UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

July 31, 2019

Research and Production Company RadICS
Attention: Anton Andrashov
RadICS Director
29 Geroyiv Stalingradu Street
25009 Kirovohrad, Ukraine

SUBJECT: FINAL NONPROPRIETARY SAFETY EVALUATION FOR "RADICS TOPICAL REPORT" (CAC NO. MF8411; EPID L-2016-TOP-0010)

Dear Mr. Andrashov:

By letter dated September 20, 2016 (Agencywide Documents Access and Management System Accession No. ML16274A346), Research and Production Corporation Radiy (RPC Radiy) submitted for the U.S. Nuclear Regulatory Commission (NRC) staff review the "RadICS Topical Report." By letter dated May 8, 2019, the NRC staff issued its draft safety evaluation (SE) on "RadICS Topical Report" (ADAMS Accession No. ML19003A471).

RPC Radiy provided comments on the draft SE by letter dated May 21, 2019 (ADAMS Accession No. ML19149A364). The comments addressed proprietary information, inconsistencies, and typographical errors.

The NRC staff has found that "RadICS Topical Report" is acceptable for referencing in licensing applications for nuclear power plants to the extent specified and under the limitations delineated in the topical report (TR) and in the enclosed final SE. The final SE defines the basis for our acceptance of the TR.

Our acceptance applies only to material provided in the subject TR. We do not intend to repeat our review of the acceptable material described in the TR. When the TR appears as a reference in license applications, our review will ensure that the material presented applies to the specific plant involved. License amendment requests that deviate from this TR will be subject to a plant-specific review in accordance with applicable review standards.

In accordance with the guidance provided on the NRC website, we request that RPC Radiy publish accepted proprietary and non-proprietary versions of the TR within three months of receipt of this letter. The accepted versions shall incorporate this letter and the enclosed final SE after the title page. Also, they must contain historical review information, including NRC requests for additional information (RAIs) and your responses. The approved versions shall include a "-A" (designating approved) following the TR identification symbol.

As an alternative to including the RAIs and RAI responses behind the title page, if changes to the TRs provided to the NRC staff to support the resolution of RAI responses, and the NRC staff reviewed and approved those changes as described in the RAI responses, there are two ways that the accepted version can capture the RAIs:

1. The RAIs and RAI responses can be included as an Appendix to the accepted version.

2. The RAIs and RAI responses can be captured in the form of a table (inserted after the final SE) which summarizes the changes as shown in the approved version of the TR. The table should reference the specific RAIs and RAI responses which resulted in any changes, as shown in the accepted version of the TR.

If future changes to the NRC's regulatory requirements affect the acceptability of this TR, NEI will be expected to revise the TR appropriately. Licensees referencing this TR would be expected to justify its continued applicability or evaluate their plant using the revised TR.

If you have any questions or require any additional information, please feel free to contact the NRC Project Manager for the review, Joseph Holonich at (301) 415-7297 or joseph.holonich@nrc.gov.

Sincerely,

/RA Leslie Perkins for/

Dennis C. Morey, Chief
Licensing Processes Branch
Division of Licensing Projects
Office of Nuclear Reactor Regulation

Docket No. 99902028

Enclosure:
Final SE

SUBJECT: FINAL NONPROPRIETARY SAFETY EVALUATION FOR “RADICS TOPICAL REPORT” (CAC NO. MF8411; EPID L-2016-TOP-0010) DATE: JULY 31, 219

DISTRIBUTION:
PUBLIC (Cover Letter)
NON-PUBLIC (Draft SE)

RidsACRS_MailCTR	MWaters, NRR
RidsNrrLADHarrison	RStattel, NRR
RidsOgcMailCenter	RAlvarado,NRR
RidsNrrDlpPlpb	RidsNrrDeEica
RidsNrrDeEicb	DTaneja, NRR
RidsNrrDlp	RidsNrrDe
RidsResOd	JHolonich, NRR
RidsNroOd	DMorey, NRR
RidsNrrDlr	PLPB r/f

ADAMS Accession Nos.: ML19134A193 *concurrence via e-mail NRR-106

OFFICE	DLP/PLPB/PM*	DLP/PLPB/LA*	DE/EICB/ABC*	DLP/PLPB/BC
NAME	JHolonich	DHarrison	RAlvaradi	DMorey (LPerkins for)
DATE	07/30/2019	07/11/2019	07/29/2019	07/31/2019

OFFICIAL RECORD COPY

U.S. Nuclear Regulatory Commission Staff

Safety Evaluation for

Topical Report 2016-RPC003-TR-001

RadICS Safety System Digital Platform

Date: August 2019

Principal Contributors: Richard Stattel
Dinesh Taneja

Enclosure

List of Abbreviations

AD – Architecture Description
ADAMS – Agencywide Documents Access and Management System
AFBL – Application Function Block Library
AIM – Analog Input Module
AOM – Analog Output Module
ASPI – Active Serial Programming Interface
ATWS – Anticipated Transients Without Scram
BTP – Branch Technical Position
CCB – Change Control Board
CCF – Common Cause Failure
CFR – Code of Federal Regulations
CGD – Commercial Grade Dedication
CM – Configuration Management
COTS – Commercial Off the Shelf
CPLD – Complex Programmable Logic Device
CRC – Cyclical Redundancy Check
D3 – Diversity and Defense in Depth
DI&C – Digital Instrumentation and Control
DIM – Digital Input Module
DOM – Digital Output Module
ED – Electronic Design
EEPROM – Electrically Erasable Programmable Read Only Memory
EMC – Electro Magnetic Compatibility
EMI – Electro Magnetic Interference
EPRI – Electric Power Research Institute
EPROM – Erasable Programmable Read Only Memory
ESD – Electro Static Discharge
F – Fahrenheit
FBL – Function Block Logic
FMEA – Failure Modes and Effects Analysis
FMEDA – Failure Modes and Effects Diagnostic Analysis
FPGA – Field Programmable Gate Array
FSC – FPGA based Safety Controller
FSMP – Functional Safety Management Plan
GDC – General Design Criteria
HDL – Hardware Descriptive Language
HICR – Highly Integrated Control Room
I&C – Instrumentation and Control
I/O – Input / Output
IAEA – International Atomic Energy Agency
IC – Integrated Circuit
IEC – International Electrotechnical Commission
IEEE – Institute of Electrical and Electronics Engineers
IERS – In Equipment Response Spectra
ISG – Interim Staff Guide
ISO – International Organization for Standardization
IVV – Independent Verification and Validation
JTAG – Joint Test Action Group
LAN – Local Area Network
LLC – Limited Liability Company
LM – Logic Module
LVDS – Linear Voltage Differential Signal
M&TE – Measurement and Test Equipment
MATS – Monitoring and Tuning System
MIL-STD – Military Standard
NPP – Nuclear Power Plant
NQA – Nuclear Quality Assurance
OBE – Operating Basis Earthquake
OCM – Optical Communications Module
PC – Personal Computer
PFBL – Platform Function Block Library
PLC – Programmable Logic Controller
PSAI – Plant Specific Action Item
PSWD – Power Supply and Watch Dog
QA – Quality Assurance
QAP Quality Assurance Program
QAPD – Quality Assurance Program Document
QMS – Quality Management System
QTS – Qualification Test Specimen
Radics LLC – Research and Production Company Radics LLC
RAI – Request for Additional Information
RFI – Radio Frequency Interference
RG – Regulatory Guide
RM – Risk Management
RPC – Research and Production Corporation
RPC Radiy – Research and Production Corporation Radiy
RPCT – Radiy Product Configuration Toolset
RPP – Radiy Proprietary Protocol
RRS – Required Response Spectrum
RS 232/485 – Recommended Standard 232 / 485
RTM – Requirements Traceability Matrix
RTS – Reactor Trip System
RUP – Radiy UDP based Protocol
SAR – Safety Analysis Report
SCSI – Small Computer System Interface
SDOE – Secure Development and Operational Environment
SIL – Safety Integrity Level
SPI – Serial Peripheral Interface
SRP – Standard Review Plan
SRS – Safety Requirements Specification
SSC – Structures Systems and Components
SSE – Safe Shutdown Earthquake
SSRAM – Synchronous Static Random-Access Memory
STA – Static Timing Analysis
TR – Topical Report
UART – Universal Asynchronous Receiver/Transmitter
UDP – User Datagram Protocol
V&V – Verification and Validation
VDC – Voltage Direct Current
VHDL – VHSIC Hardware Descriptive Language
VHSIC – Very High Speed Integrated Circuit
VM – Ventilation Module
ZPA – Zero Period Acceleration

Table of Contents

1.0 INTRODUCTION AND BACKGROUND ..... - 5 -
2.0 REGULATORY EVALUATION ..... - 7 -
3.0 TECHNICAL EVALUATION ..... - 10 -
3.1 System Background ..... - 10 -
3.2 System Description ..... - 11 -
3.2.1 RadICS Digital I&C Platform Basic Operation Description ..... - 12 -
3.2.2 RadICS Digital I&C Platform Basic Architecture ..... - 12 -
3.2.2.1 Platform Module Descriptions ..... - 17 -
3.2.2.1.1 Logic Module (LM) ..... - 17 -
3.2.2.1.2 Analog Input Module (AIM) ..... - 18 -
3.2.2.1.3 Discrete Input Module (DIM) ..... - 18 -
3.2.2.1.4 Analog Output Module (AOM) ..... - 18 -
3.2.2.1.5 Discrete Output Module (DOM) ..... - 18 -
3.2.2.1.6 Optical Communication Module (OCM) ..... - 18 -
3.2.2.2 Units for RadICS Modules ..... - 18 -
3.2.3 RadICS Platform Communications ..... - 20 -
3.2.3.1 Internal Communications Interfaces ..... - 20 -
3.2.3.1.1 Linear Voltage Differential Signal Interface (Internal / Online) ..... - 20 -
3.2.3.1.2 Watchdog Interface (Internal / Online) ..... - 21 -
3.2.3.1.3 Synchronous Static Random Access Memory Interface (Internal / Online) ..... - 21 -
3.2.3.2 External Communications Interfaces ..... - 21 -
3.2.3.2.1 Fiber Optic RUP Interfaces (External Online or Offline) ..... - 21 -
3.2.3.2.2 Fiber Optic RPP Interfaces (External / Online) ..... - 22 -
3.2.3.2.3 RS-232/485 Interfaces (External / Online) ..... - 22 -
3.2.3.2.4 Tuning Access Interface (External Online) ..... - 22 -
3.2.3.2.5 Active Serial Programming Interface (External / Offline) ..... - 22 -
3.2.3.2.6 Joint Test Action Group Interface (External / Offline) ..... - 22 -
3.2.3.2.7 Serial Peripheral Interface (External / Online) ..... - 22 -
3.2.3.2.8 Universal Asynchronous Receiver/Transmitter Interface (External / Offline) ..... - 23 -
3.2.3.2.9 Real Time Interface (External / Online) ..... - 23 -
3.2.4 Monitoring and Tuning System ..... - 23 -
3.2.5 Radics Download Station ..... - 24 -
3.3 RadICS Logic Architecture ..... - 24 -
3.3.1 RadICS Platform FPGA Logic ..... - 24 -
3.3.2 Plant Specific User Application FPGA Logic ..... - 24 -
3.3.3 Self-diagnostics CPLD Logic ..... - 25 -
3.3.4 Function Block Libraries ..... - 25 -
3.5 RadICS Platform Development Processes ..... - 31 -
3.5.1 Platform Electronic Design Development Lifecycle Process Planning ..... - 32 -
3.5.1.1 Management Plan ..... - 33 -
3.5.1.2 Development Plan ..... - 34 -
3.5.1.3 Quality Assurance Planning ..... - 36 -
3.5.1.4 Integration Plan ..... - 37 -
3.5.1.5 Safety Plan ..... - 38 -
3.5.1.6 Verification and Validation Planning ..... - 39 -
3.5.1.7 Configuration Management Planning ..... - 42 -
3.5.1.8 Test Planning ..... - 43 -
3.5.2 Logic Implementation and Design Output Documentation ..... - 44 -
3.5.2.1 Safety Analysis ..... - 45 -

3.5.2.2 V&V Analysis and Reports ..... - 46 -
3.5.2.3 Configuration Management Activity ..... - 47 -
3.5.2.4 Testing Activity ..... - 47 -
3.5.2.5 Requirements Traceability Evaluation ..... - 48 -
3.5.2.6 Failure Mode and Effect Analysis ..... - 50 -
3.5.2.7 Reliability Analysis ..... - 51 -
3.5.2.8 Requirements Specification ..... - 52 -
3.6 Equipment Qualification ..... - 53 -
3.6.1 Atmospheric (Temperature and Humidity) ..... - 55 -
3.6.2 Class 1E to Non-1E Isolation ..... - 56 -
3.6.3 Electromagnetic Interference / Radio Frequency Interference ..... - 57 -
3.6.3.1 EMI/RFI Interference ..... - 58 -
3.6.3.2 EMI/RFI Susceptibility ..... - 59 -
3.6.3.3 Electrostatic Discharge Withstand Testing (Appendix F) ..... - 59 -
3.6.3.4 Electrical Fast Transient Susceptibility (Appendix G) ..... - 59 -
3.6.3.5 Surge Withstand Capability (Appendix H) ..... - 59 -
3.6.3.6 EMI / RFI Test Results ..... - 59 -
3.6.4 Seismic Qualification ..... - 60 -
3.7 RadICS platform Integrity Characteristics ..... - 63 -
3.7.1 RadICS platform Response Time ..... - 63 -
3.7.2 Determinism ..... - 65 -
3.7.3 Self-Diagnostics / Test and Calibration Capabilities ..... - 66 -
3.8 Setpoint Determination Methodology ..... - 68 -
3.9 Diversity and Defense-in-Depth. ..... - 68 -
3.10 Communications ..... - 77 -
3.10.1 DI&C-ISG-04, Staff Position 1 - Interdivisional Communications ..... - 78 -
3.10.2 DI&C-ISG-04, Section 2 - Command Prioritization ..... - 94 -
3.10.3 DI&C-ISG-04, Section 3 - Multidivisional Control and Display Stations ..... - 94 -
3.11 Compliance to IEEE Std. 603-1991 Requirements ..... - 99 -
3.11.1 IEEE Std. 603-1991, Clause 4, “Safety System Designation” ..... - 99 -
3.11.2 IEEE Std. 603-1991, Clause 5, “Safety System Criteria” ..... - 101 -
3.11.3 IEEE Std. 603-1991, Clause 6, “Sense and Command Features – Functional and Design Requirements” ..... - 107 -
3.11.4 IEEE Std. 603-1991, Clause 7, “Execute features – functional and design requirements” ..... - 108 -
3.11.5 IEEE Std. 603-1991, Clause 8, “Power Source Requirements” ..... - 109 -
3.12 Conformance with IEEE Std. 7-4.3.2 2003-- ..... - 109 -
3.12.1 IEEE Std. 7-4.3.2 2003--, Clause 5, “Safety System Criteria” ..... - 110 -
3.13 Secure Development and Operational Environment ..... - 123 -
4.0 SUMMARY ..... - 130 -
5.0 LIMITATIONS AND CONDITIONS ..... - 131 -
6.0 GENERIC OPEN ITEMS ..... - 131 -
7.0 PLANT-SPECIFIC ACTION ITEMS ..... - 131 -
8.0 REFERENCES ..... - 134 -
Appendix A: Comments on Draft Safety Evaluation for RadICS Topical Report and NRC Staff Responses 140

SAFETY EVALUATION

BY THE OFFICE OF NUCLEAR REACTOR REGULATION

FOR RESEARCH AND PRODUCTION CORPORATION (RADICS LLC)

RadICS PLATFORM TOPICAL REPORT AND SUPPORTING DOCUMENTS

EPID NO. L-2016-TOP-0010

1.0 INTRODUCTION AND BACKGROUND

By letter dated September 20, 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16274A346), Research and Production Corporation Radiy (RPC Radiy), through its wholly owned Limited Liability Company, "Research and Production Company Radics LLC" (Radics LLC), submitted Topical Report (TR) 2016-RPC003-TR-001, "RadICS Topical Report," Revision 0 (ADAMS Accession No. ML16274A348), to the U.S. Nuclear Regulatory Commission (NRC) staff for formal review and acceptance for referencing in regulatory actions. By letter dated September 15, 2017 (ADAMS Accession No. ML17275A191), Radics LLC submitted supplemental RadICS TR design description changes and modifications. This RadICS TR supplemental design information consists of changes and modifications to the Revision 0, RadICS TR application logic functional block library self-diagnostics, periodic testing, and diversity and defense-in-depth, design descriptions. This supplemental design information is submitted as a "Revision 1" update to the RadICS TR.

The NRC staff performed an acceptance review of the RadICS TR request and supporting documents. By letter dated April 5, 2017 (ADAMS Accession No. ML16281A459), the NRC staff informed Radics LLC that it had completed an acceptance review and found that the material presented was sufficient to begin an official topical report review, however, completion of the safety evaluation (SE) was contingent upon the submittal of additional documentation. The additional documentation requested by NRC staff was subsequently submitted to support this evaluation. This documentation consisted of the following:

- Phase 2 Equipment Qualification Test Report (Ref. 8)
- D2.3 Radics LLC Tool Selection and Evaluation Report (Ref. 39)
- D11.1 Radics LLC Product Safety Manual (Ref. 35)
- D12.1 Radics LLC Functional Safety Management Audit Plan (Ref. 40)

The Radics LLC organization is based in Kropyvnytskyi, Ukraine, and is responsible for all RadICS -based application project activities. Therefore, Radics LLC is seeking the NRC's generic approval for use of RPC Radiy's RadICS Platform, as described and discussed in the RadICS TR, in nuclear safety systems in any U.S. nuclear power plant (NPP). The following supplemental letters were submitted to the NRC to provide supporting documents and requested additional information for this SE.

These supplemental documents provide additional information to clarify and support the technical positions documented in the RadICS TR.

On March 1, 2018, the NRC staff submitted Requests for Additional Information (RAIs) (Ref. 5). Radics LLC provided the responses to these RAIs as identified in Table 1.0-1 above.

Table 1.0-1 List of Supplemental Letters from Radics LLC

Document	Date Submitted	Reference
RadICS Submittal of Digital I&C [Instrumentation and Control] Platform Topical Report Support Documents	12/3/2016	2
RadICS Digital I&C Platform Topical Report Supplemental Information	9/15/2017	4
Submittal of Response to Request for Additional Information for RadICS Topical Report	4/13/2018	6
Submittal of RadICS Digital I&C Platform Topical Report Supplemental Information Update	8/2/2018	7
Submittal of Phase 2 Documents for RadICS Digital I&C Platform Topical Report	8/10/2018	8

The NRC staff conducted an audit of the RadICS platform development documents at the Kinectrics, Inc. facilities in Toronto, Canada on April 2 through 5, 2018. The NRC staff performed this audit in accordance with Office of Nuclear Reactor Regulation Office Instruction LIC-111. The purpose of this audit was to evaluate the effectiveness of Radics LLC logic development activities and to confirm that processes described in the RadICS TR are being effectively implemented to achieve a high-quality system that can be used to perform safety-related functions in a nuclear facility. During the regulatory audit, several requirement thread reviews were performed. The NRC staff confirmed how system requirements had been implemented and tested during the Radics LLC development processes. Radics LLC showed how the requirements traceability was used to confirm design development activities performed. Performance characteristics and functional capabilities of RadICS platform-based systems were observed. The results of the audit are documented in the “Regulator Audit Report for the Radics LLC Digital Platform Licensing Topical Report” (Ref. 9).

The NRC staff evaluated the development and test plans, specifications and procedures used to design, and perform verification and validation of the standardized Radics LLC circuit boards described in the TR. The NRC staff also evaluated the safety lifecycle processes to be used for development of RadICS plant-specific logic. The NRC staff did not evaluate the integration and testing of plant specific system applications, factory acceptance test of plant systems, or maintenance activities to support installed plant systems.

Section 2.0 of this SE identifies the applicable regulatory bases and corresponding guidance and regulatory acceptance criteria to which the NRC staff evaluated the RadICS platform topical

report. Section 3.0 of this SE provides the technical evaluation of the RadICS TR. Section 4.0 provides the NRC staff conclusion and Section 5.0 provides limitations and conditions that apply to applicants or licensees that reference this SE for use of the RadICS platform in safety systems of U.S. nuclear power generating stations. Section 8.0 provides a list of applicable references.

2.0 REGULATORY EVALUATION

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Rev. 7, which is referred to as the Standard Review Plan (SRP), sets forth a method for reviewing compliance with applicable sections of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities." SRP Chapter 7, "Instrumentation and Controls," was used by the NRC staff to establish acceptance criteria for this review. SRP Chapter 7 addresses the requirements for I&C systems in nuclear power plants based on light-water reactor designs. SRP Chapter 7 and Interim Staff Guidance (ISG), which augments and supplements SRP Chapter 7, principally establish the review process for digital I&C systems applied in this evaluation.

The suitability of a digital I&C platform for use in safety systems depends on the quality of its components; quality of the design process; and its Environmental Qualification, along with consideration of system implementation characteristics such as real-time performance, independence, and support of on-line surveillance requirements as demonstrated through the digital I&C platform's verification, validation, and qualification efforts. Because Radics LLC equipment is intended for use in safety systems and for safety-related applications, the platform TR was evaluated for compliance with the criteria of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603." The platform topical report was similarly evaluated against the criteria of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2."

Some review criteria within the SRP depend on the design of an assembled system for a particular application, whereas this licensing TR presents elements of hardware and board-level Field Programmable Gate Array (FPGA) programming that constitute the RadICS platform, which is intended for use in a variety of applications. As such, this SE is necessarily limited to the evaluation of compliance with the relevant regulations and guidance documents to the degree that they can be met at the platform level, because the RadICS TR scope excludes details that would support a plant-specific safety system application. This SE does not directly evaluate regulations and guidance at the system level and only evaluates the capabilities and characteristics of the RadICS platform on a generic basis with respect to support of future evaluations of safety systems at the system level.

Determination of compliance with all applicable regulations remains subject to a plant-specific licensing review of a complete system design based on the RadICS platform. Plant Specific Action Items (PSAIs) have been established to identify criteria that should be addressed by an applicant or licensee referencing this SE (see Section 7.0). These criteria are provided to facilitate an applicant's or licensee's ability to establish full compliance with the design criteria and regulations identified in SRP Chapter 7, Table 7-1, that are applicable to the applicant's or licensee's digital I&C system and that were in effect at the time of the RadICS platform review

The PSAIs identified in Section 7.0 do not obviate an applicant's or licensee's responsibility to acceptably address new or changed design criteria or regulations that apply in addition to those used to perform this SE when making changes to its facility. The following regulations are applicable to the RadICS TR:

- 10 CFR 50.54 (jj) and 10 CFR 50.55(i), Require 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.

- 10 CFR 50.55a(h), "Protection and Safety Systems," incorporates the 1991 version of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," by reference, including the correction sheet dated January 30, 1995.

- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants"

  - GDC 1, "Quality Standards and Records"
  - GDC 2, "Design Bases for Protection Against Natural Phenomena"
  - GDC 4, "Environmental and Dynamic Effects Bases"
  - GDC 13, "Instrumentation and Control"
  - GDC 20, "Protection System Functions"
  - GDC 21, "Protection System Reliability and Testability"
  - GDC 22, "Protection System Independence"
  - GDC 23, "Protection System Failure Modes"
  - GDC 24, "Separation of Protection and Control Systems"
  - GDC 25, "Protection System Requirements for Reactivity Control Malfunctions"
  - GDC 29, "Protection Against Anticipated Operational Occurrences"

- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"

- 10 CFR Part 21, "Reporting of Defects and Noncompliance"

The NRC staff used the applicable portions of the guidance provided in the following regulatory guides (RGs) and the DI&C ISG:

- RG 1.22, "Periodic Testing of Protection System Actuation Functions," Revision 0.

- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 1.

- RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," Revision 2.

- RG 1.62, "Manual Initiation of Protective Actions," Revision 1.

- RG 1.75, "Criteria for Independence of Electrical Safety Systems," Revision 3.

- RG 1.100, “Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants,” Revision 3, describes a method acceptable to the NRC staff for satisfying the seismic qualification.

- RG 1.105, “Setpoints for safety-Related Instrumentation,” Revision 3.

- RG 1.118, “Periodic Testing of Electric Power and Protection Systems,” Revision 3.

- RG 1.152, “Criteria for Use of Computers In Safety Systems of Nuclear Power Plants,” Revision 3.

- RG 1.168, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 2.

- RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 1.

- RG 1.170, “Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 1.

- RG 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 1.

- RG 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 1.

- RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Revision 1.

- RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-Related Instrumentation and Control Systems,” Revision 1.

- RG 1.209, “Guidelines for Environmental Qualification of safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” March 2007.

- DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc),” Revision 1.

- DI&C-ISG-06, “Task Working Group #6: Licensing Process,” Revision 1.

The NRC staff also used applicable portions of the guidance listed in the following SRP Chapter 7 branch technical positions (BTPs):

- BTP 7-8, “Guidance on Application of Regulatory Guide 1.22,” Revision 5.

- BTP 7-11, “Guidance on Application and Qualification of Isolation Devices,” Revision 5.

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

- BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” Revision 5.

- BTP 7-18, “Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems,” Revision 5.

- BTP 7-19, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems,” Revision 7.

- BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” Revision 5.

3.0 TECHNICAL EVALUATION

The following subsections identify and describe the RadICS platform’s components and the processes used to develop them. These sections also evaluate these components against the regulatory evaluation criteria identified in Section 2.0 of this SE.

3.1 System Background

A detailed discussion of the Radics LLC development and operational history is provided in Section 2 of the RadICS TR. RPC Radiy products were first developed in the mid 1990’s to support replacement of obsolete modules in Ukrainian power plants. Later, a new generation of replacement modules, which was based on the use of FPGA technology was developed. This is referred to by Radiy as first-generation equipment for NPP I&C equipment.

In 2002, a second generation of Radiy equipment was developed. This second-generation equipment established a platform with standardized modules that no longer needed to be specifically designed for single purpose applications.

The subject of this SE is the third generation of the FPGA-based RadICS platform. This third-generation product was designed in 2011 by Radiy and is based on the earlier second generation RadICS platform. The RadICS TR states that the third generation RadICS platform consists of an International Electrotechnical Commission (IEC) 61508:2010 Safety Integrity Level (SIL) 3 chassis level certifiable architecture. Though functional safety assessments were performed to demonstrate RadICS platform compliance with IEC 61508 SIL 3 certification requirements, the NRC’s regulatory framework does not include the SIL compliance approach. Radics LLC also requested NRC approval of the platform with respect to applicable U.S. regulations and guidance. Therefore, the NRC did not evaluate the platforms SIL 3 certification and instead performed its own SE in accordance with the regulations and guidance listed in Section 2.0 of this SE.

The RadICS platform’s components were originally designed, implemented, and qualified by RPC Radiy in compliance with European safety standards. The nuclear quality assurance (QA) program that RPC Radiy used for RadICS platform development is based on International Organization for Standardization (ISO) 9001:2015. This QA program is hereafter referred to as the RPC Radiy Quality Management System (QMS).

The RPC Radiy QMS is described in Section 3.2 of the RadICS TR. Because the RadICS platform was not originally developed in accordance with NRC regulations or endorsed standards, Radics LLC performed a commercial grade dedication (CGD) of the RadICS platform to provide reasonable assurance that this commercial grade item to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program. Section 4 of the RadICS TR describes this Radics LLC Commercial Grade Dedication activity.

Radics LLC developed a QA program which conforms to 10 CFR Appendix B. This Radics LLC QA program is described in Section 3.3.3 of the RadICS TR. The Radics LLC Commercial Grade Dedication of the RadICS platform was conducted in accordance with 10 CFR Part 21 prior to implementation in U.S. nuclear facilities to ensure quality of the Radiy platform is comparable to a product developed under a 10 CFR Part 50, Appendix B program.

Radics LLC is seeking the NRC's generic approval for use of the RadICS platform in nuclear safety I&C systems in any U.S. NPP. The scope of the RadICS platform addressed in the topical report is shown in Figure 6-2, "Context Diagram of the RadICS Platform," of the RadICS TR. This scope consists of the RadICS platform:

- Hardware design
- Digital I&C development life cycle processes (i.e., programmable logic)
- Toolset used to design and implement the RadICS platform
- Platform input and output connections
- Platform communication independence features
- Access control features used to support platform system maintenance activities
- Module connections and data protocols for loading electronic design (ED) configuration files

3.2 System Description

The RadICS platform consists of standardized electronic modules containing FPGA chips. The FPGA chips function as computational, processing, and system-internal control engines. Thus, the RadICS Platform's safety function internal logic is performed by FPGAs. The RadICS platform can be configured to produce safety system applications such as reactor trip systems and engineered safety features actuation systems. The RadICS platform also contains features that support maintenance (i.e., hot swappable modules, on-line monitoring) and safety function operation (fault-tolerance, self-diagnostic testing). RadICS chassis are of a modular design and can be installed into standardized instrumentation cabinets or racks.

Once configured, the RadICS platform operates as a single rack-mount chassis containing all required NPP inputs, outputs, and logic processing, to perform the end-user application specified safety function(s).

The platform can be configured in two to four safety division configurations. Table 6-1, "Qualified Components," of the RadICS TR, summarizes the qualified hardware components and the programmable logic configuration items that are included in the RadICS platform. Each RadICS platform module also has on-line self-diagnostic functions including a watchdog

function, cyclical redundancy check (CRC) calculations, and monitoring of FPGA performance using support circuits.

3.2.1 RadICS Digital I&C Platform Basic Operation Description

NPP field parameter signals of plant field devices (e.g., sensors, transmitters, and actuators) are provided as inputs to the RadICS platform via the input/output (I/O) external connections on the interface modules that are connected to the chassis backplane. These field device signals are connected to the I/O input modules. The user defined application logic contained in the Logic Module (LM) will process signals received from the input modules (i.e., receive signal, compare to setpoint, etc.) to determine if safety function actuation is necessary. If acquired signals exceed the LM application logic setpoint threshold, the LM will transfer the processing results to the output modules as per system design. The output module will send the safety function initiation signal via the output interface modules to the NPP end components (i.e., pumps, valves) for safety function actuation.

The LM performs input module data acquisition (i.e., NPP field parameter sensor data), executes the user configured application logic implemented within the FPGA (i.e., safety function logic), drives the output module (plant safety function actuation), and processes diagnostic data from all I/O modules installed in the chassis.

3.2.2 RadICS Digital I&C Platform Basic Architecture

The basic architecture of the RadICS platform consists of an instrument chassis into which platform modules are inserted. Each RadICS chassis must have one logic module installed to control system operation of other modules. Additional modules for the RadICS platform: I/O modules, and fiber-optic communication modules. These modules are also installed as specified by application design to support system operational requirements. The RadICS platform basic components are:

Chassis - The seismically qualified metal box frame and backplane that supports the RadICS platform modules. The chassis consists of 16 physical slots for modules and supports the use of two independent 24 V power supplies.

Backplane - The chassis contains a backplane to support transfer of data between installed modules, and to provide an interface to power supplies. Sensors for the system external field parameter and/or signal inputs and outputs are connected to the chassis via the field external connections on the backplane.

Modules - These are the highest component level of the RadICS platform design. Modules are composed of individual units which are assembled to support module functional requirements. RadICS modules perform logic processing, input / output functions, and network communications. There are seven types of hardware modules in the RadICS platform design. These are:

Logic module (LM): Contains an FPGA chip that is used for execution of end-user specific application logic (i.e., safety function actuation logic) and for data exchange with other modules in the chassis. The LMs gather the input data, execute the user-specific safety function logic, update the values for system output(s), and sends the output signals to

output modules. The LMs are also responsible for gathering platform diagnostic and general health information.

