Rolls-Royce

Désignation du document *Document name*	**Licensing Topical Report**
Affaire ☒ *Product*	***SPINLINE 3*** **NRC Qualification**
Equipement ☒ *Equipment*	***SPINLINE 3*** **Digital Safety I&C Platform**
Sous-ensemble □ *Subassembly*	
Classé 1E ou équiv. ☒ *Safety classification*	**1E**

Document contractuel (pour le client) oui □ non ☒ **Nbre de pages** 347
Contractual document *(for customer)* *yes* *no* *Number of pages*

	Niv1 / Level1	*Niv2 / Level2*
Code projet *Project code*	RNDFR	TEM1.P7
Diffusion interne: *Internal distribution*	ICC, LOG, QUA, MKT	
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 : P. Lobner *Name* **Visa :** Peter Lobner *Signature* **Date :** 1 July 09 *Date*	**Nom : S. Bazinette** *Name* **Visa :** *Signature* **Date :** 3 Juillet 09 *Date*	**Nom : M. P. Durand** *Name* **Visa :** Durand *Signature* **Date :** 3/07/09 *Date*

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*
A / 18 Dec 2008 P. Lobner		Edition originale / *First issue*
B / 30 June 2009 P. Lobner	All pages	Modification from Data Systems and Solutions to Rolls-Royce General technical and editorial update

Identification des moyens de production de ce document

Identification of document production means

Outils : *Tools*	Microsoft Office Word 2003	**Fichier :** *File*	LTR_3008503B_NP.doc

Abstract

This Licensing Topical Report (LTR) presents design, performance, and qualification information for the ***SPINLINE 3*** digital safety instrumentation and control (I&C) platform developed by RRCN. ***SPINLINE 3*** is a generic digital safety I&C platform dedicated to the implementation of Class 1E safety I&C functions. ***SPINLINE 3*** builds on the digital safety I&C systems developed by RRCN for the Électricité de France (EDF) P4 and N4 pressurized water reactor (PWR) fleet.

This LTR is the summary licensing document for the ***SPINLINE 3*** digital safety I&C platform and is organized as follows:

- Chapter 1, Introduction
- Chapter 2, ***SPINLINE 3*** Development and Operational History
- Chapter 3, Compliance With Regulations, Codes and Standards
- Chapter 4, Description of the ***SPINLINE 3*** Digital Safety I&C Platform
- Chapter 5, Equipment Qualification
- Chapter 6, Software Development Process for ***SPINLINE 3*** Platform Software and Application Software
- Appendix A: Hardware Data Sheets

The following additional documentation supports the RRCN application for NRC approval of the ***SPINLINE 3*** digital safety I&C platform:

- Hardware Qualification Documents
- Hardware Analysis Documents
- Quality Plans
- ***SPINLINE 3*** Platform Software Life Cycle Plans
- Design Analysis Report
- ***SPINLINE 3*** Application Software Life Cycle Plans

TABLE DES MATIERES
Table of contents

]]

LISTE DES FIGURES

List of Figures

LISTE DES TABLEAUX

List of Tables

0 Abbreviations and Acronyms

Term	Definition
10 CFR	Title 10 of the Code of Federal Regulations
A/D	Analog-to-Digital
ac	Alternating Current
ALARA	As Low As Reasonably Achievable
ALWR	Advanced Light Water Reactor
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrence
API	Application Programming Interface
ATU	Automated Testing Unit
ATWS	Anticipated Transients Without Scram
BAP	Backplane (Bus)
BF	Basic Functions
BOC	Beginning of Cycle
BOP	Balance of Plant
BTP	NRC Branch Technical Position
BTU	British Thermal Unit
BWR	Boiling Water Reactor
CAD	Computer Aided Design
CCF	Common Cause Failure
CDF	Core Damage Frequency
CDR	Critical Digital Review
CEZ	Ceske Energeticke Zavody
CFR	Code of Federal Regulations
CNET	French National Telecommunications Studies Center
COL	Combined Operating License
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Checks
CRT	Cathode Ray Tube

Term	**Definition**
DAC	Design Acceptance Criteria
DAR	Design Analysis Report
DBA	Design Basis Accident
DBE	Design Basis Event or Design Basis Earthquake
dc	Direct Current
DCD	Design Control Document
DG	Diesel-Generator
DI&C-ISG	Digital Instrumentation and Controls Interim Staff Guide
DPM	Dual Port Memory
DPS	Diverse Protection System
DS&S	Data Systems & Solutions, LLC
DTM	Digital Trip Module
EDF	Électricité de France
EEPROM	Electrically Erasable Programmable ROM
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPG	Emergency Procedure Guidelines
EPRI	Electric Power Research Institute
EQ	Equipment Qualification
ESD	Electrostatic Discharge
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FAT	Factory Acceptance Test
FBD	Functional Block Diagram
FCM	File Control Module
FMECA	Failure Modes and Effects Criticality Analysis
GDC	General Design Criteria
GL	Generic Letter
HEP	Human Error Probability
HFE	Human Factors Engineering
HMI	Human/Machine Interface
HRA	Human Reliability Assessment
HSI	Human-System Interface
HVAC	Heating, Ventilation, and Air Conditioning

Term	Definition
I&C	Instrumentation and Control
I/O	Input/Output
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IED	Instrument and Electrical Diagram
IEEE	Institute of Electrical and Electronic Engineers
iooj	i-out-of-j. For example, voting using 2-out-of-3 logic is referred to as 2oo3
ISA	International Society of Automation
ISI	In-Service Inspection
ISO	International Standards Organization
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
LAN	Local Area Network
LCD	Liquid Crystal Display
LCO	Limiting Conditions for Operation
LD	Logic Diagram
LDU	Local Display Unit
LED	Light Emitting Diode
LOCA	Loss of Coolant Accident
LTR	Licensing Topical Report
MC3	Modularité du Control Commande des Centrales
MCC	Motor Control Center
MCL	Master Configuration List
MCR	Main Control Room
MMI	Man-Machine Interface
MMIS	Man-Machine Interface System
MMU	Monitoring and Maintenance Unit
MTTR	Mean Time To Repair
MW	Megawatt
NDE	Nondestructive Examination
NFPA	National Fire Protection Association
NIS	Nuclear Instrumentation System
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System

Term	**Definition**
O&M	Operation and Maintenance
OBE	Operating Basis Earthquake
OLU	Output Logic Unit
OSS	Operational System Software
P&ID	Piping and Instrumentation Diagram
PAM	Post Accident Monitoring
PC	Personal Computer
PDD	Preliminary Design Document
PFD	Process Flow Diagram
PGA	Peak Ground Acceleration
PHA	Preliminary Hazard Analysis
PIE	Postulated Initiating Event
PM	Preventive Maintenance
PRC	People's Republic of China
PWR	Pressurized Water Reactor
QA	Quality Assurance
QAP	QA Plan
QMS	Quality Management System
RAM	Random Access Memory
RCS	Reactor Coolant System
RDF	Recueil de Donnes de Fiabilité
REPROM	Reprogrammable ROM
RG	Regulatory Guide
RMBK	Russian: Reaktor Bolshoy Moshchnosti Kanalniy (graphite-moderated reactor)
RMS	Root Mean Square
ROM	Read-Only Memory
RPS	Reactor Protection System
RRCN	Rolls-Royce Civil Nuclear SAS (Société Anonyme Simplifié)
RSS	Remote Shutdown System
RTS	Reactor Trip System
S/N	Signal-to-Noise
SAR	Safety Analysis Report
SCMP	Software Configuration Management Plan

Term	Definition
SDP	Software Development Plan
SDS	System Design Specification
SER	Safety Evaluation Report
SFC	Single Failure Criterion
SFTP	Shielded Foil Twisted Pair
SOE	Sequence of Events
SPIN	Système de Protection Intégré Numérique, which is the French acronym for “Digital Integrated Protection System”
SQAP	Software Quality Assurance Plan
SRM	Source Range Monitor
SRP	Standard Review Plan
SRS	Software Requirements Specification
SSDE	System and Software Development Environment
SSE	Safe Shutdown Earthquake
SVVP	Software Verification and Validation Plan
T/C	Thermocouple
TS	Technical Specification
TSAP	Test Specimen Application Program
UL	Underwriter's Laboratories Inc.
UPS	Uninterruptible Power Supply
U.S.	United States of America
USNRC	United States Nuclear Regulatory Commission
UTE-C	French Technical Institute of Electricity and Communication (French standards)
UV	Ultraviolet
V&V	Verification and Validation
v	Volts
VDU	Video Display Unit
VVER	Russian: Voda-Vodyanoi Energetichesky Reaktor (Pressurized Water Reactor)
XFMR	Transformer

1 Introduction

1.1 Purpose

This Licensing Topical Report (LTR) presents design, performance, and qualification information for the ***SPINLINE 3*** digital safety instrumentation and control (I&C) platform developed by Rolls-Royce Civil Nuclear SAS (RRCN). ***SPINLINE 3*** is a generic digital safety I&C platform designed specifically to implement Class 1E safety I&C functions. ***SPINLINE 3*** builds on the digital safety I&C systems developed by RRCN for the Électricité de France (EDF) P4 and N4 pressurized water reactor (PWR) fleet.

Designed with flexibility and safety in mind, ***SPINLINE 3*** meets the demanding functional and safety requirements for digital safety I&C systems employed in modern nuclear power plants (NPPs). This makes ***SPINLINE 3*** ideally suited for use in a variety of safety I&C applications in both new NPPs and refurbished safety I&C systems in existing NPPs. RRCN has installed ***SPINLINE 3*** digital safety I&C applications including Reactor Trip System (RTS), Engineered Safety Features Actuation System (ESFAS), Post-Accident Monitoring System (PAMS), and Nuclear Instrumentation System (NIS) in several different international reactor designs, including PWRs, Russian-designed VVER and RBMK reactors, and research reactors. RRCN concludes that the ***SPINLINE 3*** digital safety I&C platform will be readily adaptable to the needs of U.S. nuclear safety I&C applications in PWRs, BWRs and other types of reactors and nuclear facilities.

Since its launch in 1997, ***SPINLINE 3*** has been implemented in new pressurized water reactors (PWRs) at Qinshan in the People's Republic of China (PRC), and for safety I&C refurbishment in a number of existing NPPs, including:

- PWR: Tihange in Belgium, and Fessenheim and Bugey in France
- VVER: Kozloduy in Bulgaria, and Dukovany in Czech Republic
- RBMK: Ignalina in Lithuania

This document is a generic Licensing Topical Report (LTR) that is intended to be referenced by an applicant applying ***SPINLINE 3*** to a plant-specific nuclear safety application in the U.S. As such, this generic LTR focuses on the following:

- ***SPINLINE 3*** hardware design, qualification and analysis
- ***SPINLINE 3*** platform software design and software life cycle processes. As described in Section 4.4, the components of the generic platform software are:
  - The standardized, Class 1E configurable Operational System Software (OSS)
  - The Class 1E application-oriented library of re-usable software components,
  - The Class 1E software embedded in the NERVIA+ board,
  - The Class 1E software embedded in the ICTO Pulse Input board, and
  - A non-Class 1E set of tools integrated in a Software Development Environment (SSDE) called CLARISSE, which is used to design and implement the system architecture, configure the units and networks and develop the plant-specific application software.
- ***SPINLINE 3*** application software life cycle processes for developing plant-specific applications.

RRCN is seeking U.S. Nuclear Regulatory Commission (NRC) generic approval for use of ***SPINLINE 3*** in nuclear safety I&C systems in any U.S. commercial nuclear power plant, research reactor, or nuclear fuel cycle facility.

SPINLINE 3 originally was designed, qualified, and manufactured to meet European nuclear safety and quality standards. In addition, ***SPINLINE 3*** systems have demonstrated compliance with the nuclear safety regulations in several nations outside of Europe. ***SPINLINE 3*** now is managed under a quality assurance program that complies with 10CFR50 Appendix B (Reference 1-1). The purpose of this LTR is to demonstrate that the ***SPINLINE 3*** safety I&C platform and the associated quality and software life cycle processes comply with U.S. nuclear safety requirements. Compliance is demonstrated via the following licensing approach:

- Qualify ***SPINLINE 3*** hardware to meet U.S. standards. The ***SPINLINE 3*** hardware will be qualified and maintained under the 10 CFR 50 Appendix B quality program. If new boards are developed or existing boards modified for obsolescence or other reasons, the new or modified hardware will be appropriately tested and/or analyzed to maintain equipment qualification to U.S. standards.

- Develop plant-specific application software in accordance with software life cycle plans that are compliant with NRC Branch Technical Position (BTP) 7-14 (Reference 1-2)

- Commercially dedicate the ***SPINLINE 3*** OSS, application-oriented library, and embedded software, which are components of the platform software developed previously, using the process defined in EPRI TR-107330 (Reference 1-3) and approved by the NRC (Reference 1-4). The technical basis for dedication is documented in a Design Analysis Report (DAR, Reference 1-5).

- The non-Class 1E set of software tools, which are used as design aids and not as a replacement for verification and validation (V&V), are not dedicated but continue to be subject to a configuration management program.

1.2 Organization of this Licensing Topical Report

This LTR is organized as follows:

- **Chapter 1, Introduction:** This chapter provides and overview of the LTR and identifies the numerous supporting documents that will be submitted for NRC review. This chapter also provides an overview of the quality program and the quality process employed to dedicate the platform software and libraries.

- **Chapter 2, *SPINLINE 3* Development and Operational History:** This chapter provides an overview of ***SPINLINE 3*** development and operational use in many French and international NPPs where it is currently deployed in a variety of digital safety I&C applications. This historical information is intended to illustrate the substantial legacy of safety I&C developments that led to the ***SPINLINE 3*** digital safety I&C platform, which is the subject of this LTR.

- **Chapter 3, Regulations, Codes and Standards:** This chapter provides summaries of ***SPINLINE 3*** compliance with the U.S. and international regulations, codes and standards listed or referenced in the NRC Standard Review Plan, Table 7-1, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety” (Reference 1-6) plus additional standards referenced in this LTR. This chapter serves as a compliance roadmap and includes references to where additional compliance details are provided in this LTR or other supporting documents submitted by RRCN for NRC review.

- **Chapter 4, Description of the *SPINLINE 3* Digital Safety I&C Platform:** This chapter provides generic descriptions of the hardware and software that comprise the ***SPINLINE 3*** digital safety I&C platform. In addition, details are provided on how digital communications and testability are implemented in ***SPINLINE 3***. Data sheets for individual ***SPINLINE 3*** hardware items are provided in Appendix A of this LTR.

- **Chapter 5, Equipment Qualification and Analysis:** This chapter provides an overview of the generic equipment qualification program, which is described in detail in the Equipment Qualification (EQ) Plan (Reference 1-7). The ***SPINLINE 3*** qualification "envelope" is generic and is intended to meet or exceed the environmental qualification requirements for new and existing NPPs in the U.S. The EQ Plan defines the Qualification Test Specimen (QTS) and the specific test procedures and the resulting test reports for each test. This chapter also provides: (1) a summary of the board / device-level reliability analysis process and results reported separately, and (2) an overview of the setpoint analysis support process reported separately.

- **Chapter 6, Software Development Process for *SPINLINE 3* Platform Software and Application Software**: This chapter describes the development history and the software life cycle processes applicable to the ***SPINLINE 3*** platform software [i.e., the standard OSS, the application-oriented library of re-usable software components, embedded software in the ICTO Pulse Input board, and the CLARISSE SSDE]. The software life cycle processes used for the ***SPINLINE 3*** platform software were developed in the mid-1980s in connection with the development of digital safety I&C systems for the EDF P4 and N4 fleets of PWRs. These software life cycle processes are examined in more detail in the Design Analysis Report (DAR, Reference 1-5).This chapter also describes the separate software life cycle processes for plant-specific application software. These processes comply with NRC Branch Technical Position (BTP) 7-14 (Reference 1-1).

- **Appendix A, *SPINLINE 3* Hardware Data Sheets:** This appendix contains the data sheets for ***SPINLINE 3*** standard hardware items described in Section 4.3.

In this document, brackets ("[[ ]]") denote proprietary information. In the proprietary document, the two brackets denoting the end of a proprietary segment of this report may appear one or more pages following the bracket indicating the start of the proprietary segment. In the nonproprietary edition of this document, the material within the brackets is removed.

1.3 Supporting *SPINLINE 3* Licensing Documents

In addition to this LTR, RRCN will submit the following licensing documents to the NRC:

- **Hardware Qualification Documents**: The key document is the Equipment Qualification (EQ) Plan (Reference 1-7), which describes the testing performed to qualify standard ***SPINLINE*** 3 hardware in accordance with NRC requirements. The specific hardware tested is defined in the EQ Plan and the System Specification for the Qualification Test Specimen (QTS) and Test System (Reference 1-8). The EQ Plan summarizes the many test procedures and identifies the resulting test reports, which will be submitted as separate documents.
- **Hardware Analysis Documents:** These analysis documents provide the generic foundations for plant-specific failure mode and effects criticality analysis (FMECA), reliability analysis, and setpoint analysis.
- **Quality Plans:** Two 10 CFR 50 Appendix B-compliant Quality Plans will be submitted. The "Rolls-Royce Civil Nuclear SAS Quality Manual" (Reference 1-9) establishes the quality processes employed in the Meylan, France factory. The DS&S, LLC "Instrumentation & Controls US Quality Manual" (Reference 1-11) establishes the corresponding quality processes employed in the U.S. to deliver ***SPINLINE 3*** systems to U.S. customers.

- **<u>SPINLINE 3 platform Software Life Cycle Plans:</u>** The Design Analysis Report (DAR) examines how the platform software life cycle processes described in LTR Chapter 6, and the resulting software product described in LTR Chapter 4 compare to the product one would expect if BTP 7-14 software life cycle processes had been used. In connection with the DAR, reviews were been performed for: the following:
  - The processes under which the platform software was developed,
  - The quality of the software tools used in developing the platform software,
  - The processes used to generate the platform software,
  - The quality and extent of the software documentation for the platform software,
  - The quality of the software tools used in generating the application software
  - The processes used to generate the application software, and
  - The applicable processes used in designing the ***SPINLINE 3*** hardware, including the use of programmable logic.

  The favorable DAR findings on this matter support the RRCN decision to dedicate the ***SPINLINE 3*** platform software.
- **<u>Application Software Life Cycle Plans:</u>** These Plans implement NRC BTP 7-14 (Reference 1-2) in the RRCN software life cycle processes employed for plant-specific ***SPINLINE 3*** application software.

1.4 QUALITY PROGRAM

Rolls-Royce Civil Nuclear SAS located in Meylan, France, is the supplier and qualifier of ***SPINLINE 3*** hardware, software, and integrated systems. Data Systems & Solutions, LLC (DS&S), doing business as (dba) Rolls-Royce Civil Nuclear in the U.S., will deliver ***SPINLINE 3*** systems to U.S. customers.

RRCN activities are performed under the 10 CFR 50 Appendix B-compliant quality program documented in the “Rolls-Royce Civil Nuclear SAS Quality Manual” (Reference 9). A map showing the correspondence between 10 CFR 50 Appendix B, ASME NQA-1-1994 (Reference 1-10) and the RRCN quality procedures is provided in Section 3.2.

- The ***SPINLINE 3*** platform software was dedicated under this RRCN QA program.
- Manufacturing processes are defined in this Quality Management Plan and subordinate processes.
- This quality program has been audited by Global Quality Assurance. In addition, this quality program was audited by DS&S, LLC to qualify RRCN as a supplier of ***SPINLINE 3*** hardware, software and systems to DS&S, LLC.

DS&S, LLC activities are performed under the 10 CFR 50 Appendix B-compliant quality program documented in the “Instrumentation & Controls US Quality Manual” (Reference 1-11). A map showing the correspondence between 10 CFR 50 Appendix B, ASME NQA-1-1994 and the DS&S, LLC quality procedures is provided in Section 3.2.

- Rolls-Royce Civil Nuclear SAS was qualified as a supplier under this DS&S, LLC QA program.
- This quality program has been audited by U.S. utilities, NUPIC, and Department of Energy’s Idaho National Laboratory

Software quality plans and other software life cycle plans are addressed in Chapter 6.

1.5 Chapter 1 References

1-1 10 CFR 50 Appendix B, “Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants”

1-2 NRC Branch Technical Position 7-14, Rev, 5, “Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems,” US Nuclear Regulatory Commission, March 2007

1-3 EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” Electric Power Research Institute, December 1996

1-4 USNRC Letter dated July 30, 1998 to Mr. J. Naser (EPRI), “Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute (EPRI) Topical Report, TR-107330, Final Report, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants.”

1-5 “***SPINLINE 3*** Design Analysis Report,” Document No. MPR-3337, MPR Associates, Inc., June 2009

1-6 NUREG-0800, USNRC Standard Review Plan, Table 7-1, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety,” Revision 5, March 2007

1-7 “Equipment Qualification Plan”, Document No. 3 006 501C, Rolls-Royce Civil Nuclear SAS, June 2009

1-8 “System Specification of the Qualification Test Specimen and Data Acquisition System”, Document No. 3 006 404C, Rolls-Royce Civil Nuclear SAS, June 2009

1-9 “Rolls-Royce Civil Nuclear SAS Quality Manual”, Document No. 8 303 186 P, Rolls-Royce Civil Nuclear SAS, June 2009

1-10 ASME NQA-1-1994, “Quality Assurance Program Requirements for Nuclear Facilities”, American Society of Mechanical Engineers

1-11 “Instrumentation & Controls US Quality Manual”, Revision C, Document 500-9600000-10, ICQ-005-C, Data Systems & Solutions, LLC, a member of the Rolls-Royce Civil Nuclear group, June 2009

2 *SPINLINE 3* Development and Operational History

2.1 Overview

RRCN has been designing and manufacturing safety I&C systems for nuclear power plants for more than 30 years. RRCN originally developed non-software-based analog safety I&C systems for the Électricité de France (EDF) fleet of 900 MW PWRs. In the 1980s, RRCN designed and deployed two generations of software-based digital safety I&C systems for EDF’s later fleet of P4 and N4 PWRs. ***SPINLINE 3*** is the next generation of RRCN digital safety I&C systems.

This chapter provides an overview of ***SPINLINE 3*** development and operational use in the many French and international NPPs where it is currently deployed in a variety of digital safety I&C applications. This historical information is intended to illustrate the substantial legacy of safety I&C developments that led to the ***SPINLINE 3*** digital safety I&C platform, which is the subject of this LTR.

From the beginning, RRCN hardware components and systems were designed, implemented and qualified in compliance with European nuclear standards, including the International Atomic Energy Agency (IAEA) 50-C-QA code for quality assurance (Reference 2-1) and the French national code RCC-E (Reference 2-2), which prescribes requirements for qualification of electrical equipment used in French-built nuclear power plants.

The RRCN safety software evolved in stages to adapt to the introduction of new digital components and software methods and tools. These evolutionary stages started with software development “from scratch” using low-level manual coding and have now matured into processes based on high-level languages, including application-oriented languages, code re-use and automated code generation. The ***SPINLINE 3*** safety-related platform software was developed based on the guidance of the IEC 880-1986 (Reference 2-3) with enhancements to take into account the advances in software engineering, which were later reflected in the supplement to IEC 880 issued in 2000 (Reference 2-4) and in IEC 60880 Edition 2 (Reference 2-5).

As discussed in Chapter 1, the ***SPINLINE 3*** platform software originally developed under European nuclear safety standards has been dedicated and is now managed under the RRCN 10CFR50 Appendix B-compliant QA program. As described in Section 5.1, the standard ***SPINLINE 3*** hardware is qualified to meet current U.S. regulatory requirements. New plant-specific application software will be developed using the BTP 7-14-compliant software life cycle processes described in Section 6.4.

2.2 Evolution of the *SPINLINE 3* Digital Safety I&C Platform

2.2.1 Non Software-Based Safety I&C

Based on a Westinghouse design, 34 three-loop 900 MW pressurized water reactors were commissioned in France by EDF between 1978 and 1987. RRCN designed, manufactured, and is still maintaining nonsafety and safety I&C systems developed using non-software-based technologies such as MULTIBLOC for nuclear instrumentation and SILIMOG for logic functions.

2.2.2 First Generation of Software-Based Safety I&C

The EDF P4 project resulted in commissioning 20 four-loop 1,300 MW PWRs in France between 1984 and 1993. The overall I&C design made intensive use of software-based technologies for control and protection functions. In particular, RRCN developed a modular software-based technology to implement the Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS). When combined, these two systems are known as the SPIN (Système de Protection Intégré Numérique), which is a French acronym for “Digital Integrated Protection System”.

This technology uses the Motorola 6800 microprocessor with unidirectional and asynchronous communication links for data exchange. A single P4 unit’s SPIN system has 52 safety processing units distributed in a four channel architecture. Today, 20 P4 SPIN systems are in operation with a total of 1,040 safety processing units. P4 SPIN systems have accumulated 420 reactor-years of operation as of December 2008.

The P4 SPIN software consists of about 40,000 instructions written in 6800 assembly code. This software includes the application software performing the processing of the safety functions, and the Operational System Software (OSS) that performs data acquisition, actuator control, data communication, and hardware self-supervision functions.

The P4 SPIN software was developed using life cycle processes targeted to produce “close to zero faults” software. The main features are:

- A “V” model software development cycle;
- A top-down modular design;
- Design and coding rules aimed at developing reliable software;
- A Verification and Validation (V&V) team independent of the software design team;
- The verification of all design documents and source code;
- “White box” unit testing of all the software modules, achieving 100% branch coverage; and
- “Black box” validation testing performed at the processing unit level, channel/division/train level, and system level.

This main software development effort took place during the years 1981 and 1982 and was performed according to the guidance in working drafts of the future IEC 880 standard, which was intended to significantly improve the reliability of software used for the implementing nuclear safety functions. The feedback of experience gained on the P4 project was a major input to this IEC 880 standard which was eventually issued in 1986 (Reference 2-3).

2.2.3 Second Generation of Software-Based Safety I&C

The EDF N4 project deployed 1450 MW four-loop PWRs with a fully-computerized Main Control Room (MCR) that implemented new I&C technologies.

For the N4 NPPs, RRCN developed a new generation of its software-based safety I&C system technology, called N4 SPIN, which is based on the Motorola (now Freescale) MC68000 family of microprocessors and on an RRCN proprietary high-speed deterministic communications network called NERVIA. The main improvements relative to the P4 SPIN technology were:

- A reduction in the number of separate functional processing units, from seven for P4 to five for N4, enabled by the greater processing power of the 68000 microprocessor;

- The NERVIA digital communications network, which allowed for a significant reduction of electronic boards and wiring; and

- The implementation of software-based voting units for both the RPS and the ESFAS actuators.

A single N4 unit's SPIN system uses 40 safety processing units used in a four channel / two output train system architecture. Today, four N4 SPIN systems are in operation with a total of 160 safety processing units. The same digital safety I&C technology is also employed in the protection systems of 11 research reactors.

The N4 SPIN has been in operational use since the first N4 plant commissioning tests in 1991 and has been in commercial operation since 1996. N4 SPIN systems have accumulated 55 reactor-years of operation as of December 2008.

The N4 SPIN software consists of about 200,000 instructions implemented in C language, most of them generated from 200 graphical views created using a proprietary Functional Block Diagram (FBD) language named SAGA.

