification	Rolls-Royce	Requirements
Basic Design: System Design		Rolls-Royce	Design
Detailed Design	Detailed Design: Software Design Coding Software Integration Software Validation	Rolls-Royce	Implementation
Production		Rolls-Royce	
System Integration and Validation		Rolls-Royce	Test
Acceptance by customer and authorities	Acceptance: System integration & validation	Rolls-Royce with turnover to the Licensee	Installation, Checkout & Acceptance Testing
Operation		Licensee	Operation
Maintenance		Licensee	Maintenance
Retirement		Licensee	Retirement

In addition, the following activities that contribute to a secure development and operational environment are performed in a transverse manner across all life cycle phases:

- Quality assurance, including the QA records management system
- Configuration management
- Physical security and IT security management

These transverse activities are discussed in Section 4.10.

The integration of secure development and operational environment activities with *SPINLINE 3* life cycle activities is described in the following sections. A summary Regulatory Guide 1.152 compliance matrix organized by life cycle phases is provided in Appendix A.

#### 4.1 Concept phase

The Licensee may take responsibility for the concept phase and develop the functional specifications (i.e., a bid specification) for a plant-specific safety I&C system, including functional security attributes related to a establishing and maintaining a secure development and operational environment. Rolls-Royce can support the concept phase if requested by the Licensee.

#### 4.2 Basic design phase: Requirements specification

For a typical project to deliver a *SPINLINE 3* digital safety I&C system, this is the life cycle phase where Rolls-Royce first gets involved.

In the requirements specification phase shown in Figure 4-1, Rolls-Royce expands on the functional requirements developed in the concept phase and develops the System Specification for the plant-specific *SPINLINE 3* application. The System Specification defines the system configuration, including all interfaces



with external systems. Requirements related to a establishing and maintaining a secure development and operational environment are embedded in the System Specification.

As part of the effort to develop the System Specification, a Security Requirements Analysis is performed. This analysis identifies the following:

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]

#### 4.3 Basic design phase: System design

The software life cycle starts during this phase. Throughout this phase and the design, coding, integration, and software manufacturing activities in subsequent phases, all activities are subject to strict design controls, configuration management, and independent V&V.

In the system design phase shown in Figure 4-1, the requirements identified at the system level in the previous phase are developed into specific hardware and software requirements. These requirements are captured in the Hardware Design Specification and Software Requirement Specification (SRS). The SRS is prepared in accordance with established documentation guidelines (Software Guideline: SRS Documentation Guideline, 1 207 854 C). The SRS is a configuration managed document that is subject to independent V&V, which includes confirmation of the correctness and completeness of requirements.

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]

The end-of-phase software baseline and associated documentation are captured in the CM system. Document retention is addressed in Section 8.

#### 4.4 Detailed design phase

As shown in Figure 4-2, software activities in the Detailed Design Phase encompass the following:

- Software Design,
- Software Coding,
- Integration,
- Software Validation

These activities are addressed below.

As notes previously, the software life cycle processes are subject to strict design controls, configuration management, and independent V&V. The end-of-phase software baseline and associated documentation are captured in the CM system. Document retention is addressed in Section 8.



#### 4.4.1 Software Design

In the design phase shown in Figure 4-2, Rolls-Royce develops the Software Design Descriptions (SDDs) for the plant-specific **SPINLINE 3** application. The SDDs expand on the requirements in the SRS and define the final system design, including features related to a secure operational environment and all interfaces with external systems. The SDDs include the plant-specific application design and the configuration of the generic platform software. The SDDs are configuration managed documents that are prepared in accordance with established guidance (Guide for writing a SDD: SW Design Description, 1 207 855 B) and are subject to independent V&V to confirm completeness and correctness.

The CM system and records provide the framework for implementing requirements traceability. Together, these processes define the approved software baseline and provide the means to detect authorized and unauthorized modifications to that baseline.