Input/Output modules (4 types): The basic types are Analog Input module (AIM), Discrete Input module (DIM), Discrete Output module (DOM), and Analog Output module (AOM). The I/O modules provide interfaces with other devices (e.g., NPP detectors, sensors, actuators).

Optical communication module (OCM): The OCM is used to allow application Logic, running in one chassis LM, to use the data derived from I/O module in another chassis (i.e., within same safety division). The OCMs are also used to provide inter-divisional communication links to support communications between different safety divisions. Communications between safety divisions are performed through fiber-optic communications between LMs. These communication links can be used to support coincidence voting functions. Thus, each chassis LM can execute logic related to I/O within its own chassis as well as share selected data with logic (LM) in another chassis.

Ventilation Module (VM): The VM is used for driving chassis fans. The VM does not exchange data with other RadICS Modules. The VM is controlled by a Complex Programmable Logic Device (CPLD) that processes data received from fans (e.g., indication of voltage and speed) and external devices (e.g., control switches and alarms indications). The VM can detect fan failures.

All RadICS modules are composed of individual units. Units are standardized lower level components that are used to build RadICS modules. Section 6.2.5.2 of the RadICS TR lists and describes functions performed by the various units of the RadICS platform and identifies the unit composition of each platform module.

A typical chassis configuration is included as Figure 6-1, “Typical RadICS Platform Configuration,” of the RadICS TR. Table 6-1, “Qualified Components,” of the Radics LLC topical report (Ref. 1) lists the qualified platform components of the RadICS platform reviewed by the NRC. The resulting Radics LLC approved modules list is provided below as Table 3.2-1.

Table 3.2-1: Radics LLC Qualified Platform Components

Category	RadICS Platform Component	Part Number (Hardware Identifier)	Notes
Platform Hardware / Interconnections	Chassis Hardware (Including Backplane)	A007.C00.V00.R00 (469116.103-01)	
	Ventilation module	A014.C00.V00.R00 (067319.013-01)	
	Ventilation module electronic design	A011.FV00.FR00.CV00.CR00	
	Cable Assemblies	LM - 685624.881-06 AIM - 685624.882-06 AIM - 685624.882-07 AOM - 685624.883-06 AOM - 685624.883-07 DIM - 685624.884-06 DIM - 685624.884-07 DOM - 685624.885-06 DOM - 685624.885-07 BYPASS - 685624.886-06 BYPASS - 685624.886-07 FO - 685624.895-20 PS - 685624.927-03 RS232/485 - 685628.011-02	
Logic Module (LM)	Logic Module Hardware	A001.C00.V01.R00 (468243.100)	
	LM Platform electronic design	A001.FV00.FR01.CV01.CR00	
Input / Output modules	AIM	A003.C00.V00.R00 (467482.068)	
	AIM Platform electronic design	A003.FV00.FR02.CV01.CR00	
	DIM	A004.C00.V00.R00 (467482.069)	
	DIM Platform electronic design	A004.FV00.FR01.CV01.CR00	

	AOM	A002.C00.V02.R00 (467482.067)	
	AOM Platform electronic design	A002.FV00.FR02.CV01.CR00	
	DOM	A006.C00.V00.R00 (468172.057)	
	DOM Platform electronic design	A006.FV00.FR01.CV01.CR00	
Communication module	OCM	A005.C00.V00.R00 (468383.044)	
	OCM Platform electronic design	A005.FV00.FR02.CV01.CR00	
I/O Interface Protection modules	Interface Protection module for AIM, AOM, and DIM	Top: A008.C00.V00.R00 (468243.102) Bottom: A008.C01.V00.R00 (468243.102-01)	Note 1
	DOM Interface Protection module	Top: A008.C02.V00.R00 (468243.102-02) Bottom: A008.C03.V00.R00 (468243.102-03)	Note 1
	OCM Interface Protection module	A008.C06.V00.R00 (468243.103)	

Note 1: Each type of Interface module has two different versions. One has the connector on the top portion of the module and the other has the connector on the bottom portion of the module. Other than this form difference, the two versions are functionally equivalent. Both of the versions are qualified for use as part of the RadICS platform.

Figure 3.1-1 shows a picture of the Radics LLC chassis with a ventilation module configured with I/O modules and an OCM communications module.

Figure 3.1-1: RadICS platform modules in Chassis
(Source - Figure 2-2 of RadICS platform TR)

Note: The analog input for flux measurements (AIFM) (shown in this figure) is an analog input module for neutron flux measurements. This module is not approved within the scope of the RadICS platform.

Figure 3.2.2-1 below provides a high-level representation of the architecture of a RadICS-based safety system. The architecture of each RadICS-based system includes one or more chassis with ventilation modules as well as one logic module and up to 14 I/O and fiber optic communication modules per chassis as determined by the plant-specific requirements of the system. The LM(s) will contain the user specific logic that will define safety function performance of the system.

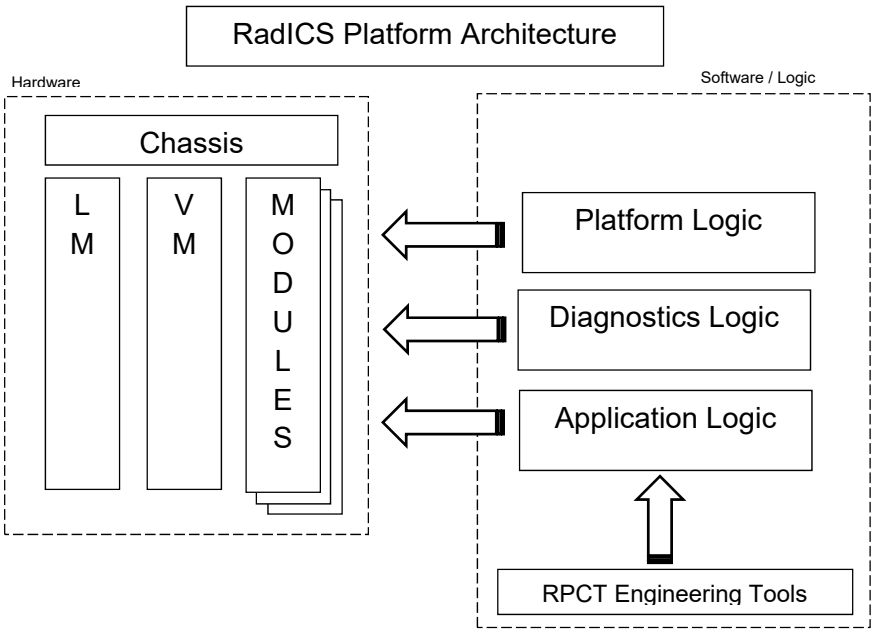

Figure 3.2.2-1: Radics LLC Subsystem Architecture Configuration
(Source - Figure 2-3 of RadICS platform TR)

The input modules installed in the RadICS chassis receive input signals. These signals are converted into digital signals, which are distributed to the logic module (LM) via the chassis backplane. Application Function Logic is performed by the LM and system output signals, such as safety actuation signals, are sent to the output modules through the chassis backplane. A Ventilation Module (VM) is used to drive RadICS fans which provide forced air cooling to the RadICS chassis electronic components. The VM contains a CPLD that processes data received from the chassis fans (e.g., indication of voltage and speed) and external devices (e.g., control switches and alarm indications). The VM is also configured to detect fan failures.

3.2.2.1 Platform Module Descriptions

The following subsections provide general functional descriptions for each of the RadICS platform modules.

3.2.2.1.1 Logic Module (LM)

The LM performs data exchange with other modules in the chassis and execution of plant-specific logic specified by the functional requirements of the safety system.

The LM includes two separately designed logic configurations: the RadICS Platform Logic and the end user Application Logic. Both levels of logic are protected from corruption by use of CRC and timing checks performed by the watchdog. A LM includes a limited set of discrete input and output signals.

The LM includes the following communications capabilities:

- A fiber optic interface, which is used for internal system communications,
- A Monitoring and Tuning System (MATS) tuning personal computer (PC) Programming Access port, and
- Three Fast Ethernet optical communication lines.

3.2.2.1.2 Analog Input Module (AIM)

The AIM is used for the acquisition of analog signals and the conversion to engineering units. The AIM has 32 independent input channels.

3.2.2.1.3 Discrete Input Module (DIM)

The DIM is used for the acquisition of discrete dry contact signals via DIU units and transmission to the LM via Linear Voltage Differential Signal (LVDS) Transceiver unit. The DIM has 32 independent input channels.

3.2.2.1.4 Analog Output Module (AOM)

The AOM is used for the conditioning of analog output signals and data exchange with LMs. The AOM has 32 independent output channels.

3.2.2.1.5 Discrete Output Module (DOM)

The DOM is used for driving the galvanically isolated dry contact signals. Its safe state is defined to be open contact. The DOM has 32 independent output channels.

3.2.2.1.6 Optical Communication Module (OCM)

The OCM is used for receiving and transmitting data via a fiber optic interface. This interface can be used to extend the RadICS platform to additional chassis. The OCM can also be used for transmitting data via RS-232/485 serial communication interfaces. The OCM has five independent optical transceiver units. Each of them performs data transfer from/to other RadICS chassis with OCMs.

3.2.2.2 Units for RadICS Modules

RadICS modules are composed of units. Units are used on more than one module and are therefore considered standardized. These units are listed and described below for reference purposes. Detailed descriptions of RadICS units are provided in Section 6.2.5.2 of the RadICS TR, “RadICS module Design Features.”

FPGA Unit - The FPGA Unit is used to provide input data acquisition, perform the main functions of module, diagnostics, output data conditioning, and data exchange with other modules.

Clock Unit - Clock Units are used to generate three separate clocks for each module. Each clock has its own reference quartz oscillator.

EEPROM Unit - The Electrically Erasable Programmable Read Only Memory (EEPROM) Unit is used for storing different information that is needed for module operation.

Input Unit - The Input Units are used to provide input data acquisition and directly interact with the I/O Interfaces.

Output Unit - The Output Units are used to provide output data conditioning and directly interact with I/O Interfaces.

Safety Override Unit - The Safety Override Unit is used to provide a trip into the safe state of modules by de-energizing the field-effect transistors in the Output Units. The Safety Override unit ensures the safe state regardless of the output control signal from the FPGA Unit.

Power Supply and Watchdog Unit - The Power Supply and Watchdog (PSWD) Unit is used to provide all hardware units with power supply voltages, control the power supply voltages, and perform hardware self-diagnostics of the FPGA Unit. The PSWD Unit is used to perform power supply, watchdog timer, and voltage control module functions with active diagnostics. Because the PSWD controls power supply to all units within a module, it has the capability of interrupting power upon detection of system critical faults. This is how the PSWD unit forces system actuation outputs to fail-safe states, upon fault detection, even when FPGA logic would not send actuate signals to the system outputs.

The PSWD Unit receives input from redundant 24 VDC power supplies and converts this voltage into the voltage levels necessary to support module operation. The PSWD Unit can detect a failure of either 24 VDC source. Upon detection, the PSWD unit uses the operating source to supply outputs for module operation. The PSWD Unit also provides overvoltage protection for the output voltages.

Address Unit - The Address Unit is only used on the LM for providing power to the jumpers placed on the backplane to determine the unique LM identifier within the chassis during module startup.

Active Serial Programming Interface Unit - The active serial programming interface (ASPI) Unit is one of the standardized interfaces on a module used for FPGA configuration. The FPGA configuration is read from the ASPI Unit and the FPGA is configured to perform its function as part of the power-up sequence. The ASPI Unit, which includes FLASH memory, is used for writing, storing and reading of FPGA configuration.

Indication Board Unit - The Indication Board Unit is used to indicate the mode and self-diagnostic status of the module on a local display unit located on the front panel of the module.

Synchronous Static Random-Access Memory Unit - The Synchronous Static Random Access Memory (SSRAM) Unit is used for storing different temporary information needed for the Application Logic in the LM.

Communication Units - The Communication Units are used to support data exchange within a single RadICS chassis and between two different chassis. Communication units also support communications to external systems. Four types of communication units are included in the

RadICS platform design: An LVDS Unit is used to support backplane communications between modules. An Opto Unit is used for optical communication with a unit in another module of the same type. A LVDS Unit provides point to point communication between two modules in the same chassis. A RS-232/485 Unit supports one-way communication to peripheral devices.

Real Time Unit - The Real Time Unit is used for receiving real-time data from an information technology system and duplicating it with timekeeping chip in a case of input signal absence. In addition to the module specific functions described in the preceding sections, each RadICS module performs self-diagnostics and can be configured to take safe-state action or to provide information to the Application Logic for further action depending on system application functional requirements. Evaluation of RadICS self-diagnostic functions is provided in Section 3.7.3 of this SE.

3.2.3 RadICS Platform Communications

There are two communication interface types used in the RadICS platform:

- Internal Interfaces – Used for On-Board communications within a RadICS module or for module to module communications within a RadICS chassis; and
- External Interfaces – Used to establish communication with another chassis or specific device.

The RadICS communication interfaces are further categorized as either Online Interfaces or Offline Interfaces.

- Online Interfaces – Communication interfaces that are capable of directly influencing a safety critical system during normal operation
- Offline Interfaces - Communication interfaces that are used for safety critical system configuration when the system is not in operation

Section 6.2.4, “Overview of RadICS Chassis Interfaces,” of the RadICS TR identifies 17 different interfaces used in the platform however not all interfaces are communication interfaces. The NRC staff identified the following communication-based interfaces to be evaluated in this SE.

3.2.3.1 Internal Communications Interfaces

- Linear Voltage Differential Signal (LVDS) Interface
- Watchdog Interface
- SSRAM Interface

DI&C-ISG-04 does not directly address or provide criteria for communication interfaces between safety-related components within a single safety division. Evaluation of the RadICS platform internal communication interfaces is being performed to support and credit functional characteristics and capabilities of a RadICS based safety system to meet functional regulatory requirements of IEEE Std. 603-1991. This evaluation is described in Section 3.10 of this SE.

3.2.3.1.1 Linear Voltage Differential Signal Interface (Internal / Online)

The LVDS interface is the RadICS chassis backplane communications pathway, which establishes internal communications between RadICS modules installed into a chassis. All

RadICS I/O modules and the OCM module include a LVDS Transceiver unit to support transfer of data to and from the LM associated with the chassis in which the module is installed.

3.2.3.1.2 Watchdog Interface (Internal / Online)

The Watchdog Interface is used to support data exchange among module FPGAs, Voltage Supervisor, and the Power Supply, and Watchdog CPLD Unit. All RadICS modules have Watchdog units and require an internal Watchdog interface. Data exchange protocols for the watchdog interface are described in Section 6.3.3.2.6 of the RadICS TR.

3.2.3.1.3 Synchronous Static Random Access Memory Interface (Internal / Online)

The SSRAM Interface is used on the LM to establish an internal communication link between the SSRAM Unit and the LM FPGA Unit. The SSRAM Unit stores temporary information needed for the application logic in the LM.

3.2.3.2 External Communications Interfaces

The RadICS platform supports the following external communications interfaces:

- Fiber optic Radiy User Datagram Protocol (UDP) Protocol (RUP) Interface
- Fiber optic Radiy Proprietary Protocol (RPP) Interface
- RS-232/485 Interface
- Tuning access interface
- Active Serial Programming Interface (ASPI)
- Joint Test Action Group (JTAG) Interface
- Serial Peripheral Interface (SPI)
- Universal Asynchronous Receiver/Transmitter (UART) Interface
- Real Time Interface

Each of these communication interfaces is described in the subsections below. Section 3.10 of this SE evaluates the communication properties of these interfaces.

3.2.3.2.1 Fiber Optic RUP Interfaces (External Online or Offline)

The LMs include fiber optic interfaces that can be used to facilitate communications between logic modules and the Monitoring and Tuning System (MATS) computer to support system monitoring and tuning functions. These interfaces use a Radiy User Datagram Protocol (UDP) - based interface protocol (RUP) for communications via fiber optical medium.

UDP uses a simple connectionless communication model with a minimum of protocol mechanism. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram but has no handshaking dialogues.

When used for MATS tuning support, these interfaces are only activated, via the tuning access interface, for offline communications with an external MATS system. Offline MATS tuning communications are bidirectional. The fiber optic RUP interfaces are also used for MATS

monitoring online support. MATS online communications are unidirectional from the LM to the MATS computer.

3.2.3.2.2 Fiber Optic RPP Interfaces (External / Online)

The fiber optic interfaces can be used to extend the RadICS platform to additional chassis. These interfaces use a data transmission protocol called Radiy Proprietary Protocol (RPP). Fiber Optic RPP Interfaces can be used to support safety critical communications between RadICS chassis.

The fiber optic RPP interfaces are external online interfaces and can be configured to provide either intra-divisional communications to a RadICS chassis within the same division or to provide inter-divisional communications to a RadICS chassis in a separate division.

3.2.3.2.3 RS-232/485 Interfaces (External / Online)

The RS-232/485 interfaces are used for one-way communication with peripheral devices. These interfaces use serial communication protocol for transmitting data in a way that can be customized to be compatible with external systems such as process plant computer systems. There are five RS-232/485 interfaces available for use within each OCM module. These interfaces are only capable of transmitting data and cannot be configured to receive data from external devices.

3.2.3.2.4 Tuning Access Interface (External Online)

Tuning access interface is a safety-related online external interface that is used to deenergize fiber optic RUP interfaces described in Section 3.2.3.2.1.

3.2.3.2.5 Active Serial Programming Interface (External / Offline)

The Active Serial Programming Interface (ASPI) Unit is one of the standardized interfaces on a module. The ASPI is used for writing, storing and reading of FPGA configurations. These FPGA configurations are stored in a memory called FLASH memory that is associated with the ASPI interface. Access to the FLASH memory is provided only during project-specific manufacturing.

3.2.3.2.6 Joint Test Action Group Interface (External / Offline)

The Joint Test Action Group (JTAG) Interface is used for configuration of Application CPLD Electronic Design (ED) in an off-line mode. The JTAG connector interface is located on the LM circuit board and is inaccessible during system operation. The JTAG connector can only be accessed by using an extender module. The extender module is not within the scope of the qualified RadICS platform because it is not intended to be installed into the system during operation.

3.2.3.2.7 Serial Peripheral Interface (External / Online)

Serial Peripheral Interface (SPI) Interfaces are used to download configuration data to EEPROMs and to upload tuning parameter changes to Tuning EEPROM while in TUNING mode. The SPI connector interfaces are located on the module circuit boards. The EEPROMs

that store tuning parameter and logic configuration data are integral components of the EEPROM units described in Section 3.2.2.2 of this SE. This interface is used for configuration of FPGA EDs in an on-line mode.

3.2.3.2.8 Universal Asynchronous Receiver/Transmitter Interface (External / Offline)

Universal Asynchronous Receiver/Transmitter (UART) Interfaces are used to download configuration data to and from EEPROMs via the FPGA while in CONFIGURATION mode. The UART connector interfaces are located on the module circuit boards. UART Interfaces are external communication interfaces that are only used in an offline mode of operation. The UART connector is inaccessible during system operation and can only be accessed by using an extender module. Extender modules are not included as qualified components of the RadICS platform and should not be installed into an operable RadICS based system during plant operations.

3.2.3.2.9 Real Time Interface (External / Online)

The Real Time Unit is used for receiving real-time data from an external information technology system and duplicating it with a timekeeping chip to maintain time signal availability in cases where input signal loss occurs. When the external time signal is present, the Real Time Unit transmits real time data to the FPGA Unit. When the external signal becomes unavailable, data from an internal timekeeping chip is instead sent to the FPGA Unit.

3.2.4 Monitoring and Tuning System

The Monitoring and Tuning System (MATS) is used to monitor system performance and to make tuning changes to the RadICS system. The MATS consists of a non-safety workstation and associated software. Tuning changes are made only when the RadICS system trip outputs are placed to the fail-safe state.

The MATS system uses a monitoring interface (see Section 3.2.3.2.1, “fiber optic RUP Interfaces”) that supports one way UDP communication from the RadICS safety system to the non-safety MATS workstation while the safety system is in operation. When tuning adjustments are required, a second tuning interface is activated, which allows tuning data to be sent from the MATS to the safety system.

RadICS safety system tuning parameters are protected from modification during normal system operation. Changes to system tuning parameters must be performed through the MATS tuning interface and this communications interface is disabled during normal operation. A system tuning access key-switch must be placed in the tuning enabled position to enable the MATS tuning interface and thus permit system tuning actions. Operation of the tuning key-switch effects a disconnection of the MATS tuning interface by removing electrical power to the associated LAN Transceiver Unit.

The MATS workstation supports the following RadICS system features:

- On-Line Monitoring
- Operational Parameter Tuning
- Checking of User Configuration and Tuning Values

- User Safety Override
- Authentication of the RadICS module Version

3.2.5 Radics Download Station

The RadICS Download Station is a version of a RadICS Chassis that is identical to the RadICS Chassis used as part of the safety system. The Download Station is used for: downloading application electronic designs to the logic module, calibrating AIMs, and calibrating AOMs. Application Logic changes to a LM are performed with the LM installed into a Download Station.

3.3 RadICS Logic Architecture

The RadICS Platform uses three different types of programmable logic: RadICS platform FPGA logic, self-diagnostics FPGA and CPLD logic, and plant specific user application FPGA logic. The system logic is implemented through the development of EDs. An ED is a set of FPGA configuration files that are installed into the RadICS Modules. RPC Radiy used a defined and controlled process to develop the RadICS Platform and project application specific EDs.

3.3.1 RadICS Platform FPGA Logic

RadICS Platform FPGA logic is the generic logic that performs basic system programmable logic controller (PLC) functions, such as acquiring input signals, communicating system data between modules via the chassis backplane bus, performing self-testing, and processing output signals to drive controlled components. The platform logic is also used to facilitate communications between RadICS chassis, and between the RadICS system and other external systems.

The Platform FPGA logic is common to RadICS platform-based systems in that all systems using a specific version of the RadICS platform have the same Platform FPGA logic for the modules used, regardless of the application requirements. Each module of the RadICS system contains platform logic to enable module specific functionality. The Platform FPGA logic is similar to the operating system software in a computer-based system in that it establishes an environment in which application specific programming can be implemented to perform system specific functions as defined by requirement specifications.

RadICS platform logic is developed by the module supplier, RPC Radiy, which uses a defined ED development lifecycle. Platform FPGA logic's EDs are therefore commercially dedicated by Radics LLC for use in nuclear safety applications in conjunction with the commercial grade dedication (CGD) of the modules in which they are installed. See Section 3.4 of this SE for an evaluation of this CGD process.

3.3.2 Plant Specific User Application FPGA Logic

RadICS plant specific user application FPGA logic is used to implement functional requirements for a plant design as specified in the system requirements specification. This plant specific logic is used only in the LMs of the system.

Plant specific FPGA logic is unique to each RadICS system LM. The plant specific FPGA logic is similar to system application software in a computer-based system in that it invokes platform

logic functionality to accomplish system specific functions as defined by requirement specifications. No plant specific FPGA logic was available for this evaluation. Therefore, determining acceptability of application logic is an activity that must be performed as part of the application development process. See PSAI 7.2.

3.3.3 Self-diagnostics CPLD Logic

Self-Diagnostic logic including fail-safe functionality of the PSWD units is implemented in CPLDs. CPLD logic is also used to perform diagnostic functions in the VM modules. CPLD Logic is created as an integral part of the platform design to implement platform generic design features. Therefore, application development activities do not impact CPLD logic designs. RadICS platform self-diagnostic functions are described and evaluated in Section 3.7.3 of this SE.

3.3.4 Function Block Libraries

The logic development processes for the FPGA and CPLD platform logic and application logic include the use of function block libraries. Function block libraries are sets of pre-programmed logic blocks that are designed to perform commonly used functions that are implemented during system design and development. Function block libraries enable logic programming using graphical interface tools. The RadICS logic development process is performed by creation of function block diagrams using function block library elements that are pre-certified by RPC Radiy. The resulting diagrams are then converted, through a series of steps, to configuration files that can be transferred into an FPGA or CPLD device or associated memory.

There are two different and distinct application logic function block libraries used for RadICS platform logic. One is used for FPGA logic development and the other is used for CPLD logic development. The elements of each library are not shared between them. Section 8.1.2 of the RadICS TR includes a detailed description of the processes used to develop each of these libraries. These libraries are commercially dedicated as components of the RadICS platform by Radics LLC.

3.4 Radics LLC Commercial Grade Dedication Program

The RadICS platform is built from RPC Radiy components that are developed to European safety standards under a nuclear quality management system (QMS) program described in Section 3.2 of the RadICS TR. The RPC Radiy QMS complies with safety requirements for I&C systems as described in IEC 61508. Though the Radiy QMS includes many activities and characteristics that support compliance with requirements of 10 CFR Part 50, Appendix B, this QMS is not a 10 CFR Part 50, Appendix B compliant program. Therefore, all products of RPC Radiy are subjected to CGD by Radics LLC before they can be used as part of a RadICS platform-based safety system in U.S. nuclear power plants.

Chapter 3 of the RadICS TR, “Quality Assurance,” describes the quality assurance programs used by RPC Radiy and Radics LLC for both development and dedication activities performed for RadICS platform’s components. Section 3.2 of the RadICS TR describes the RPC Radiy QA program and Section 3.3 describes the Radics LLC QA program.

Section 4 of the RadICS TR describes the RadICS commercial grade dedication (CGD) program. Radics LLC performed CGD under its QA program that is based on U.S. nuclear regulations to establish programs and basic measures for implementation to ensure that products of RPC Radiy meet the U.S. regulations, standards, and quality requirements of prospective RadICS system customers. Radics LLC submitted the following commercial grade dedication plans and reports as supplemental information to support this SE:

Table 3.4-1: Radics LLC Commercial Grade Dedication Documentation

Item No.	Document Title	Module / Item Designation	CGD Plan Reference (See Section 8 of this SE)	CGD Report Reference (See Section 8 of this SE)
1	Commercial Grade Dedication Activity for Digital Input Module	DIM	12	21
2	Commercial Grade Dedication Activity for Logic Module	LM	13	22
3	Commercial Grade Dedication Activity for Digital Output Module	DOM	14	23
4	Commercial Grade Dedication Activity for Analog Input Module	AIM	15	24
5	Commercial Grade Dedication Activity for Analog Output Module	AOM	16	25
6	Commercial Grade Dedication Activity for Optical Communication Module	OCM	17	26
7	Commercial Grade Dedication Activity for Test Specimen (RTS-001) / Chassis	RTS-01	18	27
8	Commercial Grade Dedication Activity for Input/Output Connections Protection Module	IOPM	19	28
9	Commercial Grade Dedication Plan for Ventilation Module	VM	20	29

These commercial grade dedication activities were used to establish technical and quality characteristics equivalent to those required of a system developed under a 10 CFR Part 50, Appendix B program. These activities were performed by an independent Radics LLC Validation and Commercial Grade Dedication department that was not involved in the RadICS platform design development. As such, the 10 CFR Part 50, Appendix B compliant Radics LLC

QA program was used to govern activities associated with dedication of RadICS platform components.

Radics LLC is not currently on the Nuclear Procurement Issues Committee (NUPIC) list or included on an applicant's approved vendor List. Therefore, an applicant referencing the RadICS TR SE should confirm that Radics LLC is added to the NUPIC list as applicable and/or confirm the Radics LLC quality processes conform to the applicant's Appendix B program – i.e., be put on the applicant's Approved Vendor List.

3.4.1 Regulatory Analysis of RadICS Commercial Grade Dedication

The regulation at 10 CFR Part 21, "Reporting of Defects and Noncompliance," establishes the framework for an acceptance process under the definition for "dedication" and this process is undertaken to provide reasonable assurance that a commercial-grade item to be used as a basic component will perform its intended safety function. Specifically, the definition for "dedication" requires that the dedication process be conducted in accordance with the applicable provisions of 10 CFR Part 50, Appendix B. Regulatory Guide 1.164 describes methods that the NRC staff considers acceptable in meeting regulatory requirements for dedication of commercial-grade items and services used in nuclear power plants. Clause 5.4.2 of IEEE Std. 7-4.3.2-2003 provides elaboration of the IEEE Std. 603-1991 criteria as it should be applied to dedication of commercial digital systems.

Electric Power Research Institute (EPRI) TR-107330 and EPRI TR-106439 documents provide more detailed guidance on the CGD of digital systems. These EPRI documents were reviewed by NRC in SEs issued July 30, 1998 (ADAMS Accession No. ML12205A265) and July 17, 1997 (ADAMS Accession No. ML092190664), respectively, as being appropriate for use in commercial grade dedication for digital systems.

EPRI TR-106439 identifies three categories of critical characteristics in terms of physical, performance, and dependability attributes. These characteristics correspond to the categories identified in Section 5.4.2.2 of IEEE Std. 7-4.3.2 2003, which are physical, performance, and development process characteristics. Determination of specific critical characteristics is accomplished by a critical design review that accounts for the requirements of the safety application and the potential hazards that could interfere with the safety function.

Under, "Requirements on the Dedicator," EPRI TR-106439 states the following: "The process of performing commercial-grade item procurement and dedication activities is itself a safety-related process and, as such, must be controlled and performed in accordance with a QA program that meets the requirements of 10 CFR Part 50, Appendix B. This applies to the dedicating entity whether it is the utility or a third-party dedicator."

Verification of the critical characteristics is at the heart of the dedication process. EPRI TR-106439 adapts four acceptance methods defined in RG 1.164 that endorses EPRI 3002002982, Revision 1 to EPRI NP-5652 and TR-102260, "Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications," to establish an approach to verify the characteristics for digital equipment. The four methods are as follows:

- Method 1 - Special Tests and Inspections
- Method 2 - Commercial Grade Survey of Supplier

- Method 3 - Source Verification
- Method 4 - Acceptable Supplier/Item Performance Record

EPRI TR-106439 states that verification of the critical characteristics for digital equipment will require the use of more than one of the methods since no one method will typically be sufficient by itself. Radics LLC used all four methods of acceptance during its CGD of RadICS platform components.

The Radics LLC QA program is implemented by the Radics QA Program Document (QAPD). The Radics LLC Quality Assurance Program (QAP) is based on NEI 11-04A, "Nuclear Generation Quality Assurance Program Description." The RadICS TR states the following: "The QAPD includes methods pertaining to managerial and administrative controls that meet the requirements of 10 CFR Part 50, Appendix B, RG 1.28, Revision 4, and NQA-1-2008/ NQA-1a-2009 Addenda."

Chapter 4 of the RadICS platform TR describes the commercial grade dedication process used to qualify RPC Radiy platform components for use in nuclear safety related applications. Separate CGD plans were developed for each RadICS platform module. Each of these plans defines a set of critical PLC characteristics for generic nuclear safety applications. The RadICS TR describes a strategy that Radics LLC followed during the CGD effort to qualify and accept the RadICS platform modules under its 10 CFR Part 50, Appendix B compliant quality assurance program.

Radics LLC performed CGD for the nine activities listed in Table 3.4-1 of this SE. These items include all RadICS components listed in Table 3.2-1 of this SE. The RadICS CGD plans outline the steps followed to dedicate the individual RadICS platform modules and components. The results of the dedication are documented in the associated CGD Reports. The RadICS CGD plans are therefore fully implemented.

Radics LLC QAP procedures are listed in Table 3-2 of the RadICS TR. The quality procedures governing the commercial grade dedication processes include procedures to address 10 CFR Part 50, Appendix B, Criterion VII, Control of Purchased Material, Equipment, and Services. These Radics LLC quality procedures require preparation of CGD plans and CGD reports to show compliance with EPRI TR-106439. The roles and responsibilities for Radics LLC personnel performing dedication process of commercial products are defined in the Radics QA program and are described in Section 3.3 of the RadICS TR. The NRC staff found that Radics LLC had followed the CGD plans for each of the items identified in Table 3.4-1 above. The NRC staff reviewed the RadICS module CGD reports and determined the Radics LLC CGD effort was performed in compliance with the criteria of EPRI TR-106439, and EPRI TR-107330, and is therefore acceptable. The Radics LLC CGD reports provide adequate documentation of the performance of CGD activities and provides references to records that support CGD findings. The CGD reports also summarize the results of the assessment of critical characteristics for each of the RadICS platform modules.