As for the P4 project, the N4 software was developed with the objective of producing "close to zero faults" software, using basically the same software life cycle processes, but with intensive use of software tools for the tasks that could be automated or assisted.

This main software development effort for the N4 project took place during the years 1988 and 1989 and was performed according to the guidance provided in IEC 880-1986 (Reference 2-3). The basic processes for developing the N4 safety software have not changed since the P4 project. However, process changes were made to take into account the evolution in languages and tools used for the N4 project and evolution in software engineering processes not explicitly required in IEC 880-1986, such as requirements for dedicated software plans.

Section 6.1 provides insights into the N4 software development process and its relevance to the ***SPINLINE3*** platform.

2.2.4 Third Generation of Software-Based Safety I&C - *SPINLINE 3*

After the N4 project, the RRCN software-based I&C technology was enhanced to improve performance and quality while simplifying the manufacturing processes. The main improvements relative to the N4 SPIN technology are:

- Hardware:
  - New electromagnetic compatibility (EMC) proofed chassis, cabling, and terminal blocks, and
  - Additional CPU, input / output (I/O) and communication boards
- Software:
  - Configurable Operational System Software (OSS),
  - An enhanced software engineering tool set, including a platform-dedicated tool to configure and set the parameters for the processing units and NERVIA networks, and
  - A non-proprietary version of the SAGA environment called the Safety Critical Application Development Environment (SCADE), developed and maintained by the software company Esterel Technologies.

This technology is referred to as ***SPINLINE 3***.

SPINLINE 3 has been implemented successfully for the refurbishment of Class 1E I&C systems on several models of PWR NPPs and on several Russian-designed NPPs, including both VVER and RBMK. ***SPINLINE 3*** also is deployed in safety I&C systems on several new PWRs in the Republic of China. ***SPINLINE 3*** systems have accumulated 85 reactor-years of operation as of December 2008.

The ***SPINLINE 3*** platform was developed between 1993 and 1996, based on the N4 technology. It includes enhancements to the N4 hardware and the development of platform software and tools needed to produce an adaptable safety I&C platform suitable for use worldwide in refurbishment of existing NPP safety I&C systems and for new construction safety I&C systems.

The life cycle processes for the ***SPINLINE 3*** platform software were established according to the guidance provided in IEC 880-1986 (Reference 2-3), and were documented in dedicated software plans. The ***SPINLINE 3*** software life cycle processes also took into account additional process enhancements employed on the N4 project and ongoing standardization works for a supplement to IEC 880, which was issued in 2000 (Reference 2-4). The ***SPINLINE 3*** software life cycle processes are further described in Section 6.2. As described in Chapter 1, the ***SPINLINE 3*** platform software has been dedicated for use in systems delivered to U.S. customers and is now managed under the RRCN 10CFR50 Appendix B QA Program.

The application software for a nuclear safety I&C system implemented using the ***SPINLINE 3*** platform is developed according to a set of plant-specific software life cycle plans that are consistent with current NRC guidance in BTP 7-14 (Reference 2-6). Details on these ***SPINLINE 3*** application software plans are presented in Section 6.4.

The experience gained at RRCN in developing several safety I&C systems using the ***SPINLINE 3*** digital I&C platform was an input to the revision of IEC 880-1986, which started in 2001 and was completed in 2006 as IEC 60880 Edition 2 (Reference 2-5). The project leader for this revision was from RRCN

2.3 RRCN Safety I&C Installations

By the end of 2008, the main safety I&C systems implemented with the ***SPINLINE 3*** technology are:

- New Nuclear Instrumentation Systems (NIS) for two Chinese PWRs
- Modernized NIS for six French PWRs and for one Belgian PWR
- Modernized safety I&C including RTS, ESFAS and support functions for four Czech VVER 440/213 NPPs
- A new diverse protection system for one Lithuanian RBMK

Other ***SPINLINE 3*** installations include source range NIS modernization at two VVER 440/213 NPPs in Bulgaria and Safety Relief Valve Control and NIS system modernization at one VVER 440/213 NPP in Armenia.

A summary of RRCN nuclear I&C references collectively implemented with all technologies is provided in Table 2.3-1.

2.4 Chapter 2 References

2-1 IAEA Safety Series 50-C-QA, Rev. 1 , “Code on the Safety of Nuclear Power Plants: Quality Assurance,” International Atomic Energy Agency (IAEA), 1988

2-2 French National Code RCC-E (*Règles de Construction et de Conception des Matériels Electriques*), Chapter B, “Design and Construction Rules for Electronic Components of PWR Nuclear Islands”

2-3 IEC 880-1986, “Software for Computers in the Safety Systems of Nuclear Power Stations,” International Electrotechnical Commission

2-4 IEC 60880-2000, “Software for Computers important to safety for Nuclear Power Plants – part 2: Software aspects of defense against common cause failure, use of software tools and of pre-developed software”, International Electrotechnical Commission

2-5 IEC 60880-2006, “Software for Computers in the Safety Systems of Nuclear Power Plants”, International Electrotechnical Commission

2-6 NRC Branch Technical Position 7-14, Rev, 5, “Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems,” US Nuclear Regulatory Commission, March 2007

Table 2.3-1: RRCN Nuclear I&C Installations

						Safety Class 1E Equipment				
Country	Utility	NPP ID	Reactor Type	Start of Ops.	Technology	RTS & ESFAS	Neutron Detectors	Neutron Instr.	Diesel Sequencing	Reactor Trip Breakers
Armenia	JSC Armenia NPP	Metsamor	VVER	5/31/1980	***SPINLINE 3***		×	×		
Belgium	Electrabel	Doel 1	PWR	8/28/1974	ANALOG		×			
	Electrabel	Doel 2	PWR	8/21/1975	ANALOG		×			
	Electrabel	Doel 3	PWR	6/23/1982	ANALOG		×			
	Electrabel	Doel 4	PWR	4/8/1985	ANALOG		×			
	Electrabel	Tihange 1	PWR	3/7/1975	SPINLINE 3		×	×		
	Electrabel	Tihange 2	PWR	10/13/1982	ANALOG		×			
	Electrabel	Tihange 3	PWR	6/14/1985	ANALOG		×			
Bulgaria	National Electricity Co	Kozloduy 3	VVER	12/17/1980	***SPINLINE 3***		×	×		
	National Electricity Co	Kozloduy 4	VVER	5/1/1982	***SPINLINE 3***		×	×		
Brazil	CTMSP	Copesp	R&D		N4		×	×		
China	GNP JVC	Daya Bay 1	PWR	8/31/1993	ANALOG		×	×		
	GNP JVC	Daya Bay 2	PWR	2/7/1994	ANALOG		×	×		
	Ling Ao Nuclear Power Co	Ling Ao 1	PWR	2/4/2002	ANALOG		×	×		×
	Ling Ao Nuclear Power Co	Ling Ao 2	PWR	12/1/2002	ANALOG		×	×		×

Table 2.3-1: RRCN Nuclear I&C Installations

						Safety Class 1E Equipment				
Country	Utility	NPP ID	Reactor Type	Start of Ops.	Technology	RTS & ESFAS	Neutron Detectors	Neutron Instr.	Diesel Sequencing	Reactor Trip Breakers
	Qinshan Nuclear Power Co	Qinshan II 1	PWR	2/6/2002	***SPINLINE 3***		×	×		
	Qinshan Nuclear Power Co	Qinshan II 2	PWR	2/4/2004	***SPINLINE 3***		×	×		
Czech Republic	Ceske Energeticke Zavody (CEZ)	Dukovany 1	VVER	2/24/1985	***SPINLINE 3***	×	×	×	×	×
	Ceske Energeticke Zavody (CEZ)	Dukovany 2	VVER	1/30/1986	***SPINLINE 3***	×	×	×	×	×
	Ceske Energeticke Zavody (CEZ)	Dukovany 3	VVER	11/14/1986	***SPINLINE 3***	×	×	×	×	×
	Ceske Energeticke Zavody (CEZ)	Dukovany 4	VVER	6/11/1987	***SPINLINE 3***	×	×	×	×	×
France	EDF	Belleville 1	PWR	10/14/1987	P4	×	×	×		×
	EDF	Belleville 2	PWR	7/6/1988	P4	×	×	×		×
	EDF	Blayais 1	PWR	6/12/1981	ANALOG		×	×		×
	EDF	Blayais 2	PWR	7/17/1982	ANALOG		×	×		×
	EDF	Blayais 3	PWR	8/17/1983	ANALOG		×	×		×
	EDF	Blayais 4	PWR	5/16/1983	ANALOG		×	×		×
	EDF	Bugey 2	PWR	5/10/1978	***SPINLINE 3***		×	×		×

Table 2.3-1: RRCN Nuclear I&C Installations

						Safety Class 1E Equipment				
Country	Utility	NPP ID	Reactor Type	Start of Ops.	Technology	RTS & ESFAS	Neutron Detectors	Neutron Instr.	Diesel Sequencing	Reactor Trip Breakers
	EDF	Bugey 3	PWR	9/21/1978	***SPINLINE 3***		×	×		×
	EDF	Bugey 4	PWR	3/8/1979	***SPINLINE 3***		×	×		×
	EDF	Bugey 5	PWR	7/31/1979	***SPINLINE 3***		×	×		×
	CEA	Cadarache / Cabri	R&D		N4	×	×	×		
	CEA	Cadarache / Eole	R&D		N4	×	×	×		
	CEA	Cadarache / Mazurka	R&D		N4	×	×	×		
	CEA	Cadarache / Minerve	R&D		N4	×	×	×		
	CEA	Cadarache / Phoebus	R&D		N4	×	×	×		
	EDF	Cattenom 1	PWR	11/13/1986	P4	×	×	×		×
	EDF	Cattenom 2	PWR	9/17/1987	P4	×	×	×		×
	EDF	Cattenom 3	PWR	7/6/1990	P4	×	×	×		×
	EDF	Cattenom 4	PWR	5/27/1991	P4	×	×	×		×
	EDF	Chinon B1	PWR	11/30/1982	ANALOG		×	×		×
	EDF	Chinon B2	PWR	11/29/1983	ANALOG		×	×		×
	EDF	Chinon B3	PWR	10/20/1986	ANALOG		×	×		×

Table 2.3-1: RRCN Nuclear I&C Installations

						Safety Class 1E Equipment				
Country	Utility	NPP ID	Reactor Type	Start of Ops.	Technology	RTS & ESFAS	Neutron Detectors	Neutron Instr.	Diesel Sequencing	Reactor Trip Breakers
	EDF	Chinon B4	PWR	11/14/1987	ANALOG		×	×		×
	EDF	Chooz B1	PWR	8/30/1996	N4	×	×	×	×	×
	EDF	Chooz B2	PWR	4/10/1997	N4	×	×	×	×	×
	EDF	Civaux 1	PWR	12/24/1997	N4	×	×	×	×	×
	EDF	Civaux 2	PWR	12/24/1999	N4	×	×	×	×	×
	EDF	Creys-Malville	FBR		ANALOG		×	×		
	EDF	Cruas 1	PWR	4/29/1983	ANALOG		×	×		×
	EDF	Cruas 2	PWR	9/6/1984	ANALOG		×	×		×
	EDF	Cruas 3	PWR	5/14/1984	ANALOG		×	×		×
	EDF	Cruas 4	PWR	10/27/1984	ANALOG		×	×		×
	EDF	Dampierre 1	PWR	3/23/1980	ANALOG		×	×		×
	EDF	Dampierre 2	PWR	12/10/1980	ANALOG		×	×		×
	EDF	Dampierre 3	PWR	1/30/1981	ANALOG		×	×		×
	EDF	Dampierre 4	PWR	8/18/1981	ANALOG		×	×		×
	EDF	Fessenheim 1	PWR	4/6/1977	***SPINLINE 3***		×	×		×
	EDF	Fessenheim 2	PWR	10/7/1977	***SPINLINE 3***		×	×		×
	EDF	Flamanville 1	PWR	12/4/1985	P4	×	×	×		×

Table 2.3-1: RRCN Nuclear I&C Installations

						Safety Class 1E Equipment				
Country	Utility	NPP ID	Reactor Type	Start of Ops.	Technology	RTS & ESFAS	Neutron Detectors	Neutron Instr.	Diesel Sequencing	Reactor Trip Breakers
	EDF	Flamanville 2	PWR	7/18/1986	P4	×	×	×		×
	EDF	Golfech 1	PWR	6/7/1990	P4	×	×	×		×
	EDF	Golfech 2	PWR	6/18/1993	P4	×	×	×		×
	EDF	Gravelines 1	PWR	3/13/1980	ANALOG		×	×		×
	EDF	Gravelines 2	PWR	8/26/1980	ANALOG		×	×		×
	EDF	Gravelines 3	PWR	12/12/1980	ANALOG		×	×		×
	EDF	Gravelines 4	PWR	6/14/1981	ANALOG		×	×		×
	EDF	Gravelines 5	PWR	8/28/1984	ANALOG		×	×		×
	EDF	Gravelines 6	PWR	8/1/1985	ANALOG		×	×		×
	CEA	Marcoule / Celestin 1	R&D		N4	×	×	×		
	CEA	Marcoule / Celestin 2	R&D		N4	×	×	×		
	EDF	Nogent 1	PWR	10/21/1987	P4	×	×	×		×
	EDF	Nogent 2	PWR	12/14/1988	P4	×	×	×		×
	EDF	Paluel 1	PWR	6/22/1984	P4	×	×	×		×
	EDF	Paluel 2	PWR	9/14/1984	P4	×	×	×		×
	EDF	Paluel 3	PWR	9/30/1985	P4	×	×	×		×

Table 2.3-1: RRCN Nuclear I&C Installations

						Safety Class 1E Equipment				
Country	Utility	NPP ID	Reactor Type	Start of Ops.	Technology	RTS & ESFAS	Neutron Detectors	Neutron Instr.	Diesel Sequencing	Reactor Trip Breakers
	EDF	Paluel 4	PWR	4/11/1986	P4	×	×	×		×
	EDF	Penly 1	PWR	5/4/1990	P4	×	×	×		×
	EDF	Penly 2	PWR	2/4/1992	P4	×	×	×		×
	EDF	Phénix	FBR	12/13/1973	ANALOG		×	×		
	CEA	Saclay / Isis	R&D		N4	×	×	×		
	CEA	Saclay / Osiris	R&D		N4	×	×	×		
	CEA	Saclay / Orphée	R&D		N4	×	×	×		
	EDF	Saint Alban 1	PWR	8/30/1985	P4	×	×	×		×
	EDF	Saint Alban 2	PWR	7/3/1986	P4	×	×	×		×
	EDF	Saint Laurent B1	PWR	1/21/1981	ANALOG		×	×		×
	EDF	Saint Laurent B2	PWR	6/1/1981	ANALOG		×	×		×
	EDF	Tricastin 1	PWR	5/31/1980	ANALOG		×	×		×
	EDF	Tricastin 2	PWR	8/7/1980	ANALOG		×	×		×
	EDF	Tricastin 3	PWR	2/10/1981	ANALOG		×	×		×
	EDF	Tricastin 4	PWR	6/12/1981	ANALOG		×	×		×
Lithuania	Ignalina NPP	Ignalina 2	RBMK	8/20/1987	***SPINLINE 3***	×	×	×		

Table 2.3-1: RRCN Nuclear I&C Installations

						Safety Class 1E Equipment				
Country	Utility	NPP ID	Reactor Type	Start of Ops.	Technology	RTS & ESFAS	Neutron Detectors	Neutron Instr.	Diesel Sequencing	Reactor Trip Breakers
South Africa	Eskom	Koeberg 1	PWR	4/4/1984	ANALOG		×	×		
	Eskom	Koeberg 2	PWR	7/25/1985	ANALOG		×	×		
South Korea	Korea Hydro	Ulchin 1	PWR	4/7/1988	ANALOG		×	x		
	Korea Hydro	Ulchin 2	PWR	4/14/1989	ANALOG		×	x		
Spain	Centrales Nucleares Almaraz-Trillo	Almaraz 1	PWR	5/1/1981	ANALOG		×			
	Centrales Nucleares Almaraz-Trillo	Almaraz 2	PWR	10/8/1983	ANALOG		×			
	Asociación Nuclear Asco-Vandellos A.I.E.	Asco 1	PWR	8/13/1983	ANALOG		×			
	Asociación Nuclear Asco-Vandellos A.I.E.	Asco 2	PWR	10/23/1985	ANALOG		×			
	Asociación Nuclear Asco-Vandellos A.I.E.	Vandellos 2	PWR	12/12/1987	ANALOG		×			
	Number of NPPs	**101**		**Number**		**39**	**101**	**88**	**8**	**64**

3 Regulations, Codes and Standards

3.1 Compliance Summary

A summary of NRC regulatory requirements and acceptance criteria for instrumentation and control (I&C) systems important to safety is found in Standard Review Plan Table 7-1 (Reference 3-1). Rolls-Royce Civil Nuclear SAS (RRCN) reviewed this table to define the scope of the regulatory requirements and acceptance criteria that applied to the generic ***SPINLINE 3*** digital safety I&C platform. Several of the items listed in SRP Table 7-1 apply to application-specific safety I&C systems. Compliance with application-specific regulatory requirements cannot be assessed in the context of a generic digital safety I&C platform that does not include the specific applications. RRCN's screening of the SRP Table 7-1 regulatory requirements to identify the subset that is applicable to the generic ***SPINLINE 3*** digital safety I&C platform is documented in Table 3.1-1.

Also included in Table 3.1-1 are the following addition items not found in SRP Table 7-1:

- 10 CFR 50.49
- 10 CFR 50 Appendix B
- 10 CFR 73.54
- Regulatory Guides 1.89, 1.100, 1.153, 1.209, and 5.71
- Digital Instrumentation and Controls Interim Staff Guides (DI&C-ISGs)-01, -02, -04, -05, and -06

This chapter provides summary compliance statements for the applicable NRC regulatory requirements listed in Table 3.1-1, including the industry standards and other documents that are endorsed by Regulatory Guides or referenced in Branch Technical Positions. Table 3.1-1 identifies the LTR sections where the compliance statement can be found. In addition, the following supporting tables are provided.

- Table 3.2-1 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to Corresponding Rolls-Royce Civil Nuclear – SAS (RRCN) QA Plans & Procedures
- Table 3.2-2 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to Corresponding Data Systems & Solutions LLC (DS&S) QA Plans & Procedures
- Table 3.6-1 Responses to NUREG/CR-6082 Communications System Questions
- Table 3.7-1 Interim Staff Guide DI&C-ISG-04, Revision 1 Compliance Matrix
- Table 3.8-1 IEEE Standard 7-4.3.2-2003 Compliance Matrix
- Table 3.8-2 IEEE Standard 603-1991 Compliance Matrix
- Table 3.10-1 IEC 880-1986 Appendix B Compliance Matrix
- Table 3.10-2 Comparison of IEC 880-1986 and NRC Branch Technical Position 7-14 Requirements

3.2 10 CFR 50, Code of Federal Regulations

3.2.1 10 CFR 50, Sections 50.34 and 50.55a

3.2.1.1 50.34(f)(2)(v) [I.D.3], Bypass and Operable Status Indication

Plant-specific applications of the ***SPINLINE 3*** digital safety I&C platform will comply with the requirement to provide automatic indication of the bypassed and operable status of safety systems. The generic ***SPINLINE 3*** platform supports indications in the main control room and hardwired discrete outputs can be provided as described in Section 4.6.2.

3.2.1.2 50.55a(a)(1), Quality Standards for Systems Important to Safety

The basic requirement is that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The ***SPINLINE 3*** digital safety I&C platform is intended for use in Class 1E safety I&C applications.

As described in Section 1.4, the RRCN and DS&S quality systems that governs all ***SPINLINE 3*** activities are compliant with 10 CFR 50 Appendix B and ASME NQA-1-1994. See Sections 3.2.3 and 3.13 for compliance details.

3.2.1.3 50.55a(h)(2), Protection Systems (IEEE Standard 603-1991 or IEEE Standard 279-1971)

As required in 50.55a(h)(2), the ***SPINLINE 3*** digital safety I&C platform complies with IEEE Standard 603-1991. IEEE Standard 603 compliance is addressed in Section 3.8.9 and in Table 3.8-2.

3.2.1.4 50.55a(h)(3), Safety Systems (IEEE Std 603-1991)

As required by 50.55a(h)(3), the ***SPINLINE 3*** digital safety I&C platform complies with IEEE Standard 603-1991. IEEE Standard 603 compliance is addressed in Section 3.8.9 and Table 3.8-2.

3.2.1.5 50.49, Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants

50.49 identifies specific requirements for qualification of electric equipment important to safety. Regulatory Guide 1.89 describes methods acceptable to the NRC for complying with 50.49. ***SPINLINE 3*** compliance with RG 1.89 is addressed in Section 3.3.6.

3.2.2 10 CFR 50 Appendix A, General Design Criteria (GDCs)

3.2.2.1 GDC 1, Quality Standards and Records

The basic requirement is that structures, systems, and components shall be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The generic ***SPINLINE 3*** digital safety I&C platform is intended for use in Class 1E safety I&C applications.

The ***SPINLINE 3*** digital safety I&C platform complies with GDC 1. The applicable quality standards are 10 CFR 50 Appendix B and ASME NQA-1-1994. See Sections 3.2.3 and 3.13 for compliance details.

3.2.2.2 GDC 2, Design Bases for Protection Against Natural Phenomena

The basic requirement is that structures, systems, and components important to safety shall be designed to withstand the effects of a range of natural phenomena without loss of capability to perform their safety functions. The ***SPINLINE 3*** digital safety I&C platform is intended for use in Class 1E safety I&C applications.

The ***SPINLINE 3*** digital safety I&C platform complies with GDC 2. The generic qualification program for ***SPINLINE 3*** is described in Section 5.1, with more details in the Equipment Qualification (EQ) Plan (Reference 3-2).

Plant-specific applications of the ***SPINLINE 3*** digital safety I&C platform will address the correspondence of the generic qualification envelope for ***SPINLINE 3*** with the site-specific qualification bounding envelopes.

3.2.2.3 GDC 4, Environmental and Dynamic Effects Design Bases

The basic requirement is that structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.

The ***SPINLINE 3*** digital safety I&C platform complies with GDC 4. The ***SPINLINE 3*** digital safety I&C platform is qualified for use in mild environments, as described in Section 5.1 and in the Equipment Qualification (EQ) Plan (Reference 3-2).

3.2.2.4 GDC 13, Instrumentation and Control

The ***SPINLINE 3*** digital safety I&C platform complies with GDC 13. As described in Section 4.3, the standard input boards enable the design of ***SPINLINE 3*** systems that can monitor a wide range of variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety.

Plant-specific applications of the ***SPINLINE 3*** digital safety I&C platform will address how the monitoring and control capability provided is appropriate to assure adequate safety.

3.2.2.5 GDC 20, Protection System Functions

Plant-specific safety I&C systems implemented on the generic ***SPINLINE 3*** digital safety I&C platform will provide the capability to comply with GDC 20. The standard ***SPINLINE 3*** hardware described in Section 4.3, the software described in Sections 4.4 to 4.6 and the software life cycle processes described in Chapter 6 are the foundations for designing and implementing plant-specific safety I&C systems that accomplish the GDC 20 safety functions.

Plant-specific applications of the ***SPINLINE 3*** digital safety I&C platform will define the specific system functions to be performed.

3.2.2.6 GDC 21, Protection Systems Reliability and Testability

Plant-specific safety I&C systems implemented on the generic ***SPINLINE 3*** digital safety I&C platform will comply with GDC 21.

SPINLINE 3 is designed for high functional reliability. A summary board/device-level hardware reliability is provided in Section 5.2 along with references to the separate detailed analyses.

The ***SPINLINE 3*** software is designed to be highly reliable. The platform software life cycle processes are described in Sections 6.2 an 6.3 and are assessed in the Design Analysis Report (DAR, Reference 3-3). The BTP 7-14 compliant application software life cycle processes are described in Section 6.4.

The in-service testing and periodic testing features of ***SPINLINE 3*** are described in Sections 4.4, 4.5 and 4.6.

The standard ***SPINLINE 3*** hardware and software described in Section 4.3 can be readily employed in system architectures with redundant and independent divisions that comply with the single failure criterion. The specific means for complying with these requirements for redundancy and independence must be assessed on a plant-specific basis.

3.2.2.7 GDC 22, Protection System Independence

Plant-specific safety I&C systems implemented on the generic ***SPINLINE 3*** digital safety I&C platform can comply with GDC 22. ***SPINLINE 3*** systems have the requisite independence of divisions to ensure that a fault in one independent division does not propagate and affect other redundant divisions. Representative ***SPINLINE 3*** single division and four division architectures are described in Section 4.2.4. As described in Section 3.7, ***SPINLINE 3*** inter-divisional communications complies with Interim Staff Guide DI&C-ISG-04.

Likewise, ***SPINLINE 3*** systems have the requisite independence to ensure that a postulated fault in a connected non-safety I&C system does not propagate and affect the safety I&C system. As described in Section 4.5, this is accomplished by one-way (broadcast only) communication from the safety I&C system to the non-safety I&C system. In addition, ***SPINLINE 3*** output relays can be connected to non-Class 1E systems. The Class 1E / non-Class 1E isolation capability of these relays is verified through qualification testing, which is described in Section 5.1 and the Equipment Qualification (EQ) Plan (Reference 3-2).

Standard ***SPINLINE 3*** hardware is qualified for a mild operating environment, with a generic qualification envelope as described in Section 5.1 and in the EQ Plan. Operation within this envelope will not result in loss of the protection function.

The in-service testing and periodic testing features of ***SPINLINE 3*** are described in Section 4.4, 4.5 and 4.6. With appropriate redundancy in an actual system, maintenance and testing activities will not result in loss of the protection function.

Diversity and defense-in-depth should be addressed in the context of an NPP's suite of safety and non-safety I&C systems. ***SPINLINE 3*** can employ signal diversity.

The design and implementation of ***SPINLINE 3*** digital communications described in Section 4.5 enables independence to be maintained between redundant divisions and between the safety I&C system and non-safety I&C systems. The inter-divisional communications provisions comply with Interim Staff Guide DI&C-ISG-04, as described in Section 3.7.4.

3.2.2.8 GDC 23, Protection System Failure Modes

Plant-specific safety I&C systems implemented on the generic ***SPINLINE 3*** digital safety I&C platform have the capability to comply with GDC 23. Modes of operation of the ***SPINLINE 3*** Operational System Software (OSS) are described in Section 4.4.3.4, which also explains the behavior of the OSS when a failure is detected.

As discussed in Section 5.2, board-level Failure Mode and Effects Analyses (FMEAs) will be documented in a separate report. Documentation of system-level failure modes will be assessed in connection with a plant-specific application of ***SPINLINE 3***.

3.2.2.9 GDC 24, Separation of Protection and Control Systems

Plant-specific safety I&C systems implemented on the generic ***SPINLINE 3*** digital safety I&C platform will comply with GDC 24.

The design and implementation of ***SPINLINE 3*** digital communications described in Section 4.5 enables separation to be maintained between the safety I&C system and non-safety I&C systems. These communications provisions comply with Interim Staff Guide DI&C-ISG-04, as described in Section 3.7.4.