[[

**Security-Related Information Withheld in Accordance with 10 CFR 2.390**

]]

#### 4.4.2 Coding

The coding phase shown in Figure 4-2 is performed only for safety-related components developed manually, using a programming language such as the “C”. Approved tools and libraries to be used in the coding phase are designated in a “List of Tools and Library Used for Software”, which is a QMS record.

Coding activities and tool use are guided by standard practice guides intended to improve the consistency of coding and code documentation, and thereby contribute to the integrity of the software being produced for a plant-specific application. These guidance documents include:

- Software Guideline: C programming rules, 1 205 955 D
- Software Guideline: C programming rules: synthesis [IL\_Prog\_C], 1 208 954 C
- Defensive programming application rules [IL\_Prog\_Def], 1 208 605 C
- Software Guideline: SCADE Design Rules, 1 208 250 F
- Definition of algorithm description language, 1 206 623 B
- Identification rules and self supervision for programming hardware components, 1203540 E

Various code analyses and code documents are prepared in this phase, including software development files, which are prepared in accordance with established guidance (Guide for writing a SW Development File, 1 208 607 B). The software development files include the results of software component tests. As shown in Figure 4-2, coding is subject to independent verification and static code analysis, which is performed in accordance with established guidance (Source code static analysis process using QA-C, 8 307 104 B).

The CM system captures the software baseline, which is comprised of the most recent approved versions of the following:

- The software executable and all the source code needed to create the executable software,
- All other managed elements related to the software (documents, data, etc.),
- Testing reference elements (test files)

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]



#### 4.4.3 Software Integration

For **SPINLINE 3** based equipment, the integration phase shown in Figure 4-2 consists of automated generation of the executable code, download of this code into the processing unit, and a check of the behavior of the main functions of the processing unit. Integration testing records are prepared in accordance with established guidance (SW Integration Test File: Documentation Guideline, 1 207 857 C). [[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]

#### 4.4.4 Software Validation

In the validation phase shown in Figure 4-2, the software V&V team validates each individual software on their hardware target, including any security requirements identified in the Software Requirement Specification (SRS) and expanded in the Software Design Descriptions (SDDs). Plans and reports for this testing are prepared in accordance with the following guides:

- Guide for writing a Software Validation Test Plan (SVTP), 1 207 858 B
- Guide for writing a Software Validation Test Report (SVTR), 1 207 859 B

This testing validates that the **SPINLINE 3** application, as implemented, is complete and correct. Validation testing provides an independent capability to detect abnormal behavior of the code. An investigation of the root cause of abnormal behavior has the capability to detect undocumented code, malicious code, and other unwanted and undocumented functions that can affect the reliable operation of the code.

The V&V activity for the “end of software project” phase consists of the following:

- Writing the technical V&V section of the “End of Project” report, which includes a qualitative evaluation of the V&V activity, based on the verification and anomaly reports
- Writing the managerial V&V section of the “End of Project” report, which includes a quantitative evaluation of the V&V effort, including person-months per phase, costs, actual versus planned
- Completing the V&V final report by including the verification and anomaly reports verifying that all verification and anomaly reports are closed and dealt with appropriately
- Performing and verifying the archiving of the configuration items generated by the development and V&V processes
- Verifying the List of Software Documents (LSD)
- Verifying the Software Configuration Management Report (SCMR)

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]

The end-of-phase software baseline and associated documentation are captured in the CM system. Document retention is addressed in Section 8.

#### 4.5 Production phase

The production phase shown in Figure 4-1 includes industrial implementation of the designed hardware and software items and checks of compliance of the produced items.

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]



To program EEPROMs with executables code files, the Production Team uses the Software Manufacturing File – Programming Instruction document (one document per software), which have been prepared in accordance with the following guides:

- Guide for writing a SMF GI: SW Manufacturing File - Generation Instruction, 1 207 860 C
- Guide for writing a SMF PI: SW Manufacturing File - Programming Instruction, 1 207 861 B

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]

The end-of-phase software baseline and associated documentation are captured in the CM system. Document retention is addressed in Section 8.