The dedication process for the RadICS platform contained two components of CGD. These were: assessment of critical characteristics and assessment of quality established for the RadICS platform. The basic U.S. licensing strategy Radics LLC used for dedicating the RadICS platform modules and components included providing a demonstration that the generic RadICS platform and the associated quality and software lifecycle processes are compliant with U.S.

nuclear safety requirements. The CGD results confirmed that required platform module critical characteristics had been implemented in the RadICS platform design. RadICS platform critical characteristics include physical, performance and dependability characteristics. The CGD also included an evaluation of the RPC Radiy ED lifecycle processes and established a basis for acceptance of RadICS platform hardware and logic. The results of the CGD activities are documented in the CGD reports referenced in Table 3.4-1 above.

Because the application logic and hardware configuration will be plant-specific, the scope of the dedication activities is limited to the RadICS platform hardware, as well as platform Function Block Logic Library (FBL) and ED logic. Application hardware configuration and logic development will be performed by a licensee and Radics LLC under a 10 CFR Part 50, Appendix B compliant QA program. See PSAI 7.2 for information on application logic development activities to be performed.

The NRC staff reviewed the Radics LLC product assessments provided in the commercial grade dedication reports and determined that safety analyses activities which were performed during the CGD were performed in accordance with the RadICS Functional Safety Management Plan (FSMP).

Based on the information provided, the NRC staff found the hardware and platform logic comprising the RadICS platform, and described in the RadICS TR, were properly dedicated and accepted into the Radics LLC 10 CFR Part 50, Appendix B, compliant quality assurance program. The NRC staff found the ED development life cycle used for the RadICS platform logic and FBL development followed a rigorous development process and that ED development plans are adequate for controlling future platform development activities. The following sections summarize the commercial grade dedication activities performed by Radics LLC for the RadICS platform components.

The NRC staff reviewed and evaluated the CGD documentation identified in Table 3.4-1 of this SE and determined that the verification methods applied to RadICS platform components during CGD were completed in accordance with the RadICS QAP and are therefore acceptable.

3.4.2 Radics LLC Verification and Dedication Methods

The RadICS CGD effort used various combinations of the following verification methods to verify that RadICS critical characteristics meet specified acceptance criterion:

1. Special Tests and Inspections of the RPC Radiy equipment,
2. Commercial Grade Survey of RPC Radiy,
3. Source Verification), and
4. Acceptable Performance Record of the Radiy equipment.

CGD plans were used to define these methods and to identify critical characteristics for each of the RadICS platform components. The CGD reports identify the applied verification methods used for each of the RadICS module critical characteristics. The scope of dedication activities performed by Radics LLC to qualify the RadICS platform included both hardware and platform logic elements of the design.

3.4.3 Identification and Verification of Critical Characteristics

The RadICS platform is comprised of the hardware modules described in Section 3.2.2.1 and platform logic described in Section 3.3.1 of this SE.

RadICS CGD plans identify activities to be performed during the CGD effort and identify critical characteristics for the RadICS platform modules and components. The RadICS CGD reports document the results of the CGD technical characteristics assessments. Critical characteristics of the RadICS platform modules and components include physical, performance and dependability characteristics.

3.4.3.1 Critical Characteristics – Physical

Per the guidance in EPRI TR-106439 and IEEE Std. 7-4.3.2-2003, critical physical characteristics of the digital system should address the size, mounting, power requirements, hardware model number, software version number and data communications of system components. EPRI TR-106439 further notes that "special tests and inspections" (i.e., Method 1 per EPRI NP-5652) is typically appropriate for verifying these characteristics.

The NRC staff reviewed the RadICS technical characteristics provided in the CGD Reports and determined that physical characteristics of the RadICS system modules were acceptably identified as platform critical characteristics (see Table 3.4-1 above for references). These critical characteristics included the module dimensions, mounting and power requirements for RadICS modules.

The NRC staff also confirmed that requirements for the RadICS platform logic were included as critical characteristics of the RadICS modules. These platform logic critical characteristics included platform firmware version and platform functional block library version control via configuration management and data communications aspects of the design.

The NRC staff concludes that Radics LLC has identified and verified critical physical characteristics associated with the RadICS platform in a fashion that is consistent with the guidance of EPRI TR-106439 and IEEE Std. 7-4.3.2-2003.

3.4.3.2 Critical Characteristics – Performance

Per the guidance on EPRI TR-106439 and IEEE Std. 7-4.3.2-2003, performance characteristics are the functionality required from the device, as well as the performance attributes associated with that functionality. Performance characteristics may include items such as response time, memory allocation, reliability, required embedded functions and environmental qualification requirements. In addition, failure management and "must-not-do" functions are also considered performance characteristics for digital systems. EPRI TR-106439 further notes that "special tests and inspections," commercial grade surveys and supplier/item performance record (i.e., Methods 1, 2, and 4 per EPRI NP-5652) are typically appropriate for verifying these characteristics.

The NRC staff reviewed the RadICS technical characteristics provided in the CGD Reports and determined that performance characteristics of the Radics LLC system modules were

adequately identified as platform critical characteristics. (See Table 3.4-1 for references). The NRC staff concludes that Radics LLC has identified and verified critical performance characteristics associated with the RadICS platform in a fashion that is consistent with the guidance of EPRI TR-106439 and IEEE Std. 7-4.3.2-2003.

3.4.3.3 Critical Characteristics – Dependability

Per the guidance on EPRI TR-106439 and IEEE Std. 7-4.3.2-2003, Dependability characteristics are those characteristics that address attributes that typically cannot be verified through inspection and testing alone and are generally affected by the process used to produce the device. This guide defines these attributes as critical characteristics to ensure that they are adequately addressed and documented during the dedication process.
The CGD effort included evaluation of processes used to produce RadICS platform logic and function block libraries and found them to be consistent with the requirements of IEEE Std. 7-4.3.2 and other referenced standards. The CGD plans defined platform development processes as critical characteristics of the RadICS platform and the CGD reports documented methods used to verify that platform development process critical characteristics were met. These critical characteristics were therefore adequately addressed and documented during the CGD process. The NRC evaluated the RadICS platform ED development processes and determined they are acceptable. See Section 3.5, “Platform Development Process,” of this SE.

The NRC staff concludes that Radics LLC has identified and verified critical dependability characteristics associated with the RadICS platform in a fashion that is consistent with the guidance of EPRI TR-106439 and IEEE Std. 7-4.3.2-2003.

3.5 RadICS Platform Development Processes

Digital I&C safety systems must be designed, developed, installed, and tested to quality standards commensurate with the importance of the safety functions to be performed. The development of safety system logic should progress according to a formally defined development life cycle. Implementation of an acceptable logic development life cycle provides the necessary logic quality. The overall RadICS platform development lifecycle is shown in Figure 7-2 of the RadICS platform TR. This lifecycle includes both hardware development activities and FPGA technology specific development activities including ED development activities. RadICS module ED development processes are described in Section 8 of the RadICS TR.

The RadICS platform module designs are developed by RPC Radiy and delivered to Radics LLC as an integral part of the RadICS platform design. As such, the platform hardware as well as logic, which includes both FPGA platform logic and PSWD CPLD logic, undergoes CGD by Radics LLC in conjunction with the modules in which the logic is installed. The FPGA and CPLD platform logic is therefore addressed in the verification of critical platform characteristics of performance and dependability described in Section 3.4.

As stated in the RadICS TR, RPC Radiy used development standards from three main international organizations for the development of the equipment dedicated as the RadICS Platform: IAEA, IEC, and IEEE. The RadICS Platform development life cycle is defined in Chapter 7 of the RadICS TR and is referred to as the RadICS safety life cycle model. This lifecycle was designed to comply with international engineering practice for software for nuclear

safety applications. As described in Section 4 of the RadICS TR, the generic RadICS Platform was commercially dedicated by Radics LLC to demonstrate how the RadICS Platform ED life cycle processes comply with U.S. nuclear safety requirements. The commercial grade dedication of the generic RadICS platform is maintained under the Radics LLC 10 CFR Part 50, Appendix B compliant quality assurance programs.

The RadICS Platform development process consists of the following three stages:

- High level system/platform design,
- Module ED development and implementation, and
- System integration and validation

These stages are further broken down into the following RadICS platform safety lifecycle phases:

- Conceive / Identify the Safety Need
- Design
- Verify
- Modify
- Install
- Commission
- Operate / Maintain
- Retire

The NRC staff evaluated all phases of the RadICS platform safety lifecycle. The RadICS Platform safety life cycle defined in Chapter 7 of the RadICS TR also expands the design and verify phases to better define the pairing of design activities with the Verification and Validation (V&V) activities for all the levels of design.

RadICS application logic is designed, configured, and implemented onto the LM FPGAs using the Radiy Product Configuration Tool (RPCT). Project specific build documents and configuration tables for RadICS application logic, are not included within the scope of this SE.

3.5.1 Platform Electronic Design Development Lifecycle Process Planning

IEEE Std. 603-1991 requires that the quality of components and modules be established and maintained in accordance with a QA program. IEEE Std. 7-4.3.2-2003 amplifies this requirement for software quality. SRP BTP 7-14 describes the basis for accepting software for safety functions as including confirmation that acceptable plans were prepared to control software development activities.

SRP BTP 7-14, Section B.2.1, “Software Life Cycle Process Planning,” identifies the software life cycle planning information subject to review in terms of the Software Plans. SRP BTP 7-14, Section B.2.2, “Software Life Cycle Process Implementation,” identifies software documents and products subject to review to evaluate whether the software life cycle development process produced acceptable design outputs.

Though the RadICS platform does not use software during operation, it does use programmable logic that is based on a hardware descriptive language that is similar to the instruction-based

languages used in software systems. Therefore, the NRC staff considers guidance for software planning and development to be applicable to the processes used for FPGA and CPLD logic development. The following sections describe and evaluate the plans used for development of RadICS platform logic.

3.5.1.1 Management Plan

A management plan describes the management aspects of a development project. BTP 7-14, Section B.3.1.1, describes acceptance criteria for management plans. Regulatory Guide 1.173 endorses IEEE Std. 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes." IEEE Std. 1074-2006 describes, in terms of inputs and outputs, a set of processes and constituent activities that are commonly accepted as comprising a controlled and well-coordinated development process. IEEE Std. 1074-2006 Chapter 3, "Project Management Process," describes an acceptable approach for project management. It states that project management processes are, "the processes that initiate, monitor, and control software projects throughout the software life cycle."

Management aspects of RadICS platform logic development are described in Sections 7 and 8 of the RadICS TR. Electronic Designs or EDs are used for implementation of logic in the RadICS platform and therefore the term Logic is synonymous with ED for the purposes of this discussion. RPC Radiy development teams develop EDs for the RadICS modules and the RadICS FBLs that are subsequently used to implement plant-specific instrumentation protection and control logic functions. An ED consists of set of FPGA configuration files that are installed into the RadICS Modules. The RadICS ED (logic) development life cycle is described in Chapter 8 of the RadICS TR. This lifecycle consists of the following phases.

- Development of Electronic Design Architecture Description (ED AD)
- Development of FBL Detailed Description
- Development of FBL Code
- Development of ED Detailed Description
- Development of ED Code
- Synthesis
- Place and Route
- Bitstream generation

Sections 8.1.1 through 8.1.8 of the TR describe each of these phases in terms of: input data, implementation details, phase outputs, and methods of verification. Each of the RadICS modules undergoes a separate development lifecycle. Thus, separate module specific sets of lifecycle documentation are generated to support overall RadICS platform development process. Since platform components are subject to a subsequent CGD by Radics LLC, the NRC staff did not review or evaluate the lifecycle documentation for these components.

RPC Radiy, functional teams include: an Electronic Design Development Team, a Function Block Library Development Team, a QA Team, a V&V Team, an Integration Team, and a Qualification Testing Team. The roles and responsibilities for each of these teams is defined within the RPC Radiy FSMP (Ref. 10). The FSMP also discusses project planning and implementation activities used for RadICS platform component development.

The RPC Radiy FSMP defines the level of independence established between each of the designated teams. Aspects of independence between these teams include management, budget and schedule considerations. The QA team and the V&V team are also independent from the design and development teams.

A level of independence between the V&V team and the design development teams is established by specifying different reporting structures within the RPC Radiy organization. The managers to which the V&V team, QA team, and the design team report are administratively and financially independent of one another. This relationship between the design / development teams and the V&V team is illustrated in Figure 1 of the RPC Radiy FSMP.

The NRC staff finds that the RPC Radiy FSMP establishes adequate organization and authority structure for the RadICS platform design, procedures, and the relationships between different development activities. The NRC staff also finds that the management structure described in the Radiy FSMP provides for adequate project oversight, control, reporting, review, and assessment of RadICS platform component design. The NRC staff concludes that the RPC Radiy FSMP meets the requirements for management planning outlined in IEEE Std. 1074-2006 as endorsed by RG. 1.173 and is therefore, acceptable.

3.5.1.2 Development Plan

A development plan describes the plan for technical project development. Section B.3.1.2 of BTP 7-14 describes characteristics expected of a software development plan for digital system development activities. The BTP indicates that the use of the software development plan should result in “a careful and deliberate development process, which will result in high-quality software.” Based on the BTP guidance, the NRC staff review focused on the definition of the development organization, identification of project risks, definition of lifecycle phase inputs and outputs, identification of methods and tools to be used, and identification of standards being followed.

The RadICS platform development process is described in Section 7.3 of the RadICS TR. The platform development process includes development of the ED logic as well as development of the platform and application FBLs. The RPC Radiy FSMP describes the process and procedures used to design, verify and validate and maintain the product Radiy FPGA based Safety Controller (FSC) (Ref. 10). FSC is the title that RPC Radiy has given to the product line that constitutes the RadICS platform. The FSMP also describes the planning activities for RadICS platform logic and FBL development during each of the defined lifecycle phases.

The basic system development strategy is described in Section 1.4, “Staged Development,” of the FSMP. In this section, the high level FSC (RadICS platform) product concepts are described in conjunction with an overall strategy with a staged process for performing product development activities. The first two stages of this plan are for platform hardware and platform logic development. A third stage FSMP is also included (Ref. 11) to address the use of offline tools to support the product line.

Section 4 of the FSMP describes the safety lifecycle used for development of the RadICS platform. The lifecycle phases defined in the FSMP are consistent with a classic waterfall model like the model discussed in Section 2.3.1 of NUREG/CR-6101. The Radics logic development lifecycle phases are listed in Section 3.5.1.1 of this SE.

The models used for RadICS platform logic development assume that each phase of the lifecycle is completed in sequential order from concept to the decommissioning or disposal phase. The NRC staff finds the RPC Radiy choice of a development lifecycle acceptable because the waterfall model is well suited for projects with known and stable requirements and where few changes to requirements are anticipated. Since RPC Radiy selected an acceptable development life cycle model, the guidance criteria of IEEE Std. 1074-2006, Clause 2.4 has been satisfied.

RadICS Safety Life Cycle Tasks (Inputs and Outputs)

BTP 7-14, Section B.3.1.2.4, states that an applicant should identify which tasks are included with each life cycle phase and state the life cycle inputs and outputs.

Table 1 of the FSMP identifies and describes lifecycle activities, which are performed for Radiy logic development during the safety lifecycle process and identifies the phases during which each activity is performed. Additional details of safety activities and documentation is provided in Section 4.2 of the FSMP. For each safety activity, a list of input documents, a description of the activity, and a list of output documents is provided. The FSMP also defines the roles and responsibilities for completion of safety lifecycle activities. The NRC staff determined that the RadICS development process meets the criterion of BTP 7-14, Section B.3.1.2.4.

RadICS Logic and FBL Integrity Scheme

As stated in Section 12.3.6 of the RadICS Platform TR, the integrity level assigned to all Radics LLC platform and application logic and FBLs are equivalent to Level 4 as defined in IEEE Std. 1012-2004. No other types of logic are included within the scope of the RadICS platform. Therefore, no graded software / logic integrity level scheme is specified for RadICS platform development.

Though IEEE Std. 1012-2004 provides guidance for establishment of a software integrity level scheme, the NRC endorsement of this standard provided in RG 1.168 states that Software used in nuclear power plant safety systems should be assigned software integrity level 4 or the equivalent, as demonstrated by a mapping between the applicant or licensee approach and software integrity level 4 as defined in IEEE Std. 1012-2004. Because RadICS platform and application logic and FBLs are used in safety systems to support safety-related functions, the NRC staff finds the software integrity level approach used for the RadICS platform acceptable. The NRC staff also reviewed the RadICS V&V planning documentation and confirmed that RadICS platform logic development V&V activities are performed to the equivalent of software integrity level 4 requirements as defined in Std. IEEE Std. 1012-2004 (see Section 3.5.1.6 of this SE for additional information on V&V activities performed).

Management and Oversight of the Safety System Development Processes

The Radiy FSMP specifies responsibilities for ensuring that the design, verification and validation, and QA activities are conducted in accordance with the FSMP plans and other referenced planning documents. The corrective action program used during RadICS platform component development process are addressed under the Radiy QMS. The anomaly resolution and reporting process is described in Section 4.1 of the overall verification and validation plan (Ref. 30). This process is designed to promptly identify and correct conditions adverse to safety and quality. The FSMP includes oversight provisions to ensure that development processes will

be followed and that deviations from the established processes will be identified and used to initiate necessary corrective actions. Corrective action processes and documentation including the FSMP (References 10 & 11) were also reviewed during the regulatory audit and were found to be effectively addressing issues and adverse conditions identified during product development.

The NRC staff determined the Radiy QMS and FSMP are consistent with the criteria provided by IEEE Std. 1074-2006, “IEEE Standard for Developing Software Life Cycle Processes,” as endorsed by RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” In addition, the FSMP acceptably addresses the development planning activity criteria of BTP 7-14. The FSMP describes acceptable methods of organizing the safety life cycle activities. The NRC staff, therefore, finds the FSMP as applied to the RadICS development processes to be acceptable.

3.5.1.3 Quality Assurance Planning

Section B.3.1.3 of BTP 7-14 describes the review criteria for software QA plans (SQAPs). The SQAP shall conform to the requirements of 10 CFR Part 50, Appendix B, and the applicant's overall QA program. The regulation at 10 CFR Part 50, Appendix B states that the applicant shall be responsible for the establishment and execution of the QA program. The applicant may delegate the work of establishing and executing the QA program, or any part thereof, but shall retain responsibility for the QA program. The SQAP would typically identify which QA procedures are applicable to specific software processes, identify particular methods chosen to implement QA procedural requirements, and augment and supplement the QA program as needed for software.

IEEE Std. 7-4.3.2-2003, Clause 5.3.1, which is endorsed by RG 1.152 provides guidance on software quality assurance. IEEE Std. 7-4.3.2-2003, Clause 5.3.1, states, "Computer software shall be developed, modified, or accepted in accordance with an approved software QA plan.”

QA planning aspects for RadICS platform logic and development are provided in the Radiy FSMP (Ref. 10). The FSMP describes the methodology used for ensuring high quality of RadICS module logic throughout the associated safety life cycles. The scope of the FSMP includes RPC Radiy platform logic, as well as platform and application FBL logic. The FSMP provides the plan for developing RadICS platform components in accordance with the SIL 3 requirements of IEC 61508. The FSMP therefore establishes policies and processes to be followed as well as documents to be produced during development of these platform components.

QA requirements for RadICS platform components including platform logic, supplied by RPC Radiy, are defined in the FSMP and are described in Section 3, “Quality Assurance,” of the RadICS TR (Ref. 1), which describes both the RPC Radiy. The Radics LLC QA programs. The RPC Radiy QMS is used for FSC (RadICS platform) development activities. The Radics LLC QA programs are used to govern CGD activities as well as application development activities for RadICS based systems.

The FSMP provides a summary of Safety Life Cycle activities performed during product development including QA activities performed throughout the lifecycle. While many of the QA activities are paired with design activities, others are performed as support activities that can be applied during any phase of development. QA activities include; monitoring of process related

metrics, procedure reviews, performance of audits, performance of tests, problem reporting, corrective action processing, design change control, configuration management, training, management, and record keeping. These activities are supported by QA methods that are described in the FSMP and in the RadICS TR. The FSMP includes a discussion of QA tasks and establishes responsibilities of organizations performing QA activities.

Documents associated with the performance of QA activities are designated as QA Records. Section 3, "Project Documentation," of the FSMP established a process for developing a document plan. The documentation identification and storage requirements for these records are defined in a FSC document plan.

During the regulatory audit, the NRC staff reviewed several Radics LLC QA procedures, which were made available for review. The NRC staff also interviewed Radics LLC and RPC Radiy personnel to assess the QA program effectiveness. These procedures were: V&V, design verification, non-conformance reporting, configuration management, secure development and operating environment, and internal and external audit. The NRC staff also reviewed work instructions for change control, RadICS technology change evaluation process, and configuration item identification. The results of the NRC regulatory audit are documented in Reference 9.

The NRC staff found that the overall QA planning effort applied to the development of RPC Radiy developed products through the CGD by Radics LLC conforms to the requirements of 10 CFR Part 50, Appendix B, and the overall RadICS platform QA program. The NRC evaluation of the Radiy QMS was limited to the platform logic development aspects which relate to the critical characteristics identified during CGD. The RPC Radiy QMS was not evaluated or determined to be compliant with the criterion of 10 CFR Part 50, Appendix B.

The RPC Radiy FSMP identifies which RPC Radiy QA procedures are applicable to specific development processes. The RPC Radiy FSMP also identifies particular methods for implementing QA procedural requirements. The NRC staff found the RPC Radiy QA processes to be an effective quality implementation of the overall Radics LLC QA programs.

The NRC staff also found the organization of the Radics LLC QA department, as described and illustrated in Section 3.3 of the RadICS TR, has sufficient authority and organizational freedom, including sufficient independence from cost and schedule to ensure that the effectiveness of the QA organization is not compromised.

The NRC staff determined the Radics LLC QA programs in conjunction with the activities defined in the RadICS platform QA plans are consistent with the QA guidance criteria of IEEE Std. 7-4.3.2-2003. Therefore, these programs provide reasonable assurance that high quality RPC Radiy platform components capable of performing assigned safety functions are produced for RadICS digital I&C systems.

3.5.1.4 Integration Plan

BTP 7-14, Section B.3.1.4 describes expectations for software integration plans. The Section indicates that such plans should contain information on tests to be performed on the integrated hardware / software (logic implementation) system. The NRC staff review focused on the clarity and completeness of the integration plans, with specific emphasis on the treatment of error handling / fault management functions and any non-conformances found during testing.

IEEE Std. 1074-2006, “IEEE Standard for Developing Software Life Cycle Processes,” Clause A. 1.2.8, “Plan Integration,” contains an acceptable approach relating to planning for integration.

Integration planning for RadICS platform module development is provided in Section 4.2.10, “Integration,” of the Radiy FSMP (Ref. 10). The RPC Radiy integration plan describes integration activities and corresponding tests to be performed for RadICS components. This plan also identifies required input documentation, and output documentation to be produced during the integration processes. There are three types of activities performed to accomplish integration requirements. These are:

- Software to Software Integration,
- Hardware to ED Integration, and
- Product / System Integration

These three types of integration activities align closely with the phases of integration described in Section 3.1.7 of NUREG/CR-6101, “Software Integration Plan.”

In addition to RadICS platform component integration activities, there are application specific integration activities that must be performed to support overall system level development and implementation. Section 7.3.4 of the RadICS platform TR, “RadICS System Integration and Validation,” describes system integration activities necessary to ensure that the programmable and nonprogrammable components of a RadICS platform-based application will work together as a system. Project-specific applications are developed using the RadICS Platform components. System level integration consists of configuring the RadICS modules, chassis, and cabinets to perform the required system functions.

The NRC staff determined the RadICS integration plans provide an acceptably documented method for performing product integration activities needed for safety related digital I&C system development. The RadICS integration activities establish coordination with the RadICS test plans and address the use of tools, techniques, and methodologies needed to perform integration activities for RadICS platform components. See PSAI 7.2 for additional activities required to be performed during application logic development.

3.5.1.5 Safety Plan

The acceptance criteria for Safety Planning are contained in the SRP, BTP 7-14, Section B.3.1.9, “Software Safety Plan (SSP)” and Section B.3.2.1, “Acceptance Criteria for Safety Analysis Activities.” These sections state that the SSP should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101, Section 3.1.5, “Software Safety Plan,” and Section 4.1.5, “Software Safety Plan,” contain guidance on SSPs. RG 1.173, Section C.3, “Software Safety Analyses,” contains guidance on safety analysis activities while NUREG/CR-6101 also addresses guidance for these analyses.

RadICS platform safety planning is provided in Sections 4.2.12, “Functional Safety Audits,” and 4.2.13, “Independent Functional Safety Assessment,” of the Radiy FSMP (Ref. 10). The RPC Radiy FSMP describes these functional safety activities and explains the objectives of these

activities. This plan also identifies required input documentation and output documentation to be produced during the functional safety audit and assessment processes.

Safety support activities are defined and addressed in Section 5 of the FSMP, “Safety Support Activities.” These activities include establishing competence and independence of personnel performing platform development activities, establishing requirements traceability, and performing periodic audits to ensure that the FSMP is being correctly followed. In addition to listing and describing these tasks, the FSMP identifies organizations responsible for performing these tasks as well as guidance on when such tasks should be performed in relation to the safety life cycle. As such, the FSMP includes descriptions of the methods used for mitigation of potential logic implementation hazards pertaining to RadICS platform components.

RPC Radiy does not have a single dedicated software or logic safety team within its organization, however the FSMP defines intended interactions between various teams by defining organization responsibilities. Several teams within the Radiy organization have responsibilities to perform safety activities and to ensure the requirements of the FSMP defined activities are followed.

The RadICS corrective action procedure addresses corrective actions for conditions adverse to quality. These deficiencies can include supplier deficiencies in process and or controls. This corrective action process is used to document safety concerns and to track actions taken to address these concerns. Corrective action processes and associated documentation were reviewed during the regulatory audit and were found to effectively address issues and adverse conditions identified during product development.

The FSMP specifies requirements for ensuring safety analysis activities have been successfully accomplished during the development life cycle. The NRC staff determined that RadICS safety life cycle documentation shows that system safety requirements have been adequately addressed for each defined safety life cycle activity.

The NRC staff determined that safety planning for RadICS components is appropriate for RadICS platform-based safety systems and is therefore acceptable. Furthermore, the NRC staff observed during the regulatory audit, that RadICS product safety planning as executed by the RPC Radiy development and Radics LLC CGD processes provides adequate assurance that safety activities will be effective in resolving safety issues presented during the design and development of a RadICS platform-based safety system.

3.5.1.6 Verification and Validation Planning

The acceptance criteria for V&V plans are contained in SRP BTP 7-14, Section B.3.1.10, “Software V&V Plan (SVVP).” This SE states that RG 1.168, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std. 1012-2004, “IEEE Standard for Software Verification and Validation,” provides methods acceptable to the NRC staff for meeting the regulatory requirements as they apply to V&V of safety system software. Regulatory Guide 1.168, specifically notes that software to be used in safety systems should be assigned integrity level 4, as defined in IEEE Std. 1012-2004. The review guidance emphasizes independence of the review organization, the quantity and quality of V&V staff and documentation of V&V activities. The NRC staff review focused on these aspects of V&V.

The RPC Radiy V&V Planning is provided as Section 7.4 of the RadICS TR, "RadICS Platform Verification and Validation" (Ref. 1). This section describes the V&V and V&V activities that are conducted for each phase of the RadICS safety life cycle. As part of the V&V activities, the applicant needs to define the system integrity scheme. See Section 3.5.1.2 of the this SE for a description of the integrity scheme used for the RadICS platform.

The RPC Radiy FSMP describes the Radiy development organization, which includes several functional teams. RPC Radiy functional teams include: an ED development team, a HW development team, a Quality Assurance (QA) team, a V&V team, and a Qualification Test team. The level of independence established between each of these teams is defined in the FSMP. Aspects of independence between these teams include management, budget and schedule. The QA team and the V&V team are independent from the development teams.

Section 7.4 of the RadICS platform TR states: "RPC Radiy V&V capabilities are provided by a department that is technically, administratively, and financially independent from the design departments." The NRC staff confirmed the levels of independence established by reviewing Independent Verification and Validation (IVV) documentation (See Section 7.4 of the RadICS TR, "RadICS Platform Verification and Validation" (Reference 1) and by performing an audit of the RPC Radiy and Radics LLC processes in Toronto CA. During this audit, the NRC staff performed interviews with members of the Design, V&V and QA organizations. The results of this audit are documented in Reference 9. The NRC staff determined that an adequate level of independence exists between these organizations and that an appropriate level of technical competence is established and maintained within the independent V&V staff. The level of independence used for the RadICS V&V effort therefore meets the requirements for software integrity level 4 as defined in IEEE Std. 1012-2004.

Section 5.7.14, "IEEE Std. 1012-2004," of the RadICS TR states the following: "RPC Radiy and RadICS ED V&V plan documentation complies with the intent of IEEE Std. 1012-2004, as described in Chapters 7 and 8 of the RadICS TR." Although the RadICS platform was not developed in accordance with IEEE Std. 1012-2004, the NRC staff notes that comprehensive and rigorous V&V processes were used for RadICS platform design and many of the RadICS V&V activities are similar to the minimum V&V tasks called for by the standard. The NRC staff also notes that CGD of RPC Radiy modules is performed by Radics LLC. These CGD activities include V&V activities that are in addition to those performed by RPC Radiy during FSC development. This dedication process includes identification of RadICS component critical characteristics as well as a verification process to ensure each of the identified critical characteristics are met. See Section 3.4 of this SE for a complete description and evaluation of the Radics LLC commercial grade dedication process.

No mapping between RPC Radiy V&V activities and V&V minimum required activities of IEEE Std. 1012-2004 was provided. However, Radics LLC identified five exceptions to conformance with the criteria of IEEE Std. 1012-2004. These exceptions are:

- The specific administrative requirements for administrative and formatting requirements specified in IEEE Std. 1012-2004, Sections 7 and 8 were not followed.
- The criticality analysis is not performed, since all RadICS module EDs are classified at the highest safety integrity level for use in safety-related systems.

- The Failure Modes and Effects Diagnostic Analysis (FMEDA) and the IEC Safety Integrity Level certification replace the hazards analyses specified in IEEE Std. 1012-2004, Section 5 and Tables 1 and 2.
- The security assessments described in Chapter 11 replace the security analyses specified in IEEE Std. 1012-2004, Section 5 and Tables 1 and 2.
- The RPC Radiy and Radics LLC approaches to V&V test documentation described in Section 12.3.4 of the RadICS TR were used as an alternative to the test documentation administrative requirements specified in IEEE Std. 1012-2004, Section 6.3.1.

Section 7.4.3, "Implementation Activities," of the RadICS TR defines a minimum set of V&V activities to be performed for RadICS platform components. The NRC staff reviewed the V&V activities list and determined the tasks to be consistent with tasks specified in IEEE Std. 1012-2004 for software integrity level 4 software.

To determine adequacy of the RadICS platform V&V processes, the NRC staff performed a comparison analysis between RadICS V&V activities listed in Section 7.4.3 of the RadICS TR and the minimum V&V tasks identified in Table 2 of IEEE Std. 1012-2004.