3.2.2.10 GDC 25, Protection System Requirements for Reactivity Control Malfunctions

Plant-specific safety I&C systems implemented on the generic ***SPINLINE 3*** digital safety I&C platform have the capability to comply with GDC 25. The specific variables to be monitored and the associated processing logic must be determined on a plant-specific basis.

3.2.2.11 GDC 29, Protection Against Anticipated Operational Occurrences

The generic ***SPINLINE 3*** digital safety I&C platform can comply with GDC 29. Operating experience with ***SPINLINE 3*** systems and the previous generations of RRCN digital safety I&C systems described in Chapter 2 has shown no instances where the capability of the safety I&C system to perform its intended safety function(s) was compromised during an anticipated operational occurrence.

3.2.3 10 CFR 50 Appendix B, Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants

As described in Section 1.4, the requirements of 10 CFR 50 Appendix B and NQA-1-1994 are implemented in the RRCN Quality Management Plan (Reference 3-4) and the DS&S, LLC Instrumentation & Controls US Quality Manual (Reference 3-5). A map showing the correspondence between 10 CFR 50 Appendix B, ASME NQA-1-1994, and the RRCN quality procedures is provided in Table 3.2-1. A similar map showing the correspondence between 10 CFR 50 Appendix B, ASME NQA-1-1994, and the DS&S quality procedures is provided in Table 3.2-2.

3.2.4 Title 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks

Title 10 CFR 73.54 requires licensees to provide a high level of assurance that digital computer and communication systems are adequately protected against cyber attacks. Even though 10CFR73.54 is written primarily for licensees, most of the provisions are applicable to the cyber security programs of suppliers of digital computer and communication systems.

As described in Section 6.5, many of the RRCN cyber security activities are integrated with other software life cycle activities. A separate Cyber Security Plan will be developed to define the cyber security activities to be implemented for a plant-specific application of ***SPINLINE 3.***

3.3 USNRC Division 1 Regulatory Guides

3.3.1 Regulatory Guide (RG) 1.22, Revision 0, Periodic Testing of Protection System Actuation Functions

The ***SPINLINE 3*** digital safety I&C platform complies with RG 1.22. The periodic testing features of ***SPINLINE 3*** are described in Section 4.6.

3.3.2 Regulatory Guide 1.47, Revision 0, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System

Plant-specific applications of the ***SPINLINE 3*** digital safety I&C platform will comply with the requirement to provide automatic indication of the bypass or inoperable status of portions of the protection system. This feature is described in Section 4.6.2.

In plant-specific applications, compliance with RG 1.47 requires further determinations that bypass or inoperable status is also provided for the following:

- Systems actuated or controlled by the protection system

- Auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety functions.

RG 1.47 endorses IEEE Standard 279-1971 with qualifications. As allowed in 50.55a(h)(2), the ***SPINLINE 3*** digital safety I&C platform complies instead with IEEE Standard 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995.

3.3.3 Regulatory Guide 1.53, Revision 2, Application of the Single-Failure Criterion to Safety Systems

RG 1.53 endorses IEEE 379-2000 with qualifications (see Section 3.8.7). The standard ***SPINLINE 3*** hardware described in Section 4.3 and the software described in Sections 4.4 through 4.6 can be implemented in system architectures with redundant and independent channels, divisions and trains that comply with the single failure criterion. Representative ***SPINLINE 3*** single division and four division architectures are described in Section 4.2.4. The specific means for complying with the single failure criterion must be assessed on a plant-specific basis.

3.3.4 Regulatory Guide 1.62, Revision 0, Manual Initiation of Protection Actions

The standard ***SPINLINE 3*** hardware described in Section 4.3 and the software described in Sections 4.4 through 4.6 can be implemented with manual initiation features that comply with RG 1.62. The generic provisions for manual initiation are described in Section 4.3.4.5. Specific manual initiation features must be defined on a plant-specific basis.

RG 1.62 endorses IEEE Standard 279-1971 with qualifications. As allowed in 50.55a(h)(2), the ***SPINLINE 3*** digital safety I&C platform complies with IEEE Standard 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995.

3.3.5 Regulatory Guide 1.75, Revision 3, Criteria for Independence of Electrical Safety Systems

RG 1.75 endorses IEEE Standard 384-1992 with qualifications (see Section 3.8.8). The standard ***SPINLINE 3*** hardware described in Section 4.3 and the software described in Sections 4.4 through 4.6 are designed to establish and maintain the independence of safety-related equipment, circuits, and auxiliary supporting features by physical separation and electrical isolation. In a plant-specific application, this is accomplished by physically separating the redundant divisions of the safety system.

Representative ***SPINLINE 3*** architectures are described in Section 4.2.4. These typical architectures include the inter-divisional communication interfaces that are needed to support voting logic. As described in Section 4.5, inter-divisional communications is accomplished using fiber optic links that maintain the electrical isolation between divisions and NERVIA communication boards that maintain the required logical data isolation between divisions.

Electrical independence between Class 1E and non-Class 1E digital systems also is established by means of fiber optic links. As described in Section 4.5.7, data isolation is assured by implementing logical data isolation in the Class 1E systems as well as providing only one-way communications from the Class 1E system to the non-Class 1E system.

3.3.6 Regulatory Guide 1.89, Revision 1, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants"

This RG describes methods acceptable to the NRC for complying with 10 CFR 50.49 with regard to qualification of electric equipment important to safety for service in NPPs. These methods ensure the equipment can perform its safety function during and after a design basis accident. This RG endorses IEEE Standard 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Stations" with qualifications (see Section 3.8.3).

As described in Section 5.1 and the Equipment Qualification (EQ) Plan (Reference 3-2), ***SPINLINE 3*** is qualified for mild environments. Qualification testing of ***SPINLINE 3*** is performed in accordance with the IEEE Standard 323-2003 subject to the enhancements and exceptions listed in Section C, "Regulatory Position" of RG 1.209, "Guidelines for Environmental Qualification of Safety Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants" (see Section 3.3.19)

3.3.7 Regulatory Guide 1.100, Revision 2, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants

This RG endorses IEEE Standard 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," with qualifications (see Section 3.8.5).

As described in Section 5.1 and the Equipment Qualification (EQ) Plan (Reference 3-2), seismic qualification testing of ***SPINLINE 3*** is performed in accordance with the IEEE Standard 344-1987 using the generic seismic spectra documented in EPRI technical report TR-107330 (see Section 3.12.1).

3.3.8 Regulatory Guide 1.105, R3, Setpoints for Safety-Related Instrumentation

This RG endorses Instrument Society of America (ISA) Standard S67.04-1994, "Methodology for the Determination of Setpoints for Nuclear Safety-Related Instrumentation," with qualifications (see Section 3.9.1).

As described in Section 5.2.3, EPRI TR-107330, Section 4.2.4 requires the qualifier to provide information about the qualified hardware to support an application specific setpoint analysis per ISA S67.04. Section 5.2 describes the approach RRCN, as both vendor and qualifier, will use for preparing the setpoint analysis support documentation for the ***SPINLINE 3*** digital safety I&C platform. This documentation will provide sufficient design specification data for a setpoint analysis to be performed on a plant-specific ***SPINLINE 3*** system.

Compliance of actual system setpoints with ISA S67.04-1994 will be addressed on a plant-specific basis.

3.3.9 Regulatory Guide 1.118, Revision 3, Periodic Testing of Electric Power and Protection Systems

This RG endorses IEEE Standard 338-1987 with qualifications. As provided in IEEE Standard 338, automatic testing provisions for programmable digital computer-based systems are subject to the testing provisions of this standard and IEEE Standard 7-4.3.2-2003. See Section 3.8.1 for compliance with IEEE Standard 7-4.3.2.

3.3.10 Regulatory Guide 1.152, Revision 2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

This RG endorses IEEE Standard 7-4.3.2-2003 with qualifications.

Compliance of the ***SPINLINE 3*** software design with IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" is addressed in Section 3.8.1 and Table 3.8-1, which addresses Regulatory Position 1.

As described in Section 6.5, many of the RRCN cyber security activities are integrated with other software life cycle activities. A separate Cyber Security Plan will be developed to define the cyber security activities to be implemented for a plant-specific application of ***SPINLINE 3.*** This RRCN Cyber Security Plan and the licensee Cyber Security Plan together will address Regulatory Positions 2.1 through 2.9.

3.3.11 Regulatory Guide 1.153, Revision 1, Criteria for Safety Systems

This RG endorses IEEE Standard 603-1991 and the correction sheet of January 30, 1995. Refer to Section 3.8.9 and Table 3.8-1 for compliance with IEEE Standard 603 and the correction sheet.

3.3.12 Regulatory Guide 1.168, Revision 1, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This RG endorses IEEE Standard 1012-1998 and IEEE 1028-1997 with qualifications.

The verification and validation (V&V) process for the ***SPINLINE 3*** platform software was established according to the guidance provided in IEC 880-1986 (see Section 3.10 for compliance matrix), and was documented in dedicated V&V plans and reports, which are described in Section 6.2. As described in Chapter 1, the ***SPINLINE 3*** platform software has been dedicated for use in systems delivered to U.S. customers and is now managed under the RRCN 10CFR50 Appendix B QA Program.

As described in Section 6.4, the V&V process for the ***SPINLINE 3*** application software complies with RG 1.168. The specific V&V activities for application software will be defined on a plant-specific basis in connection with implementation of a safety application.

3.3.13 Regulatory Guide 1.169, Revision 0, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This RG endorses IEEE Standard 828-1990 and IEEE Standard 1042-1987 with qualifications.

The configuration management (CM) process for the ***SPINLINE 3*** platform software was established according to the guidance provided in IEC 880-1986 (see Section 3.10 for compliance matrix), and was documented in dedicated CM plans and reports, which are described in Section 6.2. As described in Chapter 1, the ***SPINLINE 3*** platform software has been dedicated for use in systems delivered to U.S. customers and is now managed under the RRCN 10CFR50 Appendix B QA Program.

As described in Section 6.4, the configuration management process for the ***SPINLINE 3*** application software complies with RG 1.169. The specific configuration management activities for application software will be defined on a plant-specific basis in connection with implementation of a safety application.

3.3.14 Regulatory Guide 1.170, Revision 0, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This RG endorses IEEE Standard 829-1983 with qualifications.

The test documentation for the ***SPINLINE 3*** platform software was established according to the guidance provided in IEC 880-1986 (see Section 3.10 for compliance matrix), and was documented in dedicated test plans and reports, which are described in Section 6.2. As described in Chapter 1, the ***SPINLINE 3*** platform software has been dedicated for use in systems delivered to U.S. customers and is now managed under the RRCN 10CFR50 Appendix B QA Program.

As described in Section 6.4, the test documentation for the ***SPINLINE 3*** application software complies with RG 1.170. Test activities for ***SPINLINE 3*** application software consist of the following:

- Unit / component level tests
- Integration and system-level factory testing.
- System-level site acceptance testing

The specific testing activities for application software will be defined on a plant-specific basis in connection with implementation of a safety application.

3.3.15 Regulatory Guide 1.171, Revision 0, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This RG endorses IEEE Standard 1008-1987 with qualifications.

The ***SPINLINE 3*** platform software and application software are subject to verification and validation (V&V) testing that includes unit (component) testing, as described in Section 6.2.2.5 (OSS) and 6.4.4 (application software). As described in Section 6.2.9, the application-oriented library of re-usable components were developed using the same software life cycle processes as the OSS.

3.3.16 Regulatory Guide 1.172, Revision 0, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This RG endorses IEEE Standard 830-1993 with qualifications.

The Software Requirements Specification (SRS) for the ***SPINLINE 3*** platform software described in Section 6.2 was established according to the guidance provided in IEC 880-1986 (see Section 3.10 for compliance matrix), As described in Chapter 1, the ***SPINLINE 3*** platform software has been dedicated for use in systems delivered to U.S. customers and is now managed under the RRCN 10CFR50 Appendix B QA Program.

As discussed in Section 6.4, the application software SRS will be developed on a plant-specific basis. The licensee is responsible for demonstrating that the SRS follows the guidance contained in this RG and in the endorsed IEEE Standard 830. The generic application software plan templates are described in Section 6.4.

3.3.17 Regulatory Guide 1.173, Revision 0, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This RG endorses IEEE Standard 1074-1995 with qualifications. This RG, BTP 7-14 and the IEEE Standard 1074 provide a structured approach for developing a software life cycle program consistent with this regulatory guidance.

The life cycle processes for the ***SPINLINE 3*** platform software were established according to the guidance provided in IEC 880-1986 (see Section 3.10 for compliance matrix), and were documented in dedicated software plans, which are described in Section 6.2. The ***SPINLINE 3*** software life cycle processes also took into account additional process enhancements employed on the EDF N4 project and ongoing standardization works for a supplement to IEC 880, which was issued in 2000. Based on the analysis reported in the ***SPINLINE 3*** Design Analysis Report (DAR, Reference 3-3), RRCN concludes that the platform software complies with the intent of IEEE Standard 1074 and with Regulatory Guide 1.173. As described in Chapter 1, the ***SPINLINE 3*** platform software has been dedicated for use in systems delivered to U.S. customers and is now managed under the RRCN 10CFR50 Appendix B QA Program.

The application software life cycle Plans described in Section 6.4 implement the structured approach, described in RG 1.173. While the RG and IEEE Standard 1074 do not specify the completion of specific documents, BTP 7-14 places emphasis on the output documents as a means to demonstrate successful completion of a life cycle process. The corresponding output documents for the ***SPINLINE 3*** application software life cycle are identified in Section 6.4.

3.3.18 Regulatory Guide 1.180, Revision 1, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems Instrumentation and Control Systems

This RG endorses IEC 61000, MIL-STD-461E, IEEE Standard 1050-1996, IEEE Standard C62.41-1991, and IEEE Standard C62.45-1992 with qualifications.

As described in Section 5.1 and in the Equipment Qualification (EQ) Plan (Reference 3-2), EMI/RFI testing of the ***SPINLINE 3*** Qualification Test Specimen (QTS) will be performed in accordance with RG 1.180 revision 1. Grounding and shielding is in accordance with IEEE Standard 1050 (see Section 3.8.17). The specific test plans and test levels are described in the EQ Plan, Appendices F, G, H and I:

3.3.19 Regulatory Guide 1.209, Revision 0, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants

This RG endorses IEEE Standard 323-2003 with qualifications. As described in Section 5.1 and the Equipment Qualification (EQ) Plan (Reference 3-2), qualification testing of the ***SPINLINE 3*** is performed in accordance with IEEE Standard 323-2003, subject to the enhancements and exceptions listed in Section C, “Regulatory Position” of RG 1.209.

3.3.20 Regulatory Guide 5.71, Revision 0, Cyber Security for Nuclear Facilities

Regulatory Guide 5.71 defines the elements of a cyber security program that are deemed to be acceptable by the NRC to comply with the regulations set forth in 10CFR73.54. As described in Section 6.5, many RRCN cyber security activities are integrated with other software life cycle activities. A separate Cyber Security Plan will be developed to define the cyber security activities to be implemented for a plant-specific application of ***SPINLINE 3.*** This Plan will comply with RG 5.71 and Interim Staff Guide DI&C-ISG-01.

3.4 NUREG-0800, Chapter 7, Revision 5 Branch Technical Positions (BTPs)

3.4.1 BTP 7-8, Revision 5, Guidance on Application of Regulatory Guide 1.22

As noted in Section 3.3.1, ***SPINLINE 3*** complies with RG 1.22. The ***SPINLINE 3*** digital safety I&C platform also complies with IEEE Standard 603. Refer to Section 3.8.9 for a discussion on IEEE Standard 603 compliance. The periodic testing features of ***SPINLINE 3*** are described in Section 4.6.

3.4.2 BTP 7-11, Revision 5, Guidance on Application and Qualification of Isolation Devices

As described in Section 4.3, ***SPINLINE 3*** uses the following types of qualified isolation devices: (1) fiber optic cables, and (2) relays. Signal isolation within the NERVIA network is discussed in the Digital Instrumentation and Controls Interim Staff Guidance (DI&C ISG)-4 compliance matrix in Section 3.7.4. Qualification is described in Section 5.1 and in the Equipment Qualification (EQ) Plan (Reference 3-2).

3.4.3 BTP 7-12, Revision 5, Guidance on Establishing and Maintaining Instrument Setpoints

EPRI TR-107330, Section 4.2.4 requires the qualifier to provide information about the qualified hardware to support an application specific setpoint analysis per ISA 67.04. Section 5.2. describes how RRCN, as both vendor and qualifier, will apply this approach and prepare a setpoint analysis support document for the ***SPINLINE 3*** digital safety I&C platform. This documentation is intended to provide sufficient design specification data for a plant-specific setpoint analysis to be performed.

3.4.4 BTP 7-14, Revision 5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

The life cycle processes for the ***SPINLINE 3*** platform software were established according to the guidance provided in IEC 880-1986 (see compliance matrix in Section 3.10), and were documented in dedicated software plans, which are described in Section 6.2. The ***SPINLINE 3*** software life cycle processes also took into account additional process enhancements employed on the EDF N4 project and ongoing standardization works for a supplement to IEC 880, which was issued in 2000. Based on the mapping of platform software documentation to BTP 7-14 in Section 6.3 and the additional analysis in the Design Analysis Report (DAR, Reference 3-3), RRCN concludes that the platform software complies with the intent of BTP 7-14. As described in Chapter 1, the ***SPINLINE 3*** platform software has been dedicated for use in systems delivered to U.S. customers and is now managed under the RRCN 10CFR50 Appendix B QA Program.

RRCN's application software life cycle plans and processes comply with BTP 7-14. Refer to Section 6.4 for a mapping of the BTP 7-14 software plans to the equivalent RRCN software plans. Also in Section 6.4 is an identification of the outputs from the RRCN software life cycle processes.

3.4.5 BTP 7-17, Revision 5, Guidance on Self-Test and Surveillance Test Provisions

SPINLINE 3 self-diagnostic test and surveillance test provisions comply with BTP 7-17, as discussed in Sections 4.4, 4.5 and 4.6.

3.4.6 BTP 7-19, Revision 5, Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems

Diversity and defense-in-depth (D3) should be addressed in the context of an NPP’s suite of safety and non-safety I&C systems. ***SPINLINE 3*** systems have the capability to implement signal diversity.

3.4.7 BTP 7-21, Revision 5, Guidance on Digital Computer Real-Time Performance

The generic ***SPINLINE 3*** digital safety I&C platform addresses all of the concerns raised in this BTP:

- The ***SPINLINE 3*** architecture provides for reliable system operation and appropriate separation and independence of divisions. See example architectures in Section 4.2.4. Specific system architecture will be determined on a plant-specific basis.
- Deterministic communications inherent in ***SPINLINE 3*** systems guarantees system response time. See Section 4.5.
- The generic setpoint analysis support documentation described in Section 5.2 will provide a single, concise listing of the design specifications data for the ***SPINLINE 3*** digital safety I&C platform. This will be an input to the setpoint analyses done for plant-specific ***SPINLINE 3*** systems.
- The design basis for a ***SPINLINE 3*** system will be defined on a plant-specific basis.

3.5 USNRC Staff Requirements Memos (SRMs)

3.5.1 SRM to SECY 93-087, II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems

Refer to the BTP 7-19 discussion in Section 3.4.6.

3.6 USNRC NUREGs and NUREG/CRs

3.6.1 NUREG/CR 6082, Data Communications

Section 2 of NUREG/CR-6082 has 15 questions intended to help focus reviews of data communication systems. Table 3.6-1 provides an evaluation the ***SPINLINE 3*** platform for those questions.

3.7 USNRC Digital I&C Interim Staff Guides (ISGs)

3.7.1 DI&C-ISG-01, Rev. 0, Cyber Security

As described in Section 6.5, many RRCN cyber security activities are integrated with other software life cycle activities. A separate Cyber Security Plan will be developed to define the cyber security activities to be implemented for a plant-specific application of ***SPINLINE 3.*** This Plan will comply with RG 5.71 and Interim Staff Guide DI&C-ISG-01.

3.7.2 DI&C-ISG-02, Rev. 1, Diversity and Defense-in-Depth (D3)

Diversity and defense-in-depth (D3) should be addressed in the context of an NPP's suite of safety and non-safety I&C systems. ***SPINLINE 3*** systems can employ signal diversity.

3.7.3 DI&C-ISG-04, Rev. 1, Highly Integrated Control Rooms – Digital Communication Systems

The generic ***SPINLINE 3*** digital safety I&C platform and application-specific ***SPINLINE 3*** systems will comply with DI&C-ISG-04 requirements regarding inter-divisional communication. The generic ***SPINLINE 3*** digital safety I&C platform does not include priority logic for command prioritization. The generic design supports multi-divisional communication only in divisional voting logic and divisional display processors as described in Section 4.2.4. Refer to the DI&C-ISG-04 compliance matrix in Table 3.7-1.

3.7.4 DI&C-ISG-06, Draft, Licensing Process

The documents submitted by RRCN for the NRC generic review of the ***SPINLINE 3*** digital safety I&C platform will be generally consistent with the guidance in the May 2009 draft DI&C-ISG-06, which lists the documents expected for a plant-specific review. Many of the listed documents do not apply to the generic Tier 3 review of a digital safety I&C platform.

3.8 Institute of Electrical & Electronics Engineers (IEEE) Standards

3.8.1 IEEE Standard 7-4.3.2-2003, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

This standard is endorsed by Regulatory Guide 1.152 with qualifications. ***SPINLINE 3*** application software complies with IEEE Standard 7-4.3.2-2003. See details in the compliance matrix in Table 3.8-1.

The ***SPINLINE 3*** Class 1E Operational System Software (OSS) and other platform software were developed before this version of the IEEE standard was published. As described in Section 6.2, the OSS was developed using the life cycle process which was defined and used for the N4 project. This process was originally established based on the guidance of the International Electrotechnical Commission (IEC) Standard 880-1986 with enhancements to take into account the advances in software engineering reflected in a later revision of the standard.

Also as described in Section 6.2, the Application-Oriented Library components of the ***SPINLINE 3*** platform software were developed according to the same software life cycle process and Quality Assurance Program as the OSS

While not in strict compliance with the life cycle defined in IEEE Standard 7-4.3.2, the life cycle used in developing the ***SPINLINE 3*** platform software provides equivalent protection and high quality through production of similar documents and performance of reviews, testing, verification, validation, and quality assurance activities. As described in Section 1.1,, RRCN has dedicated the ***SPINLINE 3*** generic platform software. The technical basis for dedication is documented in a ***SPINLINE 3*** Design Analysis Report (DAR, Reference 3-3)

3.8.2 IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations

This standard is endorsed by 10CFR 50.55a(h)(2), Regulatory Guides 1.47 and 1.62. As required in 50.55a(h)(2), the ***SPINLINE 3*** digital safety I&C platform complies with IEEE Standard 603-1991 instead of IEEE Standard 279-1971. See Section 3.8.9 for details.

3.8.3 IEEE Standard 323-2003, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

This standard is endorsed by Regulatory Guide 1.209 with qualifications. An earlier edition, IEEE Standard 323-1974 is endorsed by RG 1.89.

As described in Section 5.1 and the Equipment Qualification (EQ) Plan (Reference 3-2), qualification testing of the ***SPINLINE 3*** is performed in accordance with IEEE Standard 323-2003, subject to the enhancements and exceptions listed in Section C, “Regulatory Position” of RG 1.209.

3.8.4 IEEE Standard 338-1987, Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

This standard is endorsed by Regulatory Guide 1.118 with qualifications.

As described in Section 4.6.7, periodic surveillance testing provisions of ***SPINLINE 3*** comply with IEEE Standard 338. A comparison of the coverage of self-diagnostic tests and periodic tests is provided in Section 4.6.8.4.

3.8.5 IEEE Standard 344-1987, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

This standard is endorsed by Regulatory Guide 1.100 with qualifications.

As described in Section 5.1 and the Equipment Qualification (EQ) Plan (Reference 3-2), seismic qualification testing of ***SPINLINE 3*** is performed in accordance with IEEE Standard 344-1987,

3.8.6 IEEE Standard 352-1987, Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems

As discussed in Section 5.2., generic board/module-level failure mode and effects analyses (FMEAs) will meet the requirements of IEEE Standard 352, Sections 4.1, 4.4 and 4.5.

As discussed in Section 5.2, the methods of estimating reliability of components will be based on IEC TR 62380, "Reliability Data Handbook, Universal Model for Reliability Prediction of Electronics Components, PCBs and Equipment," (see Section 3.10.3) instead of MIL HDBK 217F as suggested in IEEE Standard 352. The rationale for selecting IEC TR 62380 rather than MIL HDBK 217F is that the military handbook is significantly out of date, and has not been updated to reflect the evolution of modern electronics, while the IEC publication has been updated.

3.8.7 IEEE Standard 379-2000, Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

IEEE Standard 379-2000 is endorsed by Regulatory Guide 1.53 with qualifications. The standard ***SPINLINE 3*** hardware and software components described in Chapter 4 can be implemented in redundant and independent system architectures that comply with the single failure criterion. The specific means for complying with the single failure criterion must be assessed on a plant-specific basis.

3.8.8 IEEE Standard 384-1992, Standard Criteria for Independence of Class 1E Equipment and Circuits

This standard is endorsed by Regulatory Guide 1.75 with qualifications.

The standard ***SPINLINE 3*** hardware components described in Section 4.3 and software described in Section 4.4 through 4.6 are designed for establishing and maintaining the independence of safety-related equipment and circuits, and auxiliary supporting features by physical separation and electrical isolation. In a plant-specific application, this is accomplished by physically separating the redundant channels, divisions and trains of the safety system.

Example ***SPINLINE 3*** architectures are described in Section 4.2.4. These typical architectures include the inter-divisional communication interfaces that are needed to support voting logics. Communications between redundant divisions and trains is isolated and designed to retain the required independence. .As described in Section 4.5, inter-divisional communications is accomplished using fiber optic data links that maintain the electrical isolation between divisions.

The typical architectures described in Section 4.2.4 also include Class 1E to non-Class 1E communications interfaces. As described in Section 4.5.7, electrical isolation between the Class 1E system and the non-Class 1E system is accomplished using fiber optic data links and one-way (broadcast only) communications from the Class 1E system to the non-Class 1E system.

3.8.9 IEEE Standard 603-1991, Criteria for Safety Systems for Nuclear Power Generating Stations

This standard, with the January 30, 1995 correction sheet, is endorsed by 10 CFR 50.55a(h)(2) and Regulatory Guide 1.153. The generic ***SPINLINE 3*** digital safety I&C platform and application-specific ***SPINLINE 3*** systems comply with IEEE Standard 603. Refer to the IEEE Standard 603 compliance matrix in Table 3.8-2.

3.8.10 IEEE Standard 828-1990, IEEE Standard for Software Configuration Management Plans

This standard is endorsed by Regulatory Guide 1.169 with qualifications. Refer to the RG 1.169 compliance statement in Section 3.3.13.

3.8.11 IEEE Standard 829-1983, IEEE Standard for Software Test Documentation

This standard is endorsed by Regulatory Guide 1.170 with qualifications. Refer to the RG 1.170 compliance statement in Section 3.3.14.