#### **4.6 System integration and validation phase**

The system integration and validation phase shown in Figure 4-1 is the system life cycle phase where the hardware and software are integrated and tested in accordance with a plant-specific System Integration and Factory Test Plan. This plant-specific Plan will be prepared in accordance with the generic System Integration and Factory Test Plan template, 8 307 245 A...

As described in this generic Plan template, Rolls-Royce tests and validates system features, including the cyber security features, during factory testing to ensure that the system adequately meets the requirements stated in the Hardware Requirements Specification and the Software Requirements Specification. These results are recorded in the test documentation, which also includes the validation of any hardware configurations, integrated software testing, integrated system test, software qualification tests, and the factory acceptance testing.

The security requirements and configuration items are part of the validation of the overall **SPINLINE 3** system and are reported as such.

#### **4.7 Acceptance by customer and authorities phase**

During this phase (as shown in Figure 4-1), the system transitions from being under development by Rolls-Royce to a system ready for operational use by the Licensee. These activities will be described in a plant-specific System Installation and Site Test Plan, which will be prepared in accordance with the generic System Installation and Site Test Plan template, 8 307 243 A. The objective of site acceptance testing is to validate the completeness and correctness of the physical and logical **SPINLINE 3** system, including security features, in the intended plant environment. Rolls-Royce ensures that the following activities are conducted during this phase: [[



<b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b>
--

## 4.8 Operations and maintenance phases

The start of the operations phase marks the end of the Rolls-Royce project to deliver the **SPINLINE 3** system to the Licensee. This phase involves use by the Licensee of the **SPINLINE 3** system in its intended operational environment performing its intended safety functions.

The Licensee has the lead responsibility for security during the operations and maintenance phases. Typically, the Licensee is responsible for implementing administrative controls at the NPP to manage operation and maintenance of the **SPINLINE 3** systems in accordance with the Operations and Maintenance Manuals.

If requested by the Licensee, this phase may involve Rolls-Royce support to the Licensee in a variety of areas, including:

- Support for certain periodic testing,
- Resolving operational anomalies with the system and/or the operating and maintenance procedures,
- Implementing software changes or other system changes that cannot be accomplished by the Licensee, and
- Managing hardware obsolescence

Software updates or system design changes may be required during the operations phase. Preparation of such software modifications are performed using the same system and software life cycle processes described in Sections 4.1 to 4.7.

The systematic process employed for managing changes to the **SPINLINE 3** systems accomplishes the following:

- A modification to a safety-related system does not reduce safety or security
- Unauthorized or inadvertent modification to **SPINLINE 3** systems are prevented.

Operating procedure updates are reviewed for correctness and usability as well as mitigation measures to ensure that unauthorized access to **SPINLINE 3** system software is prevented.

## 4.9 Retirement phase

The retirement phase marks the end of the life cycle of a system. The Licensee is responsible for planning and executing the retirement phase, subject to approval as needed by the NRC. A Retirement Management Plan should be prepared by the Licensee prior to the scheduled replacement of a **SPINLINE 3** systems. A License Amendment Request (LAR) may be required.

## 4.10 Transverse activities affecting all life cycle phases

### 4.10.1 Quality Management System

All quality activities are governed by the Rolls-Royce 10 CFR Part 50 Appendix B quality management system. The applicable quality plans are the following:



- For Meylan: Rolls-Royce SAS Quality Manual (Ref. 7)
- For Huntsville: Instrumentation & Controls US Quality Manual (Ref 8)

[[

**Security-Related Information Withheld in Accordance with 10 CFR 2.390**

]]

#### **4.10.2 Configuration Management System**

The governing documents for configuration management are identified in Section 2.2.