Because there was no direct correlation between the RadICS V&V activities and the IEEE V&V tasks, each activity and task were categorized in order to establish a basis for comparison. Categories used were as follows:

- Hardware Validation Test Activity
- Platform Validation Test Activity
- Platform Integration Test Activity
- Classification Activity
- Problem Reporting / Resolution Activity
- Hazard / Risk Analysis Activity
- Requirements Traceability / Analysis
- Security Analysis / Vulnerability Analysis
- Process Improvement Activity
- Interface Activity
- Management Activity
- Failure Analysis Activity
- Document Review Activity
- Qualification Activity
- Configuration Management Activity
- Operations Integration Activity

RadICS V&V activities and IEEE tasks were then re-sorted by category. V&V activities and tasks within each category could then be compared to determine level of compliance achieved by the RadICS V&V processes.

In some cases, there were direct correlations between RadICS activities and tasks identified in IEEE Std. 1012. These tasks were identified as being addressed by the RadICS V&V process. In other cases, IEEE tasks were not identified as V&V activities but were performed under a

different process such as the configuration management process. These tasks were identified as being addressed by a RadICS program other than the V&V program.

The analysis results showed that most required V&V tasks identified in IEEE Std. 1012 could be either mapped to V&V activities within the RadICS V&V program or shown to correspond to activities performed under different RadICS processes. Four required V&V tasks were however found not to have equivalent activities performed under RadICS processes. These tasks are: (1) Criticality Analysis, (2) Hazard Analysis, (3) Operating Procedures Evaluation, and (4) Retirement Assessment.

The absence of a Criticality Analysis is acceptable because all RadICS platform logic and FBL logic is classified at the highest level for use in safety-related systems as described in Section 3.2.2 of the RadICS TR. All platform and FBL logic are also dedicated by Radics LLC under their 10 CFR Part 50, Appendix B compliant QA process. This was identified in the exceptions list provided in the RadICS TR.

The FMEDA described in Section 9.2.1 and the IEC Safety Integrity Level certification described in Section 3.2.2.3 of the RadICS TR are performed in lieu of hazards analyses activities. A description and evaluation of the FMEDA is provided in Section 3.5.2.6 of this SE. The absence of the hazard analysis was identified in the exceptions list provided in the RadICS TR.

Operating procedures and retirement assessment activities are considered by the NRC staff to be plant specific activities. The NRC staff agrees that these activities can be performed as part of the application development. It is therefore acceptable for these activities to be addressed during application development and implementation. See PSAI 7.2.

During the regulatory audit, several requirement thread reviews were performed. The NRC staff confirmed how system requirements had been implemented and how V&V activities had been performed during the RadICS development processes. Radics LLC showed how the requirements traceability was used to confirm that V&V activities of the RadICS V&V plan had been performed and documented.

The NRC staff finds the RadICS platform V&V processes and identified alternative activities to be consistent with the criteria of IEEE Std. 1012-2004, “IEEE Standard for Software Verification and Validation,” as endorsed by RG 1.168. No evaluation of RadICS application ED development V&V processes could be performed because application logic development V&V plans were provided to the NRC for review and no plant specific application was available during this evaluation. See PSAI 7.2 for more information on V&V activities to be performed during application development.

3.5.1.7 Configuration Management Planning

The acceptance criteria for software configuration management plans (SCMPs) is contained in SRP BTP 7-14, Section B.3.1.11, “Software Configuration Management Plan (SCMP),” and Section B.3.2.3, “Acceptance Criteria for Software Configuration Management Activities.” These sections state that both: (1) RG 1.173 that endorses IEEE Std. 1074-2006, Clause A.1.2.2, “Plan Configuration Management,” and (2) RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” that endorses IEEE Std. 828-2005, “IEEE Standard for Configuration Management Plans,” provide an acceptable approach for configuration management planning.

SRP BTP 7-14, Section B.3.1.11 further states that additional guidance can be found in IEEE Std. 7-4.3.2-2003, Clause 5.3.5, "Software configuration management," and in Clause 5.4.2.1.3, "Establish configuration management controls." NUREG/CR-6101, Section 3.1.3, "Software Configuration Management Plan," and Section 4.1.3, "Software Configuration Management Plan," also contain guidance on configuration management.

RadICS configuration management (CM) planning is provided as Section 7.5 of the RadICS platform TR, "Radics Configuration Management Process" (Ref. 1), and in the FSC Configuration Management Plan (Ref. 33). The CM processes are applicable to all RadICS platform logic, including: the platform and application FBLs, FPGA EDs, and software tools used for development of RadICS platform and application logic. The CM processes also apply throughout the safety lifecycle of platform and project specific applications. The RadICS platform TR describes methods for identifying platform logic element configuration items that are controlled in accordance with the configuration management program. The CM process also defines methods used to establish and maintain configuration control when changes to platform or application logic are made as well as methods for recording and reporting the status of RadICS design changes.

A change control board (CCB) is used for approving and managing the implementation of changes to the RadICS platform. A configuration management board (CMB) is also used to provide oversight and direction for the CM processes. The RadICS CM plan establishes criteria for establishment of the CCB and CMB and describes the configuration control processes including those used for system logic development. These processes include change initiation, change control and change approval.

During the regulatory audit, the NRC staff observed Radics LLC's use of configuration management tools to control access to documents and RadICS logic implementation files, manage change requests, and track changes. The NRC staff also reviewed configuration management procedures as well as configuration management forms prepared for RadICS. The NRC staff's observations during the audit support a finding of reasonable assurance that appropriate configuration management activities are being performed. The results of this audit are documented in Reference 9.

The NRC staff concludes that CM planning processes used to support RadICS platform development conform to the requirements identified in IEEE Std. 828-2005, as endorsed by RG 1.169. This meets the criteria of BTP 7-14 Clause 3.4.1.7 and is, therefore, acceptable.

3.5.1.8 Test Planning

The acceptance criteria for a test planning are contained in SRP BTP 7-14, Section B.3.1.12, "Software Test Plan (STP)." Section B.3.1.12 of BTP 7-14 contains review guidance for software test plans. Pointers are provided to the endorsements in RG 1.170, which endorses IEEE Std. 829-2008, "Test Documentation," and 1.171, which endorses IEEE Std. 1008-1987. Among the key attributes expected of a software test plan are description of the test organization(s), testing strategy, testing criteria and testing records.

RadICS platform test planning is provided in the FSC Integration Test Plan (Ref. 31), and in the FSC Safety Validation Test Plan (Ref. 32). The RadICS platform test plans describe testing activities performed for Radiy FSC as required by FSMP. The RadICS test plans provide details

of test methods and tools used during test activities and establish minimum content requirements for test documents.

The RadICS platform test plans are used in conjunction with the RadICS validation test plans to identify required test activities to be performed by the V&V team. The purpose of the validation test plan is to identify and plan validation tests or other validation methods to demonstrate that the Radiy FSC meets all requirements defined in the safety requirement specification and the overall V&V Plan (Ref. 30). The purpose of the integration test plan is to specify integration test activities to be implemented for Radiy FSC as required by the FSMP. Validation and integration test activities are performed after development of FSC RadICS platform, including all modules and components as a part of certification of the RadICS platform to show compliance with IEC 61508 requirements.

Section 7.4.5.2 of the RadICS TR also describes test planning activities for activities performed under the overall V&V plan (Reference 30). The RadICS platform V&V program as defined by the overall V&V plan includes fault insertion, integration, validation, qualification, and functional test activities.

Based on the information provided, the NRC staff determined the RadICS platform test plans acceptably cover testing performed on Radics platform FSC logic. Using this information, the NRC staff was able to map RadICS platform test activities to V&V test activities called for in IEEE Std. 1012-2004. For example, both the safety validation test plan and the integration test plan provide a description of the test organization(s), testing strategies applied and testing criteria. Requirements for testing records are also described in these plans. See Section 3.5.2.4 of this SE for evaluation of test activities and documentation exceptions to standards.

The NRC staff found that test responsibilities are assigned to appropriate personnel and that adequate provisions for re-test are included to address situations where test failures occur. RadICS test failures are documented in FSC safety validation test reports. The process for resolving test anomalies includes performance of regression analysis to determine the extent to which V&V activities shall be repeated. The RadICS platform test plans assign responsibility for test definition, design, and performance to a validation and qualification test team and a metrology test team which are under authority of the project validation and qualification manager.

The NRC staff determined the RadICS platform test plans are sufficiently comprehensive to demonstrate that a RadICS platform-based safety system will perform its required safety functions in a satisfactory manner. This meets the criteria of BTP 7-14, Clause 3.1.12 and is, therefore, acceptable. Application logic test plans were not included in the RadICS TR submittal and were therefore not within the scope of the NRC staff SE. Application Test planning is therefore a PSAI and should be addressed by PSAI 7.2.

3.5.2 Logic Implementation and Design Output Documentation

This Section summarizes the evaluation of implementation and design output documentation for the RadICS platform logic. This documentation corresponds with the safety life cycle process implementation information described in SRP BTP 7-14 Section B.2.2, “Software Life Cycle Process Implementation,” and Section B.3.2, “Acceptance Criteria for Implementation.”

SRP BTP 7-14, Section B.2.3, “Software Life Cycle Process Design Outputs,” identifies software documents and products subject to review to evaluate whether the software life cycle development process produced acceptable design outputs.

Since the RadICS TR does not identify a plant specific application, many of the documents identified in SRP BTP 7-14 are not relevant for generic review of the platform. For example, operations, maintenance, and training manuals primarily relate to a specific plant system and

support the licensee as end product user of that system. Thus, review of these documents was not within the scope of this review. See PSAI 7.2.

RadICS Platform application logic is designed, configured, and implemented onto the LM FPGAs using the Radiy Product Configuration Tool (RPCT). Project specific build documents and configuration tables for RadICS application logic, are not included within the scope of this SE. The following sections describe and evaluate implementation documentation.

3.5.2.1 Safety Analysis

The acceptance criteria for safety analysis activities are contained in the SRP, BTP 7-14, Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." This criteria states: (1) the documentation should show that the system safety requirements have been adequately addressed for each activity group; (2) no new hazards have been introduced; (3) the software requirements, design elements, and code elements that can affect safety have been identified; and (4) that all other software requirements, design, and code elements will not adversely affect safety. Further guidance on safety analysis activities can be found in NUREG/CR-6101 and RG 1.173, Section C.3, “Software Safety Analyses.”

Documentation of Radiy Safety Analysis implementation was provided by the following:

- Safety Case: Compliance with FSMP Requirements
- Functional Safety Assessment Report

The NRC staff reviewed these reports during a regulatory audit and determined that RadICS platform safety requirements have been adequately addressed. Identification of potential system hazards is addressed during each phase of the safety life cycle. Requirements, design elements, and logic elements that could affect safety are identified and safety impacts are addressed. The results of this audit are documented in Reference 9.

The NRC staff reviewed the Radics LLC product assessments provided in the commercial grade dedication reports (see Section 3.4 of this SE) and determined that safety analyses activities were performed in accordance with the RadICS FSMP. The commercial grade dedication reports provide objective evidence that the system safety requirements, as defined in the critical characteristics for each RadICS platform module, were correctly implemented, and provide reasonable assurance that no hazards were introduced into the system as a result of the FSC development activities.

RadICS platform logic elements that have the potential to affect safety were identified, and safety problems and resolutions identified during the analyses were documented and dispositioned in an acceptable manner. During the regulatory audit, the NRC staff reviewed several system logic requirements, including design and code elements, and determined they

had been implemented in a manner, which will not adversely affect the safety of a RadICS platform-based safety system.

The NRC staff determined that RadICS platform safety analysis activities are acceptable and are compliant with SRP BTP 7-14, Section B.3.2.1. Application level safety analysis tasks were not included in the RadICS TR submittal and were therefore not within the scope of the NRC

staff SE. Application safety analysis activities are therefore a plant specific action item and should be addressed by PSAI 7.2.

3.5.2.2 V&V Analysis and Reports

SRP, BTP 7-14, Section B.3.2.2, “Acceptance Criteria for Software Verification and Validation Activities,” states that the acceptance criterion for software V&V implementation is that the tasks in the SVVP have been carried out in their entirety. Documentation should exist that shows that the V&V tasks have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the requirements, design, code, integration, and installation design outputs satisfy the appropriate software development functional and process characteristics.

The RadICS Overall V&V Plan (Ref. 30) identifies the following report types to be produced to document the results of V&V activities performed:

- Review Reports (Place and Route)
- FMEDA Report
- Test Reports (LM and AIM)
- Static Code Analysis / Code Review Report
-

The NRC staff reviewed V&V reports of each type identified above during a regulatory audit to evaluate the degree to which Radics LLC V&V activities were accomplished. The results of this audit are documented in Reference 9. The NRC staff determined the RadICS V&V reports acceptably describe a detailed and thorough V&V effort. The RadICS Overall V&V Plan was implemented in a manner, which supports the development of platform logic that will perform required safety functions. The NRC staff found that activities performed and documented in the V&V reports provide reasonable assurance that V&V efforts were effectively implemented to support the development of a product that is suitable for use in safety-related nuclear applications. The V&V reports were written such that the information reviewed, level of detail, and findings of the V&V effort wereunderstandable and informative. The V&V Reports provide adequate documentation to show that V&V tasks were successfully accomplished for each safety life cycle phase.

Problems and test failures identified during the V&V effort were entered into the Radics LLC corrective action program as corrective action reports. Problem descriptions and actions required to correct or mitigate each problem were adequately documented. In some cases, test failures were justified by the designer and no corrective actions were required. For these situations, acceptance of justification was provided, and re-tests were performed to verify correct system performance. Several test failure reports were reviewed during the regulatory audit. Corrective action documentation was also reviewed and was found to be effectively addressing issues and adverse conditions identified during product test activities.

The NRC staff concludes that the development functional and process characteristics of the V&V effort are acceptable. V&V activities performed for the RadICS platform logic development are acceptable and are compliant with SRP BTP 7-14, Section B.3.2.2. See PSAI 7.2 for activities to be performed during application logic development.

3.5.2.3 Configuration Management Activity

The acceptance criteria for CM activities are identified in BTP 7-14, Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities." This acceptance criterion requires that the tasks in the software configuration management plan be carried out in their entirety. Documentation should exist that shows that the CM tasks have been successfully accomplished. In particular, the documentation should show that: (1) configuration items have been appropriately identified; (2) configuration baselines have been established for the activity group; (3) an adequate change control process has been used for changes to the product baseline; and that appropriate configuration audits have been held for the configuration items created or modified for the activity group.

The RadICS CM plan (Ref. 33) establishes requirements for implementation of a CM process during the safety life cycle of the Radiy FSC. This CM plan describes CM tasks that are performed by RPC Radiy (see Section 3.5.1.7 of this SE). The CM plan establishes a change control process as a constituent part of CM process.

Configuration Item status accounting for the RadICS platform consists of monitoring, documenting, and notifying project personnel regarding changes to RadICS platform configuration. FSC configuration audit reports provide documentation of configuration management activities performed during each phase of RadICS platform component development. Configuration audits are performed following the release of each established baseline. These audits provide a check of correctness of the RadICS configuration items functional and physical features implementation for every specific project.

RPC Radiy maintains and controls RadICS platform design documentation and program files as QA records. Changes to controlled files are tracked and can only be changed by using the approved change process. During a regulatory audit, the NRC staff reviewed the Radics LLC procedures for performing logic changes and conducted an exercise involving making a sample logic change using these procedures. The results of this audit are documented in Reference 9. The NRC staff reviewed the requirements baseline configuration audit report as a regulatory audit activity. This audit report was found to contain an acceptable level of information to show that the configuration management plan is being carried out in its entirety and that changes made to items under configuration control are being controlled, tracked, and documented in a manner which is consistent with a high-quality development process.

The NRC staff determined the CM processes and activities performed meet the requirements of IEEE Std. 828-1998 and ANSI/IEEE Standard 1042-1987 and are therefore acceptable. The RPC Radiy and Radics LLC CM activities adequately address the guidance in BTP 7-14 Section B.3.2.3.

3.5.2.4 Testing Activity

The acceptance criterion for testing activities is contained in the SRP, BTP 7-14, Section B.3.2.4, "Acceptance Criteria for Testing Activities." This SE states that RG 1.168

Rev. 2, “Regression Analysis and Testing”, Section 7.2, and RG 1.170, Rev. 1, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” that endorses IEEE Std. 829-2008, “IEEE Standard for Software Test Documentation,” and RG 1.171, Rev. 1, “Software Unit Testing for Digital Computer Software Used in Safety

Systems of Nuclear Power Plants,” that endorses IEEE Std. 1008-1987, “IEEE Standard for Software Unit Testing,” identify acceptable methods to satisfy software testing requirements.

The RPC Radiy and Radics LLC approach to V&V testing is described in Sections 7 and 8 of the RadICS TR. The overall V&V plan (Ref. 30) specifies the content of the specific test plan for which test specifications test procedures and test reports are required. The RadICS platform and application ED V&V program includes fault insertion, integration, validation, qualification, and functional test activities. Platform and application ED V&V test documentation is described in Section 7.4.5.2 of the RadICS TR.

The RadICS platform and application V&V test processes conform to the requirements in IEEE Std. 1012-2004, as endorsed by RG 1.168, Rev 1 with one exception. Instead of following the guidance of IEEE Std. 1012 and IEEE Std. 829-2008, RPC Radiy uses an alternate approach to V&V test documentation. The test documents are structured differently to reflect the use of RadICS Platform and Application ED development safety life cycle and the use of FPGA technology.

The NRC staff reviewed the alternate test documentation processes and determined that quality assurance programs for document format were followed and that alternate test documents reflect the unique test methods used to verify and validate the RadICS platform logic. This alternative approach to performing test documentation is therefore acceptable.

The RadICS test programs provide comprehensive test coverage of an integrated RadICS platform-based system. The NRC staff observed appropriate adherence to the test program procedures. Discrepancies discovered during the test performance were appropriately documented and addressed using the Radics LLC anomaly reporting process. Several test failure reports were reviewed during the regulatory audit. Corrective action documentation was also reviewed and was found to be effectively addressing issues and adverse conditions identified during product test activities. Test results and verification of test completion were documented in test reports. The RadICS test activities adequately address the guidance in BTP 7-14 Section B.3.2.4 for the platform logic.

The RadICS platform TR does not address testing activities associated with application specific logic. Therefore, plant application testing activities for RadICS platform-based safety systems must be performed during plant application development and thus could not be evaluated in this SE. See PSAI 7.2 for additional information on performing application development activities to be performed.

3.5.2.5 Requirements Traceability Evaluation

Evaluation criteria for the use of Requirements Traceability Matrices (RTM) is contained in SRP, BTP 7-14. A definition for RTM is provided in Section A.3 of the BTP. Here it is stated that: “An RTM shows every requirement, broken down into sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement.” This is further clarified in Section B.3.3, “Acceptance Criteria for Design Outputs,” in the subsection on Process Characteristics.

This SE criteria states that the RTM should show what portion of the software requirement, software design description, actual code, and test requirement addresses each system requirement.

A description of the process used by RPC Radiy to perform requirements traceability is provided in Section 7.6 of the RadICS TR. Platform functional requirements are established and categorized into three groups: Safety Requirements, Performance Requirements, and Qualification Requirements. These requirements are also further broken down to sub-categories, which are defined in Section 7.6 of the RadICS TR.

A requirement tracing tool is used to implement traceability. This tool is described in Section 7.6.4 of the RadICS TR. This tool is used to create a RTM which is used to support audits and analysis activities to access status and completion of requirements throughout the safety lifecycle.

The documentation structure used for RadICS platform design documents starts with RadICS Platform and RadICS-Based Application Functional Requirements. These functional requirements are defined in the following documents:

- Product Concept Document,
- FSC Safety Requirements Specification (Ref. 34),
- Product Architecture Document (Ref. 37), and
- Derived Safety Requirements Specification.

Traceability of all RadICS requirements and derivative requirements between these documents is established by the RTM. Establishment and verification of requirements traceability are defined as V&V activities that are performed throughout the RadICS safety lifecycle. RPC Radiy requires an independent reviewer check the requirements specifications to detect and correct the insertion of requirements that have an undesirable effect on the secure operational environment of the system.

The NRC staff reviewed the RTM and performed thread audits for several selected requirements during the regulatory audit. The results of this audit are documented in Reference 9.

The NRC staff observed that the RadICS platform RTM shows each of the requirements delineated in requirements specifications are broken down into sub-requirements. The RTM identifies implementation documents and test requirements credited to address each system requirement. The RTM provides evidence to show that each system requirement has been implemented in the system hardware and logic design and shows that V&V testing has been performed to demonstrate correct implementation of each requirement. The NRC staff determined that requirements tracing processes used for the RadICS platform hardware and logic implementation provide reasonable assurance that all requirements are correctly implemented and were consistent with BTP 7-14 criterion and are therefore acceptable.

The RadICS platform TR does not address traceability activities associated with application specific logic. Therefore, plant application requirements traceability activities for RadICS platform-based safety systems must be performed during plant application development and

thus could not be evaluated in this SE. See PSAI 7.2 for additional information on performing application development activities to be performed.

3.5.2.6 Failure Mode and Effect Analysis

Regulatory Guide 1.53, Rev. 2, "Application of the Single-Failure Criterion to Safety Systems," provides endorsement of a method acceptable to the NRC staff for satisfying the NRC's regulations as they apply to the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems. Regulatory Guide 1.53 endorses IEEE Std. 379-2000. IEEE Std. 379-2000, Clause 5.5 identifies Failure Mode and Effects Analysis (FMEA) as an example method to address common-cause failures when performing analysis to demonstrate that the single-failure criterion has been satisfied. Although no specific regulatory guidance on the format, complexity or conclusions of the FMEA exists, the FMEA should identify potential failure modes within a system to determine the effects of these failures on the system. The FMEA should demonstrate that single-failures, including those with the potential to cause a non-safety system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions.

The NRC staff reviewed the RadICS platform FMEDA methodology described in Section 9.2.1 of the RadICS TR (Ref. 1).

The RadICS FSC FMEDA was performed for each platform module and includes four groups of module components. The FMEDA analyzes potential failures in each of these component groups and categorizes the effects of these failures as defined in Section 9.2.1.2 of the RadICS TR. Failure categories are:

- Fail-Safe State (Detected/Undetected)
- Fail Dangerous State (Detected/Undetected)
- Analog Input (Deviation more than 2% of span)
- Annunciation (Detected/Undetected)
- No Effect
- Fail Dangerous (Undetected after Surveillance Test)

The RadICS FSC FMEDA results indicated that the probability for undetectable "Fail Dangerous" occurrence is extremely low. The RadICS FSC also relies upon application logic functions for detection of Type III, User defined level faults. Failure types are described in Section 3.7.3 of this SE. Because the failure analysis was performed at platform level, the FMEDA did not demonstrate that all input signal or system level failures would cause a RadICS platform-based safety system to revert to a predefined safe state. The NRC staff determined this to be acceptable based on the plant specific activities that must be performed during application development.

The fail-safe states for RadICS safety functions are generically defined in the TR as being deenergized. Applications requiring fail safe states of energized must be determined as an application specific development activity. In such cases, interposing relays or some other form of conditioning circuitry must be included in the system design to enable required fail-safe functionality upon failure detection. In addition, the FMEDA does not account for external communication interface failures and the effects they would have on system level performance.

Therefore, a system level FMEA should be performed during plant specific application development to identify potential system level failure modes, establish required fail-safe states, and to determine the effects of these failure modes on plant safety.

The NRC staff also reviewed the results of the FMEDA report during its regulatory audit and determined the level of detail for the RadICS FSC is acceptable based on the criteria of RG 1.53, Rev. 2. This FMEDA was performed by an independent certification company, Exida, to support IEC 61508 SIL 3 certification. The FMEDA methods used were found to be consistent with IEEE Standard 379 2000 as endorsed by RG 1.53 Rev. 2. The RadICS FSC FMEDA considers single detectable failures as well as identifiable but non detectable failures, failures caused by the single failure and failures resulting in spurious system safety function actuations.

Based on the NRC staff review of the RadICS FSC FMEDA, there is reasonable assurance that credible RadICS FSC failure modes have been properly identified and evaluated. Therefore, the criteria of RG 1.53 pertaining to the RadICS FSC failure modes and effects are satisfied, however system level failure modes will need to be addressed during plant application development. PSAI 7.5 of this SE identifies additional FMEA actions, that are needed during specific plant application development.

3.5.2.7 Reliability Analysis

IEEE Std. 603-1991, Clause 4.9 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that reliability goals imposed on the system design have been met. However, as discussed within RG 1.152, “Criteria for Use of Computers In Safety Systems of Nuclear Power Plants,” and DI&C-ISG-06, the NRC staff acceptance of the reliability of digital I&C systems is based on deterministic criteria for both hardware and programming. The NRC staff does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for reliability of digital computers used in safety systems.

Nevertheless, IEEE Std. 603-1991 further requires in Clause 5.15 that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed to confirm that such goals have been achieved. IEEE Std. 603-1991, Clause 6.7 requires that when sense and command features are in maintenance bypass, the safety system shall retain the capability of accomplishing its safety function while continuing to meet the single-failure criterion. Similarly, IEEE Std. 603-1991, Clause 7.5 requires that when one portion of a redundant safety system executes features is placed into a maintenance bypass condition, and then the remaining redundant portions should provide acceptable reliability. DI&C-ISG-06 states that the reliability and availability analysis should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed with further consideration of the effect of possible failures and the design features provided to prevent or limit its effects.

The RadICS FSC FMEDA, described in Section 9.2.1 of the RadICS TR, includes an analysis of failure rates associated with RadICS components. This data was used to quantify the expected performance/reliability of a RadICS platform-based system. The FMEDA for each RadICS Module considered four different groups of components that affected module functionality. These groups were: common, Input, Output, and LVDS. The results of the board/device-level

reliability analysis for each platform component group are provided in Section 9.2.1.3 of the RadICS TR.

The NRC staff determined the RadICS platform reliability analysis results of the FMEDA contain platform reliability information that can be used to demonstrate conformance to plant-specific reliability goals. Because plant- and system-specific reliability goals are not provided in the RadICS TR and instead must be established on a plant-specific basis, the NRC staff was unable to make a safety determination for this criterion. PSAI 7.6 of this SE identifies additional actions, which must be addressed during plant specific application development.

3.5.2.8 Requirements Specification

The acceptance criteria for requirements specification is contained in the "Standard Review Plan," NUREG-0800, BTP 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements Specification." This section states that RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 830, "IEEE Recommended Practice for Software Requirements Specifications." IEEE Std. 830 describes an acceptable approach for preparing software requirements specifications for safety system software. Additional guidance is provided in NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems." Sections 3.2.1 and 4.2.1 of NUREG/CR-6101 discuss software requirements specifications for "Life Cycle Software Reliability" and "Safety Activities and Recommendations, Guidelines, and Assessment," respectively.

BTP 7-14 emphasizes clarity in the requirements and specifically cites thread audits as a method to check for completeness, consistency and correctness. The requirements specifications discussed in NUREG/CR-6101, Sections 3.2.1 and 4.2.1, detail examples of the type of content that should be documented regarding the application system design. Section 3.2.1 contains sample requirement specification contents, including general description, user characteristics, performance requirements, and interface requirements. Section 4.2.1 provides a sample list of questions that an assessor may ask when reviewing a requirements specification. These questions regarding the life cycle activities highlight potential areas for improvement with respect to reliability and safety risks.

The following specification documents were provided to or audited by the NRC to support evaluation of the RadICS LLC Safety Requirements Specification (SRS) documentation:

- D3.1 RadICS Safety Requirements Specification (Ref. 34)
- D5.1 RadICS Product Architecture Document (Ref. 37)
- D3.7, RadICS Equipment Qualification Safety Requirements Specification
- D3.8, RadICS Equipment Qualification Safety Requirements Specification Review Report
- D5.4, RadICS AFBL/Application Logic Detailed Requirements Specification
- D5.5, RadICS AFBL/Application Logic Detailed Requirements Specification Review Report
- D7.21, 2015-RTS001-SWRS-011, NRC RadICS Test Specimen (RTS-001) Software Requirements Specification

The NRC staff's review in this area focused on clarity and completeness of requirements of the RadICS platform and relied on the thread audits to demonstrate that requirements were traceable through applicable RadICS platform design documentation. Section 3.5.1.6 of this SE describes of these requirement thread reviews.

The NRC staff found that the RadICS platform safety requirement documents comply with the characteristics necessary to facilitate the development of quality programmable logic for use in nuclear safety applications. The areas evaluated by NRC staff include: the functional safety qualification requirements to the Radiy FSC and environmental qualification requirements, such as electromagnetic compatibility, temperature, humidity, etc. The NRC staff also reviewed the requirements specification for application logic, in which RPC-Radiy stated that certain logic features would reduce the likelihood of negative effects resulting from tuning parameters and inputs corruption. The NRC staff determined that each of the RadICS platform requirements evaluated met the requirements of BTP-714 and was appropriately included in the associated requirements documentation. The NRC staff determined that the requirements documentation is adequately controlled by vendor processes, which include: a verification checklist for each SRS, and feedback provided by the design team (and representatives in affected areas) for any draft documents or updates. The controls for configuration management, similar to those for SRS, are discussed in Section 3.5.2.3 of this SE.

3.6 Equipment Qualification

The purpose of performing equipment qualification testing for a safety system are (1) to demonstrate that the system will not experience failures due to abnormal service conditions of temperature, humidity, electrical power, radiation, electromagnetic interference, radio frequency interference, electrical fast transient, electrostatic discharge, power surge, or seismic vibration, and (2) to verify those tests meet the plant-specific requirements.

Criteria for EQ of safety-related equipment are provided in 10 CFR Part 50, Appendix A, GDC 2, "Design Bases for Protection Against Natural Phenomena," and GDC 4, "Environmental and Dynamic Effects Bases." Additionally, the regulation at 10 CFR 50.55a(h) incorporates by reference the requirements of IEEE Std. 603-1991 which addresses both system-level design issues and quality criteria for qualifying devices. Regulatory Guide 1.209 endorses and provides guidance for compliance with IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," for qualification of safety-related computer-based I&C systems installed in mild environment locations.

To comply with the requirements of GDC 4, and IEEE Std. 603-1991, an applicant must demonstrate through environmental qualification that Instrumentation and Control systems meet design-basis and performance requirements when the equipment is exposed to normal and adverse environments. RadICS equipment is only approved for use in mild environment conditions, as defined in 10 CFR 50.49(c) and therefore, the requirements for equipment in harsh environments of 10 CFR 50.49 are not applicable.

Because Radics LLC equipment was commercially dedicated for use in safety-related applications, the guidance of SRP Chapter 7, Appendix 7.0-A (page 7.0-A-17), Section 3.8, "Review of the Acceptance of Commercial-Grade Digital Equipment," was also considered by the NRC staff during this evaluation. This SRP Section states that an acceptable set of fundamental requirements for this process is described in IEEE Std. 7-4.3.2 2003, "Qualification of Existing Commercial Computers," Clause 5.4.2, as endorsed by RG 1.152.

Section 5.4.2 of SRP Chapter 7, Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2,” states that EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” and EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-related Applications in Nuclear Power Plants,” provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

EPRI TR-107330 presents a specification in the form of a set of requirements to be applied to the generic qualification of PLCs for application and modification to SR Instrumentation and Control systems in nuclear power plants. It is intended to provide a qualification envelope corresponding to a mild environment that should meet regulatory acceptance criteria for a wide range of plant-specific SR applications. The qualification envelope that is established by compliance with the guidance of EPRI TR-107330 consists of the maximum environmental and service conditions for which qualification was validated and the range of performance characteristics for the PLC platform that were demonstrated under exposure to stress conditions. Applicants using the RadICS platform are obligated to verify that the requirements of the application are bounded by the established qualification envelope. See PSAI 7.4.