3.8.12 IEEE Standard 830-1993, IEEE Recommended Practice for Software Requirements Specifications

This standard is endorsed by Regulatory Guide 1.172 with qualifications. Refer to the RG 1.172 compliance statement in Section 3.3.16.

3.8.13 IEEE Standard 1008-1987, IEEE Standard for Software Unit Testing

This standard is endorsed by Regulatory Guide 1.171 with qualifications. Refer to the RG 1.171 compliance statement in Section 3.3.15.

3.8.14 IEEE Standard 1012-1998, IEEE Standard for Software Verification and Validation Plans

This standard is endorsed by Regulatory Guide 1.168 with qualifications. Refer to the RG 1.168 compliance statement in Section 3.3.12.

3.8.15 IEEE Standard 1028-1997, IEEE Standard for Software Reviews and Audits

This standard is endorsed by Regulatory Guide 1.168 with qualifications. Refer to the RG 1.168 compliance statement in Section 3.3.12

3.8.16 IEEE Standard 1042-1987, IEEE Guide to Software Configuration Management

This standard is endorsed by Regulatory Guide 1.169 with qualifications. Refer to the RG 1.169 compliance statement in Section 3.3.13.

3.8.17 IEEE Standard 1050-1996, Guide for Instrumentation and Control Equipment Grounding in Generating Stations

This standard is endorsed by Regulatory Guide 1.180, R1 with qualifications. The Qualification Test Specimen (QTS) grounding and shielding is described in the Equipment Qualification (EQ) Plan (Reference 3-2), in Appendices F, G, H, I and J. This grounding and shielding will be in accordance with the requirements of IEEE Standard 1050.

Grounding and shielding for plant-specific ***SPINLINE 3*** system comply with the requirements of IEEE Standard 1050.

3.8.18 IEEE 1074-1995, IEEE Standard for Developing Software Life Cycle Processes

This standard is endorsed by Regulatory Guide 1.173 with qualifications. Refer to the RG 1.173 compliance statement in Section 3.3.17.

The ***SPINLINE 3*** platform software was developed before this IEEE standard was published. The applicable life cycle processes are described in Section 6.2. Based on the analysis reported in the Design Analysis Report (DAR, Reference 3-3), RRCN concludes that the platform software complies with the intent of IEEE Standard 1074 and with Regulatory Guide 1.173.

Also see Section 6.4 for a description of the application software life cycle processes, which comply with BTP 7-14.

3.9 Instrument Society of America (ISA) Standards

3.9.1 ISA Standard S67.04-1994, Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Points

This standard is endorsed by Regulatory Guide 1.105 with qualifications.

As described in Section 5.2.3, EPRI TR-107330, Section 4.2.4 requires the qualifier to provide information about the qualified hardware to support an application specific setpoint analysis per ISA S67.04. Section 5.2 describes the approach RRCN, as both vendor and qualifier, will use for preparing the setpoint analysis support documentation for the ***SPINLINE 3*** digital safety I&C platform. This documentation will provide sufficient design specification data for a setpoint analysis to be performed on a plant-specific ***SPINLINE 3*** system.

3.10 International Electrotechnical Commission (IEC) Standards

3.10.1 IEC 880-1986, Software for Computers in the Safety Systems of Nuclear Power Stations

The life cycle processes for the ***SPINLINE 3*** platform software were established according to the guidance provided in IEC 880-1986, and were documented in dedicated software plans, which are described in Section 6.2. The ***SPINLINE 3*** software life cycle processes also took into account additional process enhancements employed on the EDF N4 project and ongoing standardization works for a supplement to IEC 880, which was issued in 2000.

Table 3.10-1 provides the OSS compliance matrix with the design requirements of IEC 880-1986 Appendix B.

Table 3.10-2 provides a comparison of IEC 880-1986 requirements with the corresponding requirements from BTP 7-14.

3.10.2 IEC 61000, Electromagnetic Compatibility (EMC)

As described in the Section 5.1, EMI/RFI testing of the ***SPINLINE 3*** Qualification Test Specimen (QTS) will be performed in accordance with RG 1.180, Revision 1, which endorses IEC 61000 and other standards. The Equipment Qualification Plan (Reference 3-2), Appendices F, G, H and I provide details on the specific IEC 61000 tests to be performed. Other EMI/RFI qualification tests are performed in accordance with MIL-STD-461E, which also is endorsed by RG 1.180, Revision 1.

3.10.3 IEC TR 62380, Reliability Data Handbook, Universal Model for Reliability Prediction of Electronics Components, PCBs and Equipment

As discussed in Section 5.2.2, the methods of estimating reliability of components will be based on IEC TR 62380 instead of MIL HDBK 217F, which is recommended in IEEE 352. The rationale for selecting IEC TR 62380 rather than MIL HDBK 217F is that the military handbook is significantly out of date, and has not been updated to reflect the evolution of modern electronics, while the IEC publication has been updated.

3.11 U.S. Military Standard

3.11.1 MIL-STD-461E, DOD Interface Standard Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment

EMI/RFI testing of the ***SPINLINE 3*** Qualification Test Specimen (QTS) will be performed in accordance with USNRC RG 1.180, Revision 1, which endorses United States Military Standard 461, Revision E (MIL-STD-461E). See Section 5.1 and the Equipment Qualification (EQ) Plan (Reference 3-2), Appendix F, for the specific MIL-STD-461E tests to be performed. Other EMI/RFI qualification tests are performed in accordance with IEC 61000.

3.12 Electric Power Research Institute (EPRI) Technical Reports and Handbooks

3.12.1 EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants

The generic qualification approach described in Chapter 5 and in the Equipment Qualification (EQ) Plan (Reference 3-2) uses guidance from EPRI TR-107330, Section 4.3.9 to define the recommended seismic test levels for seismic testing in accordance with IEEE 344. These seismic test levels are implemented in EQ Plan Appendix E.

As described in Section 5.2.3, EPRI TR-107330, Section 4.2.4 requires the qualifier to provide information about the qualified hardware to support an application specific setpoint analysis per ISA S67.04. Section 5.2.3 describes the approach RRCN, as both vendor and qualifier, will use for preparing the setpoint analysis support documentation for the ***SPINLINE 3*** digital safety I&C platform. This documentation will not provide a setpoint methodology or generate setpoint values. Rather, this documentation provides sufficient design specification data for a setpoint analysis to be performed on a plant-specific ***SPINLINE 3*** system

As described in Section 5.2.3, the component aging analysis described in EPRI TR-107330, Section 4.7.8.2 is not required for the standard ***SPINLINE 3*** hardware, which will be installed in a mild environment, where repair is possible after an accident. Aging analysis is required only where equipment is installed in a harsh environment, where repair is not possible after an accident. RRCN will not comply with the incorrect guidance in EPRI TR-107330, Section 4.7.8.2.

3.12.2 EPRI Handbook 1011710, Handbook for Evaluating Critical Digital Equipment and Systems

This EPRI Handbook was used to structure the Critical Design Review (CDR) of ***SPINLINE 3*** platform software. The results of the CDR are incorporated in this topical report, rather than being supplied in a separate Design Analysis Report (Reference 3-3)

3.13 American Society of Mechanical Engineers (ASME)

3.13.1 ASME NQA-1-1994, Quality Assurance Program Requirements for Nuclear Facilities

As described in Section 1.4, the requirements of 10CFR50 Appendix B and NQA-1-1994 are implemented in the RRCN Quality Management Plan (Reference 3-4) and the DS&S, LLC Instrumentation & Controls US Quality Manual (Reference 3-5). A map showing the correspondence between 10CFR50 Appendix B, ASME NQA-1-1994, and the RRCN quality procedures is provided in Table 3.2-1. A similar map showing the correspondence between 10CFR50 Appendix B, ASME NQA-1-1994, and the DS&S quality procedures is provided in Table 3.2-2.

3.14 Chapter 3 References

3-1 NUREG-0800, USNRC Standard Review Plan, Table 7-1, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety”, Revision 5, March 2007

3-2 “Equipment Qualification Plan”, Document No. 3 006 501C, Rolls-Royce Civil Nuclear SAS, June 2009

3-3 “***SPINLINE 3*** Design Analysis Report”, Document No. MPR-3337, MPR Associates, Inc., June 2009

3-4 “Rolls-Royce Civil Nuclear SAS Quality Manual”, Document No. 8 303 186 P, Rolls-Royce Civil Nuclear SAS, June 2009

3-5 “Instrumentation & Controls US Quality Manual”, Revision C, Document 500-9600000-10, ICQ-005-C, Data Systems & Solutions, LLC, a member of the Rolls-Royce Civil Nuclear group, June 2009

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
1. 10 CFR Parts 50 and 52							
a	50.55a(a)(1)		Quality Standards for Systems Important to Safety	Yes	3.2.1.2		
b	50.55a(h)(2)		Protection Systems (IEEE Std 603-1991 or IEEE Std 279-1971)	Yes	3.2.1.3	IEEE 603-1991	Criteria for Safety Systems for Nuclear Power Generating Stations
						IEEE 279-1971	Criteria for Protection Systems for Nuclear Power Generating Stations
c	50.55a(h)(3)		Safety Systems (IEEE Std 603-1991)	Yes	3.2.1.4	IEEE 603-1991	Criteria for Safety Systems for Nuclear Power Generating Stations
d	50.34(f)(2)(v) [I.D.3]		Bypass and Inoperable Status Indication	Yes	3.2.1.1		
e	50.34(f)(2)(xi) [II.D.3]		Direct Indication of Relief and Safety Valve Position	No			
f	50.34(f)(2)(xii) [II.E.1.2]		Auxiliary Feedwater System Automatic Initiation and Flow Indication	No			
g	50.34(f)(2)(xvii) [II.F.1]		Accident Monitoring Instrumentation	No			
h	50.34(f)(2)(xviii) [II.F.2]		Instrumentation for the Detection of Inadequate Core Cooling	No			
i	50.34(f)(2)(xiv) [II.E.4.2]		Containment Isolation Systems	No			

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
j	50.34(f)(2)(xix) [II.F.3]		Instruments for Monitoring Plant Conditions Following Core Damage	No			
k	50.34(f)(2)(xx) [II.G.1]		Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves	No			
l	50.34(f)(2)(xxii) [II.K.2.9]		Failure Mode and Effect Analysis of Integrated Control System	No			
m	50.34(f)(2)(xxiii)[II.K.2.10]		Anticipatory Trip on Loss of Main Feedwater or Turbine Trip	No			
n	50.34(f)(2)(xxiv) [II.K.3.23]		Central Reactor Vessel Water Level Recording	No			
o	50.62		Requirements for Reduction of Risk from Anticipated Transients without Scram	No			
p	52.47(b)(1)		ITAAC for Standard Design Certification	No			
q	52.80(a)		ITAAC for Combined Licensee Applications	No			
r	50.49		Environmental qualification of electric equipment important to safety for nuclear power plants	Yes	3.2.1.5		
s	73.54		Protection of Digital Computer and Communication Systems and Networks	Yes	3.2.4		
2. 10 CFR Part 50, Appendix A General Design Criteria (GDC)							
a	GDC 1		Quality Standards and Records	Yes	3.2.2.1		

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
b	GDC 2		Design Bases for Protection Against Natural Phenomena	Yes	3.2.2.2		
c	GDC 4		Environmental and Dynamic Effects Design Bases	Yes	3.2.2.3		
d	GDC 10		Reactor Design	No			
e	GDC 13		Instrumentation and Control	Yes	3.2.2.4		
f	GDC 15		Reactor Coolant System Design	No			
g	GDC 16		Containment Design	No			
h	GDC 19		Control Room	No			
i	GDC 20		Protection System Functions	Yes	3.2.2.5		
j	GDC 21		Protection Systems Reliability and Testability	Yes	3.2.2.6		
k	GDC 22		Protection System Independence	Yes	3.2.2.7		
l	GDC 23		Protection System Failure Modes	Yes	3.2.2.8		
m	GDC 24		Separation of Protection and Control Systems	Yes	3.2.2.9		
n	GDC 25		Protection System Requirements for Reactivity Control Malfunctions	Yes	3.2.2.10		
o	GDC 28		Reactivity Limits	No			
p	GDC 29		Protection Against Anticipated Operational Occurrences	Yes	3.2.2.11		

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
p	GDC 33		Reactor Coolant Makeup	No			
q	GDC 34		Residual Heat Removal	No			
r	GDC 35		Emergency Core Cooling	No			
s	GDC 38		Containment Heat Removal	No			
t	GDC 41		Containment Atmosphere Cleanup	No			
u	GDC 44		Cooling Water	No			
3. 10 CFR Part 50, Appendix B							
a	10 CFR Part 50, Appendix B		Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants	Yes	3.2.3		
4. Staff Requirements Memoranda							
a	SRM to SECY 93-087, II.Q		Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems	Yes	3.5.1		
b	SRM to SECY 93-087, II.T		Control Room Annunciator (Alarm) Reliability	No			
5. Regulatory Guides							
a	Regulatory Guide 1.22	R0	Periodic Testing of Protection System Actuation Functions	Yes	3.3.1		
b	Regulatory Guide 1.47	R0	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System	Yes	3.3.2	IEEE 279-1971	Criteria for Protection Systems for Nuclear Power Generating Stations

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
c	Regulatory Guide 1.53	R2	Application of the Single-Failure Criterion to Safety Systems	Yes	3.3.3	IEEE 379-2000	Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
d	Regulatory Guide 1.62	R0	Manual Initiation of Protection Actions	Yes	3.3.4	IEEE 279-1971	Criteria for Protection Systems for Nuclear Power Generating Stations
e	Regulatory Guide 1.75	R3	Independence of Electrical Safety Systems	Yes	3.3.5	IEEE 384-1992	Standard Criteria for Independence of Class 1E Equipment and Circuits
f	Regulatory Guide 1.89	R1	Environmental Qualification of Certain Electrical Equipment Important to Safety for Nuclear Power Plants	Yes	3.3.6	IEEE 323-1974	IEEE Standard for Qualifying Class IE Equipment for Nuclear Power generating Stations
g	Regulatory Guide 1.97	R3	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident and Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants	No		ANS 4.5-1980	Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors
		R4	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident and Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants	No		IEEE 497-2002	IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
h	Regulatory Guide 1.100	R2	Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants	Yes	3.3.7	IEEE 344-1987	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
i	Regulatory Guide 1.105	R3	Setpoints for Safety-Related Instrumentation	Yes	3.3.8	ISA S67.04-1994	Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Points
j	Regulatory Guide 1.118	R3	Periodic Testing of Electric Power and Protection Systems	Yes	3.3.9	IEEE 338-1987	Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
k	Regulatory Guide 1.151	R0	Instrument Sensing Lines	No		ISA S67.02-1980	Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants
						ASME B&PV Code, Section III	Rules for Construction of Nuclear Power Plant Components
l	Regulatory Guide 1.152	R2	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	Yes	3.3.10	IEEE 7-4.3.2-2003	Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
m	Regulatory Guide 1.153	R1	Criteria for Safety Systems	Yes	3.3.11	IEEE 603-1991	Criteria for Safety Systems for Nuclear Power Generating

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
							Stations
n	Regulatory Guide 1.168	R1	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	Yes	3.3.12	IEEE 1012-1998	IEEE Standard for Software Verification and Validation Plans
						IEEE 1028-1997	IEEE Standard for Software Reviews and Audits
o	Regulatory Guide 1.169	R0	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	Yes	3.3.13	IEEE 828-1990	IEEE Standard for Software Configuration Management Plans
						IEEE 1042-1987	IEEE Guide to Software Configuration Management
p	Regulatory Guide 1.170	R0	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	Yes	3.3.14	IEEE 829-1983	IEEE Standard for Software Test Documentation
q	Regulatory Guide 1.171	R0	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	Yes	3.3.15	IEEE 1008-1987	IEEE Standard for Software Unit Testing
r	Regulatory Guide 1.172	R0	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	Yes	3.3.16	IEEE 830-1993	IEEE Recommended Practice for Software Requirements Specifications
s	Regulatory Guide 1.173	R0	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	Yes	3.3.17	IEEE 1074-1995	IEEE Standard for Developing Software Life Cycle Processes

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
t	Regulatory Guide 1.174	R1	An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis	No			
u	Regulatory Guide 1.177	R0	An Approach for Plant-Specific Risk-Informed Decision Making: Technical Specifications	No			
v	Regulatory Guide 1.180	R1	Guidelines for Evaluating Electromagnetic and Radio- Frequency Interference in Safety-Related Instrumentation and Control Systems Instrumentation and Control Systems	Yes	3.3.18	IEEE 1050-1996	Guide for Instrumentation and Control Equipment Grounding in Generating Stations
						MIL-STD-461E	DOD Interface Standard Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment
						IEC 61000-3	Electromagnetic Compatibility (EMC) - Part 3
						IEC 61000-4	Electromagnetic Compatibility (EMC) - Part 4
						IEC 61000-5	Electromagnetic Compatibility (EMC) - Part 5
						IEEE C62.41-1991	Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
						IEEE C62.45-1992	Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits
w	Regulatory Guide 1.189	R1	Fire Protection for Operating Nuclear Power Plants	No			
x	Regulatory Guide 1.200	R1	An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities	No			
y	Regulatory Guide 1.204	R0	Guidelines for Lightning Protection of Nuclear Power Plants	No		IEEE 665-1995	IEEE Guide for Generating Station Grounding
						IEEE 666-1991	IEEE Design Guide for Electrical Power Service Systems for Generating Stations
						IEEE 1050-1996	IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations
						IEEE C62.23-1995	IEEE Application Guide for Surge Protection of Electric Generating Plants

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary							
Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
z	Regulatory Guide 1.209	R0	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	Yes	3.3.19	IEEE 323-2003	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
aa	Regulatory Guide 5.71	R0	Cyber Security Programs for Nuclear Facilities	Yes	3.3.20		
6. Branch Technical Positions (BTP)							
a	BTP 7-1	R5	Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System	No			
b	BTP 7-2	R5	Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines	No			
c	BTP 7-3	R5	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service	No			
d	BTP 7-4	R5	Guidance on Design Criteria for Auxiliary Feedwater Systems	No			
e	BTP 7-5	R5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	No			

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
f	BTP 7-6	R5	Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode	No			
g	BTP 7-7		Not used	N/A			
h	BTP 7-8	R5	Guidance on Application of Regulatory Guide 1.22	Yes	3.4.1		
i	BTP 7-9	R5	Guidance on Requirements for Reactor Protection System Anticipatory Trips	No			
j	BTP 7-10	R5	Guidance on Application of Regulatory Guide 1.97	No			
k	BTP 7-11	R5	Guidance on Application and Qualification of Isolation Devices	Yes	3.4.2		
l	BTP 7-12	R5	Guidance on Establishing and Maintaining Instrument Setpoints	Yes	3.4.3		
m	BTP 7-13	R5	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors	No			
n	BTP 7-14	R5	Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems	Yes	3.4.4		
o	BTP 7-15		Not used	N/A			
p	BTP 7-16		Not used	N/A			
q	BTP 7-17	R5	Guidance on Self-Test and Surveillance	Yes	3.4.5		

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
			Test Provisions				
r	BTP 7-18	R5	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems	Yes	3.4.6		
s	BTP 7-19	R5	Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems	Yes	3.4.7		
t	BTP 7-20		Not used	N/A			
u	BTP 7-21	R5	Guidance on Digital Computer Real-Time Performance	Yes	3.4.8		
7. Interim Staff Guidance (ISG)							
a	DI&C-ISG-01	R0	Cyber Security	Yes	3.7.1	RG 1.152, R2	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
b	DI&C-ISG-02	R1	Diversity and Defense-in-Depth (D3)	Yes	3.7.2	NUREG/ CR-6303	Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems
						BTP 7-19	Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems

Table 3.1-1. Standard Review Plan Table 7-1 Compliance Summary

Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety				Address compliance in generic *SPINLINE 3* LTR?	Location of compliance statement in LTR	Endorsed standards	
Criteria		Rev #	Title or Subject				
c	DI&C-ISG-03	R0	Risk-Informed Digital Instrumentation and Controls	No			
d	DI&C-ISG-04	R1	Highly Integrated Control Rooms – Digital Communication Systems	Yes	3.7.3	IEEE 603-1991	Criteria for Safety Systems for Nuclear Power Generating Stations
						IEEE 7-4.3.2-2003	Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
e	DI&C-ISG-05	R0	Highly Integrated Control Rooms – Human Factors	No		NUREG-0700 Rev 2	Human-System Interface Design Review Guidelines
						NUREG-0711	Human Factors Engineering Program Review Model
f	DI&C-ISG-06	Draft	Licensing Process	Yes	3.7.4		

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding RRCN SAS Quality Plans and Procedures
Introduction	**1. Purpose** **2. Applicability** **3. Responsibility** **4. Terms and Definitions**	
I - Organization	**Basic Requirement 1: Organization**	[[ ]]
	Organization Supplemental Requirements 200 Structure and Responsibility 201 General 202 Delegation of Work 203 Interface Control	[[ ]]
II - Quality Assurance Program	**Basic Requirement 2: Quality Assurance Program**	[[ ]]
	Quality Assurance Program Supplemental Requirements 200 Indoctrination and Training 201 Indoctrination 202 Training 300 Qualification Requirements 301 Nondestructive Examination (NDE)	[[

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding RRCN SAS Quality Plans and Procedures
	302 Inspection and Test 303 Lead Auditor 304 Auditors 400 Certification of Qualification 500 Records	]]
III - Design Control	**Basic Requirement 3: Design Control**	[[ ]]
	Design Control Supplement Requirements 200 Design Input 300 Design Process 400 Design Analysis 401 Use of Computer Programs 402 Document of Design Analysis 500 Design Verification 501 Methods 600 Change Control 601 Configuration Mgmt of Operating Facilities 700 Interface Control 800 Software Design Control 801 Software Design Process	[[ ]]

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding RRCN SAS Quality Plans and Procedures**
	802 Software Configuration Management 900 Documentation and Records	
IV - Procurement Document Control	**Basic Requirement 4: Procurement Document Control**	[[ ]]
	Procurement Document Control Supplemental Requirements 200 Content of the Procurement Documents 201 Scope of Work 202 Technical Requirements 203 Quality Assurance Program Requirements 204 Right of Access 205 Documentation Requirements 206 Nonconformances 207 Spare and Replacement Parts 300 Procurement Document Review 400 Procurement Document Changes	[[ ]]
V - Instructions, Procedures and Drawings	**Basic Requirement 5: Instructions, Procedures and Drawings**	[[

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding RRCN SAS Quality Plans and Procedures
		]]
VI - Document Control	**Basic Requirement 6: Document Control**	**[[**]]
	Document Control Supplemental Requirements 200 Document Control 300 Document Changes 301 Major Changes 302 Minor Changes	**[[**]]
VII - Control of Purchased Materials, Equipment and Services	**Basic Requirement 7: Control of Purchased Items and Services**	**[[**]]
	Control of Purchased Items and Services Supplemental Requirements 200 Supplier Evaluation 300 Bid Evaluation 400 Control of Supplier-Generated Documents 500 Acceptance of Item or Service	**[[**]]

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding RRCN SAS Quality Plans and Procedures
	501 General 502 Methods of Acceptance 503 Certificate of Conformance 504 Source Verification 505 Receiving Inspection 506 Post installation Testing 507 Acceptance of Services Only 600 Control of Supplier Nonconformances 700 Commercial Grade Items and Services 701 General 702 Utilization 703 Critical Characteristics 704 Dedication 705 Supplier Deficiency Correction 800 Records	
VIII - Identification and Control of Materials, Parts and Components	**Basic Requirement 8: Identification and Control of Items**	[[ ]]
	Identification and Control of Items Supplemental Requirements 200 Identification Methods 201 Item Identification	[[ ]]

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding RRCN SAS Quality Plans and Procedures
	202 Physical Identification 300 Specific Requirements 301 Identification and Traceability of Items 302 Limited Life Items 303 Maintaining Identification of Stored Items	
IX - Control of Special Processes	**Basic Requirement 9: Control of Processes**	**[[**]]
	Control of Processes Supplemental Requirements 200 Process Control 201 Special Processes 202 Acceptance Criteria 203 Special Requirements 300 Responsibility 400 Records	**[[**]]
X - Inspection	**Basic Requirement 10: Inspection**	**[[**]]
	Inspection Supplemental Requirements 200 Inspection Requirements 300 Inspection Hold Points 400 Inspection Planning	**[[**

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding RRCN SAS Quality Plans and Procedures
	401 Planning 402 Sampling 500 In-Process Inspection 600 Final Inspections 601 Resolution of Nonconformances 602 Inspection Requirements 603 Modifications, Repairs, or Replacements 700 Records	]]
XI - Test Control	**Basic Requirement 11: Test Control**	**[[ ]]**
	Test Control Supplemental Requirements 200 Test Requirements 300 Test Procedures (other than for computer programs) 400 Computer Program Test Procedures 500 Test Results 600 Test Records	**[[**]]
XII - Control of Measuring and Test Equipment	**Basic Requirement 12: Control of Measuring and Test Equipment**	**[[**]]
	Control of Measuring and Test Equipment Supplemental Requirements	**[[**]]

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding RRCN SAS Quality Plans and Procedures**
	200 Selection 300 Calibration and Control 301 Calibration 302 Reference Standards 303 Control 304 Commercial Devices 400 Records 401 General 402 Reports and Certificates	
XIII - Handling, Storage and Shipping	**Basic Requirement 13: Handling, Storage and Shipping**	[[ ]]
	Handling, Storage and Shipping Supplemental Requirements 200 Special Requirements 300 Procedures 400 Tools and Equipment 500 Operators 600 Marking or Labeling	[[ ]]
XIV - Inspections, Test and Operating Status	**Basic Requirement 14: Inspections, Test and Operating Status**	[[

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding RRCN SAS Quality Plans and Procedures
		]]
XV - Nonconforming Materials, Parts of Components	**Basic Requirement 15: Control of Nonconforming Items**	[[ ]]
	Control of Nonconforming Items Supplemental Requirements 200 Identification 300 Segregation 400 Disposition 401 Control 402 Responsibility and Authority 403 Personnel 404 Disposition 405 Reexamination	[[ ]]
XVI - Corrective Action	**Basic Requirement 16: Corrective Action**	[[ ]]
XVII - Quality Assurance Records	**Basic Requirement 17: Quality Assurance Records**	[[ ]]
	Quality Assurance Records Supplemental Requirements 200 Generation of Records 300 Authentication of Records 400 Classification	

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding RRCN SAS Quality Plans and Procedures**
	401 Lifetime Records 402 Nonpermanent Records 500 Receipt Control of Records 600 Storage 700 Retention 800 Maintenance of Records	
XVIII - Audits	**Basic Requirement 18: Audits**	**[[**]]
	Audits Supplemental Requirements 200 Scheduling 300 Preparation 301 Audit Plan 302 Personnel 303 Selection of Audit Team 400 Performance 500 Reporting 600 Response 700 Follow-up Action 800 Records	**[[**]]
Subpart 2.7	**Basic Requirements: Quality Assurance Requirements for Computer Software for Nuclear Facility Applications**	**[[**