The CM system captures the software baseline, which is comprised of the most recent approved versions of the following:

- The software executable and all the source code needed to create the executable software,
- All other managed elements related to the software (documents, data, etc.),
- Testing reference elements (test files)

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]

#### **4.10.3 Physical and IT Security**

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**



**Rolls-Royce**

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]



## 5 RESPONSIBILITIES

The **SPINLINE 3** project team is responsible for developing the plant-specific application and integrating the complete software system, which is comprised of the configured generic platform software and the application software that was built from the pre-developed libraries and software tools. The roles and responsibilities of the primary members of the project team are listed below.

- The **Project Manager** (PM) is responsible for achieving the project objectives including security. The PM is the primary point of contact with the customer.
- The **Project Quality Assurance Manager** (QAM) is responsible for verifying that the system development activities, including the security activities, are performed in accordance with approved QA processes.
- The **Software Development Manager** (SDM) is responsible for achieving the software project objectives, including security.
- The **Software Verification and Validation Manager** (SVVM) is responsible for checking the correct implementation of security requirements in the software design.
- The **Software Quality Assurance Manager** (SQAM) is responsible for verifying that application software development activities, including software security activities, are performed in accordance with approved software QA processes.



## 6 VULNERABILITY ASSESSMENT AND RISK MANAGEMENT

Regulatory Guide 1.152 (Ref. 2) Regulatory Positions 2.1 to 2.5 require that the digital safety system development process should identify and mitigate potential security vulnerabilities in each phase of the digital safety system life cycle. The process for performing this vulnerability assessment is described in this section. The vulnerability assessment is in a separate document, 3 014 543 A (Ref. 3).

### 6.1 Vulnerability assessment for the Rolls-Royce factory in Meylan, France

A vulnerability assessment will be performed for the **SPINLINE 3** development environment at the Rolls-Royce factory in Meylan, France. There currently is no **SPINLINE 3** development environment at the Rolls-Royce factory in Huntsville, Alabama, USA. A vulnerability assessment will be performed for the **SPINLINE 3** development environment at the Rolls-Royce factory in Huntsville, Alabama prior to any **SPINLINE 3** project work being performed there.

The vulnerability assessment addresses the development environments for the generic **SPINLINE 3** platform software and future plant-specific application software and integrated systems.

- The **SPINLINE 3** generic platform software, which includes pre-developed libraries, is a mature software package that is in the maintenance phase of its software life cycle. The configuration management program is an important tool for ensuring the continuing integrity of the current baseline of the generic platform software. The development environment and the processes for modifying the generic platform software are in place at the Meylan factory
- A plant-specific **SPINLINE 3** system will be developed by Rolls-Royce under contract for a U.S. Licensee. The development environment and the processes for developing plant-specific application software and integrated systems are in place at the Meylan factory

This vulnerability assessment examines the nonmalicious threats that are appropriate for a factory development environment through completion of the Factory Acceptance Test (FAT). These nonmalicious threats are listed in Table 6-1.

**Table 6-1. Nonmalicious threats addressed in the vulnerability assessment**

[[

**Security-Related Information Withheld  
in Accordance with 10 CFR 2.390**

]]

The assessment identifies the mitigating measures in place to provide confidence that a secure development environment has been established and is being maintained at the Rolls-Royce factory. The results of this vulnerability assessment are presented in separate document, 3 014 543 A (Ref. 3).

## **6.2 Vulnerability assessment for a plant-specific *SPINLINE 3* system installed at a Licensee's facility**

The vulnerability assessment in 3 014 543 A (Ref. 3) does not address the secure operational environment at the Licensee's facility. As noted in Regulatory Guide 1.152 (Ref. 2), security controls applied to the latter phases of the lifecycle that occur at a Licensee's site (i.e., site installation, operation, maintenance, and retirement) are not part of the 10 CFR 50.55a (Ref. 5) licensing process and fall under the purview of other Licensee programs.