Radics LLC used the guidance provided in EPRI TR-107330 to establish the testing approach to meet the guidance criteria of IEEE Std. 323-2003 as endorsed by RG 1.209. The qualification program developed for the RadICS Qualification Test Specimen (QTS) addressed environmental qualification for a mild, controlled environment, such as the main control room and auxiliary electrical equipment rooms. The basis for the testing program was conformance with the guidance contained in EPRI TR-107330, Section 4.3. The results of the qualification program establish the qualification envelope of the RadICS platform.

EQ testing of the RadICS platform equipment was performed in accordance with criteria of RG 1.209 and IEEE Std. 323-2003 to demonstrate performance under a variety of environmental conditions by a company named Kinectrics Inc., which is a test laboratory located in Toronto, Ontario, Canada. Kinectrics provided overall qualification testing services including: Environmental (Atmospheric), Seismic, and Class 1 E to Non-1 E Isolation. Radiation testing was not performed because RadICS equipment is only approved for installation into mild environments.

Kinectrics subcontracted with Ultra Tech Group of Labs located in Oakville, Ontario, Canada (with authorization from Radics LLC) to provide Electromagnetic Interference / Radio Frequency Interference (EMI/RFI) Emissions and Susceptibility, Electrical Fast Transient, Electrostatic Discharge and Surge Withstand qualification testing services. Laboratory testing services were performed in accordance with the Radics LLC services procurement specification, which invoked the Kinectrics 10 CFR Part 50, Appendix B Quality Manual.

A description of equipment qualification and analysis for the RadICS equipment was provided as Section 9 of the RadICS TR (Ref. 1). In addition, an Equipment Qualification Test Plan was submitted to the NRC for review (Ref. 38). The results of RadICS EQ testing were submitted to the NRC as an Equipment Qualification Test Summary Report (Ref. 8).

A QTS was used during test activities. The test application logic was specifically designed and implemented in the QTS to support qualification testing of the RadICS platform while providing generic functionality of the test system. This QTS was developed in accordance with EPRI TR-107330 and includes a representative sampling of the RadICS Platform components.

The assembled components of the RadICS Platform QTS include the following types of hardware modules and components:

- Chassis and Backplane
- Logic Module
- Analog Input Modules
- Discrete Input Modules
- Analog Output Modules
- Discrete Output Modules
- Optical Communication Modules
- Equipment Protection Modules for External Interfaces
- Fan Cooling Hardware
- Chassis and Module Connections
-

The QTS Master Configuration List was used to document the RadICS QTS hardware and firmware tested. The NRC staff also confirmed that all RadICS platform components identified in Table 3.2 1 of this SE are included as a component of the QTS and were thus subjected to the qualification tests performed.

3.6.1 Atmospheric (Temperature and Humidity)

Table 9-1 of the RadICS topical report (Ref. 1) specifies the qualification envelope for temperature and humidity to be 40 to 122 Deg. F (4.4 to 50 Deg. C) and 10 to 90% relative humidity (non-condensing). Environmental test levels are specified to be 35 to 140 Deg. F (1.7 to 60 Deg. C) and 5 to 95% relative humidity (non-condensing), thus encompassing the platform temperature and humidity specifications.

Environmental Temperature and Humidity qualification testing of the RadICS platform test specimen was performed in accordance with EPRI TR-107330 as stated in the EQ test plan. The NRC staff evaluated the Radics LLC EQ test results to determine compliance with the criteria of RG 1.209 and IEEE Std. 323-2003 for mild environment installations and to determine if EQ test plans were being followed. The NRC staff confirmed that EPRI TR 107330, Sections 4.3.6, “Environmental Requirements,” and 6.3.3, “Environmental Testing Requirements,” criteria were met.

Section 4.3.6.2 of EPRI TR-107330 requires that the generic PLC meet its performance requirements over normal and abnormal environmental conditions. Radics LLC specified temperature and humidity environmental test levels that equaled or exceeded these conditions including applied margins and therefore the criterion was met.

The Radics LLC test specimen performance requirements were verified during and following exposure to abnormal environmental conditions, which exceeded the test specification levels listed above, according to a time varying profile that was similar to the profile outlined in IEEE 323 2003. Verification of QTS performance requirements included conduct of both operability and prudency tests as defined in RadICS EQ test plans and test procedures.

The test configuration was designed to produce the worst case expected temperature rise across the module chassis as is specified in Section 6.2.1.1 of EPRI TR-107330.

The Radics LLC QTS was monitored before, during and after each test to confirm that no equipment failures or abnormal functions occurred. System self-diagnostics were also functioning as an integral feature of the RadICS design and no system abnormalities were detected during tests.

To demonstrate PLC performance in specified environmental conditions, Section 4.3.6.3 of EPRI TR-107330 requires that the test PLC operate for the environmental (temperature and humidity) withstand profile given in Figure 4-4 of the TR. Temperature test profiles used for Radics LLC testing are provided in as Figure 6 of Appendix C in the RadICS equipment qualification test summary report (Ref. 8). This profile was found by the NRC staff to be compliant with the methodology outlined in Section 4.3.6.3 of EPRI TR-107330. A pre-qualification acceptance test was performed prior to subjecting the RadICS QTS to the environmental conditions profile and a series of operability checks was performed at various environmental conditions during profile execution. The RadICS QTS operated satisfactorily during these tests and all operability and prudency tests were completed satisfactorily. The NRC staff found that the RadICS platform equipment is therefore acceptable for installations where environmental conditions do not exceed the established qualification envelope. See PSAI 7.4.1.

3.6.2 Class 1E to Non-1E Isolation

Isolation testing of the RadICS QTS was performed in accordance with IEEE Std. 384 and Section 6.3.6 of EPRI TR-107330. IEEE Std. 384-1992 states that: (1) the isolation device prevents shorts, grounds, and open circuits on the Non-Class 1E side from unacceptably degrading the operation of the circuits on the Class 1E side, and (2) the isolation device prevents application of the maximum credible voltage on the Non-Class 1E side from degrading unacceptably the operation of the circuits on the Class 1E side. The details of the tests are described in Appendix I, “Class 1E to Non-1E Isolation Test Summary,” of the RadICS equipment qualification test summary report (Ref. 8).

The class 1E to Non-1E isolation testing was performed at the Kinectrics test facility. The QTS Master Configuration List was used to document the RadICS QTS hardware and firmware tested. The 1E to non-1E isolation testing was performed after completion of Electrostatic Discharge (ESD) testing.

The qualification of the RadICS platform is based on a system design that permits Non-1E connections to the analog and discrete input and output interfaces. Isolation test signals were applied to the lead wires of the following QTS input and output points:

- Analog Input
- Discrete Inputs
- Analog Outputs
- Discrete Outputs
- RS 232/485 (on OCM)

The RadICS communication interfaces were not tested because these networks use fiber optic cable connections, which are incapable of transmitting electrical faults.

The RadICS Equipment Qualification Summary Report (Ref. 8) documents the results of the execution of RadICS 1E to Non-1E Isolation test procedure. The summary is the result of the executed test plan that addressed the test approach, equipment to be tested, sequence of testing, test procedures, test specimen mounting, service conditions, test levels, performance monitoring, acceptance criteria, and documentation.

QTS isolation test inputs were subjected to test voltage levels of 250 VAC and 250 VDC for 30 seconds. During tests, the operation of the QTS was monitored and system performance data was recorded.

The NRC staff confirmed the following: For analog inputs, the group to group applied voltages were greater than 30 volts peak. For discrete AC inputs, applied group isolation test voltages were greater than maximum voltage which would be applied if a line-to-line short to a three conductor 120 VAC cable occurred. For discrete DC inputs, applied group isolation test voltages were greater than 250 volts which is specified in Section 4.6.4 of EPRI TR-107330. For discrete AC outputs, applied group isolation test voltages were greater than maximum voltage which would be applied if a line-to-line short to a three conductor 120 VAC cable occurred. For discrete DC outputs, applied group isolation test voltages were more than twice the normal output signal level.

The NRC staff also confirmed that during these tests, the RadICS module interfaces were subjected to test voltage levels for greater than 30 seconds. Test results showed no disruption in operation of any other module within the QTS or disruption in operation of the RadICS chassis backplane. Application of test voltages did not cause a change of greater than 0.05% to another channel in the same module. Operability and prudency testing of the QTS was conducted before and after Class 1E to Non-1E Isolation testing. Results of these tests showed no degradation of RadICS QTS occurred during isolation testing.

The NRC staff reviewed the qualification test summary report (Ref. 8) and determined that the RadICS platform met the criteria of IEEE Std. 384-1992 and Sections 4.6.4 and 6.3.6 of EPRI TR-107330. It is the responsibility of the license to verify that maximum test voltages cited in the equipment qualification summary report to which the RadICS equipment is qualified to operate are not exceeded for all RadICS 1E to Non-Class 1E interfaces (see PSAI 7.4.2).

3.6.3 Electromagnetic Interference / Radio Frequency Interference

Regulatory Guide 1.180, Rev. 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-Related Instrumentation and Control Systems,” endorses MIL-STD -461E, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” and IEC 61000 series standards for the evaluation of the impact of EMI, radio-frequency interference (RFI) and power surges on SR Instrumentation and Control systems, and to characterize the electromagnetic (EM) emissions from the Instrumentation and Control systems.

EPRI TR-107330 includes electromagnetic compatibility (EMC) testing as part of the overall program to generically qualify a PLC for SR application in a NPP. Specific criteria for electromagnetic emissions, EMI susceptibility, electrostatic discharge withstand, power surge withstand, and isolation capability are given in Sections 4.3, “Hardware Requirements,” and 4.6, “Electrical,” of the guide while the qualification approach is specified in Section 6.3, “Qualification Tests and Analysis Requirements.”

EPRI TR-102323, “Guideline for Electromagnetic Interference Testing in Power Plants,” provides alternatives to performing site-specific EMI/RFI surveys to qualify digital safety Instrumentation and Control equipment for a plant’s Electro Magnetic environment. In a SE issued in 1996, the NRC staff concluded that the recommendations and guidelines in EPRI TR-102323 provide an adequate method for qualifying digital I&C equipment for a NPP’s EM environment without the need for plant-specific EMI/RFI surveys if the plant-specific EM environment is confirmed to be similar to that identified in EPRI TR-102323.

RadICS equipment environmental testing is described in the RadICS platform TR as follows:

- EMI and RFI qualification testing for the RadICS platform is described in Section 9.1.2.5.
- Electrical Fast Transient (EFT) testing is described in Section 9.1.2.6.
- Surge Withstand testing is described in Section 9.1.2.7.
- ESD testing is described in Section 9.1.2.8.

EMI, RFI, EFT, Surge Withstand, and ESD testing of the Radics LLC QTS was performed in 2018 at the UltraTech test facility in Toronto, Canada. The Radics LLC QTS was installed in the EMI/RFI test chamber in accordance with test specimen mounting criteria of EPRI TR-107330, Section 6.3.2.1 as specified in the test plan. The QTS was mounted in a single open chassis. The test grounding and shielding configuration was established in accordance with IEEE Std. 1050-1996 criterion.

The power to the QTS was supplied from a QTS 24 VDC power supply. This power supply was not included as part of the QTS and is therefore not qualified as a component of the RadICS platform.

The RadICS platform QTS components were subjected to EMI/RFI testing to demonstrate compliance with the applicable EMI/RFI emissions and susceptibility requirements of NRC RG 1.180. The specific test configuration of the Radics LLC equipment is described in Section 5.0, “Test System,” of the RadICS Equipment Qualification Test Summary Report (Ref. 8). The sections that follow describe tests performed and summarize the results obtained.

3.6.3.1 EMI/RFI Interference

EMC testing was performed in accordance Radiy LLC QTS. The specific EMI/RFI Emissions tests performed for the RadICS QTS are listed below:

- MIL-461E, CE101: “Conducted Emissions, AC and DC Power Leads, (30 Hz to 10 kHz)”
- MIL-461E, CE102: “Conducted Emissions, AC and DC Power Leads, (10 kHz to 2 MHz)”
- MIL-461E, RE101: “Radiated Emissions, Magnetic Field, (30 Hz to 100 kHz)”
- MIL-461E, RE102: “Radiated Emissions, Electric Field, Antenna Measurement (2 MHz to 1 GHz for radiated emissions and 1 GHz to 10 GHz for radiated susceptibility)”

3.6.3.2 EMI/RFI Susceptibility

EMI/RFI Susceptibility tests performed for the RadICS QTS as follows:

- IEC 61000-4-6: “Conducted Susceptibility, Induced RF Fields, Power/Signal Leads, (150 KHz to 80 MHz)”
- IEC 61000-4-16: “Conducted Susceptibility, Common Mode Disturbance, Power/Signal Leads, (15 Hz to 150 kHz)”
- IEC 61000-4-8: “Radiated Susceptibility, Magnetic Field, Helmholtz Coil Exposure, (60 Hz)”
- IEC 61000-4-9: “Radiated Susceptibility, Magnetic Field, Pulsed, (60 Hz)”
- IEC 61000-4-10: “Radiated Susceptibility, Magnetic Field, Damped Oscillatory, (100 kHz to 1 MHz)”
- IEC 61000-4-3: “Radiated Susceptibility, High Frequency, Antenna Exposure, 26 MHz to 1 GHz)”
- MIL-STD-461 E, RS103: “Radiated Susceptibility, High Frequency, Antenna Exposure (1 GHz to 10 GHz)”

3.6.3.3 Electrostatic Discharge Withstand Testing (Appendix F)

EPRI TR-107330, Section 4.3.8, ESD Withstand Requirements,” states that PLC platforms and associated devices shall have ESD withstand that conforms to EPRI TR-102323, Revision 1. The RadICS ESD testing was performed in accordance with the Radics LLC qualification test plan. This test conformed to the specific ESD Test methods defined in IEC 61000-4-2, Electromagnetic Compatibility (EMC), Part 4-2, “Testing and Measurement Techniques, Electrostatic Discharge Immunity Test.”

3.6.3.4 Electrical Fast Transient Susceptibility (Appendix G)

The following electrical fast transient susceptibility tests were performed for the RadICS QTS:

- IEC 61000-4-4, “Power Leads: Test Voltage Level: 2 kV maximum”
- IEC 61000-4-4, “Signal Leads: Test Voltage Level: 1 kV maximum”

3.6.3.5 Surge Withstand Capability (Appendix H)

The following surge withstand tests were performed for the RadICS QTS:

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

3.6.3.6 EMI / RFI Test Results

The EMI/RFI test acceptance criteria for the RadICS QTS included monitoring of equipment performance before during and after each test. Detailed test acceptance criteria are described in the summary of RadICS “Equipment Qualification Test Summary Report” (Ref. 8).

This report also includes test results summaries for these tests. The NRC staff reviewed these acceptance criteria and confirmed test results as follows:

- There was no disruption of QTS operation during these tests.
- There was no disruption of the QTS backplane signals that could result in a loss of the ability to generate a trip.
- The test did not cause damage to or failure of any components of the QTS.
- The RadICS QTS met allowable equipment emission limits as specified in RG 1.180, Revision 1, for conducted and radiated emissions.
- The RadICS QTS operated as intended during and after application of the EMI/RFI test levels specified in RG 1.180 for conducted and radiated susceptibility.
- Evaluation of normal RadICS QTS operating performance data (inputs, outputs, and diagnostic indicators) demonstrated operation as intended.
- The emissions did not cause the discrete I/O states to change.
- Analog I/O levels did not vary by more than 3 percent and calibration accuracy was checked following tests.
- QTS self-diagnostic data indicated correct operation of the power supply assembly, the cooling fan assembly, the LM, the I/O modules, and QTS communications.

The NRC staff reviewed Appendices E through H of the RadICS Equipment qualification summary report and determined that the tested Radics LLC system met the EMI/RFI test acceptance criteria discussed above and is qualified for operation up to the tested limits described above. Operability and prudency tests were also performed before and after EMI/RFI test activities.

Before using the RadICS platform equipment in SR systems in NPP, licensees must determine that plant-specific EMI requirements do not exceed the capabilities of the Radics LLC system as approved in this SE. This determination and the suitability of the Radics LLC system for a particular plant and application are the responsibility of the licensee. See PSAI 7.4.3.

3.6.4 Seismic Qualification

Regulatory Guide 1.100, Revision 3 describes methods that the NRC staff considers acceptable for use in seismic qualification of electrical and active mechanical equipment. The regulatory guide provides an endorsement of IEEE Std. 344-2004 with exceptions and clarifications. Clause 5 of IEEE Std. 344-2004, states:

> "The seismic qualification of equipment should demonstrate an equipment's ability to perform its safety function during and/or after the time it is subjected to the forces resulting from one Safe Shutdown Earthquake (SSE). In addition, the equipment must withstand the effects of a number of Operating Basis Earthquakes (OBEs) prior to the application of a SSE."

An OBE is a seismic event during which all equipment necessary for continued plant operation without undue risk to the health and safety of the public is required to remain functional. An SSE is the maximum considered earthquake in the design of a nuclear power plant and the earthquake for which structures, systems and components (SSCs) important to safety are designed to remain functional.

Regulatory Guide 1.61, Rev. 1, “Damping Values for Seismic Design of Nuclear Power Plants,” establishes evaluation guidance for applicants and licensees regarding the acceptable damping values to be used in the elastic dynamic seismic analysis and design of SSCs, where energy dissipation is approximated by viscous damping.

Section 4.3.9 of EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for safety-Related Applications in Nuclear Power Plants,” provides additional guidance for establishing seismic withstand requirements for digital protection systems.

Prior to performing the OBE and SSE tests, a resonance search procedure was conducted to confirm no abnormalities in cabinet structure or mounting and to identify QTS resonance points. Though several resonant frequencies were identified during this test, all occurred at frequencies greater than 33 Hz. These resonances were analyzed and the QTS was determined to be rigid.

Table 9-1, “Generic Qualification Envelope for the RadICS Digital Safety I&C Platform,” of the RadICS platform TR specifies the seismic qualification requirements to be 5 triaxial OBE tests with a Required Response Spectrum (RRS) curve given as Figure 4-5 in EPRI TR-107330 with a peak acceleration of 9.8 g between 4.5 and 16 Hz and minimum zero period acceleration (ZPA) of 4.9 g followed by one triaxial SSE test with a RRS curve given as Figure 4-5 in EPRI TR-107330 with a peak acceleration of 14 g between 4.5 and 16 Hz and minimum ZPA of 7 g. These requirements are for seismic category 1 safety systems. The maximum SSE and OBE levels shown in Figure 4-5 of EPRI TR-107330 are (maximum acceleration) 14 g and 9.75 g respectively, at frequencies greater than 3 Hz, based on 5% damping. Since the RadICS design is generic, there is no plant specific SSE or OBE acceleration level with which to evaluate and compare test results with. Instead, the test acceleration levels listed above represent the qualified envelope established for RadICS platform. Therefore, licensees referencing this SE must ensure their plant-specific In-Equipment Response Spectra (IERS) are enveloped by the RadICS platform Test Response Spectrum qualification envelope. See Plant-Specific Action Item 7.4.4.

To demonstrate that the RadICS platform meets the requirements for Seismic Category 1 safety system, the QTS was subjected to accelerated aging, by performing OBE tests, followed by a seismic stimulation test representing SSE conditions.

Seismic Testing was performed in accordance with the requirements of RG 1.100, Revision 3, and IEEE Std. 344-2004. Seismic tests were performed at the Kinectrics test facility in Toronto, Canada in March of 2018. A system level cabinet test specimen intended to represent a fully loaded safety RadICS chassis was used during the qualification test. The RadICS test chassis was the same chassis that was used during other equipment qualification tests. The NRC staff reviewed the equipment test subject component list as well as the equipment under test layout configurations and documented in the RadICS Equipment Qualification Test Summary Report (Ref. 8). The NRC staff confirmed that a reasonable representative configuration was employed.

A summary of seismic test results was provided in Appendix D of the RadICS Equipment Qualification Test Summary Report (Ref. 8). Resonance tests confirmed no abnormalities in cabinet or component structures.

Chassis and component physical integrity and correct functional operation of QTS were verified before, during and after excitation.

The NRC staff reviewed the seismic test specifications defined in the equipment qualification test plan (Ref. 38), and confirmed the acceleration levels to be consistent with Radics LLC cabinet and component specifications identified in Table 9-1 of the RadICS TR. The NRC staff reviewed the test frequency spectra and confirmed that specified qualification motion acceleration levels were achieved for the qualification frequency range.

An applicant referencing this SE will need to confirm that RadICS platform equipment seismic qualification levels are within plant specific design basis seismic conditions for SSE and OBE earthquakes. This is PSAI 7.4.4.

Acceleration levels specified for generic plant SSE in EPRI TR-107330 are greater than the acceleration envelope established for RadICS equipment. Because of this, RadICS platform equipment does not meet the criteria for generic seismic qualification.

The results of the seismic test show that:

- Seismic testing of the Radics LLC QTS was performed in accordance with the criterion of IEEE Standard 344-2004.
- The Radics LLC QTS met all applicable performance requirements before, during and after application of the seismic test vibration levels.
- Results of the operability tests performed after seismic testing show that exposure to the seismic, test conditions had no adverse effect on the RadICS QTS performance.
- The seismic test results demonstrate that the RadICS platform is suitable for qualification as seismic Category 1 equipment.
- The seismic test results demonstrate that the representative equipment mounting configurations used during testing are adequate to support seismic qualification of RadICS based safety systems.
- Seismic withstand performance requirements were not demonstrated for the maximum acceleration level of 14G for a generic SSE.

The NRC staff reviewed the RadICS seismic test results and confirmed that the seismic acceleration levels to which the representative platform components were tested met or exceeded the seismic resistance specifications for the RadICS platform as provided in Table 9-1 of the RadICS Platform Topical Report (Ref. 1).

Based on review of the RadICS seismic test results and supporting analysis, the NRC staff determined that the RadICS platform does not fully satisfy the guidance criteria of EPRI TR-107330 because seismic withstand performance requirements were not demonstrated for the maximum acceleration level of 14G for a generic SSE. However, the NRC staff finds that seismic qualification of the RadICS platform has been acceptably demonstrated for OBE and SSE events up to acceleration levels shown in the OBE and SSE test results spectra in the RadICS Equipment Qualification Test Report (Ref. 8). The use of Radics LLC system equipment for the performance of safety system functions in a nuclear power plant, requires licensees to determine that plant-specific seismic requirements do not exceed RadICS system seismic withstand capabilities. A Plant using the RadICS platform is therefore required to establish plant specific seismic criteria for the system to be installed. Licensees referencing this

SE should ensure their plant-specific IERS are enveloped by the RadICS platform Test Response Spectrum qualification envelope. See PSAI 7.4.4.

3.7 RadICS platform Integrity Characteristics

The NRC SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," states that a special concern for digital computer-based systems is confirmation that the real time performance of the system is adequate to ensure completion of protective actions within the critical time periods identified within Clause 4.10 of IEEE Std. 603-1991. SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provides supplemental guidance to evaluate the real-time performance of digital systems and architectures and discusses the identification of bounding real-time performance specifications and the verification of these specifications to demonstrate real-time performance. The establishment of predictable performance and behavior for a platform supports the future evaluation of a safety system that is based on the platform. The following sections describe performance capabilities of the RadICS platform.

3.7.1 RadICS platform Response Time

10 CFR Part 50, Appendix A, GDC 20, 21, 23, and 25 constitute general requirements for timely operation of the protection features. To support these requirements, SRP BTP 7-21 provides the following guidance:

- The feasibility of design timing may be demonstrated by allocating a timing budget to components of the system architecture to ensure that an entire system meets its timing requirements.
- Timing requirements should be satisfied by design commitments.

Two regulations provide the basis for this guidance. The first is 10 CFR 50.55a(h) and its incorporation of IEEE Std. 603-1991 by reference. The second is 10 CFR 50.36(c)(1)(ii)(A), which provides basis for timing by requiring the inclusion of the limiting safety systems settings for nuclear reactors in the plant technical specifications, "so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded."

Each licensee should provide its plant-specific safety function response time design bases as response time performance requirements to be satisfied by the safety system. The actual response time of a RadICS safety system will be determined by its overall configuration for a plant specific application; therefore, each licensee must determine that the RadICS platform response time characteristics are suitable for its plant-specific application (see PSAI 7.3). The following information addresses the use of RadICS platform response time characteristics in support of future plant-specific suitability determinations.

The RadICS TR, Section 6.10, "Timing Diagrams and Work Cycles," describes platform timing performance characteristics. Response times for a RadICS platform-based safety system are determined by fixed work cycles of the FPGAs that control the operation of the systems safety functions. Once a RadICS system is initialized and placed into operation the internal modules of that system operate on a fixed duration work cycle which is not dependent on the logic functions performed. All functions of the RadICS system, including input processing, application logic processing and output processing, are performed during each work cycle. The work cycle

duration for each RadICS module is defined by platform specifications and is tested by RPC Radiy as part of platform design verification and validation testing. Platform components are further verified during the CGD process for each module. Module critical characteristics include module functional and performance characteristics. Tests are performed documented and reviewed in accordance with the Radics LLC CGD processes to verify that module functional and performance characteristics are met.

Section 6.10 of the RadICS TR also includes a timing analysis, which provides timing allocations for each of the following system functions:

- Receive and transmit data to and from input modules to the LM,
- Perform application logic processing in the LM,
- Transmit results of application logic processing to system output modules, and
- Pause to allow output elements in the output modules to transition to the new state.

The NRC staff notes that communication times associated with transmitting data between input and output modules and the LM are included as elements of the overall LM work cycle. Timing diagrams of the RadICS work cycle are also provided to show that cumulative time elements support the overall work cycle time period. The work cycle time period is fixed and is not dependent on a system configuration or application specific design. The response time characteristics of the resulting safety functions are deterministic because they are predictable, not variable, repeatable, and measurable.

The TR also provides a second timing diagram, which shows timing associated with communications between two RadICS platforms. A system configuration that relies upon communication between separate RadICS chassis would need to account for the additional amount of time needed to assure transfer of data. An example of this would be a safety system channel that sends trip decision information to a separate RadICS voter chassis which would in turn drive actuation logic to perform required trip functions. In such a system, the time response characteristics of each separate RadICS chassis, as well as, the data communication time would need to be accounted for.

Though individual RadICS module response times are deterministic, actual system level response times may depend on the number and types of communications interfaces being used to implement system specific requirements. The method described in the TR provides a means of determining the system response time once the application design configuration becomes available to the developer. This method includes allocation of a timing budget to all components of the RadICS system architecture.

To satisfy a typical response time performance requirement for a plant specific application, a RadICS platform-based system must acquire and condition the input signals representing the start of a response time performance requirement, transmit the signal to the RadICS LM, perform logic processing, generate an output signal, and transmit the output to the output module, which represents the end of a response time performance requirement for a specified application process. These RadICS platform response time components do not include (1) the earlier plant process delays through the sensor input to the platform and (2) the latter delays through a final actuating device to affect the plant process. Therefore, the licensee's plant-specific safety function response time design bases should address these response time components separately from the response time performance requirements specified for the licensee's RadICS platform-based system. Testing must also be performed to confirm RadICS

system response time performance to assure that plant specific time response requirements are met. See PSAI 7.3.

3.7.2 Determinism

The review guidance of SRP Chapter 7, Appendix 7.1-C, Section 6.1, "Automatic Control," identifies considerations that address digital computer-based systems for the evaluation of the automatic control capabilities of safety system sense and command features. This review guidance advises that the evaluation should confirm that the system's real time performance is deterministic and known. SRP BTP 7-21 discusses design practices for computer-based systems that should be avoided, and these practices include non-deterministic data communications, non-deterministic computations, interrupts, multitasking, dynamic scheduling, and event-driven design. SRP BTP 7-21 further states that methods for controlling the associated risk to acceptable real time performance should be described when such practices are employed.

EPRI TR-107330 provides specifications and guidance intended to achieve a deterministic execution cycle with deterministic behavior that ensures an application and its constituent tasks will be completed within specified time limits. In particular, EPRI TR-107330, Section 4.4.1.3, "Program Flow Requirements," specifies that, where scanning of the inputs and application program execution are performed in parallel, methods should assure that the input scan and application program execution are completed each cycle.

RadICS control processes are performed by the systems modules in accordance with defined deterministic work cycles of the module FPGAs. Section 6.10 of the RadICS TR describes each of the control processes included in the working cycles of the RadICS system and provides a method for determining the processing time of a work cycle based on a specific system configuration. This method provides a means of determining the minimum and maximum cycle time based upon the Radics LLC hardware configuration details. Once, known, this work cycle overall response time provides assurance that each consecutive process is completed prior to initiation of the next cyclic process.

The RadICS FPGA design does not incorporate or use interrupts. System ED logic is executed in accordance with pre-defined logic configurations and all logic functions are completed during each work cycle of each FPGA in the system. Initiation of subsequent work cycles occurs only upon completion of the previous work cycle. Each RadICS module performs its assigned logic functions independently of all other modules in the system and therefore each module operates at a known deterministic periodic rate. When data transfer is required to support completion of a safety function, the maximum cycle time for all system modules involved in the data transfer operation is considered in the timing analysis. Because modules operate asynchronously from each other and because they may have different work cycle periods, the timing analysis includes provisions for a second cycle to insure function completion of all required logic operations. The resulting response time characteristics of the safety functions are deterministic because they are predictable, and not variable, and because they are repeatable, and measurable.

The RadICS module ED development process includes performance of a Static Timing Analysis (STA) activity. The STA is performed during the place and route stage of FPGA development as a V&V activity to establish FPGA ED timing characteristics and to determine if module timing requirements are achievable as part of a timing simulation prior to implementation of the ED

onto the FPGA hardware. The STA is successfully completed if the ED Netlist files are free of timing violations against predefined timing constraints. Timing performance of RadICS hardware after ED implementation is then verified on the equipment during factory tests.

The NRC staff determined that design features, operation of the RadICS system, and PSAI 7.3 provide sufficient confidence that RadICS based safety systems will operate deterministically to meet the recommendations of BTP 7-21 and is therefore acceptable.

3.7.3 Self-Diagnostics / Test and Calibration Capabilities

The regulation at 10 CFR Part 50, Appendix A, GDC 21, requires in part that the protection system be designed for in-service testability commensurate with the safety functions to be performed. It also requires a design that permits periodic testing of its functioning when the reactor is in operation, including the capability to test channels independently to identify failures and losses of redundancy that may have occurred.

RadICS platform diagnostics features are described in Section 6.4 of the RadICS TR. Diagnostics are executed at both the application and the platform level to detect failures that are potentially unsafe. These failures converted to safe events by setting all safety outputs to safe states. Application level diagnostics should be evaluated by the licensee.

The general diagnostics concepts used in the RadICS design include three groups of self-diagnostic functions. These are: hardware self-diagnostics, interface and data transmission self-diagnostics, and platform ED self-diagnostics. These diagnostics functions are specifically designed to detect and respond to anticipated system failure modes. The RadICS TR describes three fault types. Self-diagnostic functions are designed to mitigate these faults. These fault types are:

Type I – Faults that result in platform control logic being unable to guarantee a trip to the safe state, which is a de-energized state for RadICS based systems.
Type II – Faults that result in hardware or part of the ED to be incapable of performing its functions but do not affect the system's ability to initiate the safe state.
Type III – User defined level faults. The user defines criticality of detected errors and their processing algorithm. The responses to Type III faults are not addressed by the RadICS platform design. Methods to identify and mitigate these faults must be implemented within application design during plant specific development activities.

EPRI TR-107330 provides guidance and requirements applicable to PLC-based system's diagnostics and test capability so that the combination of self-diagnostics and surveillance testing will detect failures that could prevent a PLC from performing its intended safety function. The range of conditions for which diagnostics or test capabilities are to be provided includes processor stall, executive program error, application program error, variable memory error, module communications error, module loss of configuration, excess scan time detection, application not executing, and field device (e.g., sensor, actuator) degradation or fault. The means of detection include watchdog timer, checksum for firmware and program integrity, read/write memory tests, communications monitoring, configuration validation, heartbeat, and self-diagnostics or surveillance test support features. EPRI TR-107330 identifies diagnostics that are executed upon power-up and diagnostics that run continuously thereafter.