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding RRCN SAS Quality Plans and Procedures
		]] -
	Quality Assurance Requirements for Computer Software for Nuclear Facility Applications Supplemental Requirements 200 General Requirements 201 Documentation 202 Review 203 Software Configuration Management 204 Problem Reporting and Corrective Action 300 Software Acquisition 301 Procured Software and Software Services 302 Otherwise Acquired Software 400 Software Engineering Method 401 Software Design Requirements 402 Software Design 403 Implementation 404 Acceptance Testing 405 Operation 406 Maintenance 407 Retirement 500 Standards, Conventions, and other Work Practices	[[ ]]

Table 3.2-1. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding RRCN SAS QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding RRCN SAS Quality Plans and Procedures**
	600 Support Software 601 Software Tools 602 System Software	

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding DS&S LLC QA Plans and Procedures
Introduction	**1. Purpose** **2. Applicability** **3. Responsibility** **4. Terms and Definitions**	[[ ]]
I - Organization	**Basic Requirement 1: Organization**	**[[**]]
	Organization Supplemental Requirements 200 Structure and Responsibility 201 General 202 Delegation of Work 203 Interface Control	**[[**]]
II - Quality Assurance Program	**Basic Requirement 2: Quality Assurance Program**	[[

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding DS&S LLC QA Plans and Procedures
		]]
	Quality Assurance Program Supplemental Requirements 200 Indoctrination and Training 201 Indoctrination 202 Training 300 Qualification Requirements 301 Nondestructive Examination (NDE) 302 Inspection and Test 303 Lead Auditor 304 Auditors 400 Certification of Qualification 500 Records	[[ ]]
III - Design Control	**Basic Requirement 3: Design Control**	[[ ]]
	Design Control Supplement Requirements 200 Design Input 300 Design Process 400 Design Analysis 401 Use of Computer Programs	[[

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding DS&S LLC QA Plans and Procedures**
	402 Document of Design Analysis 500 Design Verification 501 Methods 600 Change Control 601 Configuration Mgmt of Operating Facilities 700 Interface Control 800 Software Design Control 801 Software Design Process 802 Software Configuration Management 900 Documentation and Records	]]
IV - Procurement Document Control	**Basic Requirement 4: Procurement Document Control**	[[ ]]
	Procurement Document Control Supplemental Requirements 200 Content of the Procurement Documents 201 Scope of Work 202 Technical Requirements 203 Quality Assurance Program Requirements	[[ ]]

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding DS&S LLC QA Plans and Procedures
	204 Right of Access 205 Documentation Requirements 206 Nonconformances 207 Spare and Replacement Parts 300 Procurement Document Review 400 Procurement Document Changes	
V - Instructions, Procedures and Drawings	**Basic Requirement 5: Instructions, Procedures and Drawings**	[[ ]]
VI - Document Control	**Basic Requirement 6: Document Control**	[[ ]]
	Document Control Supplemental Requirements 200 Document Control 300 Document Changes 301 Major Changes 302 Minor Changes	[[ ]]

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding DS&S LLC QA Plans and Procedures
VII - Control of Purchased Materials, Equipment and Services	**Basic Requirement 7: Control of Purchased Items and Services**	[[ ]]
	Control of Purchased Items and Services Supplemental Requirements 200 Supplier Evaluation 300 Bid Evaluation 400 Control of Supplier-Generated Documents 500 Acceptance of Item or Service 501 General 502 Methods of Acceptance 503 Certificate of Conformance 504 Source Verification 505 Receiving Inspection 506 Post installation Testing 507 Acceptance of Services Only 600 Control of Supplier Nonconformances 700 Commercial Grade Items and Services 701 General 702 Utilization 703 Critical Characteristics 704 Dedication	[[ ]]

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding DS&S LLC QA Plans and Procedures**
	705 Supplier Deficiency Correction 800 Records	
VIII - Identification and Control of Materials, Parts and Components	**Basic Requirement 8: Identification and Control of Items**	[[ ]]
	Identification and Control of Items Supplemental Requirements 200 Identification Methods 201 Item Identification 202 Physical Identification 300 Specific Requirements 301 Identification and Traceability of Items 302 Limited Life Items 303 Maintaining Identification of Stored Items	[[ ]]
IX - Control of Special Processes	**Basic Requirement 9: Control of Processes**	[[ ]]
	Control of Processes Supplemental Requirements 200 Process Control 201 Special Processes 202 Acceptance Criteria	[[ ]]

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding DS&S LLC QA Plans and Procedures**
	203 Special Requirements 300 Responsibility 400 Records	
X - Inspection	**Basic Requirement 10: Inspection**	[[ ]]
	Inspection Supplemental Requirements 200 Inspection Requirements 300 Inspection Hold Points 400 Inspection Planning 401 Planning 402 Sampling 500 In-Process Inspection 600 Final Inspections 601 Resolution of Nonconformances 602 Inspection Requirements 603 Modifications, Repairs, or Replacements	[[ ]]

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding DS&S LLC QA Plans and Procedures**
	700 Records	
XI - Test Control	**Basic Requirement 11: Test Control**	**[[**]]
	Test Control Supplemental Requirements 200 Test Requirements 300 Test Procedures (other than for computer programs) 400 Computer Program Test Procedures 500 Test Results 600 Test Records	**[[**]]
XII - Control of Measuring and Test Equipment	**Basic Requirement 12: Control of Measuring and Test Equipment**	**[[**]]
	Control of Measuring and Test Equipment Supplemental Requirements 200 Selection 300 Calibration and Control 301 Calibration 302 Reference Standards 303 Control 304 Commercial Devices	**[[**]]

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding DS&S LLC QA Plans and Procedures
	400 Records 401 General 402 Reports and Certificates	
XIII - Handling, Storage and Shipping	**Basic Requirement 13: Handling, Storage and Shipping**	[[ ]]
	Handling, Storage and Shipping Supplemental Requirements 200 Special Requirements 300 Procedures 400 Tools and Equipment 500 Operators 600 Marking or Labeling	[[ ]]
XIV - Inspections, Test and Operating Status	**Basic Requirement 14: Inspections, Test and Operating Status**	[[ ]]
XV - Nonconforming Materials, Parts of Components	**Basic Requirement 15: Control of Nonconforming Items**	[[

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding DS&S LLC QA Plans and Procedures**
		]]
	Control of Nonconforming Items Supplemental Requirements 200 Identification 300 Segregation 400 Disposition 401 Control 402 Responsibility and Authority 403 Personnel 404 Disposition 405 Reexamination	[[ ]]
XVI - Corrective Action	**Basic Requirement 16: Corrective Action**	[[

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding DS&S LLC QA Plans and Procedures
		]]
XVII - Quality Assurance Records	**Basic Requirement 17: Quality Assurance Records**	**[[**]]
	Quality Assurance Records Supplemental Requirements 200 Generation of Records 300 Authentication of Records 400 Classification 401 Lifetime Records 402 Nonpermanent Records 500 Receipt Control of Records 600 Storage 700 Retention 800 Maintenance of Records	**[[**]]
XVIII - Audits	**Basic Requirement 18: Audits**	**[[**]]
	Audits Supplemental Requirements 200 Scheduling 300 Preparation	**[[**]]

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures		
10 CFR 50 App B Requirement	**ASME NQA-1-1994 Requirement**	**Corresponding DS&S LLC QA Plans and Procedures**
	301 Audit Plan 302 Personnel 303 Selection of Audit Team 400 Performance 500 Reporting 600 Response 700 Follow-up Action 800 Records	
Subpart 2.7	**Basic Requirements: Quality Assurance Requirements for Computer Software for Nuclear Facility Applications**	[[ ]]
	Quality Assurance Requirements for Computer Software for Nuclear Facility Applications Supplemental Requirements 200 General Requirements 201 Documentation 202 Review 203 Software Configuration Management 204 Problem Reporting and Corrective Action 300 Software Acquisition 301 Procured Software and Software Services 302 Otherwise Acquired Software	[[

Table 3.2-2. 10 CFR 50 Appendix B and ASME NQA-1-1994 Map to the Corresponding DS&S, LLC QA Plans & Procedures

10 CFR 50 App B Requirement	ASME NQA-1-1994 Requirement	Corresponding DS&S LLC QA Plans and Procedures
	400 Software Engineering Method	
	401 Software Design Requirements	
	402 Software Design	
	403 Implementation	
	404 Acceptance Testing	
	405 Operation	]]
	406 Maintenance	
	407 Retirement	
	500 Standards, Conventions, and other Work Practices	
	600 Support Software	
	601 Software Tools	
	602 System Software	

Table 3.6-1 Responses to NUREG/CR-6082 Communications System Questions	
NUREG/CR-6082 Question	***SPINLINE 3***
2.1.1. Is it an event-based or state based system?	[[ ]]
2.1.2. Is there an accurate picture of the layout?	[[ ]]
2.1.3. Are the data rates known between all nodes of the architecture? Are they known for upset and error conditions?	[[ ]]
2.1.4. Is the message mix known? Is it known for upset and error conditions?	[[ ]]
2.1.5. Are the timing and delay requirements known?	[[ ]]
2.1.6. Is the system "deterministic" and the effects of error recovery accounted for?	[[ ]]

Table 3.6-1 Responses to NUREG/CR-6082 Communications System Questions

NUREG/CR-6082 Question	*SPINLINE 3*
2.1.7. Is the actual link capacity including interface, operating system and protocol performance effects being quoted, or is the vendor basing calculations on raw media bandwidth?	[[ ]]
2.1.8. What are the media requirements?	[[ ]]
2.1.9. Does the design meet independence requirements?	[[ ]]
2.1.10. What are the communications error performance requirements?	[[ ]]
2.1.11. What are the protocol requirements? What services should the protocol provide?	[[ ]]
2.1.12. Is the medium proprietary? Are the protocols proprietary?	[[ ]].
2.1.13. Is there theoretical support for performance and reliability?	[[ ]]
2.1.15. Is there experimental support for performance and reliability?	[[ ]]

Table 3.6-1 Responses to NUREG/CR-6082 Communications System Questions

NUREG/CR-6082 Question	*SPINLINE 3*
2.1.16. Is there an installed base? If proprietary, how many suppliers support the medium and the protocol software?	[[ ]]
2.1.17. Is there a good match between nodes processors, networks controllers, and operating system and protocol stack?	[[ ]]

[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
1	**INTERDIVISIONAL COMMUNICATIONS**		
	1	A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions	[[ ]]
	2	The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.	[[

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
			]]
	3	A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system.	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix			
Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.	[[ ]]
	4	The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function.	[[ ]]
		The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information.	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B.	[[ ]]
		Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner.	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.	See above
	5	The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
	6	The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	[[ ]]
	7	Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor.	[[ ]]
		Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message.	[[

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
			]].
		Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #		ISG-04 Requirements	Compliance of the *SPINLINE 3* generic platform
	8	Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.	[[ ]]
	9	Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		within a memory device.	
	10	Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. “Hardwired logic” as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a “TRUE” or “1” at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.	
	11	Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division.	[[ ]]
		For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.	See above
	12	Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute “single failures” as described in the single failure criterion of 10 CFR Part 50, Appendix A.	[[ ]]
		Examples of credible communication faults include, but are not limited to, the following: 1. Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or	[[

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		electrical noise. 2. Messages may be repeated at an incorrect point in time. 3. Messages may be sent in the incorrect sequence. 4. Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message. 5. Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages. 6. Messages may be inserted into the communication medium from unexpected or unknown sources. 7. Messages may be sent to the wrong destination, which could treat the message as a valid message. 8. Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption. 9. Messages may contain data that is outside the expected range. 10. Messages may appear valid, but data may be placed in incorrect locations within the message. 11. Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm). 12. Message headers or addresses may be corrupted.	

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix			
Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
			]]
	13	Vital[iii] communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.	[[ ]]
	14	Vital[iii] communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.	[[ ]]
	15	Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
	16	Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 CFR. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)	• [[ ]]
	17	Pursuant to 10 CFR. § 50.49, the medium used in a vital[iii] communications channel should be qualified for the anticipated normal and post-accident environments.	[[ ]]
		For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.	See above
	18	Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
	19	If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.	[[ ]]
	20	The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.	[[ ]]
2	**COMMAND PRIORITIZATION**		
			[[ ]]
3	**MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS**		
3.1		**Independence and Isolation** The following provisions are applicable to multidivisional control and display stations. These guidance provisions do not apply to	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		conventional hardwired control and indicating devices (hand switches, indicating lamps, analog indicators, etc.).	
	1	**Nonsafety stations receiving information from one or more safety divisions:** All communications with safety-related equipment should conform to the guidelines for interdivisional communications.	[[ ]]
	2	**Safety-related stations receiving information from other divisions (safety or nonsafety):** All communications with equipment outside the station's own safety division, whether that equipment is safety-related or not, should conform to the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself	[[ ]]
	3	**Nonsafety stations controlling the operation of safety-related equipment:** Nonsafety stations may control (see note above) the operation of safety-related equipment, provided the following restrictions are enforced: • The nonsafety station should access safety-related plant equipment only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules. • A nonsafety station should not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function. This provision should be implemented within the safety-related system, and must be	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		unaffected by any operation, malfunction, design error, software error, or communication error in the nonsafety equipment. In addition: • The nonsafety station should be able to bypass a safety function only when the affected division has itself determined that such action would be acceptable. • The nonsafety station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.) • The nonsafety station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.	

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
	4	**Safety-related stations controlling the operation of equipment in other safety-related divisions:** Safety-related stations controlling (see note above) the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that control the operation of safety-related equipment. • A control station should access safety-related plant equipment outside its own division only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules. • A station must not influence the operation of safety-related equipment outside its own division when that equipment is performing its safety function. This provision should be implemented within the affected (target) safety-related system, and should be unaffected by any operation, malfunction, design error, software error, or communication error outside the division of which those controls are a member. In addition: • The extra-divisional (that is, “outside the division”) control station should be able to bypass a safety function only when the affected division itself determined that such action would be acceptable. • The extra-divisional station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix		
Section #	**ISG-04 Requirements**	**Compliance of the *SPINLINE 3* generic platform**
	make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.) • The extra-divisional station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.	

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
	5	**Malfunctions and Spurious Actuations:** The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with these requirements, as set forth in 10 C.F.R. § 50.34 and 50.59, include but are not limited to the following: • Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multidivisional control and display station. • Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor. • Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed. • No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command. For example: When the operator requests any safety function or other important function, the system	[[ ]]

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements	Compliance of the *SPINLINE 3* generic platform
	should respond “do you want to proceed?” The operator should then be required to respond “Yes” or “No” to cause the system to execute the function. Other question-and-confirm strategies may be used in place of the one described in the example. The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors. • Each control processor or its associated communication processor should detect and block commands that do not pass the communication error checks. • Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may warrant the inclusion of additional qualification criteria or	

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements		Compliance of the *SPINLINE 3* generic platform
		measures in addition to those described herein. • Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses. • The design should have provision for an "operator workstation disable" switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations. • Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions	
3.2		**Human Factors Considerations**	This will be determined on a plant-specific basis.
3.3		**Diversity and Defense-in-Depth (D3) Considerations**	This will be determined on a plant-specific basis.

Table 3.7-1 Interim Staff Guide DI&C-ISG-04 Rev. 1 Compliance Matrix

Section #	ISG-04 Requirements	Compliance of the *SPINLINE 3* generic platform

ISG-04 Notes

[i] IEEE 603-1991 (cited in 10CFR50.55a(h)) provides the following definitions:

channel: "An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined."

division: "The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components."

For the purposes of this guidance document, the terms *channel* and *division* are further described below. Note that the following is for illustrative purposes, and is not intended to impose requirements or new interpretations:

A *safety channel* as used herein is a set of safety-related instruments and equipment, along with the associated software, that together generate a protective actuation or trip signal to initiate a single protective function. While an analog/hardwired system would have each functional circuit clearly assigned to only one channel, the processor and other components in a digital system may be assigned to multiple channels within a single division.

A *safety division* is the collection of all safety channels that are powered by a single power division. Different channels perform different functions. Different divisions perform the same set of functions, and are redundant to one another. Licensing typically credits redundancy among divisions. The voting logic that generates the final actuation signal to an item of plant equipment typically resides in one division and receives input from redundant channels in all divisions. For the purposes of this guidance, it is to be assumed that each of the actuation signals entering the voting logic that establishes the final actuation signal to an item of plant equipment is in a different division, regardless of the particular usage of the term "division" for a particular nuclear power plant.

[ii] "Processor" may be a CPU or other processing technology such as simple discrete logic, logic within an FPGA, an ASIC, etc.

[iii] "Vital" communications as used herein are communications that are needed to support a safety function. Failure of vital communications could inhibit the performance of the safety function. The most common implementation of vital communications is the distribution of channel trip information to other divisions for the purpose of voting.

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix				
Section #	**Section Title**	**Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements**	**Compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
4	Safety system design basis	No requirements beyond IEEE Standard 603		
5	Safety system criteria	See specific subsections, below		
5.1	Single-failure criterion	No requirements beyond IEEE Standard 603		
5.2	Completion of protective action	No requirements beyond IEEE Standard 603		
5.3	Quality	Section 5.3 requirements addresses software quality. These are in addition to IEEE Standard 603, which addresses hardware quality.	[[ ]]	
5.3.1	Software development		[[	

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix				
Section #	Section Title	Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements	Compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
			]]	
5.3.1.1	Software quality metrics		[[ ]]	
5.3.2	Software tools		[[ ]]	
5.3.3	Verification and validation		[[	

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix				
Section #	Section Title	Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements	Compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
			]]	
5.3.4	Independent V&V (IV&V) requirements		[[ ]]	
5.3.5	Software configuration management		[[ ]]	
5.3.6	Software project risk management		[[ ]]	

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix				
Section #	**Section Title**	**Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements**	**Compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
5.4	Equipment qualification	Section 5.4 requirements are necessary to qualify digital computers for use in safety systems and are in addition to the equipment qualification criteria in IEEE Standard 603.	[[ ]]	
5.4.1	Computer system testing		[[ ]]	
5.4.2	Qualification of existing commercial computers		[[ ]]	
5.4.2.1	Preliminary phase of the COTS dedication process		[[ ]]	
5.4.2.2	Detailed phase of the COTS		[[ ]]	

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix				
Section #	**Section Title**	**Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements**	**Compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
	dedication process			
5.4.2.3	Maintenance of commercial dedication		[[ ]]	
5.5	System integrity	Section 5.5 requirements are necessary to achieve system integrity in digital equipment for use in safety systems and are in addition to the system integrity criteria in IEEE Standard 603.		
5.5.1	Design for computer integrity		[[ ]]	

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix				
Section #	**Section Title**	**Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements**	**Compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
5.5.2	Design for test and calibration		[[ ]]	[[ ]]
5.5.3	Fault detection and self-diagnostics		[[ ]]	
5.6	Independence	In addition to the requirements of IEEE Standard 603, this section addresses independence of data communication between safety channels or between safety and non-safety systems.	[[	

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix				
Section #	**Section Title**	**Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements**	**Compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
			]]	
5.7	Capability for test and calibration	No requirements beyond IEEE Standard 603		
5.8	Information displays	No requirements beyond IEEE Standard 603		
5.9	Control of access	No requirements beyond IEEE Standard 603		
5.10	Repair	No requirements beyond IEEE Standard 603		

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix

Section #	Section Title	Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements	Compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
5.11	Identification	Section 5.11 supplements IEEE Standard 603 with additional requirements to ensure that the computer system hardware and software are installed in the appropriate system configuration	[[ ]]	
5.12	Auxiliary features	No requirements beyond IEEE Standard 603		
5.13	Multi-unit stations	No requirements beyond IEEE Standard 603		
5.14	Human factor considerations	No requirements beyond IEEE Standard 603		

Table 3.8-1. IEEE Standard 7-4.3.2-2003 Compliance Matrix				
Section #	**Section Title**	**Relationship of IEEE Standard 7-4.3.2-2003 requirements to IEEE Standard 603-1991 requirements**	**Compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
5.15	Reliability	In addition to the requirements of IEEE Standard 603, when reliability goals are identified, the proof of meeting the goals shall include the software	[[ ]]	
6	Sense and command features—functional and design requirements	No requirements beyond IEEE Standard 603		
7	Execute features—functional and design requirements	No requirements beyond IEEE Standard 603		
8	Power source requirements	No requirements beyond IEEE Standard 603		

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix				
Section #	**Section Title**	**Are there supplementary requirements in** **IEEE Standard 7-4.3.2-2003?**	**IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
4	Safety system design basis		[[ ]]	[[ ]]
5	Safety system criteria	See specific subsections, below		
5.1	Single-failure criterion		[[ ]]	[[ ]]

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix

Section #	Section Title	Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?	IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
5.2	Completion of protective action			[[ ]]
5.3	Quality	Yes. IEEE Standard 7-4.3.2 Section 5.3 provides additional requirements for software quality.	[[ ]]	
5.4	Equipment qualification	Yes. IEEE Standard 7-4.3.2 Section 5.4 provides additional requirements to qualify digital computers for use in safety systems.	[[ ]]	[[ ]]
5.5	System integrity	Yes. IEEE Standard 7-4.3.2 Section 5.5 provides additional requirements to achieve system integrity in digital equipment for use in safety systems.	[[	

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix

Section #	Section Title	Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?	IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
			]]	
5.6	Independence	Yes. IEEE Standard 7-4.3.2 Section 5.6 provides additional requirements for independence of data communications	[[ ]]	[[ ]]
5.6.1	Between redundant portions of a safety system		[[ ]]	
5.6.2	Between safety systems and effects of design basis event		[[ ]]	[[

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix				
Section #	**Section Title**	**Are there supplementary requirements in** **IEEE Standard 7-4.3.2-2003?**	**IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
				]]
5.6.3	Between safety systems and other systems		[[ ]]	
5.6.4	Detailed criteria	Yes. This section of IEEE Standard 603 refers to IEEE Standard 7-4.3.2 and IEEE Standard 384.	[[ ]]	

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix

Section #	Section Title	Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?	IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
5.7	Capability for test and calibration		[[ ]]	[[ ]]
5.8	Information displays			
5.8.1	Displays for manually controlled actions		[[ ]]	[[ ]]
5.8.2	System status indication		[[ ]]	[[ ]]

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix

Section #	Section Title	Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?	IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
5.8.3	Indication of bypasses		[[ ]]	[[ ]]
5.8.4	Location			[[ ]]
5.9	Control of access		[[ ]]	[[ ]]

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix				
Section #	**Section Title**	**Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?**	**IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
5.10	Repair		[[ ]]	[[I]]
5.11	Identification	Yes. IEEE 7-4.3.2 Section 5.11 provides additional requirements to ensure that the computer system hardware and software are installed in the appropriate system configuration	[[ ]]	[[ ]]
5.12	Auxiliary features			[[ ]]

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix

Section #	Section Title	Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?	IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
5.13	Multi-unit stations		[[ ]]	
5.14	Human factor considerations		[[ ]]	[[ ]]
5.15	Reliability	Yes. IEEE 7-4.3.2 Section 5.15 provides additional requirements on reliability analysis	[[ ]]	[[ ]]
6	Sense and command features—functional and design requirements	See specific subsections, below		
6.1	Automatic control		[[ ]]	[[ ]]
6.2	Manual control		[[ ]]	[[ ]]

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix				
Section #	**Section Title**	**Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?**	**IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform**	***SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications**
6.3	Interaction between the sense and command features and other systems			[[ ]]
6.4	Derivation of system inputs			[[ ]]
6.5	Capability for testing and calibration	See specific subsections, below		
6.5.1	Checking the operational availability		[[ ]]	
6.5.2	Means of assuring the operational availability		[[ ]]	
6.6	Operating bypasses		[[ ]]	[[ ]]

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix

Section #	Section Title	Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?	IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
6.7	Maintenance bypass		[[ ]]	[[ ]]
6.8	Setpoints		[[ ]]	[[ ]]
7	Execute features—functional and design requirements		[[ ]]	
7.1	Automatic control		[[ ]]	
7.2	Manual control		[[ ]]	
7.3	Completion of protective action		[[ ]]	
7.4	Operating bypass		[[ ]]	
7.5	Maintenance bypass		[[ ]]	
8	Power source requirements			

Table 3.8-2. IEEE Standard 603-1991 Compliance Matrix

Section #	Section Title	Are there supplementary requirements in IEEE Standard 7-4.3.2-2003?	IEEE Standard 603 compliance of the *SPINLINE 3* generic digital safety I&C platform	*SPINLINE 3* interface criteria for NPP-specific digital safety I&C applications
8.1	Electrical power sources		[[ ]]	[[ ]]
8.2	Non-electrical power sources		[[ ]]	
8.3	Maintenance bypass		[[ ]]	

Table 3.10-1. IEC 880-1986 Compliance Matrix	
IEC Recommendations	**RRCN Practice**
B1 Design procedures	
B1.*a* Changeability	
Software design shall easily allow changes At an early design stage it should be identified which characteristics of the software to be developed and its functional requirements are likely to change during its life cycle During further design stages modules should be chosen such that the most probable modifications result in the change of one or two modules only Modifiability should be carefully counter- balanced with resulting overhead in run time and memory space	[[ ]]
B1.*b* Top-down approach	
A top-down approach shall be used in design General aspects should precede specific ones At each level of refinement the whole system should be completely described and verified Areas of difficulty should be identified as far as possible at an early stage in the design procedure Principal decisions should be discussed and documented as soon as possible After any major decision affecting other system parts, the alternatives	[[