Using the vulnerability assessment in 3 014 543 A (Ref. 3) as a starting point, Rolls-Royce and the Licensee will extend the vulnerability assessment of the intended safety I&C system through the operational and maintenance phase at the Licensee's nuclear power plant.

This is a broader scope vulnerability assessment than the assessment presented in 3 014 543 A (Ref. 3), and should include the following additional threats that are unique to the operational environment at the nuclear power plant:

- Inadvertent access to the operational system at the nuclear power plant
- Unauthorized, unintended, or unsafe modifications to the software in the operational system
  - Setpoint changes and any other changes that normally can be made to the installed system
  - Replacement of the EEPROM in a processor board
- Inadvertent operator action
- Undesirable behavior from connected systems

The results of this plant-specific vulnerability assessment will be included as part of the Licensee's LAR.



## 7 REVIEWS AND AUDITS

Periodic quality reviews and audits are conducted in accordance with the requirements of the following quality and configuration management procedures:

- General QMS review and audit guidance:
  - Audits, 8 303 239 N
- Generic platform software review and audit guidance:
  - Section 11, “Monitoring Application of the Quality Plan” of the Software Modification Quality Plan, 1 208 686 B
- Application software review and audit guidance:
  - Section 6, “Reviews and Audits” of the Software Quality Assurance Plan (SQAP) (generic template), 8 307 208 B
  - Section 4.4, “Configuration Audits and Reviews” of the Software Configuration Management Plan (SCMP) (generic template), 8 307 209 B

These reviews and audits are tools for confirming that procedures for maintaining a secure development and operational environment are being properly implemented.



## 8 TRAINING

Training increases the awareness, knowledge, and responsibility of all internal and external personnel working at the Rolls-Royce factory or the Licensee's premises.

### 8.1 General training for Rolls-Royce employees

New Rolls-Royce employee induction includes the following:

- Background checks are made
- Human Resources issue of an "employee welcome pack" to new-hires on arrival, containing the corporate code of ethics and professional conduct and other documents that addresses security issues, including the correct use of IT resources.
- All employees must sign a receipt to signify that they have read these documents.
- Employment contracts contain a confidentiality agreement.
- Compulsory training is given to underscore the rules regarding ethics, confidentiality, integrity, security, and use of IT resources.

General security training is periodically conducted to reinforce good security behaviors.

### 8.2 Specific training related to acceptable software life cycle processes

Software staff is trained to use the Rolls-Royce software quality procedures identified in Section 2.

The V&V staff receive additional training in accordance with the "Software Guideline: Software V&V Team Training Plan", 1 208 210 C.

### 8.3 General training for contractors and external personnel

Contractor and external persons working at the Rolls-Royce factory are provided with a security briefing that includes the following:

- All external workers sign a confidentiality agreement.
- The training provided to Rolls-Royce staff is also given to all external personnel working on site.



## 9 RECORDS RETENTION AND HANDLING

Software electronic files, documentation, and security records are retained in accordance with the following documents:

- Basic records retention guidance is provided in Section XVII of the I&C France Quality Manual and procedure 8 303 320 M, Control of Records.
- The software files are regularly backed up and archived in accordance with procedure 1 204 971 G, Operating Rules of the Computer Center
- Configuration management records for a plant-specific **SPINLINE 3** system will be archived in accordance with Section 2.7 of the SCMP that will be created from the generic SCMP template, document 8 307 209 B.
- Rolls-Royce will retain security-related records in accordance with contractual requirements stipulated by the customer. If not otherwise stipulated, Rolls-Royce will maintain security-related records for the operating life of the system.

Quality Management System document records are under the control of different librarians/custodians than the code archives.



