Rolls-Royce

Désignation du document *Document name*	***SPINLINE 3* Secure Development and Operational Environment**

Affaire *Product*	X	***SPINLINE 3* NRC Qualification**
Equipement *Equipment*	X	***SPINLINE 3* Digital Safety I&C Platform**
Sous-ensemble *Subassembly*		
Classé 1E ou équiv. *Safety classification*	X	**1E**

Document contractuel (pour le client) *Contractual document (for customer)* oui *yes* [ ] non *no* [X] **Nbre de pages** *Number of pages* 44

	Niv1 / Level1	*Niv2 / Level2*
Code projet *Project code*	E.RE01	17.00

Diffusion interne: *Internal distribution* ICC, QUA, KLI, LOG

Diffusion externe: *External distribution* NRC

Tampon archivage / *Archive stamp*

Version française

Rédigé par *Written by*	**Vérifié par** *Checked by*	**Approuvé par** *Approved by*
Nom : *Name* **Visa :** *Signature* **Date :** *Date*	**Nom :** *Name* **Visa :** *Signature* **Date :** *Date*	**Nom :** *Name* **Visa :** *Signature* **Date :** *Date*

English version

Rédigé ou traduit par *Written or translated by*	**Vérifié par** *Checked by*	**Approuvé par** *Approved by*
Nom : Peter Lobner *Name* **Visa:** Peter Lobner *Signature* **Date : 15 June 2011** *Date*	**Nom : Hélène Tabouret** *Name* **Visa :** *Signature* **Date :** 28/06/11 *Date*	**Nom :** MP. DURAND *Name* **Visa :** *Signature* **Date :** 28/06/11 *Date*

The document contains information which is proprietary and confidential to Rolls-Royce SAS which may not, without the prior written consent of Rolls-Royce SAS, be used or reproduced, in whole or in part, or communicated to any person not employed by Rolls-Royce SAS. © Rolls-Royce plc 2009
Le document contient des informations confidentielles et propriété de Rolls-Royce SAS et ne peut, sans l'accord écrit préalable de Rolls-Royce SAS, être utilisé ou reproduit, en totalité ou en partie, ou être communiqué à un tiers. © Rolls-Royce plc 2009

Rolls-Royce

TABLEAU DE MISE A JOUR
Record of revisions

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

Identification des moyens de production de ce document
Identification of document production means

Outils : *Tools*	Microsoft Office Word	**Fichier :** *File*	SDOE Vulnerability Assessment_3 014 543A_NSR.doc

Rolls-Royce

TABLE DES MATIERES
Table of contents

1 INTRODUCTION 4
2 DEFINITION OF THE THREAT 5
3 ADVERSARY SEQUENCE DIAGRAM 8
4 THE VULNERABILITY ASSESSMENT 10
5 CONCLUSIONS 11
6 REFERENCES 12

1. INTRODUCTION

Regulatory Guide 1.152 (Ref. 1) 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 secure development and operational environment for the generic ***SPINLINE 3*** digital safety instrumentation & control (I&C) platform software and the application software development life cycle is described in Rolls-Royce document 3 013 962 A (Ref. 2), which also defines the process to be used by Rolls-Royce for conducting a vulnerability analysis in compliance with the requirements of Regulatory Guide 1.152.

This vulnerability assessment addresses 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; therefore, this factory is not included in this vulnerability assessment.

This 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.

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.

This vulnerability assessment does not address the secure operational environment at the Licensee's facility. 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. 3) licensing process and fall under the purview of other Licensee programs.

Using this vulnerability assessment 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.

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.

2. DEFINITION OF THE THREAT

The threat and scope of the vulnerability analysis are prescribed in Section C, “Regulatory Position” of Regulatory Guide 1.152 (Ref. 1).

The threat is broadly described as a predictable set of acts (e.g. inadvertent actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system. For a digital safety I&C system, this includes unauthorized, unintended, and unsafe modifications to the system.

This vulnerability assessment examines the threats that are appropriate for a factory development environment, from the start of design through completion of the Factory Acceptance Test (FAT). These threats and their access attributes are defined in Table 2-1.

[[

Security-Related Information Withheld in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

]]

6. REFERENCES

1. 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
2. ***SPINLINE 3*** Secure Development and Operational Environment, 3 013 962 A, Rolls-Royce, 30 June 2011
3. 10 CFR 50.55a, “Codes and Standards”, USNRC

Table 4-2. *SPINLINE 3* Vulnerability Assessment of the Secure Development Environment at the Rolls-Royce Factory

[[

Security-Related Information Withheld in Accordance with 10 CFR 2.390

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

Rolls-Royce

Security-Related Information Withheld
in Accordance with 10 CFR 2.390

]]