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
should be considered and their risks be documented Consequences for other system parts which are implied by individual decisions should be identified The interval between levels should be small enough to permit a clear understanding of the decision process involved within the step The program design and development should proceed using one or more higher level descriptive formalism, such as used in mathematical logic, set theory, pseudo code, decision tables, logic diagrams or other graphic aids or problem oriented languages As far as possible automatic development aids should be used Documentation should be such that the specifier is able to understand and check both the design and the program Coding should be among the final steps taken	]]
B1.*c* Intermediate verification	
The intermediate product shall be continuously verified (Clause A1) It should be shown that each level of refinement is complete and consistent in itself It should be shown that each level of refinement is consistent with the previous level Consistency checks should be made by neutral personnel These personnel should only mark deficiencies and not recommend any action	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix	
IEC Recommendations	**RRCN Practice**
B1.*d* Changes during development	
Changes which are necessary during program development shall begin at the earliest design stage which is still relevant to the change Changes should proceed from the general stage to the more specific stages If any module is changed, it should be retested according to the principles described earlier, before it is reintegrated into the system In addition the environment of the changed module should be retested, as far as it is affected by the change Documentation of major changes should include the requirements, code parts, data areas, control flow characteristics and time aspect that were affected or not affected Changes affecting already tested parts or the work of other persons should be evaluated and reviewed prior to incorporation NOTE – This procedure is valid for changes that affect the work of only one person and for modifications that affect the whole system. In the latter case the recommendations of Chapter 10 apply additionally.	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B1.*d* System reconfiguration	
The experience gained with any system to be adapted for new applications shall be taken into account The state of the system should be assessed before adaptation One should rather try to use system parts or modules with extensive operating experience than to formally verify new ones Decided changes or amendments should proceed as recommended in Table B1.b and B1.d and Chapter 9 At code level each change should be made separately Already verified parts or modules should be left unchanged NOTE – Any amendment of a system that does not result in a change according to Table B1.d spoils its clarity.	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B2 Software Structure	
B2.a Control and access structure	
Programs and program parts shall be grouped systematically Specific system operations should be performed by specific parts The software should be partitioned so that aspects which handle such functions as: - computer external interfaces (e.g. devices driving, interrupt handling); - real time signals (e.g. clock); - parallel processing (e.g. scheduler); - store allocation; - special functions (e.g. utilities); - mapping standard «functions» onto the particular computer hardware; are separated from «application» programs with well defined interfaces between them The program structure should permit the implementation of anticipated changes with a minimum of effort (see also Table B1.a) It should be made clear which structuring methods are being used In one processor the program system should work sequentially, as far as possible A program or a program part should be broken down into clear and intelligible modules when it contains more than 100 executable statements	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix	
IEC Recommendations	**RRCN Practice**
B2.b Modules	
Modules shall be clear and intelligible Each module should correspond to a specific function A module should have only one entry. Although multiple exits may be sometimes necessary, single exits are recommended No module should exceed a limit specified for the particular system (e.g. 50 or 100 statements, or the amount of coding which can be placed on one page. Only under special circumstances are longer modules allowed) The interfaces between modules should be as simple as possible, uniform throughout the system and fully documented The number of input and output parameters of modules should be limited to a minimum It should be clearly stated which interface data are only used, only defined or redefined	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B2.c Operating system	
Operating system use shall be restricted Only thoroughly tested operating systems should be used ; preferably the existing operating experience should be quantitatively known If possible no operating system should be used If an operating system is considered necessary its use should be restricted to a few simple functions It should contain only the necessary functions One particular operating system function should be called always in a similar way Device drivers should be taken from the operating system rather than specially developed Operating system functions should be rigorously defined and should have well defined interfaces If a dedicated operating system or a dedicated part is developed for a special safety application, these recommendations should be followed New releases should be treated according to Tables B1.d and B1.e Other standardized programs or program parts should be treated as operating systems	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B2.d Execution time	
Technical process behaviour influence on execution time shall be kept low The execution time of any system or part of a system under peak load conditions should be short compared to the execution time beyond which the system safety requirements are violated The results produced by a sequential program shall not be dependent on either – the time taken to execute the program, or – the time (referenced to an independent "clock") at which execution of the programs is initiated Execution of sequential programs which receive or transmit data from / to other sequential programs shall be synchronized with those other programs The programs should be designed so that operations are performed in a correct sequence independent of their speed of execution Run time differences depending on input parameters should be small Run time differences depending on input parameters should be documented Code parts for which execution time depends on input parameters should be short The amount of parameters read during one computation cycle should be constant	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix	
IEC Recommendations	**RRCN Practice**
B2.e Interrupts	
The use of interrupts shall be restricted Interrupts may be used if they simplify the system Software handling of interrupts must be inhibited during critical parts (e.g. time critical, critical to data changes) of the executed function If interrupts are used, parts not interruptable should have a defined maximum computation time, so that the maximum time for which an interrupt is inhibited can be calculated Interrupts usage and masking shall be thoroughly documented	[[ ]]
B2.f Arithmetic expressions	
Simple arithmetic expressions shall be used instead of complex ones Decisions should not depend on voluminous arithmetic calculations As far as possible, simplified previously verified arithmetic expressions should be used If voluminous arithmetic expressions are used, they should be coded so that their consistency with the specified arithmetic expression can be shown easily from the code	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B3 Self supervision	
B3.a Plausibility checks	
Plausibility checks shall be performed (defensive programming) The correctness or plausibility for intermediate results should be checked as often as possible, at least to within a small percentage of computer capacity (redundancy) Where safety related results are involved identical results should be evaluated, using different methods (diversity) Re-try procedures should be used The ranges of: – input variables; – output variables; – intermediate parameters should be checked, including array bound checking	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B3.b Safe output	
If a failure is detected the system shall produce a well defined output If possible, complete and correct error recovery techniques should be used Even if correct error recovery cannot be guaranteed, failure detection must lead to well-defined output If error recovery techniques are used the occurrence of any error shall be reported The occurrence of a persistent error affecting the system function shall be recorded	[[ ]]
B3.c Memory contents	
Memory contents shall be protected or monitored Memory space for constants and instructions shall be protected or supervised against changes Unauthorized reading and writing should be prevented The system should be secure against code or data changes by the plant operator	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix	
IEC Recommendations	**RRCN Practice**
B3.d Error checking	
Error checking shall be performed at a detailed coding level Counters and reasonableness traps (relay runners) should insure that the program structure has been run through correctly The correctness of any kind of parameter transfer should be checked, including parameters type verification When addressing an array its bounds should be checked Called routines should check whether the calling module is entitled to do so The run time of critical parts should be monitored (e.g. by a watchdog timer) Assertions should be used	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix	
IEC Recommendations	**RRCN Practice**
B4 Detailed design and coding	
B4.a Branches and loops	
Branches and loops should be handled cautiously Conditional and unconditional branches should be avoided as far as they obscure the relationship between problem structure and program structure, as much sequential code as possible should be used Backward going branches should be avoided, loop statements should be used instead (only for higher level languages) Branches into loops, modules or subroutines must be barred Branches out of loops should be avoided, if they do not lead exactly to the end of the loop. Exception: failure exit In modules with complex structure, macros, procedures or subroutines should be used so that structure stands out clearly As a special measure to support program proving and verification computed GOTO or SWITCH statements as well as label variables should be avoided Where a list of alternative branches or case controlled statements are used, the list of branch or case conditions must be an exhaustive list of possibilities. The concept of a «default branch» should be reserved for failure handling Loops should only be used with constant maximum loop variable ranges	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B4.b Subroutines and procedures	
Subroutines or procedures should be organized as simply as possible They should have only a minimum number of parameters They should communicate exclusively via their parameters to their environment All parameters should have the same form (e.g. no mixing of call by name and value) Subroutines should have only one entry point Subroutines should return to only one point for each subroutine call. Exception; default exit The return point should immediately follow the point of call	[[ ]]
B4.c Nested structures	
Nested structures shall be handled with care Nested macros should be avoided Procedure valued parameters should be avoided Joining of different types of program action by means of nested loop statement or nested procedures should be avoided, if they obscure the relationship between problem structure and program structure Hierarchies of procedures and loops should be used, if they clarify the system structure	[[ ]] .

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B4.d Addressing and arrays	
Simple addressing techniques shall be used Only one addressing technique should be used for each data type Bulky computations of indexes should be avoided Arrays should have a fixed, predefined length The number of dimensions in every array reference should equal the number of dimension in its corresponding declaration	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix	
IEC Recommendations	**RRCN Practice**
B4.e Data structures	
Data structures and naming conventions shall be used uniformly throughout the system Variables, arrays and memory cells should have a single purpose and structure. The use of equivalence techniques should be avoided Each variable's name should reflect: – type (array, variable, constant); – region of validity (local, global program, module); – kind (input, output, internal, derived, count, array length); – significance System parameters that can changes should be identified and their values assigned at a well defined outstanding code position Constants and variables should be located in different parts of the memory NOTE – Many real time program systems make use of a universally accessible or similar resource. When such global data structures are used, they should be accessed via standard resource handling procedures or via communication with standard resource manipulating tasks.	[[ ]]
B4.f Dynamic changes	
Dynamic changes to executable code shall be avoided	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix	
IEC Recommendations	**RRCN Practice**
B4.g Intermediate tests	
Intermediate tests shall be performed during the program development The approach to testing should follow the approach to design (e.g. during top down design testing should be made by using simulation of not yet existing system parts - stubs - ; after completion of system development this should be followed by bottom up integration testing) Each module should be tested thoroughly before it is integrated into the system and the test results documented A formal description of the test inputs and results (test protocol) should be produced Coding errors which are detected during program testing should be recorded and analysed Incomplete testing should be recorded In order to facilitate the use of intermediate test results during final validation the former degree of testing achieved should be recorded (e.g. all paths through the module tested)	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B5 Language dependent recommendations	
B5.a Sequences and arrangements	
Detailed rules shall be elaborated for the arrangement of various language constructs The recommendations should include sequence of declarations Sequence of initializations Sequence of non-executable code / executable code Sequence of parameters types Sequence of formats	[[ ]]
B5.b Comments	
Relations between comments and executable or non-executable code shall be fixed by detailed rules It should be made clear what has to be commented The position of comments should be uniform Form and style of comments should be uniform	[[ ]]

Table 3.10-1. IEC 880-1986 Compliance Matrix

IEC Recommendations	RRCN Practice
B5c Assembler	
If an assembler language is used, extended programming rules shall be followed Branching instructions using address substitution must not be used. Branch table contents should be constant All indirect addressing should follow the same scheme Indirect shifting should be avoided Multiple substitutions or multiple indexing within a single machine instruction should be avoided The same macro should always be called with the same number of parameters Labels should be referred to by names rather than by absolute or relative addresses Subroutine call conventions should be uniform throughout the system and specified by further rules	[[ ]]
B5.d Coding Rules	
Detailed coding rules shall be issued It should be made clear, where and how code lines are to be indented Module layout should be fixed uniformly Further details should be regulated according to need	[[ ]]

Table 3.10-2. Comparison of IEC 880-1986 & NRC Branch Technical Position 7-14 Requirements

BTP 7-14 Guidance			Corresponding IEC 880 Guidance	
Activity Group		BTP Section		IEC Section
Planning	**Plans**		**Plans**	
	Software Management Plan (SMP)	B.3.1.1		
	Software Development Plan (SDP)	B.3.1.2		
	Software Quality Assurance Plan (SQAP)	B.3.1.3	Software Quality Assurance Plan	3.2
	Software Integration Plan (Sent)	B.3.1.4	System Integration Plan	7.1
	Software Installation Plan (Snit)	B.3.1.5		
	Software Maintenance Plan (Saint)	B.3.1.6		
	Software Training Plan (SMTP)	B.3.1.7	Training Program, Training Plan	10.2.1, 10.2.2
	Software Operations Plan (SOP)	B.3.1.8		
	Software Safety Plan (SSP)	B.3.1.9		
	Software Verification and Validation Plan (SVVP)	B.3.1.10	Software Verification Plan	6.2.1
			System Validation Plan	8
	Software Configuration Management Plan (SCMP)	B.3.1.11		
	Software Test Plan (STP)	B.3.1.12	Commissioning Test Plan	10.1.1
Requirements	**Design Outputs**		**Design Outputs**	
	Software Requirements Specification (SRS)	B.3.3.1	Software Functional Requirements Specification	4
	Process Implementation			

Table 3.10-2. Comparison of IEC 880-1986 & NRC Branch Technical Position 7-14 Requirements

BTP 7-14 Guidance			Corresponding IEC 880 Guidance	
Activity Group		**BTP Section**		**IEC Section**
	Software Requirements Safety Analysis			
	V&V Requirements Analysis Report		Functional Requirements Verification Report	6.1
	Software Configuration Management Requirements Report			
Design (Development – Design and Coding)	**Design Outputs**		**Design Outputs**	
	Software Architecture Description (SAD)	B.3.3.2	Program Development Report	5.3
	Software Design Specification (SDS)	B.3.3.3	Software Performance Specification	5.4.1
	Process Implementation			
	Software Design Safety Analysis			
	V&V Design Analysis Report		Software Design Verification Report	6.1, 6.2.2
			Software Coding Verification Report	6.1, 6.2.3
	Software Configuration Management Design Report			
Implementation (Verification)	**Design Outputs**			
	Code Listings (CL)	B.3.3.4	Software Test Specification	6.2.3.1
			Periodic Test Program	10.3.1
	Process Implementation			
	Code Safety Analysis Report			
	V&V Implementation Analysis & Test Report		Software Test Report	6.2.3.2
			Periodic Test Coverage Assessment	10.3.2

Table 3.10-2. Comparison of IEC 880-1986 & NRC Branch Technical Position 7-14 Requirements

BTP 7-14 Guidance			Corresponding IEC 880 Guidance	
Activity Group		**BTP Section**		**IEC Section**
	Software Configuration Management Implementation Report			
Integration	**Design Outputs**			
	System Build Documents (SBD)	B.3.3.5		
	Process Implementation			
	Integration Safety Analysis			
	V&V Integration Analysis & Test Report		Integrated System Verification Test Report	7.7
	Software Configuration Management Integration Report			
Validation	**Design Outputs**			
	None			
	Process Implementation			
	Validation Safety Report			
	V&V Validation Analysis & Test Report		Periodic Tests, Test Coverage Analysis Report	10.3.2
			System Validation Report	8.1
	Software Configuration Management Validation Report			
Installation	**Design Outputs**			
	Installation Configuration Tables (ICT)	B.3.3.6		
	Operation Manuals (OM)	B.3.3.7	User Manual	10.2.2

Table 3.10-2. Comparison of IEC 880-1986 & NRC Branch Technical Position 7-14 Requirements

BTP 7-14 Guidance			Corresponding IEC 880 Guidance	
Activity Group		**BTP** **Section**		**IEC** **Section**
	Software Maintenance Manuals (SMM)	B.3.3.8		
	Software Training Manuals (STM)	B.3.3.9		
	Process Implementation			
	Installation Safety Analysis			
	V&V Installation Analysis & Test Report		Commissioning Test Report	10.1.1
	Software Configuration Management Installation Report			
Operations and Maintenance (Maintenance and Modification, Operations)	**Design Outputs**			
	None		Software Modification Request	9.2
			Periodic Test Requirements	10.3.2
	Process Implementation			
	Change Safety Analysis			
	V&V Change Report		Software Modification Analysis Report	9.3
	Software Configuration Management Change Report			

4 Description of the *SPINLINE 3* Digital Safety I&C Platform

4.1 Overview

4.1.1 Design Criteria

SPINLINE 3 has been designed to comply with U.S. and international nuclear safety I&C requirements. Compliance with 10 CFR 50, USNRC Regulatory Guides, Interim Staff Guides, and Branch Technical Positions, industry standards, and other guidance applicable to digital safety I&C systems is documented in Chapter 3. The resulting ***SPINLINE 3*** digital safety I&C platform has the following general attributes:

- Fail-safe: ***SPINLINE 3*** assures that, in case of detected failure, the outputs associated with a central processing unit (CPU) achieve a pre-defined safe position.

- Fault-tolerance: ***SPINLINE 3*** supports system architectures that meet the redundancy requirements of the single failure criterion. In addition, ***SPINLINE 3*** processors can automatically reconfigure their voting logic to accomplish the intended safety function with one or more divisions out of service.

- Diversity: ***SPINLINE 3*** supports system architectures that employ signal diversity to defend against common cause failures. ***SPINLINE 3*** also can be deployed as a diverse system as part of a plant-level defense-in-depth and diversity (D3) strategy.

- Functional isolation: ***SPINLINE 3*** equipment and communications design prevents propagation of failures between redundant equipment in separate divisions. In addition, communication paths to non-safety I&C systems are electrically isolated with one-way communications from ***SPINLINE 3*** to the non-safety I&C system. This prevents faults in a non-safety I&C system from affecting ***SPINLINE 3***.

- Determinism: For all processing, the same inputs produce the same outputs within a guaranteed response time

- Cyber Security: The features of ***SPINLINE 3*** help the licensee to reduce the threat of cyber attacks on its safety systems. The main features for cyber security are: the ***SPINLINE 3*** software is developed with an independent V&V process and is fully reviewable. It can be demonstrated to be free from malicious code. Changes to the software can be made only by replacing the memories on the CPU board and therefore, need physical access to cabinets that are located in secured areas in the NPP. Communications within the safety system and with other systems are performed using the proprietary safety NERVIA network which does not allow for dynamic modification of the communication scheme and for cyber attacks by hackers. Communication is not allowed from the non-safety plant systems, such as through a plant network, to ***SPINLINE 3.***

- Ease of use: Operation and maintenance are simplified by automated on-line system supervision, fault detection and self-diagnosis.

- Flexibility: Through carefully controlled processes, many system operating characteristics can be updated without hardware modification.

- Modularity: ***SPINLINE 3*** can be delivered either in standard chassis to be integrated into existing cabinets (for refurbishment purposes) or in new cabinets.

- Scalability: ***SPINLINE 3*** has been deployed internationally in a wide variety of safety I&C applications, including Reactor Trip System (RTS), Engineered Safety Feature Actuation System (ESFAS), Nuclear Instrumentation System (NIS), and diverse trip system applications.

4.1.2 Qualification and Dedication

All ***SPINLINE 3*** hardware is Class 1E qualified, as described in Chapter 5 and in the Equipment Qualification (EQ) Plan (Reference 4-1).

The ***SPINLINE 3*** safety-related Operational System Software (OSS) and other ***SPINLINE 3*** safety-related platform software were developed based on the guidance of the IEC 880-1986 (Reference 4-2) with enhancements to take into account the advances in software engineering as reflected in a later revision of the standard. Features of the ***SPINLINE 3*** platform software are described in Section 4.4. The software life cycle processes that apply to ***SPINLINE 3*** safety-related platform software are described in Section 6.2. The ***SPINLINE 3*** platform software has been dedicated using the process defined in EPRI TR-107330 (Reference 4-3) and approved by the NRC (Reference 4-4). The technical basis for dedication is documented in a Design Analysis Report (DAR, Reference 4-5). The dedicated platform software is managed under the RRCN Quality Management Program (Reference 4-6), which complies with 10 CFR 50 Appendix B (Reference 4-7).

Safety application software deployed on ***SPINLINE 3*** systems will be developed on a plant-specific basis using the software life cycle processes described in Section 6.4. These processes meet the requirements of IEEE 7-4.3.2 and NRC Branch Technical Position 7-14 (References 4-8 and 4-9, respectively).

4.1.3 Operation and Maintenance

SPINLINE 3 has the following features to support operation and maintenance.

- Setpoint value adjustments may be needed during a reactor operating cycle or between cycles. These adjustments are made using a Local Display Unit (LDU), which has the functionality described in Section 4.4.3.5.5, and a secure protocol and a consistency check that is performed between redundant parts. Setpoints are stored in EEPROM on the ***SPINLINE 3*** processor board, so they are retained even after power is lost and restored.

- A dedicated station, the Monitoring and Maintenance Unit (MMU) described in Section 4.6.10, supervises process information and failure signaling. This station delivers an automatic diagnosis to facilitate quick repair in case of a fault. This diagnosis indicates which board has failed or is failing. Periodic tests, initiated by plant operators, are automatically executed and provide a high degree of fault coverage.

4.1.4 State-of-the-Art Performance

The wide range of input/output (I/O) boards and their capabilities allows ***SPINLINE 3*** to fit any nuclear safety I&C application need. The use of powerful CPU boards and high speed data networks assures rapid response times even for complex functions and, above all, the response time is guaranteed by the deterministic features of the ***SPINLINE 3*** platform.

4.1.5 Quality

As described in Sections 1.4, the RRCN Quality Manual (Reference 4-6), which governs the ***SPINLINE 3*** digital safety I&C platform complies with 10 CFR 50 Appendix B (Reference 4-7) and ASME NQA-1-1994 (Reference 4-17). Compliance with 10 CFR 50 Appendix B is described in more detail in Section 3.2 and NQA-1 compliance is described in more detail in Section 3.13.

4.2 Main Features of *SPINLINE 3*

4.2.1 Introduction

SPINLINE 3 provides a set of standardized, modular components and tools that were designed from the start as Class 1E I&C systems, including:

- Hardware components: chassis, I/O and processing boards, power supplies and other components. See Section 4.3 for a description of ***SPINLINE 3*** hardware components. Hardware data sheets are in Appendix A.

- Platform software, which is comprised of the Class 1E standardized Operational System Software (OSS), the Class 1E application-oriented library of re-usable software components, Class 1E software embedded in the NERVIA+ board, Class 1E software embedded in the ICTO Pulse Input board, and a non-Class 1E set of tools integrated in a Software Development Environment (SSDE) called CLARISSE. See Section 4.4 for a description of the ***SPINLINE 3*** platform software\.

The design and implementation of the hardware components and the platform software comply with US Nuclear Regulatory Commission (NRC) requirements. Compliance summaries for specific NRC codes, guides and endorsed industry standards are provided in Chapter 3.

4.2.2 Software Based Digital Technology

SPINLINE 3 is based on digital technology, which simplifies implementation of the functional requirements and avoids the need for certain specific hardware development. The main benefits of the ***SPINLINE 3*** software-based approach are:

- Functional requirement implementation: The development of any kind of I&C function (e.g., logic functions, analog functions, closed loop control, and computations) is possible without the need for specific hardware design, using the ***SPINLINE 3*** hardware components and the CLARISSE System and Software Development Environment (SSDE).

- Stability and accuracy of analog values: ***SPINLINE 3*** analog electronic concentrates in analog I/O boards. These boards are permanently monitored for drift and have a defined accuracy. They do not require operator adjustment or calibration during on site operation. Once digitized, the values of analog input signals and triggering thresholds can be processed without being subject to analog drift.

- Adaptability: Changes in functional requirements can be dealt with by software modifications when they do not affect the I/O interface. When I/O changes are needed, the system parameters are adapted accordingly and I/O boards can be added as necessary.

- System supervision: Supervision of the safety I&C system can be achieved without increasing the complexity of the safety classified units. With the isolation provided in a ***SPINLINE 3*** system, data available on the safety networks may be sent via a one-way (broadcast only) data link to non-safety classified data systems for cross-comparisons and other diagnostic purposes.

- Automated periodic testing: ***SPINLINE 3*** provides features that enable automation of comprehensive periodic testing of each function.

4.2.3 Standardized Components

SPINLINE 3 hardware and software components are standardized, mature products that are both modular and scaleable. The standardized hardware components are:

- 19 inch 6U chassis that can fit many standard cabinets
- A full range of input and output (I/O) boards for discrete and analog data, neutron instrumentation, thermodynamic instrumentation, actuator control, and other I&C functions.
- A 25 MHz 68040 Freescale microprocessor CPU board, with two megabytes of read-only flash memory, two megabytes of write-protected RAM for operational system software and application software execution, two megabytes of RAM for data space, and 64 kilobytes of non-volatile EEPROM memory. This board can support up to six NERVIA communication interfaces.
- High speed, deterministic Class 1E digital communications network: NERVIA is a 10 megabit/s, broadcast type network that implements a time-based token bus communications protocol. The medium is either optical fiber or Shielded-Foil Twisted-Pair (SFTP) cable. It is used for communications within the safety system and for one-way (broadcast only) communications to non-safety units. Both NERVIA hardware and software comply with Class 1E requirements.
- Interface to an external non-safety computer through the NERVIA digital communications network. ***SPINLINE 3*** may also interface with other analog or digital systems using networks, serial links, or appropriately isolated wired links.

The hardware components are described in Section 4.3. Data sheets for ***SPINLINE 3*** standard hardware components are in Appendix A

The components of the ***SPINLINE 3*** platform software are:

- The standardized, Class 1E configurable Operational System Software (OSS), which provides the interface between the local and remote data delivered by the I/O and communication link boards and the application software. The OSS also provides continuous self-diagnostic testing of the hardware and services to the application software.
- The Class 1E application-oriented library of re-usable software components,
- The Class 1E software embedded in the NERVIA+ board,
- The Class 1E software embedded in the ICTO Pulse Input board, and
- A non-Class 1E set of tools integrated in a Software Development Environment (SSDE) called CLARISSE, which is used to design and implement the system architecture, configure the units and networks and develop the plant-specific application software.

These components of the ***SPINLINE 3*** platform software are described in Section 4.4 The RRCN software life cycle processes for the ***SPINLINE 3*** platform software are described in Sections 6.2 and 6.3. The software life cycle processes for the plant-specific application software are described in Section 6.4.

4.2.4 Architectures

[[

]]

Figure 4.2-1 Representative Four Division Architecture

4.2.5 Redundancy

SPINLINE 3 modular architecture is convenient for building redundant systems. ***SPINLINE 3*** provides two kinds of redundancy management:

- **Hardware-based active redundancy management:** Safety I&C systems typically are comprised of several separate, independent divisions (typically three or four). Output signals from each division are issued through output boards into the hardware voting logic.

- **Software-based active redundancy management:** This is mainly implemented in units receiving data from several divisions, either from output units or functional processing units. Software-based redundancy provides for voting reconfiguration capability, with reconfiguration occurring upon detection of an inhibition signal or on detection of a failure of a division. For instance, a software two-out-of-four (2oo4) vote implemented in the voting unit will become a two-out-of-three (2oo3) vote when one division is unavailable (for instance during periodic testing). The general design principle of this reconfiguration, and of the redundant architecture, is to comply with the single failure criterion provided in IEEE Standard 379 (Reference 4-10). This feature also improves system reliability and availability without degrading safety.

4.2.6 Deterministic Behavior

[[

]]

4.2.7 Separation

Physical and electrical separation is implemented in the design of plant-specific ***SPINLINE 3*** systems, with each division being powered from one or two separate and independent Class 1E power sources associated with that division. In addition, inter-divisional communication through NERVIA networks is implemented using optical fiber, which provides electrical isolation between divisions.

Exchange of data between units through NERVIA networks does not involve synchronisation mechanisms at protocol level (i.e.; no hand-shaking, no acknowledge, no synchronized clock time, no master station). This feature avoids the risk of disabling one or several units on a network as a consequence of the failure of a single unit or station. The management of redundant units is easy to achieve as networks work independently of the status of the connected units and units work independently of the status of the connected networks.

The NERVIA network provides flexibility. For instance, the NERVIA networks can be used to implement communication with divisional Class 1E video display units for information display and safety system control. The NERVIA network can be configured to supply data from all divisions to a single video display unit, as shown in **Erreur ! Source du renvoi introuvable.**. Based on guidance from NRC Interim Staff Guide DI&C ISG-04 (Reference 4-11), the multi-divisional Class 1E video display unit can also provide control capabilities. As shown in the figure, these Display Networks can be implemented as one-way (broadcast only) communications paths to the display processor for data display only. With access to data from all divisions, each division display processor can perform a variety of calculations (i.e., average, maximum, minimum, deviations for alarming, etc.) or run applications that are not required as part of the basic trip functions of the system. The Class 1E digital video display unit (VDU) is not in the scope of the ***SPINLINE 3*** digital safety I&C platform.

Non-Class 1E units are isolated from Class 1E units. Nevertheless, Class 1E units may need to transmit data to non-Class 1E units. ***SPINLINE 3*** makes this possible through a one-way (broadcast only) NERVIA communications network from the Class 1E system to the Non-Class 1E system via a fiber-optic link. Non-Class 1E units can only receive data. Such units can read the data available on the NERVIA network but they cannot transmit data on the network. Therefore, they cannot interfere with the Class 1E functions. This design ensures that Non-Class 1E units cannot prevent Class 1E units from performing their safety function.

NERVIA communications are described in detail in Section 4.5.

4.2.8 Safety-oriented Features

[[

]]

4.2.9 Alarms and Signaling on Failure

A Class 1E application developed with ***SPINLINE 3*** digital safety I&C platform will include alarms and signaling of detected failures in the Control Room. In order to help the maintenance operator, further detailed information can be obtained from the non-Class 1E Monitoring and Maintenance Unit (see Section 4.6.10).