The RadICS platform self-diagnostics as described in Section 6.4 of the TR use multiple methods of identifying system faults. These methods include monitoring of system power sources, watchdog functions, communications data validation, logic configuration integrity checks, and memory checking. Both startup diagnostics and continuous run time diagnostic functions are included in the RadICS design.

RadICS self-diagnostics test functions can be used to support compliance to GDC 21. However, determination of full compliance with this criterion is dependent on the specific safety system design as well as the plant specific safety functions performed by the system. Therefore, determination of GDC 21 compliance is a plant-specific evaluation item. See PSAIs 7.8 and 7.9.1.

IEEE Std. 603-1991, Clause 5.7 states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability shall be provided during power operation, and shall duplicate, as closely as practicable, performance of the safety function. IEEE Std. 603-1991, Clause 5.7 allows exceptions to testing and calibration during power operation.

The PSWD unit described in Section 3.2.2.2 of this SE performs platform self-diagnostics functions described in this section. RadICS self-diagnostics test functions can be used to support justification for such exceptions or to support compliance with system test and calibration requirements. However, determination of full compliance with these criteria is dependent on the specific safety system design as well as the plant specific safety functions performed by the system. Therefore, determination of IEEE Std. 603, Clause 5.7 compliance is a plant-specific evaluation item. See PSAI 7.8.

SRP, Chapter 7, Appendix 7.1-C, Section 5.7, “Capability for Test and Calibration,” includes criteria for test provisions of digital computer-based systems. It states that licensees should address the increased potential for system failures such as data errors and computer lockup. See PSAI’s 7.5, and 7.9.1.

The NRC staff found that RadICS self-diagnostics functions capable of addressing the RadICS system failures by identifying expected failures and by providing the capability to annunciate such failures to the operator. Including these capabilities in a system design is a Plant Specific Action Item. See PSAI 7.9.1.

SRP BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” states that automatic diagnostics and self-test features should preserve channel independence, maintain system integrity, and meet the single-failure criterion during testing. Additionally, the benefits of diagnostics and self-test features should not be compromised by additional complexity that may result from the implementation of diagnostics and self-test features. The scope and extent of interfaces between safety software and diagnostic software such as self-test routines should be designed to minimize the complexity of the integrated software.

Based on RadICS platform development processes, and platform validation test results, the NRC staff found that RadICS platform self-diagnostics do not adversely affect channel independence or system integrity. See PSAI 7.8. Radics LLC self-diagnostic features were not found to be exceedingly complex and thus would be unlikely to adversely affect safety functions of the system during operation. The RadICS self-diagnostics can be used to support the single

failure criterion during testing; however, compliance with single failure criteria must be addressed on a plant specific basis.

A combination of self-tests, periodic testing, and surveillance are necessary to successfully detect failures and support effective maintenance of a RadICS based system for a plant specific application. Specifically, periodic surveillance tests must be performed to detect failures or problems that are not detectable by platform self-diagnostic functions. The RadICS design includes provisions for incorporation of application ED features to address application specific failure modes (Type III faults). Maintenance activities including periodic surveillance testing will be defined based on plant-specific application requirements. In addition, methods of failure management must be defined for a plant-specific application. See PSAI 7.9.1.

3.8 Setpoint Determination Methodology

The RadICS TR includes Section 9.2.2, “Setpoint Analysis Support,” to support the NRC staff evaluation of instrument setpoints criterion. This Section describes a separate analysis support document that lists the accuracy, drifts, and other relevant specifications of the RadICS digital safety platform that are needed by a licensee to support performance of a system specific setpoint analyses. Such an analysis would be used to establish new or to validate existing system setpoints. Though determination of safety system setpoints is a plant-specific activity that cannot be evaluated at the generic platform level, the methods used for performing this activity are outlined in the TR.

The NRC staff reviewed the RadICS setpoint analysis support methodology using the criteria of IEEE Std. 603 1991, Clause 6.8, BTP 7-12, Revision 6, “Guidance on Establishing and Maintaining Instrument Setpoints,” and RG 1.105, “Setpoint for safety-related instrumentation.” The RadICS methodology considers factors that have the potential to affect the instrument uncertainties for analog input and analog output processing of a RadICS based system. The RadICS contribution to instrument uncertainties at various temperatures are provided in a setpoint analysis support document. Other factors considered in the method include repeatability, instrument drift, power supply voltage variation, operating humidity level, and arithmetic operations errors. This allows licensees to assess the effects of conditions resulting from design basis events on instrument accuracy. The NRC staff determined the methods outlined in the Radics LLC setpoint analysis support methodology to satisfy the criteria of RG 1.105. These methods therefore provide an acceptable process for determining setpoints to be used in a RadICS platform-based safety system. See PSAI 7.7 for licensee required actions for addressing system setpoints when using a RadICS platform-based system.

3.9 Diversity and Defense-in-Depth.

Digital instrumentation and control (DI&C) systems can be vulnerable to common-cause failure (CCF) caused by software errors or software developed logic, which could defeat the redundancy achieved by hardware architecture.

This Section describes and evaluates the diversity strategy used for the RadICS platform design. This includes an evaluation of the component designs and principles of operation for RadICS platform-based systems. This evaluation provides limited safety conclusions because the demonstration of adequate diversity and defense-in-depth (D3) requires the context of a specific nuclear power plant’s overall D3 analysis to address mitigation of vulnerabilities, which are inherently plant-specific. See PSAI 7.9. Therefore, this evaluation is limited to the methods

for addressing diversity within a RadICS platform-based system. This evaluation considers the RadICS principles of operation, platform design and process attributes that can either preclude or limit certain types of CCFs.

NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," dated February, 2010, builds upon NUREG/CR-6303 and provides guidance to the NRC staff and nuclear industry for use after an applicant or licensee has performed a D3 assessment per NUREG/CR-6303 and determined some diversity in a safety system is needed to mitigate the consequences of potential CCFs identified through a prior evaluation of safety system design features. NUREG/CR-7007 evaluates the characteristics and efficacy diversity strategies.

BTP 7-19 Evaluation

Section 10 of the RadICS TR, as supplemented by Reference 7, identifies four defensive measures to provide protection against CCFs. These measures are: (1) Development Process Quality (2) Hardware Independence principals, (3) Platform diversity, and (4) Defense-in-Depth. Section 10.3.3 provides a RadICS Platform Diversity Assessment. This Section specifically identifies technology specific CCF vulnerabilities of the RadICS equipment and describes internal diversity design features of the equipment, which provide protection to address these vulnerabilities.

BTP 7-19 states that a D3 evaluation should demonstrate plant vulnerabilities to CCFs have been adequately addressed in the context of an overall suite of I&C systems. Furthermore, BTP 7-19 establishes a position, which recognizes that software based, or software logic based digital system development errors are a credible source of CCF. BTP 7-19 provides guidance to evaluate the applicant's or licensee's D3 assessment, including the design of manual controls and displays to ensure conformance with the NRC positions on D3. Though the RadICS platform does not use software, it does use programmable logic that is based on a hardware descriptive language that is similar to the instruction-based languages used in software systems. Therefore, the NRC staff considers the criteria of BTP 7-19 to be applicable to the RadICS platform design.

The RadICS platform cannot be confirmed to meet all of the NRC staff positions within BTP 7-19 because a system level D3 assessment requires availability of a system specific design. Therefore, a plant specific evaluation must be performed at the time of application development. This is PSAI 7.9. The RadICS platform does, however, include several internal design features that can be credited by a licensee to meet or support the criteria of BTP 7-19. These diverse design features are discussed and evaluated below.

BTP 7-19 Point 1 states the following:

> The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.

The RadICS TR does not include a plant specific application. Therefore, the effects of a CCF on plant operation or plant safety cannot be assessed as part of this SE and instead must be addressed by a licensee during application development. The RadICS platform does however

contain design features described in Section 10 of the RadICS TR including protective measures for identifying and mitigating platform component CCFs. A licensee can credit these features in a plant specific D3 assessment to determine if common mode failures of the RadICS based system have been adequately addressed. See PSAI 7.9.

BTP 7-19 Point 2 states the following:

> In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis Section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

The RadICS FMEDA identifies the effects of postulated failures on the RadICS equipment performance. As such, this document provides essential platform specific information that a licensee can use in performing the D3 assessment. [

]

Because the RadICS TR does not include a plant specific application or plant specific accident analysis on which to base a D3 analysis, the NRC staff is unable to determine that a RadICS based safety system will meet the criteria of BTP 7-19 Point 2. However, it is evident that mitigation features of the RadICS design can be used by a licensee to support a subsequent plant specific D3 analysis to meet this requirement. Conformance with these criteria should therefore be addressed as part of PSAI 7.9.

BTP 7-19 Point 3 states the following:

> If a postulated common-mode failure could disable a safety function, then a diverse means with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

Equipment, which is independent from the primary means to provide a safety function and implements the diverse means, is commonly referred to as a diverse actuation system. Some RadICS platform design features can be credited as [

]

Section 10 of the RadICS TR, “Diversity and Defense-In-Depth,” as supplemented by Reference 7, describes measures employed in the RadICS platform design to provide defense

against CCFs at the system level. [

]

Section 10.3.3 of the RadICS TR, “RadICS Platform Diversity Assessment,” as supplemented by Reference 7, describes several internal diversity features [

] in RadICS modules.

The RadICS platform design includes [

] See PSAI 7.9.

To address the potential for incorrect FPGA logic implementation error, the RadICS TR refers to the quality of the development process as an additional defensive measure to protect the system against CCFs. Evaluation of these development processes is provided in Section 3.5 of

this SE. However, the NRC does not recognize the quality of the development processes as a diverse means to perform either the same function or a different function in the event of a CCF. Point 3 of BTP 7-19 states the following in regard to independence requirements of a diverse protection system:

> The independence requirements of a diverse protection system from the safety protection system (i.e., physical, electrical, and communication separation) are defined in IEEE Std 603-1991. The diverse means could be safety-related and part of a safety division and would then be subject to meeting divisional independence requirements. The diverse means could also be nonsafety-related in which case the IEEE Std 603-1991 requirement to separate safety-related equipment from that which is not safety-related would still apply and would require independence of the two systems. In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system.

As previously mentioned, each module [

]

Though similar logic development life cycle processes are used for the FPGA and CPLD programming, the [

] described in Section 3.2.3.1.2 of this SE. This communication [

]

[

]

The NRC staff reviewed the characteristics of the [ ] as provided in Section 10.3.3 of the RadICS TR, as supplemented by Reference 7, and determined that the [

] are classified as safety-related, they are of sufficient quality to perform the necessary function under the associated event conditions. The RadICS platform design therefore meets the independence criteria of BTP 7-19, Point 3.

The NRC staff's evaluation of the RadICS TR addresses the BTP 7-19 Point 3 topics of "Adequate Diversity" and "Manual Operator Actions" which state, in part, the following:

> … When an independent and diverse method is needed as backup to an automated system used to accomplish a required safety function, the backup function can be accomplished via either an automated system, or manual operator actions performed in the main control room. The preferred independent and diverse backup method is generally an automated system. The use of automation for protective actions is considered to provide a high-level of licensing certainty. If automation is used as the backup, it should be provided by equipment that is not affected by the postulated RPS CCF …

When manual operator actions are used to provide a backup for functions performed by a RadICS based safety system, these actions should use independent and diverse equipment that is not affected by postulated CCFs. Consistent with the requirements of IEEE Std. 603-1991, Clause 6.2, "Manual Control," and applicable BTP 7-19 guidance, the point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs and should achieve system-level actuation at the lowest possible level in the safety system architecture. The controls may be connected either to discrete hardwired components or to simple, dedicated, and diverse, digital equipment that performs the coordinated actuation logic. Manual controls are not within the scope of this evaluation and must be addressed as a plant specific action. See PSAI 7.9.3.

Evaluation of RadICS Platform Diversity Using NUREG/CR-7007

Section 10 of the RadICS TR describes system and design features of the RadICS platform that provide diversity to address the potential for platform and application logic CCF. Though not required for this evaluation, the NRC staff used NUREG/CR-7007 as a tool to obtain information on the relative degree of diversity achieved by the RadICS platform design. The results of this effort were used to inform the safety conclusions of this evaluation but were not used as a basis for these conclusions. The NRC staff reviewed the content of Section 10 of the TR, as supplemented by Reference 7, to evaluate manufacturer claims regarding the ability of RadICS platform design and process attributes to either preclude or limit certain types of CCFs.

Table 3.8-1, below, provides a summary of the NRC staff's evaluation of RadICS diversity strategies in relation to the baseline diversity strategies presented in NUREG/CR-7007. This data is provided for information only, however, a licensee using the RadICS platform wishing to credit the platforms diverse design features may use this information to support its method of addressing logic CCFs in the system.

Table 3.8-1 Evaluation of RadICS Diversity Strategies

NUREG/CR-7007 Diversity Strategy	**Summary of NRC Staff Evaluation**
1) Design "RadICS Diversity Assessment" (see Reference 7, Section 10.3.3)	The RadICS platform equipment is designed using an FPGA manufacturer's technology on circuit boards within a defined instrumentation architecture and framework. RadICS modules include [

	] The NRC staff determined the RadICS platform approach to design diversity contributes to diversity of two equipment designs that use different approaches within a similar technology (NUREG/CR-7007, Section 2.2.3.1).
2) Equipment Manufacturer "RadICS Diversity Assessment" (see Reference 7, Section 10.3.3)	The RadICS platform equipment is designed by a [ ] There is no [ ] than the FPGA design. The NRC staff determined the RadICS platform approach to mitigating equipment manufacturer related CCFs falls into the category of same manufacturer producing fundamentally different equipment designs for the FPGA and the [ ] (See NUREG/CR-7007, Section 2.2.3.2).
3) Logic Processing Equipment "RadICS Diversity Assessment" (see Reference 7, Section 10.3.3)	The RadICS platform equipment is designed using [ ] The NRC staff determined the RadICS platform approach includes an element of logic processing equipment diversity. However, the degree of logic processing equipment diversity is limited due to similarities between FPGA and [ ]
4) Functional "RadICS Diversity Assessment" (see	The RadICS platform equipment design contains [ ]

Reference 7, Section 10.3.3)	The NRC staff determined the RadICS platform itself does provide a measure of functional diversity, because [ ]
5) Life-Cycle "RadICS Diversity Assessment" (see Reference 7, Section 10.3.3)	The RadICS platform development approach uses the [ ] The NRC staff determined the RadICS platform [ ]
6) Logic "RadICS Diversity Assessment" (see Reference 7, Section 10.3.3)	The RadICS platform equipment includes [ ] The NRC staff determined the RadICS platform provides a degree of logic diversity, because the RadICS platform uses [ ]
7) Signal "RadICS Diversity Assessment" (see Reference 7, Section 10.3.3)	The RadICS platform can support overall instrumentation architectures that include signal diversity implementing "different reactor or process parameters sensed by different physical effects," "different reactor or process parameters sensed by the same physical effect," and/or "the

	same reactor or process parameter sensed by a different redundant set of similar sensors" (see NUREG/CR-7007, Section 2.2.3.7). The RadICS platform equipment supports implementation of the signal diversity strategy. However, any signal diversity provided by a RadICS platform-based system would be based on application specifications. The NRC staff determined the RadICS platform itself does not provide signal diversity, because signal diversity requires specification of different signal inputs, which is application-specific and is not provided at the platform level. Therefore, this SE for the RadICS TR cannot make a determination regarding the adequacy of application-specific signal diversity.

RadICS Diversity Safety Conclusion

Based on this evaluation, the NRC staff determined the RadICS platform design, development and test approaches provide a [ ] of the RadICS modules. Consistent with NUREG/CR-6303, the NRC staff determined that licensees can use these diversity attributes in future system applications of the RadICS platform for plant-specific evaluations to determine whether platform and application logic CCFs can be eliminated from further consideration. In the absence of comprehensive testing, elimination of CCFs from further consideration is allowed by BTP 7-19 when sufficient diversity has been demonstrated by an applicant or licensee. The NRC staff further determined the RadICS platform supports inclusion of application-specific functional diversity and signal diversity, which could be implemented to achieve an additional degree of overall system diversity beyond the diversity provided by the platform design. The NRC staff determined that platform concepts alone should not be considered as sufficient diversity to eliminate the need for either a diverse actuation system or a best estimate safety analysis on a generic basis. Therefore, an applicant's or licensee should perform an application specific D3 analyses. The NRC agrees that some diversity strategies, as evaluated in Table 3.8-1 could be credited in the D3 analyses performed by a licensee. This D3 analysis should explicitly identify whether and how the RadICS platform's diversity attributes are credited and should identify any additional diversity strategies that the applicant or licensee includes in its design basis

The applicant's or licensee's D3 analysis should either (1) demonstrate adequate diversity exists to mitigate plant vulnerabilities without the need for a diverse actuation system, or (2) determine the need for a diverse actuation system to provide adequate mitigation against plant vulnerabilities. See PSAI 7.9.

3.10 Communications

The RadICS platform supports intra-divisional and inter-divisional serial data communication with other RadICS based systems and communications between RadICS systems and external

systems. Section 3.2.3 of this SE describes the data communication aspects of the RadICS platform.

Digital communication between independent systems may have the potential to compromise their independence unless appropriated measures are taken to ensure their independence. DI&C-ISG-04, Rev. 1, "Task Working Group #4: Highly-Integrated Control Rooms Communications Issues (HICRc)," establishes criteria to ensure independence in the presence of digital communication. The NRC staff therefore evaluated the RadICS communication interfaces using the criteria of DI&C ISG-04.

The NRC Task Working Group 4, "Highly Integrated Control Rooms-Communications Issues," developed interim NRC staff guidance on the review of communications issues applicable to digital safety systems. DI&C-ISG-04 contains NRC staff positions on three areas of interest: (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations. Section 6.3, "Communications," of the RadICS platform TR (Ref. 1) describes the Communications interfaces and protocols used in the RadICS platform. Section 3.2.3, "RadICS Platform Communications," of this SE describes the RadICS system communication features. A "RadICS platform DI&C-ISG-04 Conformance Analysis," which contains Radics LLC's assessment of RadICS Platform conformance to the provisions of DI&C-ISG-04, Revision 1, was provided as Appendix B of the RadICS TR.

Evaluation of a safety system to guidance criteria of DI&C-ISG-04 is a plant-specific activity that requires an assessment of a completed system design. Because the RadICS TR (Ref. 1) does not address specific applications or establish a definitive safety system design, the evaluation against this guidance is limited to consideration of the means provided within the platform to address issues related to interactions among safety divisions and between safety-related equipment and equipment that is not safety-related. A complete safety RadICS based system design will require further evaluation against this guidance. The following subsections provide an evaluation of each RadICS platform communication method against applicable DI&C-ISG-04 criteria. A plant-specific action item is included in this SE for licensees to fully address relative criteria of DI&C-ISG-04. See PSAI 7.10.

3.10.1 DI&C-ISG-04, Staff Position 1 - Interdivisional Communications

Staff Position 1 of DI&C-ISG-04 provides guidance on the review of communications, which includes transmission of data and information among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. This ISG guidance does not apply to communications within a single safety division. This NRC staff position states that bidirectional communications among safety divisions and between safety and non-safety equipment may be acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. It also states that systems, which include communications among safety divisions and/or bidirectional communications between a safety division and non-safety equipment should adhere to the guidance provided in 20 points described in the NRC staff position for Interdivisional Communications in DI&C-ISG-04 Rev. 1.

The methods by which the RadICS platform either meets these points or provides an acceptable alternative method of complying with NRC regulations are discussed below. In several instances, satisfying the criteria in these points cannot be determined without a complete application system design. For those points, this evaluation will highlight features of the RadICS

platform that would support the point and provide guidance for addressing specific items during subsequent application development. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 1

Staff Position 1, Point 1, states the following:

> … 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 IEEE Std. 603-1991. It is recognized that division voting logic must receive inputs from multiple safety divisions.

The RadICS TR describes a generic RadICS platform, which does not define a specific communication architecture for a safety division to be applied to all safety applications. Without a specific system with a specific application, the NRC staff is unable reach a safety conclusion on this point.

Section 6.3 of the TR describes the different types of communication interfaces and communication protocols available to the platform. Among these interfaces are the fiber optic RPP interfaces that can be used to establish communication links between OCMs in different safety system divisions. These interfaces use a RPP, which is described in Section 6.3.3.1.1 of the RadICS TR.

The RadICS platform described in the TR includes capabilities to comply with the guidance provided in Staff Position 1, Point 1. For example, the RadICS safety system logic modules operate independently from the OCMs. The RadICS OCMs also have diagnostic capabilities to monitor the status of each fiber optic inter-divisional communication interface. These communications diagnostics have the ability to identify loss or corruption of communication data which is required to support safety functionality. A loss or corruption of data can therefore be addressed by application logic in order to retain the ability of the safety system to perform safety functions without reliance on external data.

The NRC staff recognizes that the RadICS platform provides allowances for implementation of system features that could comply with the guidance provided by Staff Position 1, Point 1. However, evaluation of this point will require plant-specific analysis to satisfy the criteria of this staff position. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 2

Staff Position 1, Point 2, states the following:

> … 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.

To address this criterion, the NRC staff evaluated the RadICS fiber optic RPP interfaces, which provide communications between LMs or OCMs in different safety divisions and the RadICS Local Area Network (LAN) interfaces, which provide communication links between the RadICS LM and the non-safety-related MATS.

Fiber Optic RPP Interface (Interdivisional Communication):

The RadICS fiber optic RPP interface includes communication independence features described in Section 6.3.3.1.1 of the TR. Establishment of functional independence between system nodes of this interface however, must be addressed during plant application development.

RadICS fiber optic RPP communications features that are designed to protect or diagnose data to or from other safety divisions are listed below:

- Data validation using CRC on received data.
- Corruption of data
- Unintended repetition of data
- Incorrect sequence of received data
- Ability to detect loss of data updates
- Unacceptable delay in data transfer
- Continuous monitoring of communication interface status
- Detection of communications failure
- Physical separation and electrical isolation are provided by use of fiber optic cabling between nodes of the point to point interface.

The NRC staff determined that, when using RPP interfaces, RadICS safety system chassis can be protected from adverse influences caused by information or signals originating from a different safety division provided that safety applications are developed to perform required safety functions without reliance on data received through these interfaces.

Fiber Optic RUP Interface (Safety to Non-Safety Communication):

The RadICS fiber optic RUP interfaces are used to support communications between the RadICS safety system and the non-safety MATS. These interfaces include communication independence features described in Section 6.3.3.1.2 of the TR. RadICS fiber optic RUP Communications features are the same as those identified for the RPP interface.

The MATS monitoring interface is a one-way communications path from the safety system to the MATS system. Because this interface prohibits communication to the safety system, there is no potential for MATS monitoring communications to inhibit or delay the safety functions being performed by the RadICS system. The means of enforcing one-way communications through the MATS monitoring system interfaces involves the use of Radiy UDP-based protocols which are broadcast only protocols which require the initiating unit to send broadcast messages to the associated LAN interfaces.

The MATS tuning PC interface is disabled during normal safety system operation. The means of disabling this interface involves [ ] During normal system operation, there is no potential for MATS tuning communications to inhibit or delay the safety functions being performed by the RadICS system. The MATS tuning interface can however be enabled for system tuning, diagnostics, or surveillance testing purposes. During these controlled activities it is necessary to protect the integrity of the safety system logic and system setpoints. This is accomplished through the use of administrative controls and procedures.

The NRC staff determined that RadICS safety system chassis can be protected from adverse influences caused by information or signals originating from the fiber optics RUP interfaces to the MATS. The NRC staff recognizes that the RadICS platform provides allowances for implementation of system features that could meet the guidance criteria provided by Staff Position 1, Point 2. However, evaluation of this point will require plant-specific analysis to satisfy the criteria of this staff position. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 3

Staff Position 1, Point 3, states the following:

> … 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 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.

Section 2.3.1 of the TR describes a representative reactor trip system (RTS). Fiber optic RPP interfaces are used to support communications between system components in different safety divisions. This example uses cross divisional communications for performing coincidence voting functions. The RadICS platform provides capabilities for implementation of system cross divisional system features that could affect compliance with this position. However, Radics LLC stated in the TR that the only input coming from outside of a division are the input needed for the system coincidence voting logic. In cases where cross divisional communications are used to support other safety system functionality, a plant-specific analysis will be required to satisfy the criteria of this staff position. Thus, without a specific system design, the NRC staff cannot reach a safety determination on criteria of this point. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 4

Staff Position 1, Point 4, states the following:

> … 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. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be SR [safety-related], and must be designed, qualified, fabricated, etc., in accordance with 10 CFR Part 50, Appendices 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. 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 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.

The RadICS fiber optic RPP and fiber optic RUP MATS communications interfaces use [

] transfer data to the communication FPGA logic unit.

The RadICS platform uses an alternative method to the shared memory between distinct processing devices method described in DI&C-ISG-04. This alternative method [

] each safety function.

All of the RadICS platform logic circuits are developed as safety-related, which meets Point 4's guidance that safety function processors, communications processors, the data exchange memory resource, supporting circuits, and programming be developed as safety-related.

The RadICS platform communication logic circuits non-intrusively exchange information with the safety function logic circuits so a failure of the communication logic processing cannot adversely affect the performance of the safety function processing.

The NRC staff determined the RadICS platform alternative method, which [

] of each safety function without adverse effect from the communication processing.

The NRC staff determined the RadICS platform LM and OCM modules support meeting the criteria of Point 4 using this alternative method because each has been developed as safety-related and can be used to ensure deterministic behavior of safety functions. The NRC staff further determined plant-specific actions are necessary to ensure that plant specifications document the safety analysis that applies to its safety function determinism and that plant-specific implementation, V&V, and testing efforts demonstrate these safety functions will be performed within the established safety design bases timeframes, including any lack of access or delays related to the communication activities. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 5

Staff Position 1, Point 5, states the following:

> … 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.

The RadICS platform provides an alternative approach to [

]

communication activities cannot delay or otherwise adversely affect the performance of the safety functions. The RadICS platform is also designed such that failures of the system to meet timing requirements will [

] so that corrective actions can be taken.

Safety system development activities require development of specifications for the RadICS logic module that include response time specifications. The RadICS platform architecture provides features to ensure determinism by establishing expected response time performance variances.

Although the platform communication architecture does not [ ] to meet the criteria of Point 5 with respect to cycle-time performance, because the [ ] system external communications.

The NRC staff determined the RadICS platform communication components support the criteria of Point 5 because the RadICS platform supports [ ] in response to a system's failure to meet its plant-specific limiting cycle time. The NRC staff further determined plant-specific actions are necessary to ensure plant-specifications satisfies the criteria of Point 5 with respect to [ ] in excess of the limiting cycle time. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 6

Staff Position 1, Point 6, states the following:

> … the safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

The RadICS platform provides an FPGA approach that implements communication logic circuits that [ ] cannot delay or otherwise adversely affect the performance of the safety functions. The RadICS external communication functions are configured as point to point interfaces and use communications protocols that do not perform communication handshaking and do not accept interrupts from connected devices.

The RadICS optical communications module meets the criteria of Point 6 because the fiber optic RPP communication logic circuits do not include handshaking or safety function logic interrupts. The communication activities performed in the optical communications module do not handshake or interrupt the safety functions performed by the logic module.

The fiber optic RUP MATS monitoring system interfaces on the logic module meet the criteria of Point 6 because the communication logic circuits that provide this transmit-only protocol do not include handshaking and do not interrupt safety function logic circuits within the logic module FPGA.

The fiber optic RPP MATS tuning system interface meets the criteria of Point 6, because the communication logic circuits that provide this bidirectional protocol do not include handshaking with nor interrupt of the safety function logic circuits within the logic module.

The NRC staff determined the RadICS platform communication components satisfies the criteria of Point 6 because safety function logic circuits do not perform communication handshaking and do not accept interrupts. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 7

Staff Position 1, Point 7, states the following:

> … 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. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

The RadICS platform implements communication [

] See discussion in Staff Position 1, Point 4. Each transmitted data packet includes a pre-defined format and sequence in accordance with the communication protocol of the interface being used. Section 6.3.3.1 of the RadICS TR describes each of the communications protocols used for each available RadICS platform interface. For each communication protocol all RadICS data is sent during each transmission cycle in a pre-defined format without regard to whether it has changed since the previous transmission. The RadICS receiving instruments perform validation of the data and only accept and use data that conforms to the pre-defined communication protocol message format.

Point 7 does not apply to the fiber optic RUP MATS monitoring interfaces on the logic modules or to the OCM RS 232/485 interfaces because these interfaces are configured as one-way communications interfaces and they cannot be used by a RadICS platform-based safety system to receive data.

The fiber optic MATS tuning Interface uses RUP protocols in its data structure; however, this interface is normally disabled by the tuning access interface when the RadICS system is in operation. Therefore, the criterion of Point 7 does not apply to the MATS tuning Interface.

The NRC staff determined the RadICS platform communication components support meeting the criteria of Point 7 because the RadICS platform supports plant-specific message formats, protocols, and transmission cycles that satisfy the criteria of Point 7. The NRC staff further determined plant-specific actions are necessary to ensure plant-specifications adequately define all message formats, protocols and transmission cycles (as applicable) to each use of these interfaces. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 8

Staff Position 1, Point 8, states the following:

> … data exchanged between redundant safety divisions or between safety and non-safety 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.

The NRC staff reviewed communications protocols used for data exchanged over the RadICS fiber optic RPP interfaces, described in Section 6.3.3 of the RadICS TR, and determined that dedicated communication logic circuits are designed to manage this data in a manner, which cannot adversely impact safety functions performed by the RadICS safety logic in either the

source division or safety logic in the destination division(s). All divisions connected via fiber optic RPP interfaces are protected with the same communications processing design, which uses data validity checks, and independent parallel communication logic processing.

Communication of data to the MATS monitoring system through the fiber optic RUP Interfaces is performed in a manner that preserves the integrity of the safety system logic and that does not adversely affect the safety functions of the system. Safety system tuning parameter integrity is maintained through the use of non-volatile memory, which cannot be altered unless the MATS tuning PC is enabled via the tuning access interface.

The NRC staff determined that the data exchange between safety divisions and between safety- and non-safety-related MATS workstations satisfies Staff Position 1, Point 8. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 9

Staff Position 1, Point 9, states the following:

> …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 within a memory device.

The alternative method described in Staff Position 1, Point 4 above uses the RadICS platform development processes to create separate units that provide dedicated pre-specified physical areas within the LM FPGA to store incoming message data and to segregate input data from output data. These pre-specified areas within the LM FPGA are not used for other purposes. The NRC staff determined the RadICS platform alternative method to that associated with Point 4 provides an acceptable means of satisfying the guidance in Point 9 because received communications data is stored and segregated in pre-determined and dedicated locations within the LM FPGA. As such, the NRC staff determined the RadICS platform satisfies the criteria of

Point 9, as applicable to FPGA technology. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 10

Staff Position 1, Point 10, states the following:

> … that 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 a

> key lock 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 affect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

The RadICS FPGA platform and application logic cannot be modified during normal system RUN mode operation. The programming ports used to modify FPGA or CPLD logic on system modules are inaccessible during normal system operation. To modify system platform or application logic designs, the associated module must be [

] Restoring the safety system to the normal functional RUN operational mode requires a safety override reset operation. RadICS operational modes for each RadICS module are described in Section 6.2.6 of the RadICS TR. Safety Override Operation is described in Section 6.7 of the RadICS TR.