## 10 REFERENCES

1. Licensing Topical Report, 3 008 503 C, Rolls-Royce
2. Draft Regulatory Guide DG-1249, "Criteria for the Use of Computer Systems in Safety Systems of Nuclear Power Plants (Proposed Revision 3 of Regulatory Guide 1.152)", dated March 2010
3. *SPINLINE 3* Secure Development and Operational Environment Vulnerability Assessment, document 3 014 543 A, Rolls-Royce, 30 June 2011
4. 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks", USNRC
5. 10 CFR 50.55a, "Codes and Standards", USNRC
6. 10 CFR Part 50 Appendix B, "Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants"
7. "Rolls-Royce SAS Quality Manual", Document No. 8 303 186 P, Rolls-Royce, June 2009
8. "Instrumentation & Controls US Quality Manual", Revision C, Document 500-9600000-10, ICQ-005-C, Data Systems & Solutions, LLC, a member of the Rolls-Royce group, June 2009



**Appendix A - SPINLINE 3 Regulatory Guide 1.152 Compliance Matrix**

<b>Table A-1. SPINLINE 3 DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152) Compliance Matrix</b>					
<b>RG 1.152 Regulatory Position</b>	<b>RG 1.152 Life Cycle Phase</b>	<b>Corresponding Rolls-Royce Life Cycle Phase</b>	<b>Text of RG 1.152 Regulatory Positions 2.1 to 2.5</b>	<b>RG 1.152 R3 compliance of the SPINLINE 3 generic digital safety I&amp;C platform and associated life cycle processes</b>	<b>SPINLINE 3 interface criteria for NPP-specific digital safety I&amp;C applications</b>
2.1	Concepts Phase	Requirements Phase	In the concepts phase, the licensee and developer should identify safety system security capabilities that should be implemented. A licensee should describe these security design features as part of its application.	[ ]	
<b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b>					





**Table A-1. SPINLINE 3 DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152) Compliance Matrix**

RG 1.152 Regulatory Position	RG 1.152 Life Cycle Phase	Corresponding Rolls-Royce Life Cycle Phase	Text of RG 1.152 Regulatory Positions 2.1 to 2.5	RG 1.152 R3 compliance of the SPINLINE 3 generic digital safety I&C platform and associated life cycle processes	SPINLINE 3 interface criteria for NPP-specific digital safety I&C applications
2.2	Requirements Phase	Requirements Phase (continued)	<p>Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and nonsafety digital systems.</p> <p><b>System Features</b></p> <p>The Licensee and developer should define the security functional performance requirements and system configuration; interfaces external to the system; and the requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance.</p> <p>The security requirements intended to ensure reliable system operation should be part of the overall system requirements.</p> <p>Therefore, the verification and validation process of the overall system should ensure the correctness, completeness, accuracy, testability, and consistency of the system security requirements</p>		
				<b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b>	



Table A-1. SPINLINE 3 DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152) Compliance Matrix				
RG 1.152 Regulatory Position	RG 1.152 Life Cycle Phase	Corresponding Rolls-Royce Life Cycle Phase	Text of RG 1.152 Regulatory Positions 2.1 to 2.5	RG 1.152 R3 compliance of the SPINLINE 3 generic digital safety I&C platform and associated life cycle processes
			<p>Requirements specifying the use of predeveloped software and systems (e.g., reused software and commercial off-the-shelf (COTS) systems) should address the reliability of the safety system (e.g., by using predeveloped software functions that have been tested and are supported by operating experience)</p>	<p>SPINLINE 3 interface criteria for NPP-specific digital safety I&amp;C applications</p>
			<p><b>Development Activities</b></p> <p>During the development of requirements, measures should be taken to ensure that the requirements development processes and documentation are secure such that the system does not contain undocumented code (e.g., backdoor</p>	
				<p><b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b></p>