4.3 Hardware

4.3.1 Introduction

The ***SPINLINE 3*** hardware is built from a set of modular, standardized components, including chassis, electronic boards, and cabling, suitable to implement nuclear safety I&C systems in either new or refurbished NPPs. Data sheets for ***SPINLINE 3*** standard hardware components are provided in Appendix A. Hardware compliance with applicable codes, guides and industry standards is summarized in Chapter 3. The hardware is qualified for nuclear power plant environmental conditions, as described in Chapter 5 and in the Equipment Qualification Plan (Reference 4-1).

4.3.2 Description of the chassis and backplane bus

[[

]]

4.3.3 Summary of Electronic Boards and Electronic Modules

[[

]]

4.3.4 Description of the *SPINLINE 3* Hardware Building Blocks

[[

]]

4.4 *SPINLINE 3* Software

4.4.1 Introduction

[[

]]

4.4.2 *SPINLINE 3* General Software Architecture

[[

]]

4.4.3 Operational System Software (OSS)

[[

]]

4.4.4 System and Software Development Environment (SSDE)

[[

]]

4.4.5 Application Software

[[

]]

4.4.6 Generic Design Elements Against Software Common Cause Failure (CCF)

[[

]]

4.5 Communications

This section provides a generic description of how digital communications are implemented using the NERVIA digital communication network hardware and software to achieve intra-divisional and inter-divisional communications within a safety I&C system and to also achieve one-way communications between the safety I&C system and non-safety I&C systems. Communication hardware is described in Section 4.3.4.

In NUREG/CR-6082 (Reference 4-16), a set of 15 questions are posed to help reviewers focus attention on issues important to safety, reliability and performance. RRCN's answers to those questions are presented in Section 3.6,

4.5.1 The Open Systems Interconnection (OSI) Model

[[

]]

4.5.2 NERVIA Basic Concepts

[[

]]

4.5.3 NERVIA Software

[[

]]

4.5.4 Detailed Operation

[[

]]

4.5.5 Communication Failures Detection

[[

]]

4.5.6 Isolation and Independence Enforced on Data “Gateways” to Non-Class 1E Computer Systems

[[

]]

4.5.7 Compliance With NRC Communications Requirements

Compliance with NRC inter-divisional communications requirements for Class 1E I&C systems, as defined in the NRC Interim Staff Guide DI&C-ISG-04 (Reference 4-11), is documented in Section 3.7 and Table 3.7-1.

4.6 Testability

Safety equipment such as the Reactor Protection System or the Engineered Safety Features Actuation System does not produce any actuating signal when the plant is operating normally. In order to ensure that the equipment is capable of operating when needed, it is essential to set a strategy to verify the capacity of each part of the equipment to fulfill its functions. That is the purpose of testing the platform periodically.

Testability involves all the features implemented to detect all failures that can render the equipment incapable of performing its function. Features that provide testability include self-diagnostic tests, surveillance functions, and periodic tests. Several features have already been described in previous sections:

- See Section 4.4.3.5 for a description of the normal test and self-diagnostic test functions performed by the OSS every cycle
- See Section 4.4.3.6 for a description of how the OSS detects and manages hardware failures
- See Sections 4.5.6 and 4.2.9 for descriptions of communications failure detection and the associated alarming and signaling of communications failures

This section describes the principles and the methodology used to perform tests in order to verify the capability of safety systems to perform their functions in accordance with the design and safety requirements. This section gives an overview of the strategy used for testing. The different categories of tests are described.

The section is structured as follows:

- The overall strategy,
- Detailed description of periodic tests of ***SPINLINE 3*** equipment

4.6.1 Overall Strategy for Testing

The main objective of the testing strategy is to ensure, by means of failure detection, that the performance requirements defined in the design basis for automatic actuation and manual control are fulfilled.

The testing strategy includes the verification of the main parameters, which are accuracy, calibration, setpoint values, and response time.

The testing strategy is based on a combination of the following:

- Self-diagnostic tests that run as part of each cycle,
- Surveillance functions that are performed during refueling outages, and
- Periodic tests that are performed during plant operation.

A combination of tests is required to reduce the time when the unit is out of operation during the periodic tests. The strategy for testing arises from considerations associated with the safety objectives of:

- Optimizing failure detection,
- Avoidance of spurious trips and/or actuations,
- Reducing maintenance costs and
- Optimizing the testing period and duration.

4.6.2 Basic Concepts

[[

]]

4.6.3 Design Principles for Testability

[[

]]

4.6.4 Self-diagnostic Tests

[[

]]

4.6.5 Surveillance Functions

[[

]]

4.6.6 Periodic Tests

[[

]]

4.6.7 Description Self-diagnostic Testing Features of *SPINLINE 3* Equipment

[[

]]

4.6.8 Automated Testing Units (ATU)

The ATUs are non-Class 1E automatic devices to facilitate systematic testing. An ATU is manually plugged in the front of the tested cabinet for testing a unit. Once the maintenance staff starts the test, the tests are automatically processed. A written report is printed.

The ATUs are designed with these basic features:

- The ATUs produce signals equivalent to all types of input signals, coming from sensors (analog and discrete) or from networks.
- The ATUs receive the output signal from the tested unit by connection to the network.

[[

]]

4.6.9 Monitoring and Maintenance Unit (MMU)

The Monitoring and Maintenance Unit (MMU) is a non-Class 1E unit that is dedicated to process the result of self-diagnostic tests in order to help the maintenance operator to identify the location of the required corrective action in case of a failure:

- On a ***SPINLINE 3*** module: By using the results of the self-diagnostic tests performed by each unit,
- On a ***SPINLINE 3*** communication link: By using the results of the self-diagnostic tests performed by the NERVIA networks,
- On a sensor: By cross checking the values acquired by identical instrument channels in separate divisions.

MMUs are connected using a one-way NERVIA communication network to all the digital units and process the surveillance functions including the comparison between redundant measurements, in order to detect a wrong operation or a wrong parameterization of a unit. The comparison is adequate to detect, for example, a drifting sensor.

[[

]]

4.7 Cyber security characteristics of *SPINLINE 3* systems

[[

]]

4.8 Chapter 4 References

4-1 "Equipment Qualification Plan", Document No. 3 006 501C, Rolls-Royce Civil Nuclear SAS, June 2009

4-2 IEC 880-1986, "Software for Computers in the Safety Systems of Nuclear Power Plants," International Electrotechnical Commission

4-3 EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," Electric Power Research Institute, December 1996

4-4 USNRC Letter dated July 30, 1998 to Mr. J. Naser (EPRI), "Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute (EPRI) Topical Report, TR-107330, Final Report, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."

4-5 "***SPINLINE 3*** Design Analysis Report", Document No. MPR-3337, MPR Associates, Inc., June 2009

4-6 Rolls-Royce Civil Nuclear SAS Quality Manual, Document No. 8 303 186 P, Rolls-Royce Civil Nuclear SAS, June 2009

4-7 10 CFR 50 Appendix B, "Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants"

4-8 IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers

4-9 NRC Branch Technical Position 7-14, Rev, 5, "Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems," US Nuclear Regulatory Commission

4-10 IEEE Standard 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers

4-11 Interim Staff Guide DI&C-ISG-04, Revision 1, "Highly-Integrated Control Rooms – Digital Communication Systems," US Nuclear Regulatory Commission, 6 March 2009

4-12 IEEE Standard 802.3i-1990, "IEEE Standard for Information Exchange Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications," Institute of Electrical and Electronics Engineers

4-13 Interim Staff Guide DI&C-ISG-02, “Diversity and Defense-in-Depth (D3),” US Nuclear Regulatory Commission, 26 September 2007

4-14 NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems”, Lawrence Livermore National Laboratory, December 1994

4-15 IEC 60880-2006, “Software for Computers in the Safety Systems of Nuclear Power Plants,” International Electrotechnical Commission

4-16 NUREG/CR-6082, “Data Communications,” Lawrence Livermore National Laboratory, August 1993

4-17 ASME NQA-1-1994, “Quality Assurance Program Requirements for Nuclear Facilities”, American Society of Mechanical Engineers

4-18 Regulatory Guide 5.71, Rev. 0, “Cyber Security for Nuclear Facilities”

5 Equipment Qualification and Analysis

5.1 Equipment Qualification

Environmental qualification testing of the ***SPINLINE 3*** Qualification Test Specimen (QTS) will be performed in accordance with the requirements of U.S. Nuclear Regulatory Commission (USNRC) Regulatory Guide (RG) 1.89, “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,” (Reference 5-1) and requirements of Institute of Electrical and Electronics Engineers (IEEE) Standard 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Stations” (Reference 5-2). This standard is subject to the enhancements and exceptions listed in Section C, “Regulatory Position” of USNRC Regulatory Guide 1.209, “Guidelines for Environmental Qualification of Safety Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants” (Reference 5-3).

The environmental qualification testing of the ***SPINLINE 3*** QTS is also performed in accordance with the requirements for qualifying digital computers IEEE Standard 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations” (Reference 5-4) and USNRC Regulatory Guide 1.152, Revision 2 (Reference 5-5).

Seismic qualification testing will be performed in accordance with Regulatory Guide 1.100, “Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants” (Reference 5-6), IEEE Standard 344-1987 (Reference 5-7) and the generic seismic spectra provided in Electric Power Research Institute (EPRI) Technical Report (TR)107330 (Reference 5-9)

EMC qualification testing will be performed in accordance with the guidance provided in Regulatory Guide 1.180, Revision 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems” (Reference 5-8).

EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants” (Reference 5-9), describes an approach for generically qualifying commercial Programmable Logic Controllers (PLCs) for safety-related applications. This approach was found acceptable by the USNRC as documented in USNRC Safety Evaluation Report (SER) Letter dated July 30, 1998 to Mr. J. Naser of the EPRI (Reference 5-10). The generic qualification approach for the ***SPINLINE 3*** platform uses guidance from EPRI TR-107330 as applicable to meet the requirements of IEEE Standard 323-2003 and other USNRC guidance.

5.1.1 Equipment to be Tested

The equipment to be tested is the RRCN ***SPINLINE 3*** QTS. In accordance with EPRI TR-107330 (Reference 5-9), a representative sampling of the ***SPINLINE 3*** platform components are identified for evaluation and qualification testing. The assembled components of the ***SPINLINE 3*** QTS include the following types of hardware modules and components:

- Chassis
- Power Supply Modules and Chassis
- Digital Processing Modules
- Communication Modules
- Signal Input Modules
- Signal Output Modules
- Signal Conditioning Modules
- Terminal Blocks
- Cable and Wire Sets
- Fan Cooling Hardware
- Power Distribution Hardware

The QTS will be exercised during qualification testing by a test system comprised of an industrial-grade data acquisition system (DAS) and a test specimen application program (TSAP). This test system is a non-qualified system whose purposes are to: (1) generate a series of known inputs to the QTS, and (2) monitor the corresponding outputs of the QTS. Correct correspondence between input and output before, during, and after qualification tests and lack of spurious behavior are the key results that will demonstrate the predictable behavior of ***SPINLINE 3*** hardware during normal and abnormal plant operating conditions.

A detailed description of the ***SPINLINE 3*** QTS and the test system is provided in the “System Specification for the Qualification Test Specimen and Data Acquisition System” (Reference 5-11). Test specimen and test system arrangement and wiring drawings will be prepared to provide additional hardware configuration information. A Master Configuration List (MCL), will be prepared to provide detailed ***SPINLINE 3*** QTS configuration information such as component serial numbers and software version numbers.

5.1.2 Equipment Qualification (EQ) Testing

The Equipment Qualification (EQ) Plan (Reference 5-12) defines the scope of testing to be performed and provides a test plan for each of the individual qualification tests. The basic qualification test sequence is shown in Figure 5.1-1 and the individual tests are described briefly in this Section.

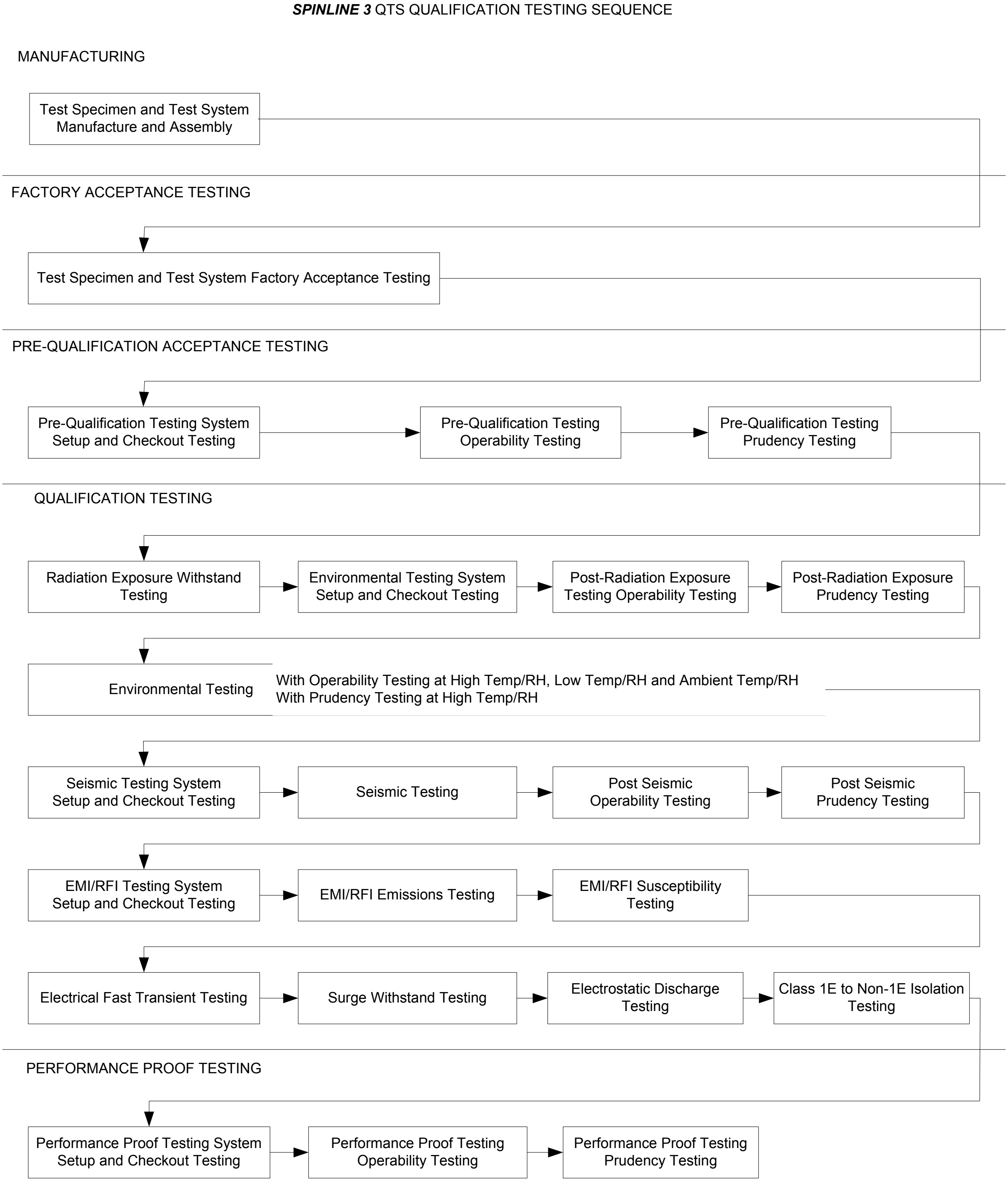
SPINLINE 3 QTS QUALIFICATION TESTING SEQUENCE
MANUFACTURING
Test Specimen and Test System Manufacture and Assembly
FACTORY ACCEPTANCE TESTING
Test Specimen and Test System Factory Acceptance Testing
PRE-QUALIFICATION ACCEPTANCE TESTING
Pre-Qualification Testing System Setup and Checkout Testing
Pre-Qualification Testing Operability Testing
Pre-Qualification Testing Prudency Testing
QUALIFICATION TESTING
Radiation Exposure Withstand Testing
Environmental Testing System Setup and Checkout Testing
Post-Radiation Exposure Testing Operability Testing
Post-Radiation Exposure Prudency Testing
Environmental Testing
With Operability Testing at High Temp/RH, Low Temp/RH and Ambient Temp/RH
With Prudency Testing at High Temp/RH
Seismic Testing System Setup and Checkout Testing
Seismic Testing
Post Seismic Operability Testing
Post Seismic Prudency Testing
EMI/RFI Testing System Setup and Checkout Testing
EMI/RFI Emissions Testing
EMI/RFI Susceptibility Testing
Electrical Fast Transient Testing
Surge Withstand Testing
Electrostatic Discharge Testing
Class 1E to Non-1E Isolation Testing
PERFORMANCE PROOF TESTING
Performance Proof Testing System Setup and Checkout Testing
Performance Proof Testing Operability Testing
Performance Proof Testing Prudency Testing

Figure 5.1-1. *SPINLINE 3* QTS Qualification Testing Sequence

5.1.2.1 Factory Acceptance Testing

Factory Acceptance Testing is performed at the end of the manufacturing and assembly phase to demonstrate compliance of the ***SPINLINE 3*** QTS and Test System with the “System Specification of the Qualification Test Specimen and Data Acquisition System” (Reference 5-11).

During Factory Acceptance Testing, the ***SPINLINE 3*** QTS will be powered with the input/outputs operating under control of the TSAP and the connected test system simulation devices. The input/output field circuits will be configured with loads representative of the types intended for connection to the corresponding input/output module points, and other devices required for monitoring of the circuit operations.

5.1.2.2 Pre-Qualification Acceptance Testing

The objective of Pre-Qualification Acceptance Testing is to demonstrate that the ***SPINLINE 3*** QTS hardware and the Test Specimen Application Program (TSAP) operate as intended prior to start of qualification testing, and to provide baseline acceptance data for qualification testing implementation of the Operability and Prudency Tests. Section 5.2 of EPRI TR 107330 (Reference 5-9) provides guidance for implementation of pre-qualification acceptance testing.

5.1.2.3 Radiation Exposure Withstand Testing

The radiation exposure withstand testing demonstrates that the ***SPINLINE 3*** QTS will not experience failures or unacceptable degradation due to expected radiation exposure from normal and abnormal service conditions as required by Regulatory Guide 1.89 (Reference 5-1) and IEEE Standard 323 (Reference 5-2). Section 4.3.6 of EPRI TR 107330 defines the normal and abnormal radiation exposure levels the test specimen must withstand (i.e., the test specimen must continue to meet the manufacturer specified performance levels).

As described in the EQ Plan, radiation exposure withstand test acceptance criteria are based on Section 4.3.6 of EPRI TR-107330.

5.1.2.4 Environmental Testing

The environmental testing demonstrates that the ***SPINLINE 3*** QTS will not experience failures due to abnormal service conditions of temperature and humidity as required by Regulatory Guide 1.89 (Reference 5-1) and IEEE Standard 323 (Reference 5-2), subject to enhancements and exceptions listed in Section C of Regulatory Guide 1.209 (Reference 5-3). Section 4.3.6 of EPRI TR 107330 defines the recommended normal and abnormal temperature and humidity exposure levels the test specimen must withstand (i.e., the test specimen must continue to meet the manufacturer specified performance levels).

As shown in Figure 5.1-1, environmental testing is performed after completion of radiation exposure withstand testing, and includes performance of the post radiation exposure withstand testing Operability and Prudency Tests. The following describes the environmental testing sequence:

- Assemble the ***SPINLINE 3*** QTS in the Environmental Test chamber.
- Perform the Pre-Environmental Testing System Setup and Checkout Test.
- Perform the Post Radiation Exposure Withstand Testing Operability and Prudency Testing.
- Expose the ***SPINLINE 3*** QTS to varying temperature and humidity conditions according to the Environmental Testing procedures.
- Perform Environmental Testing Operability and Prudency Testing at the times identified in the Environmental Testing procedures.
- Remove the ***SPINLINE 3*** QTS from the Environmental Test chamber.

As described in the EQ Plan, the Environmental Test acceptance criteria are based on Section 4.3.6 of EPRI TR-107330.

5.1.2.5 Seismic Testing

Seismic testing demonstrates the suitability of the ***SPINLINE 3*** platform for qualification as a Category 1 seismic device based on seismic withstand testing performed on the ***SPINLINE 3*** QTS in accordance with Regulatory Guide 1.100 (Reference 5-6) and IEEE Standard 344 (Reference 5-7). Section 4.3.9 of EPRI TR 107330 defines the seismic test levels to which the test specimen will be exposed, while the test specimen continues to meet the manufacturer specified performance levels.

As shown in Figure 5.1-1, seismic testing is performed after completion of environmental testing. The following describes the seismic testing sequence:

- Setup the ***SPINLINE 3*** QTS on the Seismic Test table.
- Perform the Pre-Seismic Testing System Setup and Checkout Test.
- Perform Resonance Search testing on the ***SPINLINE 3*** QTS components.
- Perform five seismic tests to the specified Operating Basis Earthquake (OBE) test levels.
- Perform one seismic test to the specified Safe Shutdown Earthquake (SSE) test level.
- Perform Post-Seismic Testing Operability and Prudency Testing.
- Remove the ***SPINLINE 3*** QTS from the Seismic Test table.

As described in the EQ Plan, the seismic test acceptance criteria are based on Section 4.3.9 of EPRI TR-107330.

5.1.2.6 EMI/RFI Testing

The objective of EMI/RFI testing is to demonstrate the suitability of the ***SPINLINE 3*** platform for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility levels. EMI/RFI testing of the ***SPINLINE 3*** QTS will be performed in accordance with USNRC Regulatory Guide 1.180, Revision 1, using additional guidance from EPRI TR-107330 as applicable. The specific EMI/RFI tests to be performed include:

EMI/RFI Emissions Tests

- MIL-461E, CE101 (Reference 5-13): Conducted Emissions, Low Frequency, AC and DC Power Leads
- MIL-461E, CE102 (Reference 5-13): Conducted Emissions, High Frequency, AC and DC Power Leads
- MIL-461E, RE101 (Reference 5-13): Radiated Emissions, Magnetic Field, QTS Surfaces and Leads
- MIL-461E, RE102 (Reference 5-13): Radiated Emissions, Electric Field, Antenna Measurement

EMI/RFI Susceptibility Tests

- IEC 61000-4-6 (Reference 5-14): Conducted Susceptibility, Induced RF Fields, Power/Signal Leads

IEC 61000-4-13 (Reference 5-15):	Conducted Susceptibility, Harmonics/Interharmonics, Power Leads
IEC 61000-4-16 (Reference 5-16):	Conducted Susceptibility, Common Mode Disturbance, Power/Signal Leads
IEC 61000-4-8 (Reference 5-17):	Radiated Susceptibility, Magnetic Field, Helmholtz Coil Exposure
IEC 61000-4-9 (Reference 5-18):	Radiated Susceptibility, Magnetic Field, Pulsed
IEC 61000-4-10 (Reference 5-19):	Radiated Susceptibility, Magnetic Field, Damped Oscillatory
IEC 61000-4-3 (Reference 5-20):	Radiated Susceptibility, High Frequency, Antenna Exposure

As described in the EQ Plan, the EMI/RFI test acceptance criteria are based on Section 4.3.7 of EPRI TR-107330 and USNRC Regulatory Guide 1.180, Rev. 1.

As shown in Figure 5.1-1, EMI/RFI testing is performed after completion of seismic testing. The following describes the EMI/RFI testing sequence:

- Setup the ***SPINLINE 3*** QTS in the EMI/RFI test chamber.
- Perform the Pre-EMI/RFI Testing System Setup and Checkout Test.
- Perform EMI/RFI Emissions Testing.
- Perform EMI/RFI Susceptibility Testing.

5.1.2.7 Electrical Fast Transient (EFT) Testing

The objective of EFT testing is to demonstrate the suitability of the ***SPINLINE 3*** platform for qualification as a safety-related device with respect to EFT susceptibility levels. EFT testing of the ***SPINLINE 3*** QTS will be performed in accordance with USNRC Regulatory Guide 1.180, Rev. 1 (Reference 5-8), using additional guidance from EPRI TR-107330 as applicable. The specific EFT test to be performed is IEC 61000-4-4, “Electromagnetic Compatibility (EMC), Part 4-4: Testing and Measurement Techniques, Electrical Fast Transient/Burst Immunity Test,” (Reference 5-21).

As described in the EQ Plan, the EFT acceptance criteria are based on Sections 4.6.2 and 4.3.7 of EPRI TR-107330 and USNRC Regulatory Guide 1.180, Rev. 1.

5.1.2.8 Surge Withstand Testing

The objective of surge withstand testing is to demonstrate the suitability of the ***SPINLINE 3*** platform for qualification as a safety-related device with respect to surge withstand levels. Surge withstand testing of the ***SPINLINE 3*** QTS will be performed in accordance with USNRC Regulatory Guide 1.180, Rev. 1, using additional guidance from EPRI TR-107330 as applicable. The specific surge withstand tests to be performed include:

- IEC 61000-4-5, “Electromagnetic Compatibility (EMC), Part 4-5: Testing and Measurement Techniques, Surge Immunity Test,” (Reference 5-22), and,
- IEC 61000-4-12, “Electromagnetic Compatibility (EMC), Part 4-12: Testing and Measurement Techniques, Oscillatory Waves Immunity Test,” (Reference 5-23).

As described in the EQ Plan, the surge withstand test acceptance criteria are based on Section 4.6.2 of EPRI TR-107330 and USNRC Regulatory Guide 1.180, Rev. 1.

5.1.2.9 Electrostatic Discharge (ESD) Testing

The objective of ESD testing is to demonstrate the suitability of the ***SPINLINE 3*** platform for qualification as a safety-related device with respect to ESD withstand levels. EPRI TR-107330, Section 4.3.8, requires that the test specimen under qualification be tested for ESD withstand capability in accordance with the requirements of EPRI TR-102323-R1 (Reference 5-24). In accordance with EPRI TR-102323, the specific ESD Test to be performed is IEC 61000-4-2 "Electromagnetic Compatibility (EMC), Part 4-2: Testing and Measurement Techniques, Electrostatic Discharge Immunity Test," (Reference 5-25). USNRC Regulatory Guide 1.180, Revision 1 (Reference 5-8) provides no guidance for ESD Testing.

As described in the EQ Plan, the ESD acceptance criteria are based on Sections 4.3.8 of EPRI TR 107330

5.1.2.10 Class 1E to Non-Class 1E Isolation Testing

The objective of Class 1E to non-Class 1E isolation testing is to demonstrate the suitability of the ***SPINLINE 3*** platform for qualification as a safety-related device with respect to providing electrical isolation at non-Class 1E field connections, as required by IEEE Standard 384 (Reference 5-26). EPRI TR-107330, Section 6.3.6, requires that the test specimen under qualification be tested for Class 1E to non-Class 1E isolation capability in accordance with the requirements of EPRI TR-107330, Section 4.6.4.

As described in the EQ Plan, the Class 1E to non-Class 1E isolation testing acceptance criteria are based on Sections 4.6.4 of EPRI TR-107330.

5.1.2.11 Performance Proof Testing

The objective of performance proof testing is to demonstrate the continuing acceptable operation and performance of the ***SPINLINE 3*** QTS following completion of all hardware qualification testing. EPRI TR-107330, Section 5.5 requires a final performance of the operability test procedure on completion of electrostatic discharge testing. As an alternative to this requirement, performance proof testing will include a final performance of both the Operability and Prudency test procedures following completion of all hardware qualification testing, and comparison of the test results to the results for all previous performances of the Operability and Prudency test procedures.