RadICS safety system tuning parameters are also protected from modification during normal system operation. Changes to system tuning parameters must be performed through the MATS tuning interface and this communications interface is disabled during normal operation. A system tuning access key-switch must be placed in the tuning enabled position to enable the MATS tuning interface and thus permit system tuning actions. Operation of the tuning key-switch effects a [

] Such an operation is controlled through the use of approved procedures and can only be performed when the associated RadICS safety division being tuned is inoperable. The MATS tuning PC can only be connected to a single safety division at a time because it is only equipped to support a single communications link.

The NRC staff determined the RadICS platform design supports the criteria of Point 10, because the RadICS platform's maintenance communication architecture can be configured to protect safety system logic designs and tuning parameters from alteration during system operation. The NRC staff determined the criteria to physically restrict the capability of making tuning parameter changes to only one redundant safety division at a time are met by the design of the MATS interfaces, which does not support simultaneous connection of the MATS tuning PC to redundant safety divisions. The NRC staff further determined plant-specific actions should verify whether plant-specifications identify administrative controls and include additional design features (i.e., a safety-qualified hardware switch and detection and indication of bypass)

to govern use of the MATS tuning PC. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 11

Staff Position 1, Point 11, states the following:

> … 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.

The RadICS platform does not contain conventional software instructions or instruction sequences. Instead, the RadICS platform modules contain configured hardware logic circuits that are contained in the systems FPGA devices. Once a RadICS platform-based instrument has been programmed and placed into operation as a plant-specific system, none of the available digital data communication interfaces supports alteration of the configured FPGA logic circuits. Information or messages received through fiber optic RPP or MATS tuning interfaces cannot be used to control the execution of the safety division application logic.

The RadICS platform also provides design features (monitoring and indication capabilities) to alert operators when a safety division is bypassed or rendered inoperable. These design features are intended to detect and indicate when the MATS tuning interface is activated or if a system module is removed from service.

The NRC staff determined the RadICS platform's provisions for interdivisional communication satisfies the criteria of Point 11 because these provisions explicitly preclude any ability to change the safety division logic circuits, which is the FPGA equivalent to conventional processor software. Furthermore, the NRC staff determined available RadICS platform features can be used to ensure a RadICS platform-based instrument has been bypassed or is otherwise out-of-service when system tuning, or safety system logic reprogramming activities are performed. The NRC staff further determined plant-specific actions should verify whether plant-specifications include these additional design features (i.e., a qualified hardware switch and detection and indication of bypass) to govern use of the MATS interfaces, as applicable to plant-specific safety functions. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 12

Staff Position 1, Point 12, states the following:

> … communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures" as described in the single failure criterion of 10 CFR Part 50, Appendix A. This SE provides 12 examples of credible communication faults but cautions that the possible communication faults are not limited to the list of 12.

The RadICS platform implements communication [ ] as described in Point 4. Each transmitted data packet includes a pre-defined format and sequence in accordance with the communication protocol of the interface being used. Section 6.3.3.1 of the RadICS TR describes each of the communications protocols used for each available RadICS platform interface.

RadICS system diagnostics are designed to detect and address communication faults at the receiving end of the communications interface. These diagnostics monitor communications ports during system operation and [ ] upon detection of a fault.

Radics LLC provided an analysis of the 12 example credible communication faults in Appendix B of the RadICS TR. This analysis describes how various faults are handled by a RadICS platform-based system. The NRC staff confirmed that all 12 of the example faults provided in Staff Position 1, Point 12 were included in this analysis. Methods employed to ensure that communications faults do not affect safety functions include:

- Use of CRC to identify and handle invalid communications,
- Use of point to point communication architecture with physical configuration control for the fiber optic interfaces to eliminate potential for multiple data sources,
- Message sequence and timing control measures to prevent data distortion, and
- Use of broadcast communication protocols that do not rely on handshaking between the source and destination modules.

For each of the identified communications faults, the analysis determined that the effects of the fault on a RadICS based safety system did not adversely affect the performance of required safety functions. The NRC staff therefore determined the RadICS platform design satisfies Staff Position 1, Point 12. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 13

Staff Position 1, Point 13, states the following:

> … vital 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.

Fiber optic RPP point-to-point interfaces are used for vital communications between divisions of the RadICS platform-based systems. [

]

Error-correcting methods are not used in the RadICS platform design. Instead, data is transmitted over the fiber optic RPP interface during each control logic cycle. [

] The effectiveness of these provisions was verified by testing and documented as part of equipment qualification.

RadICS platform design includes provisions for ensuring that received messages are correct and are correctly understood by receiving communications and safety function logic circuits. The RadICS platform design includes error detection diagnostics for handling corrupt, invalid, as well as untimely or otherwise questionable data received over fiber optic RPP communication interfaces. The NRC staff therefore determined the RadICS platform design satisfies Staff Position 1, Point 13. See PSAI 7.10 for plant-specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 14

Staff Position 1, Point 14, states the following:

> … vital 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.

RadICS platform fiber optic RPP interfaces are configured as point-to-point communications interfaces between safety system divisions. These interfaces use dedicated fiber optic media connections to transfer messages directly from the sending nodes to receiving nodes. Point-to-point source and destination node configuration of the fiber optic RPP interfaces are application dependent. The RadICS platform design does not include use of equipment outside the associated sending or receiving division; however, licensees referencing this SE should confirm that no equipment outside of the safety division is configured for use in the transmission of messages through the fiber optic RPP interfaces of the system. The NRC staff, therefore, determined the RadICS platform design satisfies Position 1, Point 14 as long as plant specific design configurations do not introduce out of division dependencies. See PSAI 7.10 for plant-specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 15

Staff Position 1, Point 15, states the following:

> … communications 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.

RadICS fiber optic RPP communication interfaces use a fixed data format of data sets. These data sets are transmitted during every FPGA execution cycle. [ ] The NRC staff therefore determined the RadICS platform design satisfies the criteria in Staff Position 1, Point 15. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 16

Staff Position 1, Point 16, states the following:

> … network connectivity, liveliness, and real-time properties essential to the safety application should be verified in the protocol. Liveliness in particular, is taken to mean that no connection to any network outside the division can cause a RTS/ESFAS [engineered safety features actuation system] 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, 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 Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Source: NUREG/CR-6082, Section 3.4.3).

The RadICS fiber optic RPP interfaces use message sequence and timing control measures to identify and manage communications interface issues that could potentially affect interface connectivity. These measures include the capability of [ ] received from the communications interface. Connectivity to devices that are outside of a division are restricted through the use of a point-to-point network architecture and the use of broadcast data transmissions that do not rely on the use of handshaking signals between communications modules. The RadICS fiber optic RPP communications protocols are not susceptible to network stalling and are therefore capable of supporting vital safety communications without adverse impact to system safety functions.

The NRC staff determined that safety function response to fiber optic RPP communication errors, including deadlock and livelock, is application dependent. The NRC staff therefore determined the RadICS platform design satisfies Staff Position 1, Point 16 as long as plant-specific applications are implemented in a manner, which does not introduce communication data dependencies. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 17

Staff Position 1, Point 17, states the following:

> … pursuant to 10 CFR 50.49, the medium used in a vital 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.

Cross divisional communications for a RadICS platform-based system will be performed over fiber optic RPP communications interfaces. These interfaces are described in Section 3.2.3.2.2 of this SE. All fiber optic RPP interdivisional communications are made via fiber optic media. RadICS platform components are qualified for operation in a mild environment. Qualifications include seismic, temperature and humidity, and EMI/RFI.

Fiber optic cables are selected and qualified on a plant specific basis with consideration for installed plant environments. The fiber optic cabling provides electrical isolation between safety divisions as well as EMI/RFI protection for system components. The fiber optic interface components on the LM and OCM modules were subject to environmental qualifications as discussed in Section 3.6 of this SE. The generic qualification of the RadICS platform encompasses both the hardware and the logic design used in the system.

The qualification of the RadICS platform does not include qualification of the fiber optic cables used to connect the fiber optic RUP and RPP interfaces. Therefore, a plant-specific evaluation will be required for plant-specific applications of a RadICS platform that uses fiber optic cables to connect interfaces between safety divisions and to MATS.

The NRC staff determined that the RadICS platform meets the guidance provided by Staff Position 1, Point 17. However, as noted above, fiber optic cables used to connect fiber optic RPP and RUP interfaces for a safety system will require a plant-specific evaluation to verify these cables are qualified for the environment in which they will be used. Furthermore, safety applications using the RadICS platform will require plant-specific review to confirm that the plant-specific environment is consistent with the qualification envelope defined in the RadICS TR and in Section 3.6 of this SE. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 18

Staff Position 1, Point 18, states the following:

> … provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

An analysis of RadICS fiber optic RPP and RUP interface communication faults was provided in Appendix B of the RadICS Platform TR. This analysis describes how system level hazards caused by various communications faults are handled by a RadICS platform-based system.

Nevertheless, potential hazards posed to specific safety functions relating to interdivisional communications must be analyzed at the plant application level.

The NRC staff determined that for the RadICS platform, the additional activity to perform failure modes and effects analyses for plant-specific applications meets the intent of the guidance provided in Staff Position 1, Point 18. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 19

Staff Position 1, Point 19, states the following:

> … the communications data rates be such that they will not exceed the capacity of a communications link or the ability of nodes to handle traffic, and that all links and nodes have sufficient capacity to support all functions. To do this, 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 and that communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

RadICS communication data rates and data quantity are constant during system RUN mode operation. These are established during FPGA electronic design development. Communication rates must be within the bandwidth capacity for each communication interface. The FPGA development tool does not allow establishment of communication rates that are beyond the capability of the applicable interface. If excess communication rates are attempted, then the FPGA design tool will produce errors that must be resolved before the electronic design can be implemented.

The NRC staff confirmed the deterministic response time of the RadICS communication interfaces are factored into the total response time of a safety function application. The total safety function response time must be confirmed through application level testing.

The NRC staff determined the RadICS platform supports meeting the criteria of Point 19. The NRC staff further determined plant-specific actions should verify Point 19 is met by performance of a plant-specific analysis to ensure that plant performance requirements are met. This PSAI should also ensure plant-specific V&V and factory and system acceptance testing confirm that plant-specific performance requirements, as defined in the plant design basis (e.g., UFSAR), dependent on data communications are met. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 1, Point 20

Staff Position 1, Point 20, states the following:

> …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.

A discussion of the RadICS platform response time is provided in Section 3.7.1 of this SE. To ensure that a safety system based on the RadICS platform meets its application system

response time requirements, the execution time for all of the systems tasks is calculated and measured during system development. This calculation includes terms to address the response time of communications, memory processing and associated circuits.

The NRC staff determined the RadICS platform supports meeting the criteria of Staff Position 1, Point 20. However, the plant-specific design must be evaluated for a plant-specific application because this time will depend on the system configuration, plant application logic, and communication interfaces used. When implementing a RadICS safety system the licensee must review the plant-specific timing analyses and validation tests for the RadICS system in order to verify that it satisfies plant-specific requirements for system response time presented in the accident analysis in the plants safety analysis report. See PSAI 7.10 for plant-specific actions pertaining to DI&C-ISG-04.

3.10.2 DI&C-ISG-04, Section 2 - Command Prioritization

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function blocks, which receive device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device.

The design of field device interfaces and the determination of means for command prioritization were not provided in the RadICS TR. If a RadICS platform-based design is used for the development of a command prioritization system, then an additional evaluation of that system against the criteria of DI&C-ISG-04 Section 2 should be performed by the licensee. Since the RadICS TR does not address a specific application involving command prioritization, no evaluation against this staff position could be performed. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

3.10.3 DI&C-ISG-04, Section 3 - Multidivisional Control and Display Stations

Section 3 of DI&C-ISG-04 provides guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division, and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation. RadICS platform includes a MATS subsystem to perform monitoring tuning of the system. Control over how the MATS is used during operation is a PSAI. See PSAIs 7.8 and 7.10. Below is an evaluation of how the RadICS based system can be used to meet the applicable guidance criteria.

Staff Position 3.1-1

This position pertains to non-safety stations receiving information from one or more safety divisions. It states:

> All communications with safety-related equipment should conform to the guidelines for interdivisional communications.

Interdivisional communications for the RadICS platform are conducted through the fiber optic RPP interfaces. These interfaces are described in Section 3.2.3.2.2 of this SE. The NRC staff evaluated the RadICS fiber optic RPP communications features and determined them to satisfy the criteria for interdivisional communications, however, some aspects of interdivisional

communications are plant-specific and therefore must be evaluated when a RadICS based plant system is developed. Details of this evaluation are provided in Section 3.10.1 of this SE. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Communications between safety-related RadICS equipment and non-safety equipment are conducted through either fiber optic RUP or RS 232/485 communications interfaces. These are described in Sections 3.2.3.2.1 and 3.2.3.2.3 of this SE respectively. RadICS safety processors can only send data to external non-safety-related systems such as the MATS monitoring PC or

a process plant computer during plant operations. The NRC staff evaluated the RadICS MATS as well as the RS 232/485 communications features and determined them to satisfy the criteria for interdivisional communications. The NRC staff therefore determined that safety to non-safety communications conform to the guidance provided for interdivisional communications as discussed in Section 3.10.1 of this SE.

Staff Position 3.1-2

This position pertains to safety-related stations receiving information from other divisions (safety or non-safety). It states the following:

> 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.

Both safety-related communications via fiber optic RPP interfaces and non-safety-related communications via fiber optic RUP or RS232/485 interfaces were evaluated by the NRC staff and were found to support the guidance provided for interdivisional communications as discussed in Section 3.10.1 of this SE. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 3.1-3

This position pertains to non-safety stations controlling the operation of safety-related equipment. It states the following:

> Non-safety stations may control the operation of safety-related equipment, provided the following restrictions are enforced.

The RadICS platform design does not include provisions for operation of safety-related equipment from non-safety-related workstations. The only non-safety workstations included in the RadICS platform are the MATS workstations. A description of the Radics LLC MATS workstations is provided in Section 3.2.4 of this SE.

The MATS monitoring workstations communicate with system logic modules through fiber optic RUP interfaces. These interfaces are one-way broadcast point to point communication links, which are not capable of supporting transfer of data or commands from a non-safety device to the safety-related RadICS logic modules.

Connections to external systems can be made using the RS232/485 serial interfaces. These interfaces are one-way point-to-point communication links, which are not capable of supporting transfer of data or commands from an external device to the safety-related RadICS logic modules.

The MATS tuning interface is disabled by the tuning access interface during plant operations and therefore does not have the capability of transferring data or commands from a non-safety device to the safety-related RadICS logic modules. Temporary enabling of the tuning access interface can be performed to support maintenance and surveillance related activities. These activities are not intended to be used for the control of safety-related equipment. Administrative control measures should be taken by the licensee to ensure removal of any safety logic module from service prior to enabling the tuning access interface. The NRC staff determined that RadICS MATS tuning design satisfies the criteria of Command Prioritization Staff Position 3.1-3. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 3.1-4

This position pertains to safety-related stations controlling the operation of equipment in other safety-related divisions. It states the following:

> Safety-related stations controlling the operation of equipment in other divisions are subject to constraints similar to those described above for non-safety stations that control the operation of safety-related equipment.

The RadICS platform design does not include provisions for operation of equipment in other safety-related divisions.

This position also states the following:

> 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.

The RadICS equipment cannot be used to control equipment in different divisions and therefore this criterion is not applicable to the RadICS platform design.

This position also states the following:

> 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.

RadICS cross divisional communications is conducted through fiber optic RPP communications interfaces. The NRC staff evaluated these interfaces and determined that communications of data through the fiber optic RPP interfaces will not influence the operation of safety-related RadICS equipment provided plant-specific requirements are correctly implemented.

See Section 3.10.1 of this SE for a detailed assessment of RadICS fiber optic RPP communications interfaces.

This position also states the following:

> 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.

RadICS equipment cannot be used to control equipment or to initiate safety function bypass in other divisions and therefore this criterion is not applicable to the RadICS platform design.

This position also states the following:

> 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 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.)

Because RadICS equipment cannot be used to control equipment in different divisions, there is no potential for safety RadICS equipment to suppress or otherwise affect the safety functions being performed in another safety division.

This position also states the following:

> 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.

Because RadICS equipment cannot be used to control equipment in different divisions, there is no potential for RadICS equipment to change the bypass state of safety functions performed in another safety division.

The NRC staff determined that the RadICS platform can be used to satisfy Position 3.1-4 of DI&C-ISG-04. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

Staff Position 3.1-5

This position pertains to malfunctions and spurious actuations. It states the following:

> 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.

The NRC staff determined that RadICS equipment is functionally independent from equipment in other divisions and from non-safety systems. Therefore, failures of RadICS equipment cannot affect the operation of equipment that is external to the RadICS safety system. The RadICS platform design therefore satisfies this criterion. However, fully addressing plant safety analysis requirements remains a plant-specific criterion and must be addressed during application development.

This position also states the following:

> 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.

The RadICS platform-based safety systems do not perform non-safety control functions. The RadICS platform is designed to maintain functional independence between system safety function logic modules. Compliance to plant safety analysis requirements is plant plant-specific and must be addressed during application development.

This position also states the following:

> 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 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.

The RadICS platform does not include provisions for safety display or control devices. Therefore, this criterion is not applicable to RadICS safety equipment.

RadICS safety system tuning parameters are protected from modification during normal system operation. Changes to system tuning parameters must be performed through the MATS tuning interface which is disabled during normal operation. A system tuning access key-switch must be placed in the tuning enabled position to enable the MATS tuning interface and thus permit

system tuning actions. Operation of the tuning key-switch effects a disconnection of the MATS tuning interface by removing electrical power to the associated LAN Transceiver unit.

System level compliance with this position is dependent on plant-specific design and must be evaluated during plant specific application development.

This position also states the following:

> Each control processor or its associated communication processor should detect and block commands that do not pass the communication error checks.

The RadICS platform does not include provisions for safety display or control devices. Therefore, this criterion is not applicable to RadICS equipment. System level compliance with this position is dependent on plant-specific design and must be evaluated during plant specific application development.

The NRC staff determined that the RadICS platform can be used to support compliance with the guidance of Position 3.1-5 of DI&C-ISG-04. See PSAI 7.10 for plant specific actions pertaining to DI&C-ISG-04.

3.11 Compliance to IEEE Std. 603-1991 Requirements

For applicable nuclear power generating stations, the regulation at 10 CFR 50.55a(h) requires that safety systems meet the requirements stated in IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995. The NRC staff evaluation is based on the guidance contained in SRP Chapter 7, Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” which provides acceptance criteria for this standard. This NRC staff evaluation also addresses the RG 1.153, “Criteria for Safety Systems,” endorsement of IEEE Std. 603-1991.

3.11.1 IEEE Std. 603-1991, Clause 4, “Safety System Designation”

Clause 4 of IEEE Std. 603-1991 states that a specific basis shall be established for the design of each safety system of the nuclear power generating station. SRP Chapter 7, Appendix 7.1-C, Section 4, “Safety System Designation,” provides acceptance criteria for these requirements. The determination and documentation of the design basis for a safety system is a plant-specific activity that is dependent on the plant design. Since the RadICS TR does not address a specific application of the platform, the design basis for a safety system is not available for review and no evaluation of the RadICS platform against these regulatory requirements could be performed. Nevertheless, the applicant provided a summary of compliance to the criteria of IEEE Std. 603 in Section 12.2.1, “Regulatory Guide 1.153,” of the RadICS TR.

Section 5.7.8 of the RadICS TR states that RadICS platform features that would support compliance with IEEE Std. 603-1991 for a specific project are described in Section 12 of the TR. The NRC staff reviewed Section 12 of the TR and evaluated the capabilities of the RadICS platform to address the criterion of IEEE Std. 603-1991 as follows. See PSAI 7.11 for plant specific actions pertaining to IEEE Std. 603 1991.

Clause 4.7 Range of Conditions for Safety System Performance

This clause states that the range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform shall be documented.

The RadICS Platform TR (Ref. 1) partially addresses this criteria by establishing documentation for the qualified range of operation of a RadICS based safety system. Table 9-1 of the RadICS TR documents the range of environmental conditions to which the RadICS Platform components are qualified to operate. Section 9, "Equipment Qualification and Analysis," of the RadICS TR documents additional details of equipment qualifications and provides references to specific qualification standards, test procedures and test reports that provide a basis for the RadICS component qualifications. This documentation can be used to support a plant specific application of the RadICS platform provided plant specific environmental conditions do not exceed the established conditions to which the RadICS platform is qualified. See Section 3.6 of this SE for evaluation of RadICS platform equipment qualification.

Clause 4.8 Functional Degradation of Safety System Performance

This clause states that conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems) shall be documented.

The RadICS Platform design partially addresses this criterion by incorporating design features that establish independence between the safety system components of a RadICS based safety system and non-safety-related systems connected via isolation devices and the RadICS Fiber Optic MATS interfaces. The documentation provided in the RadICS TR can be credited for compliance with functional independence and isolation requirements of IEEE Std. 603. See Section 3.10.1 of this SE for evaluation of communication interfaces between the RadICS system and non-safety related systems.

Clause 4.9 Reliability

This clause states methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design shall be documented.

The RadICS platform TR (Ref. 1) partially addresses this criteria by providing documented basis for the platform self-diagnostics functions. RadICS self-diagnostic features are described in Section 6.4, "Platform Diagnostics," of the TR and an evaluation of these platform features is provided in Section 3.7.3 of this SE.

Section 9.2.1.3 of the TR also partially addresses this criterion by providing predicted reliability values for RadICS modules. These values can be used by a licensee to support a reliability analysis to show compliance with plant specific reliability requirements. Section 3.5.2.7 of this SE documents the NRC staff SE of the reliability characteristics of a RadICS safety system.

3.11.2 IEEE Std. 603-1991, Clause 5, “Safety System Criteria”

Clause 5 of IEEE Std. 603-1991 requires that safety systems maintain plant parameters, with precision and reliability, within acceptable limits established for each design basis event. The power, I&C portions of each safety system are required to be comprised of more than one safety group of which any one safety group can accomplish the safety function.

The establishment of safety groups that can accomplish a given safety function is a plant-specific activity and the topical report scope does not include specific applications. Therefore, the following evaluations against the requirements of IEEE Std. 603-1991 Section 5 are limited to assessing capabilities and characteristics of the RadICS platform that are relevant to satisfy each requirement. See PSAI 7.11.

The following clauses were not evaluated because addressing compliance with this guidance is a plant-specific activity that depends on the system design. Therefore, NRC staff determinations are not provided for these clauses.

- Clause 5.2, Completion of Protective Action
- Clause 5.8, Information Displays
- Clause 5.11, Identification
- Clause 5.12, Auxiliary Features
- Clause, 5.13, Multi-Unit Stations
- Clause 5.14, Human Factors Considerations

IEEE Std. 603-1991, Clause 5.1, “Single Failure Criterion”

This clause requires that the safety system be able to perform its safety function required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

Since the RadICS TR does not address a specific application for approval, the evaluation against this requirement is limited to consideration of the means provided within the RadICS platform to address failures. The NRC staff evaluation of the capabilities and characteristics of the RadICS platform that are relevant to the Single-Failure Criterion are documented in Section 3.7.3, Self-Diagnostics and Test and Calibration Capabilities, and in Section 3.5.2.6, Failure Mode and Effects Analysis, of this SE.

IEEE Std. 603-1991, Clause 5.3, “Quality”

Clause 5.3 of IEEE Std. 603-1991 states that the components and modules within the safety system must be of a quality that is consistent with minimum maintenance requirements and low

failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program. SRP Chapter 7, Appendix 7.1-C, Section 5.3, “Quality,” provides acceptance criteria for the quality requirement. This acceptance criteria states that the QA provisions of 10 CFR Part 50, Appendix B, apply to a safety system.

The RadICS platform components are manufactured by a supplier company, RPC Radiy, under a QMS. Section 3, “Quality Assurance,” of the RadICS TR provides descriptions of both the RPC Radiy and the Radics LLC quality assurance programs. Below is a summary of these programs.

RPC Radiy QA Program

The RPC Radiy organizational structure is described and illustrated in Section 3.2 of the TR. Product development activities are performed by various design bureaus in accordance with a pre-defined Radiy product life cycle and services model. RPC Radiy uses a QMS to perform QA activities to support all activities of this life cycle. The RPC Radiy QMS is based on international standards organization (ISO) 9001:2015, “Quality Management Systems.” The RPC Radiy QMS is a certified ISO 9001:2015 program. RPC Radiy design and QMS practices are also compliant with safety requirements for I&C systems described in IEC 61508.

This RPC Radiy QMS has not been assessed by the NRC staff to be compliant to 10 CFR Part 50, Appendix B. Therefore, Radics LLC performs CGD of the RadICS platform components received from RPC Radiy.

Radics LLC QA Program

Radics LLC is responsible for all RadICS-based application project activities. However, Radics LLC does not perform the design and manufacturing of the individual RadICS platform components which are supplied by RPC Radiy; so Radics LLC will perform CGD of these components. The Radics LLC QA program is described and illustrated in Section 3.3 of the TR. This Section of the TR describes various departments and bureaus that are involved in RadICS-based application projects. The roles and responsibilities for each of these organizations are also described. Two figures are provided in the TR to illustrate the organization structure and responsibilities and workflow interfaces, in relation to product life cycle activities. Section 3.5.1.3 of this SE also provides an evaluation of the RPC Radiy, and Radics LLC QA programs.

The Radics LLC 10 CFR Part 50, Appendix B based QA policy is established in the RadICS QAPD (QAPD-001), which was reviewed by the NRC staff during the regulatory audit in Toronto (Ref. 9). The NRC staff confirmed that the RadICS platform is maintained under the Radics LLC, Appendix B based QAPD, which is intended to satisfy the requirements of Appendix B during all phases of the product life cycle. The Radics LLC Appendix B based QAPD assigns major functional responsibilities for activities and key processes related to the design, procurement, manufacturing, testing, inspection, modification, shipment and other related product realization activities for DI&C systems and components. However, Application Logic and implementation of its specific life cycle processes are outside the scope of this review and should be addressed in plant-specific reviews. See PSAI 7.11.

Commercial grade dedication activities are conducted in accordance with Radics LLC 10 CFR Part 21 compliant commercial grade dedication processes and are conducted by an

organization that is independent from the platform component design organization. Radics LLC uses a 10 CFR Part 50, Appendix B based QAPD to govern activities related to development of RadICS systems. The Radics LLC Appendix B based QAPD is also used to govern the RadICS component commercial grade dedication activities.

Based on the review of the RadICS platform application development processes, operating experience, life cycle design output documentation, and testing and review activities, the NRC staff finds the dedication evidence of the RadICS platform components in conjunction with Radics QA processes to be acceptable for demonstrating built-in quality. Thus, the RadICS platform hardware and ED logic implementations show sufficient quality to be suitable for use in safety-related nuclear applications. Assuring supplier quality during application development is the responsibility of the licensee. Thus, a licensee must assure that supplier quality is in accordance with the licensee's Appendix B program. See PSAI 7.11.

IEEE Std. 603-1991, Clause 5.4, "Equipment Qualification"

This clause contains the equipment qualification requirements. SRP Chapter 7, Appendix 7.1-C, Section 5.4, "Equipment Qualification," provides acceptance criteria for IEEE Std. 603-1991, Clause 5.4.

The evaluation of the environmental qualification for the RadICS platform is contained in Section 3.6 of this SE. This SE also identifies plant-specific actions necessary to demonstrate that the RadICS platform performance as bounded by its established qualification envelope satisfies the requirements of the plant-specific installation environment for plant-specific safety functions.

The NRC staff evaluation provided in Section 3.6 determined that the RadICS platform EQ provides an acceptable type test to establish a documented set of platform safety functions, and range of installation conditions for the RadICS platform. The NRC staff concludes that the RadICS platform equipment is suitable for reference by licensees and conforms to Reg. Guide 1.209's endorsement of IEEE Std. 323-2003 for qualification of SR computer-based I&C systems installed in mild environment locations. The NRC staff further determined that the RadICS platform is capable of satisfying IEEE Std. 603-1991, Clause 5.4 criteria, provided that environmental conditions of the installed location remain within the established RadICS platform qualification levels.

IEEE Std. 603-1991, Clause 5.5, "System Integrity"

This clause states that the safety systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," provides acceptance criteria for system integrity.

Determination of system integrity is a plant-specific activity that requires an assessment of a full system design against a plant specific design basis. A platform-level assessment can only address those characteristics that support fulfillment of this requirement by a system design based on the platform. Since the RadICS TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the integrity demonstrated by the RadICS platform and its features to assure a safe state can be achieved in the presence of failures. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.5.

The RadICS platform design has several characteristics that can be used to establish a high level of system integrity. These characteristics are described and evaluated in Section 3.7 of

this SE. Though specific ranges of applicable conditions are not enumerated in the TR, platform components are qualified to ranges of conditions that are typically acceptable for nuclear power plant applications. Licensees using a Radics LLC based safety system are required to ensure that enumerated plant design conditions are within the conditions for which the RadICS platform

components are qualified. For most safety applications, re-qualification of Radics LLC components beyond established qualification levels will not be necessary.

Radics LLC based systems are also designed to operate in a deterministic manner. The NRC staff evaluated the deterministic attributes of the RadICS platform and the results of that evaluation are in Section 3.7.2 of this SE. Deterministic performance and high reliability are attributes of the RadICS platform, which can support compliance with System Integrity criteria of Clause 5.5 of IEEE Std. 603 1991.

IEEE Std. 603-1991, Clause 5.6, “Independence”

This clause contains the requirements for physical, electrical, and communications independence. SRP Chapter 7, Appendix 7.1-C, Section 5.6, “Independence,” provides acceptance criteria for system independence.

The specific redundancy needed for a RadICS platform-based safety system is intended to be defined at the system level during the application development. Therefore, the determination of independence is a plant-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those characteristics of the RadICS platform that can support fulfillment of this requirement by a system design based on the platform. The platform’s evaluation against this requirement is limited to consideration of the digital communications for the system, which are described in Section 3.2.3 and evaluated in Section 3.10 this SE. Because the RadICS TR does not address a specific application or establish a definitive safety system design. See PSAI 7.11.

IEEE Std. 603-1991, Clause 5.6.1, “Between Redundant Portions of a Safety System”

This clause states that the safety systems be designed such that there is sufficient independence between redundant portions of a safety system such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.

Specific redundancy needed for a RadICS platform-based system will be defined at the system level during the plant specific application development to accomplish the safety function during and following any design basis event requiring that safety function.

The RadICS platform includes several design characteristics, which can be used to support compliance with this position. For example, communication between redundant divisions of a Radics LLC based safety system can be performed using Fiber Optic RPP Communications Interfaces. These Interfaces are described in Section 3.2.3.2.2 and evaluated in Section 3.10 of this SE. The NRC staff determined that Fiber Optic RPP Communications provide an acceptable means of performing communications between redundant safety divisions while maintaining divisional communications independence.

RadICS platform Data Communications are performed using optical transceiver units, which provide electrical isolation between safety divisions for these interfaces. The NRC staff reviewed the optical transceiver units and determined they provide an acceptable means of establishing electrical independence between safety divisions of a RadICS platform-based safety system.

Though compliance with this clause remains a plant-specific requirement, these design characteristics of the RadICS platform discussed above can be used in a plant specific design to support conformance to the criteria of Clause 5.6.1 of IEEE Std. 603-1991.

IEEE Std. 603-1991, Clause 5.6.2, "Between Safety Systems and Effects of Design Basis Event"

This clause states that the safety systems required to mitigate the consequences of a specific design basis event must be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Clause 5.6.2 further states that environmental qualification in accordance with 5.4 is one method that can be used to meet this requirement.