Table A-1. SPINLINE 3 DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152) Compliance Matrix				
RG 1.152 Regulatory Position	RG 1.152 Life Cycle Phase	Corresponding Rolls-Royce Life Cycle Phase	Text of RG 1.152 Regulatory Positions 2.1 to 2.5	RG 1.152 R3 compliance of the SPINLINE 3 generic digital safety I&C platform and associated life cycle processes
			coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system.	SPINLINE 3 interface criteria for NPP-specific digital safety I&C applications
2.3	Design Phase	Design Phase	<p><b>System Features</b></p> <p>The safety system security requirements identified in the system requirements specification should be translated into specific design configuration items in the system design description.</p> <p>The safety system security design configuration items intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems.</p>	
<b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b>				







**Table A-1. SPINLINE 3 DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152) Compliance Matrix**

RG 1.152 Regulatory Position	RG 1.152 Life Cycle Phase	Corresponding Rolls-Royce Life Cycle Phase	Text of RG 1.152 Regulatory Positions 2.1 to 2.5	RG 1.152 R3 compliance of the SPINLINE 3 generic digital safety I&C platform and associated life cycle processes	SPINLINE 3 interface criteria for NPP-specific digital safety I&C applications
			<p>The developer should ensure that the transformation of the security design configuration items from the system design specification are correct, accurate, and complete.</p>		
			<p><b>Development Activities</b></p> <p>The developer should implement security procedures and standards to minimize and mitigate any tampering with the developed system.</p>		





**Table A-1. SPINLINE 3 DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152) Compliance Matrix**

RG 1.152 Regulatory Position	RG 1.152 Life Cycle Phase	Corresponding Rolls-Royce Life Cycle Phase	Text of RG 1.152 Regulatory Positions 2.1 to 2.5	RG 1.152 R3 compliance of the SPINLINE 3 generic digital safety I&C platform and associated life cycle processes	SPINLINE 3 interface criteria for NPP-specific digital safety I&C applications
2.5	Test Phase	Test	<p>COTS systems are likely to be proprietary and generally unavailable for review. In addition, a reliable method may not exist for use in determining security vulnerabilities for operating systems (e.g., operating system suppliers often do not provide access to the source code for operating systems and callable code libraries). In such cases, unless the application developer can modify such systems, the security development activity should ensure that the features within the system do not compromise the required security functions of the system in such a manner that the reliability of the safety system would be degraded.</p> <p>The objective of testing security functions is to ensure that the system security requirements are validated by the execution of integration, system,</p>		
					<p><b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b></p>



**Table A-1. SPINLINE 3 DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152) Compliance Matrix**

RG 1.152 Regulatory Position	RG 1.152 Life Cycle Phase	Corresponding Rolls-Royce Life Cycle Phase	Text of RG 1.152 Regulatory Positions 2.1 to 2.5	RG 1.152 R3 compliance of the SPINLINE 3 generic digital safety I&C platform and associated life cycle processes	SPINLINE 3 interface criteria for NPP-specific digital safety I&C applications
			<p>and acceptance tests where practical and necessary. Testing includes system hardware configuration (including all connectivity to other systems, including external systems), software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing</p>		
			<p><b>System Features</b></p>		
			<p>The security requirements and configuration items intended to ensure reliable system operation are part of the validation of the overall system requirements and design configuration items. Therefore, security design configuration items are just one element of the overall system validation. Each system security feature should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access and/or the effects of undesirable behavior of connected systems and does not reduce the reliability of system's safety functions</p>		
			<p><b>Development Activities</b></p> <p>The developer should configure and enable the designed security features correctly.</p>		
					<p><b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b></p>



**Table A-1. SPINLINE 3 DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152) Compliance Matrix**

RG 1.152 Regulatory Position	RG 1.152 Life Cycle Phase	Corresponding Rolls-Royce Life Cycle Phase	Text of RG 1.152 Regulatory Positions 2.1 to 2.5	RG 1.152 R3 compliance of the SPINLINE 3 generic digital safety I&C platform and associated life cycle processes	SPINLINE 3 interface criteria for NPP-specific digital safety I&C applications
			<p>The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features.</p>	<p><b>Security-Related Information Withheld in Accordance with 10 CFR 2.390</b></p>	