As shown in Figure 5.1-1, performance proof testing is performed after completion of Class 1E to non-Class 1E testing. The following describes the performance proof testing sequence:

- Remove the ***SPINLINE 3*** QTS and test system from the EMI/RFI test chamber.
- Reassemble the ***SPINLINE 3*** QTS and test system
- Perform the Performance Proof Testing System Setup and Checkout Test.
- Perform Performance Proof Testing Operability Testing.
- Perform Performance Proof Testing Prudency Testing.

Acceptance criteria for performance monitoring of the ***SPINLINE 3*** QTS during Performance Proof Testing will be as specified separately in the System Setup and Checkout, Operability and Prudency Test procedures. In addition, comparison of the Performance Proof Operability and Prudency Test data to all other Operability and Prudency test data shall not indicate an unacceptable change in performance of the ***SPINLINE 3*** QTS hardware.

5.1.2.12 Operability Testing

The objective of operability testing is to demonstrate the continuing correct function and performance of the ***SPINLINE 3*** QTS throughout qualification testing. Section 5.3 of EPRI TR-107330 describes the specific functional and performance tests to be performed as part of operability testing. These tests will be implemented in the ***SPINLINE 3*** QTS operability test procedure as they are applicable to the ***SPINLINE 3*** QTS design. Section 5.5 of EPRI TR-107330 identifies the points at which the operability tests should be performed during hardware qualification testing.

As shown in Figure 5.1-1, operability testing is performed at the following times during hardware qualification testing.

- With Pre-Qualification Acceptance Testing
- At the completion of Radiation Exposure Withstand Testing
- At the completion of the high temperature, high humidity phase of Environmental Testing
- At the completion of the low temperature phase of Environmental Testing
- At the completion of the low humidity phase of Environmental Testing
- At the completion of Environmental Testing
- At the completion of Seismic Testing
- With Performance Proof Testing

5.1.2.13 Prudency Testing

The objective of prudency testing is to demonstrate the continuing correct function and performance of the ***SPINLINE 3*** QTS throughout qualification testing. Section 5.4 of EPRI TR-107330 describes the specific functional and performance tests to be performed as part of prudency testing. These tests will be implemented in the ***SPINLINE 3*** QTS prudency test procedure as they are applicable to the ***SPINLINE 3*** QTS design. Section 5.5 of EPRI TR-107330 identifies the points at which the prudency tests should be performed during hardware qualification testing.

As shown in Figure 5.1-1, prudency testing is performed at the following times during hardware qualification testing.

- With Pre-Qualification Acceptance Testing
- At the completion of Radiation Exposure Withstand Testing
- At the completion of the high temperature, high humidity phase of Environmental Testing
- At the completion of Seismic Testing
- With Performance Proof Testing

5.1.3 Generic Qualification Envelope

Successful execution of the Equipment Qualification (EQ) Plan (Reference 5-12) will qualify the generic ***SPINLINE 3*** digital safety I&C platform for the qualification envelope summarized in Table 5.1-1.

Table 5.1-1. Generic Qualification Envelope for the *SPINLINE 3* Digital Safety I&C Platform						
Equipment Qualification Category	**LTR Section**	**EQ Plan Section**	**Regulatory Requirements**	**Source of Qualification Test Specification**	**Qualification Envelope and Test Levels**	**Qualification Test Acceptance Criteria**
Radiation Exposure	5.1.2.3	Appendix C	Regulatory Guide 1.89 (Ref. 5-1) and IEEE Standard 323-2003 (Ref. 5-2)	Section 4.3.6 of EPRI TR-107330	[[ ]]	Section 4.3.6 of EPRI TR-107330
Environmental (Temperature & Humidity)	5.1.2.4	Appendix D	Regulatory Guide 1.89 (Ref. 5-1) and IEEE 323 (Ref. 5-2), subject to enhancements and exceptions listed in Section C of Regulatory Guide 1.209 (Ref. 5-3).	Section 4.3.6 of EPRI TR-107330, modified	[[ ]]	Section 4.3.6 of EPRI TR-107330
Seismic	5.1.2.5	Appendix E	Regulatory Guide 1.100 (Ref. 5-6) and IEEE Standard 344 (Ref. 5-7)	Section 4.3.9 of EPRI TR-107330. The OBE and SSE tests shall follow the RRS curve given as Figure 4-5 in EPRI TR-107330 within the limits of the seismic test table, with the exception that the minimum ZPA requirements are met.	[[ ]] [[ ]] [[ ]]	Section 4.3.9 of EPRI TR-107330.m\

Table 5.1-1. Generic Qualification Envelope for the *SPINLINE 3* Digital Safety I&C Platform						
Equipment Qualification Category	**LTR Section**	**EQ Plan Section**	**Regulatory Requirements**	**Source of Qualification Test Specification**	**Qualification Envelope and Test Levels**	**Qualification Test Acceptance Criteria**
EMI/RFI	5.1.2.6	Appendix F	USNRC Regulatory Guide 1.180, Revision 1 (Ref. 5-8)	**EMI/RFI Emissions Tests**		
				MIL-461E, CE101 (Ref. 5-13): Conducted Emissions, Low Frequency, AC and DC Power Leads	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
				MIL-461E, CE102 (Ref. 5-13): Conducted Emissions, High Frequency, AC and DC Power Leads	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
				MIL-461E, RE101 (Ref. 5-13): Radiated Emissions, Magnetic Field, QTS Surfaces and Leads	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
				MIL-461E, RE102 (Ref. 5-13): Radiated Emissions, Electric Field, Antenna Measurement	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
				EMI/RFI Susceptibility Tests		
				IEC 61000-4-6 (Ref. 5-14): Conducted Susceptibility, Induced RF Fields, Power/Signal Leads	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
						Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]

Table 5.1-1. Generic Qualification Envelope for the *SPINLINE 3* Digital Safety I&C Platform

Equipment Qualification Category	LTR Section	EQ Plan Section	Regulatory Requirements	Source of Qualification Test Specification	Qualification Envelope and Test Levels	Qualification Test Acceptance Criteria
				IEC 61000-4-13 (Ref. 5-15): Conducted Susceptibility, Harmonics/Interharmonics, Power Leads	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
				IEC 61000-4-16 (Ref. 5-16): Conducted Susceptibility, Common Mode Disturbance, Power/Signal Leads	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
						Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
				IEC 61000-4-8 (Ref. 5-17): Radiated Susceptibility, Magnetic Field, Helmholtz Coil Exposure	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
						Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
				IEC 61000-4-9 (Ref. 5-18): Radiated Susceptibility, Magnetic Field, Pulsed	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
				IEC 61000-4-10 (Ref. 5-19): Radiated Susceptibility, Magnetic Field, Damped Oscillatory	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]

Table 5.1-1. Generic Qualification Envelope for the *SPINLINE 3* Digital Safety I&C Platform						
Equipment Qualification Category	**LTR Section**	**EQ Plan Section**	**Regulatory Requirements**	**Source of Qualification Test Specification**	**Qualification Envelope and Test Levels**	**Qualification Test Acceptance Criteria**
				IEC 61000-4-3 (Ref. 5-20): Radiated Susceptibility, High Frequency, Antenna Exposure	[[ ]]	Section 4.3.7 of EPRI TR-107330 and USNRC RG 1.180, Rev. 1 [[ ]]
Electrical Fast Transient (EFT)	5.1.2.7	Appendix G	USNRC Regulatory Guide 1.180, Rev. 1 (Ref. 5-8)	IEC 61000-4-4, “Electromagnetic Compatibility (EMC), Part 4-4: Testing and Measurement Techniques, Electrical Fast Transient/Burst Immunity Test,” (Ref. 5-21)	[[ ]] [[ ]]	Sections 4.6.2 and 4.3.7 of EPRI TR-107330 and USNRC Regulatory Guide 1.180, Rev. 1

Table 5.1-1. Generic Qualification Envelope for the *SPINLINE 3* Digital Safety I&C Platform						
Equipment Qualification Category	**LTR Section**	**EQ Plan Section**	**Regulatory Requirements**	**Source of Qualification Test Specification**	**Qualification Envelope and Test Levels**	**Qualification Test Acceptance Criteria**
Surge Withstand	5.1.2.8	Appendix H	USNRC Regulatory Guide 1.180, Rev. 1 (Ref. 5-8)	Table 22 of USNRC RG 1.180, Rev. 1 defines the IEC 61000-4-12 Ring Wave and IEC 61000 4-5 Combination Wave surge withstand levels for power supplies installed in Category B locations with surge waveform Low Exposure levels	[[.]]	Section 4.6.2 of EPRI TR-107330 and USNRC Regulatory Guide 1.180, Rev. 1.
				Table 15 of USNRC RG 1.180, Rev. 1 defines the IEC 61000-4-12 Ring Wave and IEC 61000 4-5 Combination Wave surge withstand levels for signal leads in Low Exposure locations with Level 2 surge waveforms.		
				IEC 61000-4-5, “Electromagnetic Compatibility (EMC), Part 4-5: Testing and Measurement Techniques, Surge Immunity Test,” (Ref. 5-22)	[[ ]]	
				IEC 61000-4-12, “Electromagnetic Compatibility (EMC), Part 4-12: Testing and Measurement Techniques, Oscillatory Waves Immunity Test,” (Ref. 5-23).		

Table 5.1-1. Generic Qualification Envelope for the *SPINLINE 3* Digital Safety I&C Platform

Equipment Qualification Category	LTR Section	EQ Plan Section	Regulatory Requirements	Source of Qualification Test Specification	Qualification Envelope and Test Levels	Qualification Test Acceptance Criteria
Electrostatic Discharge (ESD)	5.1.2.9	Appendix I	EPRI TR 107330, Section 4.3.8, requires that the test specimen under qualification be tested for ESD withstand capability in accordance with the requirements of EPRI TR-102323-R1. USNRC Regulatory Guide 1.180, Revision 1 (Ref. 5-8) provides no guidance or requirements for ESD Testing.	IEC 61000-4-2 “Electromagnetic Compatibility (EMC), Part 4-2: Testing and Measurement Techniques, Electrostatic Discharge Immunity Test.”	[[ ]]	Sections 4.3.8 of EPRI TR-107330
Class 1E to Non-Class 1E Isolation	5.1.2.10	Appendix J	IEEE Standard 384 (Ref. 5-26). EPRI TR 107330, Section 6.3.6, requires that the test specimen under qualification be tested for Class 1E to non-Class 1E isolation capability in accordance with the requirements of EPRI TR-107330, Section 4.6.4	Sections 4.6.4 of EPRI TR-107330	[[ ]] [[ ]]	Sections 4.6.4 of EPRI TR-107330

5.2 Equipment Analysis

This section describes the following generic analyses that have been performed to establish the foundations for future system-level analyses for plant-specific ***SPINLINE 3*** systems:

- Board/device-level predictive reliability and safety analyses, which includes the following:
  - Failure Modes and Effects Criticality Analysis (FMECA)
  - Reliability analysis
- Setpoint analysis support
- Limited life parts analysis

5.2.1 Predictive reliability and safety analysis

5.2.1.1 Objective

The objectives of the board/device-level predictive reliability and safety analyses are to provide generic failure mode and effects criticality analysis (FMECA) and reliability data for the ***SPINLINE 3*** hardware boards/devices identified in Section 4.3. These generic results are intended to be used as input data to support a system-level FMECA and reliability analysis for an NPP-specific ***SPINLINE 3*** system.

This section includes a summary of the predicted reliability of ***SPINLINE 3*** electronic boards and other components.

5.2.1.2 Approach for the FMECA

Generic board/device-level FMECAs have been prepared in accordance with the guidance in IEC 60812 (Reference 5-27). Unless otherwise noted, IEC 62380 (Reference 5-28) provides the distribution of failure modes and failure rates of the components that comprise the board/device being analyzed. These FMECAs are consistent the failure mode and effects analysis (FMEA) guidance of IEEE Standard 352-1987, Sections 4.1, 4.4, and 4.5 (Reference 5-29).

- Each board-level FMECA includes the following information on the device being analyzed:
  - General description
  - External functional analysis that identifies the device boundaries and the external systems that interact with the device
  - Functional block diagram of the device
  - Description of the function blocks

- The FMECA is used to identify the effects of the failure modes of each function block in the device and define the potential malfunctions of the device. For each board/device-level malfunction, the FMECA assesses the ability to detect the malfunction.

- For each board/device, the FMECA results are presented in table format following the format and content guidance in IEC 60812

5.2.1.3 Results of the board/device-level FMECAs

The results of the board level FMECAs are documented in References 5-30 to 5-41.

5.2.1.4 Approach for the reliability analysis

The methods used to estimate the reliability of ***SPINLINE 3*** boards/modules are based on the following:

- For all RRCN modules that are installed in a rack, the analyses have been recently updated and are based on IEC 62380, "Reliability Data Handbook, Universal Model for Reliability Prediction of Electronics Components, PCBs and Equipment," (Reference 5-28) instead of MIL HDBK 217F, which is recommended in IEEE Standard 352 (Reference 5-27). IEC TR 62380 provides more current data for modern electronic hardware than MIL HDBK 217F
- For all RRCN modules that are installed in the cabinet but outside of the rack, the analyses are based on MIL HDBK 217F. These modules are MV16 and the output relay terminal block,
- For modules from other manufacturers, the analyses are based on MIL HDBK 217F. These items are all installed in the cabinet but outside of the rack.

5.2.1.5 Results of the board/device-level reliability analyses

The results of the board level reliability analyses are documented in References 5-30 to 5-41. A summary of the predicted reliability for each board/device is presented in Table 5.2-1.

Table 5.2-1. Summary of the Predicted Reliability of *SPINLINE 3* Electronic Boards and Other Components

Board Installed in the Chassis	Overall failure rate (h-1)	RRCN Predictive Safety and Reliability Analysis Report	Source of Component-level Failure Data
[[ ]]	[[ ]]	5 100 436 882 B (Reference 5-30)	IEC 62380
[[ ]]	[[ ]]		
[[ ]]	[[ ]]	5 100 436 348 B (Reference 5-31)	IEC 62380
[[ ]]	[[ ]]		
[[ ]]	[[ ]]	5 100 435 707 C (Reference 5-32)	IEC 62380
[[ ]]	[[ ]]		
[[ ]]	[[ ]]	1 479 513 B (Reference 5-33)	IEC 62380
[[ ]]	[[ ]]		
[[ ]]	[[ ]]	5 100 437 019 B (Reference 5-34)	IEC 62380
[[ ]]	[[ ]]		

Table 5.2-1. Summary of the Predicted Reliability of *SPINLINE 3* Electronic Boards and Other Components			
Board Installed in the Chassis	**Overall failure rate (h-1)**	**RRCN Predictive Safety and Reliability Analysis Report**	**Source of Component-level Failure Data**
[[ ]]	[[ ]]	3 008 651 A (Reference 5-35)	IEC 62380
[[ ]]	[[ ]]		
[[ ]]	[[ ]]	6 648 805 C (Reference 5-36)	IEC 62380
[[ ]]		1 208 933 B (Reference 5-37)	IEC 62380
[[ ]]	[[ ]]		
[[ ]]	[[ ]]		
[[ ]]	[[ ]]		
[[ ]]		1 208 933 B (Reference 5-37	IEC 62380
[[ ]]	[[ ]]		
[[ ]]	[[ ]]		
[[ ]]	[[ ]]		
[[ ]]	[[ ]]	3 000 180 B (Reference 5-38	IEC 62380
[[ ]]	[[ ]]		
Modules Installed Outside the Chassis			
[[ ]]	[[ ]]	None. Overall failure rate obtained from manufacturer of the product.	MIL HDBK 217F
[[ ]]	[[ ]]	None. Overall failure rate obtained from manufacturer of the product.	MIL HDBK 217F
[[ ]]	[[ ]]	None. Overall failure rate obtained from manufacturer of the product.	MIL HDBK 217F
[[ ]]	[[ ]]	None. Overall failure rate obtained from manufacturer of the product.	MIL HDBK 217F

Table 5.2 1. Summary of the Predicted Reliability of SPINLINE 3 Electronic Boards and Other Components			
Board Installed in the Chassis	**Overall failure rate (h-1)**	**RRCN Predictive Safety and Reliability Analysis Report**	**Source of Component-level Failure Data**
[[ ]]		None. Overall failure rate obtained from manufacturer of the product.	
[[ ]]	[[ ]]		MIL HDBK 217F
[[ ]]	[[ ]]		Telcordia
[[ ]]	[[ ]]	5 100 436 936 A (Reference 5-39)	MIL HDBK 217F
[[ ]]	[[ ]]	5 100 436 935 A (Reference 5-40)	MIL HDBK 217F
[[ ]]	[[ ]]	3 008 991 B (Reference 5-41)	IEC 62380
[[ ]]	Failure rate not considered because this is a very simple module (screw terminal block with a integrated circuit)	None	
[[ ]]	Failure rate not considered because this is a very simple module (screw terminal block with a integrated circuit)	None	

5.2.2 Setpoint Analysis Support

5.2.2.1 Objective

EPRI TR-107330, Section 4.2.4 (Reference 5-9) recommends that the qualifier provide information about the qualified hardware to support an application-specific setpoint analysis. USNRC Regulatory Guide 1.105, Rev 3 (Reference 5-42) endorses ISA S67.04-1994 (Reference 5-43), with qualifications, as the basis for performing an application-specific setpoint analysis.

The recommended setpoint analysis support information includes the following:

A. Calibrated accuracy, including hysteresis and non-linearity, of the analog inputs and outputs

B. Repeatability of the analog inputs and outputs

C. Temperature sensitivity of the analog inputs and outputs

D. Drift with time of the analog inputs and outputs

E. Power supply variation effects on the analog inputs and outputs

F. Error contribution of any arithmetic operations needed to implement a setpoint. The accuracy shall be based on using two additions and one multiplication on an input value plus a comparison. The error contributions shall be provided for both integer and floating point calculations.

In addition, EPRI recommends that the qualification process identify those components, if any, on analog I/O modules that are sensitive to the following.

G. Components where vibration could affect accuracy (e.g. potentiometers).

H. Components where radiation exposure could affect accuracy.

I. Components where relative humidity could affect accuracy.

The objective of the Setpoint Analysis Support Document (Reference 5-44) is to provide a single, concise listing of the accuracy, drift, and other relevant specifications of the ***SPINLINE 3*** digital safety I&C platform. These specifications are intended to enable a licensee to calculate instrument measurement uncertainties and establish critical control setpoints for a plant-specific ***SPINLINE 3*** system based on ISA RP67.04.02.

5.2.2.2 Approach

The Setpoint Analysis Support document provides the data recommended in EPRI TR-107330 for the following ***SPINLINE 3*** components:

•	8PT100	Temperature conditioning board
•	16E.ANA ISO	Analog signals acquisition and analog to digital conversion board
•	32ETOR TI SR	ON-OFF isolated acquisition board (not redounded)
•	ICTO	Pulse Count Board
•	32ACT	Actuator Drive Board
•	6SANA ISO	Analog Outputs board
•	MV16	Actuators voting module combining ON-OFF inputs
•	8SRELAY Type 1	Relay module based on Relay Type 1
•	8SRELAY Type 2	Relay module based on Relay Type 2

The accuracy specifications have been compiled from manufacturer’s documentation and the results of qualification testing of the ***SPINLINE 3*** Qualification Test Specimen (QTS)

5.2.3 Limited Life Parts Analysis

EPRI TR-107330, Section 4.7.8.2 (Reference 5-9) requires the qualifier to perform a component aging analysis on the qualified hardware based on the normal and abnormal environmental conditions to which it is exposed. The purpose of this analysis is to provide a “qualified life” for components associated with the digital I&C platform under qualification.

Qualified life is a term not typically applied to digital I&C equipment intended for installation in a mild environment, because accelerated aging is not part of the equipment qualification program. In addition, IEEE Standard 323-2003 (Reference 5-2), Section 4.1 states that, “A qualified life is not required for equipment located in a mild environment and which has no significant aging mechanisms.” USNRC Regulatory Guide 1.209, Paragraph C.(1), (Reference 5-3) states that, “The NRC does not consider the age conditioning (of IEEE Standard 323-2003) to be applicable because of the absence of significant aging mechanisms on microprocessor-based modules.”

The types of electronic components that typically have life limits are batteries and electrolytic capacitors. Any batteries in ***SPINLINE 3*** hardware are identified in the Operations and Maintenance Manuals (OMMs) and regular replacement is performed throughout the operating lifetime of the system. There are no electrolytic capacitors or other components with known life limits in the generic ***SPINLINE 3*** hardware described in Section 4.3.

Plant-specific ***SPINLINE 3*** systems will be examined during the design phase to confirm if any life limited components are introduced in the hardware for a specific application. If any such components are identified, appropriate measures will be identified in the OMMs to manage the life-limited component.

5.3 Chapter 5 References

5-1 U.S. Nuclear Regulatory Commission Regulatory Guide 1.89, Revision 1, “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,” June 1984

5-2 IEEE 323-2003, “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”

5-3 U.S. Nuclear Regulatory Commission Regulatory Guide 1.209, Revision 0, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” March 2007.

5-4 IEEE 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”

5-5 U.S. Nuclear Regulatory Commission Regulatory Guide 1.152, R2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

5-6 U.S. Nuclear Regulatory Commission Regulatory Guide 1.100, Revision 2, “Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants,” June 1988

5-7 IEEE 344-1987, “Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.”

5-8 U.S. Nuclear Regulatory Commission Regulatory Guide 1.180, Revision 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control System,” October 2003.

5-9 EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” December 1996

5-10 USNRC Letter dated July 30, 1998 to Mr. J. Naser (EPRI), “Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute (EPRI) Topical Report, TR-107330, Final Report, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants.”

5-11 “System Specification of the Qualification Test Specimen and Data Acquisition System,” Document No. 3006404, , Rolls-Royce Civil Nuclear SAS, December 2008

5-12 "Equipment Qualification (EQ) Plan", Document No. 3006501A, , Rolls-Royce Civil Nuclear SAS, December 2008

5-13 Military Standard 461E, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” August 20, 1999

5-14 IEC 61000-4-6, “Testing and Measurement Techniques, Immunity to Conducted Disturbances Induced by Radio-Frequency Fields,” May 2006.

5-15 IEC 61000-4-13, “Testing and Measurement Techniques, Harmonics and Interharmonics Including Mains Signaling at A.C. Power Ports, Low Frequency Immunity Tests,” March 2002.

5-16 IEC 61000-4-16, “Testing and Measurement Techniques, Tests for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz,” July 2002.

5-17 IEC 61000-4-8, “Testing and Measurement Techniques, Power Frequency Magnetic Field Immunity Test,” March 2001.

5-18 IEC 61000-4-9, “Testing and Measurement Techniques, Pulse Magnetic Field Immunity Test,” March 2001.

5-19 IEC 61000-4-10, “Testing and Measurement Techniques, Damped Oscillatory Magnetic Field Immunity Test,” March 2001.

5-20 IEC 61000-4-3, “Testing and Measurement Techniques, Radiated, Radio-Frequency, Electromagnetic Field Immunity Test,” February 2006.

5-21 IEC 61000-4-4, “Testing and Measurement Techniques, Section 4: Electrical Fast Transient/Burst Immunity Test,” July 2004.

5-22 IEC 61000-4-5, “Testing and Measurement Techniques, Section 5: Surge Immunity Test,” November 2005.

5-23 IEC 61000-4-12, “Testing and Measurement Techniques, Section 12: Oscillatory Waves Immunity Tests,” September 2006.

5-24 EPRI TR-102323-R1, “Guidelines for Electromagnetic Interference Testing in Power Plants,” January 1997.

5-25 IEC 61000-4-2, “Testing and Measurement Techniques, Section 2: Electrostatic Discharge Immunity Test,” April 2001.

5-26 IEEE 384-1981, “Standard Criteria for Independence of Class 1E Equipment and Circuits.”

5-27 IEC 60812 (2nd edition) 2006-01, "Analysis techniques for system reliability – Procedure for Failure Mode and Effects Analysis (FMEA)", International Electrotechnical Commission, 2006

5-28 IEC TR 62380 (1st edition) 2004-08, “Reliability Data Handbook, Universal Model for Reliability Prediction of Electronics Components, PCBs and Equipment,” International Electrotechnical Commission, 2004

5-29 IEEE 352-1987, “Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.”

5-30 “RTD conditioning board: 8PT100 and I.8PT100 Interface board”, Report 5 100 436 882 B, Rolls-Royce Civil Nuclear SAS, 2009

5-31 “Analog input board: 16E.ANA ISO and I.16EANA interface board", Report 5 100 436 348 B, Rolls-Royce Civil Nuclear SAS, 2009

5-32 Digital isolated input board: 32ETOR TI SR and I.32ETOR TI interface board”, Report 5 100 435 707 C, Rolls-Royce Civil Nuclear SAS, 2009

5-33 “Calibrated pulse acquisition board: ICTO and I.ICTO interface board”, Report 1 479 513 B, Rolls-Royce Civil Nuclear SAS, 2009

5-34 “Actuator drive board: 32ACT and I.32ACT interface board”, Report 5 100 437 019 B, Rolls-Royce Civil Nuclear SAS, 2009

5-35 “Analog output board: 6SANA ISO and I.6SANA interface board”, Report 3 008 651 A, Rolls-Royce Civil Nuclear SAS, 2009

5-36 “CPU board: UC25N+”, Report 6 648 805 C, Rolls-Royce Civil Nuclear SAS, 2009

5-37 “NERVIA+ daughter board and “I.NERVIA+ interface board”, Report 1 208 933 B, Rolls-Royce Civil Nuclear SAS, 2009

5-38 “ALIM 48V/5V-24V power supply board and I.ALIM 48 interface board”, Report 3 000 180 B, Rolls-Royce Civil Nuclear SAS, 2009

5-39 “Actuation voting module: MV16”, Report 5 100 436 936 A, Rolls-Royce Civil Nuclear SAS, 2009

5-40 “Output relays terminal block: 8SRELAY1 and 8SRELAY2”, Report 5 100 436 935 A, Rolls-Royce Civil Nuclear SAS, 2009

5-41 “32ETOR input terminal block”, Report 3 008 991 B, Rolls-Royce Civil Nuclear SAS, 2009

5-42 U.S. Nuclear Regulatory Commission Regulatory Guide 1.105, Rev. 3, "Setpoints for Safety-Related Instrumentation", December 1999

5-43 ISA RP 67.04.02-2000, “Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation.”, Instrument Society of America

5-44 "Setpoint Analysis Support", Report 3 009 397A, Rolls-Royce Civil Nuclear SAS, 2009

6 Software Development Process for *SPINLINE 3* Platform Software and Application Software

6.1 *SPINLINE 3* Platform Software Development History

[[

]]

6.2 *SPINLINE 3* Operational System Software (OSS) Development Process

[[

]]

6.3 *SPINLINE 3* Platform Software Design and Development Analyses – IEC 880 and BTP 7-14

[[

]]

6.4 *SPINLINE 3* Application Software Development Process

[[

]]

6.5 Cyber Security Plan

[[

]]

6.6 Chapter 6 References

[[

]]

Appendix A : Hardware Data Sheets

[[

]]