Determining the effects of design basis events and establishing the physical separation of the safety system from the effects of those events are plant-specific activities. However, the qualification of the RadICS platform under the generic service conditions required in EPRI TR-107330 can be used to demonstrate the capability of a safety system based on the platform to satisfy this requirement. The evaluation of the environmental qualification for the RadICS platform is contained in Section 3.6 of this SE. This SE also identifies plant-specific actions to demonstrate that the RadICS platform performance as bounded by its EQ satisfies the requirements of the plant-specific installation environment for the plant-specific safety functions.

Based upon the installation of RadICS platform equipment in a mild environment, which is bounded by the equipment qualification discussed and evaluated in Section 3.6 of this SE, the NRC staff determined that the RadICS platform features can be used to support compliance with IEEE Std. 603-1991 Clause 5.6.2. A referencing applicant or licensee must address the plant-specific actions associated with confirming the application and installation have been bounded by the RadICS platform EQ including each boundary/interface condition. Compliance to this clause can only be demonstrated by application design that assures that redundant equipment are not susceptible to the effects of a design basis event. See PSAI 7.11.

IEEE Std. 603-1991, Clause 5.6.3, "Between Safety Systems and Other Systems"

This clause states that the safety systems be designed such that credible failures in and consequential actions by other systems will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a single random failure.

Evaluation of this clause requires identification of credible failures in and consequential actions by other systems as documented in the applicant's or licensee's plant-specific design basis. The RadICS platform provides digital communication design features that can support independence between a RadICS platform-based safety system and other interfacing systems, which are discussed in Section 3.2.3 and evaluated in Section 3.10 of this SE.

The RadICS platform design can support use of interconnected equipment. However, because the RadICS TR does not include plant specific information on external systems, the NRC staff is unable to evaluate the effects of connected system on RadICS system operation. Therefore, adequate independence between RadICS systems and external systems should be established during plant-specific application development. See PSAI 7.10.

IEEE Std. 603-1991, Clause 5.7, “Compatibility for Testing and Calibration”

This clause contains testing and calibration requirements. Determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements (e.g., accuracy) that apply. In addition, the establishment of the types of surveillance necessary for the safety system to ensure detection of identifiable single failures that are only announced through testing is a plant-specific activity.

Since the RadICS TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to enable testing and calibration of redundant portions of a safety system. Section 3.7.3 of this SE discusses the RadICS platform’s self-diagnostic capabilities, which can be used to support IEEE Std. 603-1991, Clause 5.7 criteria.

IEEE Std. 603-1991, Clause 5.9, “Control of Access”

This clause states; the design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

The RadICS platform design includes provisions for controlling access to RadICS equipment while in service. Section 3.13 of this SE includes an evaluation of these provisions. These provisions include physical access controls to Radiy modules, logic access controls and software access controls of the MATS system. Use of these provisions can be administratively controlled by the system operators. Implementation of administrative controls is an application specific activity which must be performed during plant application development. See PSAI 7.11.

IEEE Std. 603-1991, Clause 5.10, “Repair”

This clause states that safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

The self-diagnostic features of the RadICS platform design can be used to support compliance with this criterion. These include self-identification of faulted modules, on-line modular replacement capabilities, and internal redundancy options, which can be implemented in a plant-specific design. Section 3.7.3 of this SE includes an evaluation of self-diagnostic features. The NRC staff determined the RadICS platform design is generally capable of supporting timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. However, some aspects of a system repair capabilities must be determined during application development and therefore compliance with this position should be confirmed during plant application development. See PSAI 7.11.

IEEE Std. 603-1991, Clause 5.15, "Reliability"

Clause 5.15 of IEEE Std. 603-1991 requires appropriate analysis of system designs to confirm that any established reliability goals, either quantitative or qualitative, have been met.

The evaluation against this requirement is limited to consideration of the reliability characteristics of the platform and its components. The NRC staff's review of RadICS platform reliability is further addressed Section 3.5.2.7 of this SE. This review identifies an activity to be performed as part of the plant-specific application of the RadICS platform. Because plant and system specific reliability goals are not provided in the RadICS TR and instead must be established on a plant-specific basis, the NRC staff was unable to make a safety determination for this criterion. See PSAI 7.11.

A description of RadICS platform component reliability is included in Section 9.2.1 of the RadICS TR, "Failure Modes, Effects, and Diagnostic Analysis." This description includes a discussion of expected failures, failure rates, and failure effects of RadICS equipment. The NRC staff determined the TR contains platform reliability information that can be used to demonstrate conformance to plant specific reliability goals.

3.11.3 IEEE Std. 603-1991, Clause 6, "Sense and Command Features – Functional and Design Requirements"

The requirements of this clause, in addition to the requirements of Clause 5, apply to the Sense and Command Features of a safety system.

The functional and design requirements for the sense and command features of a safety system are dependent solely on the specific application. Since the RadICS TR does not address a specific application of the platform, include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the RadICS platform against these regulatory requirements could be performed. Specifically, the following requirements were not evaluated:

- Clause 6.1, Automatic Control
- Clause 6.2, Manual Control
- Clause 6.3, Interaction between Sense and Command Features and other Systems
- Clause 6.4, Deviation of System Inputs
- Clause 6.6, Operating Bypass
- Clause 6.7, Maintenance Bypass

IEEE Std. 603-1991, Clause 6.5, "Capability for Testing and Calibration"

Clause 6.5 of IEEE Std. 603-1991 requires that a means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation.

The RadICS platform contains design features that are inherent in the platform design, as well as, features that can be implemented during application development to support a plant's methods of checking operational availability of the system through the self-diagnostic and periodic testing. The NRC staff's review of the RadICS self-diagnostics, test and calibration

capabilities is provided in Section 3.7.3 of this SE. Because determination of specific input sense and command requirements are plant-specific, the NRC staff considers this criterion to be a plant specific action. See PSAI 7.11.

IEEE Std. 603-1991, Clause 6.8, "Setpoints"

This clause is related to determination of sense and command feature setpoints. This requirement for setpoints primarily addresses factors beyond the scope of a digital platform (e.g., plant design basis limits, modes of operation, and sensor accuracy). The RadICS TR does not address a specific application or establish a definitive safety system, which is necessary to demonstrate the adequacy of setpoints that are associated with IEEE Std. 603-1991, Clause 4.4. Therefore, the setpoint uncertainty must be addressed in a plant-specific analysis. A description of the RadICS platform Setpoint Determination Methodology is provided in Section 9.2.2 of the RadICS TR. This Section describes the approach to be used to prepare the setpoint analysis support documentation for RadICS platform-based digital safety systems. The NRC staff's review of this approach is provided in Section 3.8 of this SE. The NRC staff determined the Radics LLC Setpoint methodology provides an acceptable process for establishing setpoints in a RadICS platform-based safety system.

Because determination of setpoints is not performed at the generic platform level, compliance with this criterion to determine adequacy of established setpoints remains a plant-specific activity, which must be performed during system development. See PSAI 7.11.

3.11.4 IEEE Std. 603-1991, Clause 7, "Execute features – functional and design requirements"

Section 7 of IEEE Std. 603-1991 contains five clauses that apply to execute features of safety systems. Execute features are the electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling.

Since the RadICS TR does not address a specific application of the platform, include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the RadICS platform against these regulatory requirements could be performed. Specifically, the following requirements were not evaluated:

- Clause 7.1, Automatic Control
- Clause 7.2, Manual Control
- Clause 7.3, Completion of Protective Action
- Clause 7.4, Operating Bypass
- Clause 7.5, Maintenance Bypass

Establishment of compliance with these criteria are a plant-specific action. See PSAI 7.11.

3.11.5 IEEE Std. 603-1991, Clause 8, "Power Source Requirements"

Clause 8 of IEEE Std. 603-1991 states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems, and that specific criteria unique to the Class 1E power systems can be found in IEEE Std. 308-1980.

Power supply requirements for the RadICS platform are described in Section 6.8, "PSWD Operation," of the RadICS platform TR. A RadICS system receives input from two 24 VDC power sources for operation. These power inputs are distributed to each of the system modules through connections on the chassis backplane. Each module contains a PSWD unit that receives the two 24 VDC inputs and converts these to voltage levels necessary to support module operation. The PSWD units are sub-components of the modules in which they are installed and therefore are included the RadICS analysis of platform equipment qualification in Section 3.6 of this SE. However, determination of the power sources external to the RadICS equipment to be provided to a RadICS platform-based safety system (i.e., 24 VDC power supplies, or 120 VAC power to the 24 VDC power supplies) is a plant-specific activity and will need to be addressed during plant system development. See PSAI 7.11.

3.12 Conformance with IEEE Std. 7-4.3.2-2003

RG 1.152, Revision 3, "IEEE Standard Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," states that conformance with the requirements of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants.

SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," contains guidance for the evaluation of the application of the requirements of IEEE Std. 7-4.3.2.

The requirements of IEEE Std. 7-4.3.2-2003 supplement the requirements of IEEE Std. 603 -1991 by specifying criteria that address hardware, software, firmware, and interfaces of computer-based safety systems. Consequently, the structure of IEEE Std. 7-4.3.2-2003 parallels that of IEEE Std. 603-1991. For those clauses where IEEE Std. 7-4.3.2-2003 contains no requirements beyond those found in IEEE Std. 603-1991 and SRP Chapter 7, Appendix 7.1-D contains no additional guidance, no review for compliance with IEEE Std. 7-4.3.2-2003 is required. Specifically, Clauses 4, 6, 7, and 8 were not reviewed. Thus, the subsections below are limited to those clauses where further evaluation is warranted. The review against the criterion of IEEE Std. 603-1991 is documented in Section 3.11 of this SE.

The NRC staff's evaluation is limited to consideration of generic platform design features, which do not depend on specific application development. All other aspects of IEEE Std. 7-4.3.2 conformance are plant specific criteria, which must be addressed during plant system development. The NRC staff identified PSAI 7.12 as an action to establish conformance with the IEEE Std. 7-4.3.2 clauses discussed below.

3.12.1 IEEE Std. 7-4.3.2-2003, Clause 5, "Safety System Criteria"

Clause 5 of IEEE Std. 7-4.3.2-2003 contains requirements to supplement the criteria of IEEE Std. 603-1991 Clause 5. In addition, SRP Chapter 7, Appendix 7.1-D, Section 5 contains specific acceptance criteria for IEEE Std. 7-4.3.2-2003, Clause 5.

The implementation of a computer-based safety system is a plant-specific activity. Since the RadICS TR does not address a specific application, the evaluation against the following requirements addresses the capabilities and characteristics of the RadICS platform that are relevant for adherence to each criterion of IEEE Std. 7-4.3.2.

IEEE Std. 7-4.3.2-2016, Clause 5.1, "Single-failure criteria"

IEEE Std. 7-4.3.2-2003 does not include criteria beyond those identified in IEEE Std. 603-1991 for Single Failure Criteria, however, the current version of IEEE Std. 7-4.3.2-2016 does include additional criteria. The NRC staff, therefore, reviewed RadICS platform design conformance to the current version of this criteria.

Clause 5.1 of IEEE Std. 7-4.3.2-2016 states that functions that are assumed to malfunction independently in the safety analysis shall not be affected by failure of a single programmable digital device (PDD).

Although this criterion is plant-specific and must be further addressed during safety system development, the NRC staff determined that a RadICS platform-based safety system has the capability of meeting these criteria provided that functional independence characteristics are established in accordance with the system design basis requirements of IEEE Std. 603-1991. Independence criteria are further addressed in the NRC staff evaluation of IEEE Std. 7-4.3.2, Clause 5.6.

Clause 5.1 of IEEE Std. 7-4.3.2-2010 also states that functions shall be configured (e.g., functionally distributed) such that a single PDD malfunction or software error shall not result in spurious actuations that are not enveloped in the plant design bases, accident, anticipated transients without scram (ATWS) provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of a single PDD malfunction or software error.

Distribution of functions within a RadICS based safety system is determined during application system development activities. The NRC staff considers a RadICS subsystem including a logic module to be a single PDD for the purposes of the criteria of IEEE Std. 7-4.3.2-2010. As such, allocation of safety functions to a single RadICS subsystem should consider plant design bases, accident analyses, and ATWS provisions. This criterion is plant-specific and must be addressed during safety system development.

IEEE Std. 7-4.3.2-2003 Clause 5.3, "Quality"

Clause 5.3 of IEEE Std. 7-4.3.2-2003 states that hardware quality is addressed in IEEE Std. 603-1998, and that software quality is addressed in IEEE/EIA Std. 12207.0-1996 and supporting standards. Clause 5.3 further states that the digital computer development process should include the development activities for both computer hardware and software, the

integration of the hardware and software, and the integration of the PDD with the safety system. Clause 5.3 includes six sub-clauses to identify activities beyond the requirements of IEEE Std. 603-1991 that are necessary to meet quality criterion for digital safety systems including software.

The RadICS platform components are developed to support a variety of safety critical applications in compliance with International Organization for Standardization (IS0)-9001. Radics LLC purchases and performs commercial grade dedication of the RadICS platform components to qualify them for use in safety-related applications for U.S. Nuclear Power Plants. To support this SE, Radics LLC submitted commercial grade dedication summary reports for each of the RadICS components of the platform (Ref. 8). These documents describe the Radics LLC commercial grade dedication activities and component qualification requirements. Section 3.4 of this SE includes an evaluation of the CGD processes used for the RadICS platform components.

IEEE Std. 7-4.3.2 also states: “In addition to the requirements of IEEE Std. 603-1998, the following activities necessitate additional requirements that are necessary to meet the quality criterion”

- Software Development – The equivalent of a software development activity is the logic ED development process described in Section 8 of the RadICS TR. See Section 3.5 of this SE for evaluation of RadICS logic development processes.
- Qualification of existing commercial computers – RadICS does not use computers however, commercial grade modules are qualified for use in RadICS systems by means of a 10 CFR Part 50, Appendix B QAPD commercial grade dedication process. See Section 3.4 of this SE for additional information on the Radics LLC commercial grade dedication processes.
- Use of software tools – Software tools are used extensively as part of the logic development processes. See evaluation of software tools criterion below.
- Verification and Validation – V&V activities performed on RadICS products are defined in a V&V plan. Details of the RadICS V&V processes are provided in Section 7.4 of the RadICS TR. RadICS V&V is evaluated in Section 3.5.1.6 of this SE.
- Configuration Management – CM activities performed for RadICS products are defined in a CM plan. Details of the RadICS configuration management processes are provided in Section 7.5 of the RadICS TR. RadICS configuration management is evaluated in Section 3.5.1.7 of this SE.
- Risk Management – The RadICS TR states: “The use of the FSMP described in Section 3.2.2.3 satisfies the risk management requirements of IEEE Std. 7-4.3.2-2003 Section 5.3.6.” See evaluation of Clause 5.3.6 below.

The Radics LLC QAPD employed for RadICS platform components is compliant with 10 CFR Part 50, Appendix B. All RadICS platform hardware and software development and maintenance activities are governed by the Radics LLC Appendix B QAPD as described in Section 3 of the RadICS TR (Ref. 1). An evaluation of the QAPD is provided in Section 3.5.1.3 of this SE.

Activities for development of RadICS platform-based I&C systems for US NPPs will be performed under the 10 CFR Part 50, Appendix B-compliant QAP. However, evaluation of development process implementation including system integration activities used for plant

application software must be evaluated for conformance with Clause 5.3 criteria during plant application development. See PSAI 7.12.

IEEE Std. 7-4.3.2-2003, Clause 5.3.1, "Software Development"

Clause 5.3.1 of IEEE Std. 7-4.3.2-2003 requires an approved software QAP consistent with the requirements of IEEE/EIA 12207.0-1996 for all software that is resident at runtime.

EPRI TR-106439, as accepted by the NRC SE dated July 17, 1997, and EPRI TR-107330, as accepted by the NRC SE dated July 30, 1998, provide guidance for the evaluation of existing commercial computers and software.

The RadICS logic development processes are evaluated in Section 3.5 of this SE. The RadICS CGD process is conducted in accordance with 10 CFR Part 21 to ensure the RadICS platform has the technical critical characteristics and level of quality consistent with a product developed under a 10 CFR Part 50, Appendix B compliant program. Logic implementation quality planning for the RadICS EDs is evaluated in Section 3.5.1.3 of this SE. The NRC staff found it to be acceptable for use in nuclear safety applications. Plant application logic QA planning activities must be performed in conjunction with application development activities. See PSAI 7.12.

IEEE Std. 7-4.3.2-2003 Clause 5.3.1.1, "Software Quality Metrics"

Clause 5.3.1.1 of IEEE Std. 7-4.3.2-2003 states that the use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met.
Since the RadICS platform logic is dedicated rather than developed under the Radics LLC QA program, this requirement does not apply within the context of development activities for the generic RadICS platform logic. Activities performed following commercial grade dedication of the RadICS platform components are however, subject to the established 10 CFR Part 50, Appendix B compliant Radics LLC QAP.

Section 7.7, "Development Process Metrics," of the RadICS TR (Ref. 1) describes processes used for tracking process related metrics during platform logic development. It states that "Quality metrics are used throughout the RadICS life cycle to assess the effectiveness of the software QA program." Process quality metrics include: anomaly reports, V&V open issues, and test coverage data.

The NRC staff determined quality metrics are considered throughout the RadICS logic development life cycle to assess whether logic ED quality requirements are met. It is noted that the responsibilities for the QA manager to develop measurable data relating to the effectiveness of the Radics LLC QAP should be included in a plant-specific QAP. An evaluation of metric usage for the application logic development must be conducted during plant-specific application development for any system based on the RadICS platform. See PSAI 7.12.

IEEE Std. 7-4.3.2-2003 Clause 5.3.2, "Software Tools"

Clause 5.3.2 of IEEE Std. 7-4.3.2-2003 states that software tools used to support software development processes and V&V processes shall be controlled under configuration

management, and that the tools shall either be developed to a similar standard as the safety related software, or that the software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

Software tools used to support RadICS FBL and ED development activities are described in Section 8.3 of the RadICS TR. Several commercial tools are used to produce the FBL and the ED logic for the RadICS Modules. Radics LLC also submitted a Tool Selection and Evaluation Report (Ref. 39) to support this evaluation. The RadICS TR lists eight different software tool types and eleven specific software tools that are used during RadICS logic development activities. The functions of each tool are described in the TR and a tool classification is assigned based upon specific tool characteristics and usage. The TR also identifies configuration items generated for each software tool.

Software tools used for RadICS FBL and ED development were not themselves developed in accordance with the Radics LLC 10 CFR Part 50, Appendix B QA program and are thus not classified as safety-related. These software tools are used in a manner such that defects not detected by the software tools will be detected by V&V activities described in the RadICS V&V Plan (Section 7.4, “RadICS Platform V&V,” of the RadICS TR, Reference 1) and corrected through the Radics LLC corrective action programs (See Section 3.3.4, “Corrective Action Program,” of the RadICS TR).

The NRC staff reviewed Section 8.3 of the RadICS TR and confirmed these tools are used in a manner, which is consistent with the criteria of IEEE Std. 7-4.3.2 Clause 5.3.2. The NRC staff also confirmed that software tools used for RadICS FBL and ED logic development are controlled under the Radics LLC configuration management program and that justifications for tool selection were provided in the Radics LLC Tool Selection and Evaluation Report (Ref. 39). The NRC staff could not evaluate the use of software tools for plant application logic development during this SE because no safety application was provided. The use and control of development tools for plant specific logic designs must be addressed during safety system application development. See PSAIs 7.2 and 7.12.

IEEE Std. 7-4.3.2-2003, Clause 5.3.3, “Verification and Validation”

Clause 5.3.3 of IEEE Std. 7-4.3.2-2003 states that a V&V program should be applied throughout the system development life cycle, and states that the software V&V effort shall be performed in accordance with IEEE Std. 1012-1998. This clause further states that requirements for the highest software integrity level 4 shall be applied to software developed using IEEE Std. 7-4.3.2.

The NRC evaluated the Radics LLC Verification and Validation program, described in Section 7.4 of the RadICS TR, and determined it to be compliant with the criteria of IEEE Std. 1012-2004, which is endorsed by RG 1.168. Though software is not used in the operating RadICS system, platform and application logic are developed using a software integrity level that is equivalent to software integrity level 4, as defined in IEEE Std. 1012-1998. Details of this evaluation are provided in Section 3.5.1.6 of this SE. See PSAI 7.12.

IEEE Std. 7-4.3.2-2003, Clause 5.3.4, “Independent V&V Requirements”

Clause 5.3.4 of IEEE Std. 7-4.3.2-2003 defines the levels of independence required for the V&V effort, in terms of technical independence, managerial independence, and financial

independence. This clause also requires development activities to be verified and validated by individuals or groups with appropriate technical competence who are also different than the individuals or groups who performed the development activities.

The NRC evaluation of the Radics LLC verification and validation processes, described in Section 7.4 of the RadICS TR, included an assessment of the type and level of independence maintained between the Application Design Bureau and the Verification and Validation and CGD Departments at Radics LLC. Evaluation of the RadICS V&V planning is provided in ection 3.5.1.6 of this SE. The NRC staff determined that Radics LLC's Verification and Validation and CGD Departments are adequately independent from the organization performing design activities. The Verification and Validation and CGD Departments do not report to members of the Application Design Bureau and therefore managerial independence is established. The Verification and Validation and CGD departments are not subject to the same budget constraints as is the Application Design Bureau and therefore financial independence is established. The Verification and Validation and CGD Department members are trained and qualified to levels comparable to members of the Application Design Bureau and therefore the Verification and Validation and CGD departments are technically competent and technical independence is established.

IEEE Std. 7-4.3.2-2003, Clause 5.3.5, "Software Configuration Management"

Clause 5.3.5 of IEEE Std. 7-4.3.2-2003 states that SCM shall be performed in accordance with IEEE Std. 1042-1987, and that IEEE Std. 828-1998 provides guidance for the development of software configuration management plans. IEEE Std. 828-2005 is endorsed by RG 1.169.

The NRC evaluated the Radics LLC configuration management program, described in Section 7.5 of the RadICS TR, and determined it to be compliant with the criteria of IEEE Std. 828-2005 as endorsed by RG 1.169. Details of this evaluation are provided in Section 3.5.1.7 of this SE. The NRC staff also confirmed that Radics LLC Configuration Management program includes all of the minimum required activities listed in Clause 5.3.5 of IEEE Std. 7-4.3.2-2003. See PSAI 7.12.

IEEE Std. 7-4.3.2-2003 Clause 5.3.6, "Software Project Risk Management"

Clause 5.3.6 of IEEE Std. 7-4.3.2-2003 defines the risk management (RM) required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.3.6, "Software Project Risk Management," provides acceptance criteria for software project Risk Management. This clause states that software project risk management is a tool for problem prevention and be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. It also states that software project risks may include technical, schedule, or resource related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety-related functions. Additional guidance on the topic of rick management is provided in IEEE/EIA Std. 12207.0-1996, "IEEE Standard for Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology – Software Life Cycle Processes," and IEEE Std. 1540-2001, "IEEE Standard for Life Cycle Processes B Risk Management."

Risk management is part of the overall project RadICS planning process and is addressed as part of the RadICS management plan. See Section 3.5.1.1 of this SE.

Risk management for a RadICS system includes identification and assessment of risk factors associated with a project. Potential risks identified during any phase of the Radics LLC development lifecycle process are identified and methods for addressing and mitigating these risks are then implemented. The RadICS system design planning work instructions describe risk areas to be considered and provide guidance for identifying and addressing risk items. Risks and hazards associated with RadICS-based systems are also addressed by the processes established by the FSMP. These processes are further discussed in the Clause 5.4.2.1 below.

The RadICS system design planning work instructions call for a project specific management plan to describe methods used for risk identification, assessment and management, with particular attention to risks that have the potential for compromising safety. The project specific management plan would also describe the mechanisms for tracking risk factors and implementing contingency plans.

The Radics LLC Software Quality Assurance Plan also describes several activities that can be used to identify project risks during RadICS system development. The Radics LLC Quality Assurance process includes methods of identifying and addressing product quality issues during development as well as processes for escalating issues that pose risks to RadICS logic quality or safety goals.

The NRC staff determined that risk management has been adequately implemented within the RadICS safety life cycle as a tool for problem prevention. Risk Management is performed at all levels of the Radics LLC system project development process and the risk management processes provide adequate coverage for potential RadICS platform problem areas. RadICS project risks include technical, schedule, and resource related risks that could compromise quality goals, or affect the ability of the RadICS safety system to perform safety-related functions. RadICS Risk management processes therefore meet the criteria of IEEE Std. 7-4.3.2-2003, Clause 5.3.6. See PSAI 7.12.

IEEE Std. 7-4.3.2-2003, Clause 5.4, “Equipment Qualification”

Clause 5.4 of IEEE Std. 7-4.3.2-2003 defines computer equipment qualification requirements. SRP Chapter 7, Appendix 7.1-D, Section 5.4, “Equipment Qualification,” provides acceptance criteria for computer EQ. IEEE Std. 7-4.3.2, Clause 5.4 states that in addition to the EQ criteria provided by IEEE Std. 603-1991 and Section 5.4 of SRP Chapter 7, Appendix 7.1-C, additional criteria, as defined in Sections 5.4.1 and 5.4.2, are necessary to qualify digital computers for use in safety systems. These sections are discussed below.

IEEE Std. 7-4.3.2-2003, Clause 5.4.1, “Computer System Testing”

Clause 5.4.1 of IEEE Std. 7-4.3.2-2003 discusses the software that should be operational on the computer system while qualification testing is being performed. SRP Chapter 7, Appendix 7.1-D, Section 5.4.1, “Computer System Testing,” provides acceptance criteria for computer EQ testing. IEEE Std. 7-4.3.2, Clause 5.4.1 states that computer EQ testing should be performed while the computer is functioning, with software and diagnostics that are representative of those used in actual operation.

Section 3.6 of this SE discusses the evaluation of the environmental qualification program for the RadICS platform. Radics LLC complied with the guidance of EPRI TR-107330 for the generic qualification of a PLC platform. EQ testing of the RadICS platform-based representative system was performed while the test system modules were functioning. Test application logic and standard platform diagnostic functions (as described in Section 6.4 of the RadICS TR), representative of those to be used in actual operation were in operation during EQ testing. The test application logic was specifically designed to support qualification testing of the RadICS platform while providing generic functionality of the test system. Based on the evaluation in Section 3.6 of this SE and review of the RadICS equipment qualification test summary report (Ref. 8), the NRC staff concludes that the Radics LLC qualification program met the requirement for computer testing of the RadICS platform, subject to satisfactory resolution of the plant-specific action items in Section 3.4 of this SE.

IEEE Std. 7-4.3.2-2003, Clause 5.4.2, "Qualification of Existing Commercial Computers"

Clause 5.4.2 of IEEE Std. 7-4.3.2-2003 defines the Qualification of Existing Commercial Computers for use in SR applications in nuclear power plants. SRP Chapter 7, Appendix 7.1-D, Section 5.4.2, "Qualification of Existing Commercial Computers," states that EPRI TR-106439 and EPRI TR-107330 provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

Radics LLC commercially dedicated the pre-developed RadICS platform logic in accordance with guidance of EPRI TR-106439 and generically qualified the RadICS platform in accordance with the guidance of EPRI TR-107330. Section 3.4 of this SE includes an evaluation of the CGD processes used to support RadICS platform development.

The NRC staff determined the generic qualification of the RadICS platform, performed in conjunction with commercial grade dedication activities, complies with the guidance of both EPRI TR-106439 and EPRI TR-107330. There are plant specific activities that must be performed during application development to ensure conformance with these criteria for specific plant environmental conditions. See PSAI 7.4.

IEEE Std. 7-4.3.2-2003, Clause 5.4.2.1, "Preliminary Phase of the commercial off the shelf (COTS) Dedication Process"

This clause of IEEE Std. 7-4.3.2-2003 specifies that the risks and hazards of the dedication process are to be evaluated, the safety functions identified, configuration management established, and the safety category of the system determined.

Risks and hazards associated with RadICS-based systems are addressed by the processes used for product development through a program established by a FSMP (Ref. 10). The RPC Radiy FSMP describes the process and procedures used to design; verify and validate; and maintain the Radiy FSC which constitutes the components of the RadICS platform. The FSMP also defines management responsibilities including responsibilities for performing risk management activities.

The NRC staff reviewed the RPC Radiy FSMP (Ref. 10) and confirmed that risk management is performed at all levels of the Radiy FSC project development process and the risk management

processes provide adequate coverage for potential RadICS platform component logic and hardware problem areas.

Risks and hazards of the dedication process are evaluated by Radiy LLC as a project management activity to be performed during plant specific application development. The safety functions for a plant system are identified during application development which is not included in the scope of this evaluation. Radiy LLC processes for establishing configuration management during application development are described in Section 7.5 of the TR and are evaluated in Section 3.5.1.7 of this SE. The NRC staff determined that risk management has been adequately implemented within the RPC Radiy processes as a tool for problem prevention. The established RadICS processes for addressing system risks and hazards therefore satisfy the criteria of IEEE Std. 7-4.3.2-2003, Clause 5.4.2.1.

IEEE Std. 7-4.3.2-2003 Clause 5.4.2.2, "Detailed Phase of the COTS Dedication Process"

This clause of IEEE Std. 7-4.3.2-2003 involves evaluation of the commercial grade item for acceptability based on detailed acceptance criteria. In particular, critical characteristics of the COTS item are to be evaluated and verified. The characteristics are identified in terms of physical, performance, and development process attributes. This requirement is addressed by the guidance in EPRI TR-106439. Specifically, a critical design review is specified to identify physical, performance, and dependability (i.e., development process) characteristics, which are then verified by one or more of the fours methods identified in the guide.

RadICS platform components are developed in accordance with a FSMP for the purpose of being qualified for use in nuclear safety applications. Radics LLC performs commercial grade dedication of these components using a 10 CFR Part 50, Appendix B compliant QA program to facilitate their use in RadICS platform-based designs. The Radics LLC commercial grade dedication processes are described in Section 4 of the RadICS TR, and is evaluated in Section 3.4 of this SE.

Platform component changes or new product development activities are governed by the Radics LLC 10 CFR Part 50, Appendix B compliant quality assurance processes. Therefore, RadICS platform components are COTS components and these components will continue to be dedicated as commercial grade components.

The characteristics for each CGD component of the RadICS platform are identified in terms of physical, performance, and development process attributes. A critical design review is performed to identify physical, performance, and dependability characteristics, and these characteristics are verified using acceptable methods. CGD reports (Refs. 21 through 29)

provide documented evidence of compliance with each of the characteristics described using acceptable methods of verification. Section 3.4 of this SE provides an evaluation of this CGD process. The established RadICS processes for performing platform component CGD activities therefore satisfy the criteria of IEEE Std. 7-4.3.2-2003, Clause 5.4.2.2.

IEEE Std. 7-4.3.2-2003, Clause 5.4.2.3, "Maintenance of Commercial Dedication"

This clause of IEEE Std. 7-4.3.2-2003 specifies that documentation supporting CGD of a computer-based system or equipment is to be maintained as a configuration control item.

In addition, modifications to dedicated computer hardware, software, or firmware are to be traceable through formal documentation.

All components of the RadICS platform are commercially dedicated and maintained by Radics LLC. These components are designed and developed in accordance with European nuclear safety standards and are then dedicated under the Radics LLC 10 CFR 50, Appendix B compliant quality assurance program.

The NRC staff reviewed the RadICS Commercial Grade Dedication Plan and determined that documents supporting CGD of RadICS components are maintained as configuration control items. Section 3.4 of this SE provides an evaluation of this CGD process. Modifications to dedicated RadICS components are traceable through formal QA documentation. The processes used to dedicate and maintain RadICS components therefore comply with Clause 5.4.2.3 of IEEE Std. 7-4.3.2.

IEEE Std. 7-4.3.2-2003, Clause 5.5, “System Integrity”

Clause 5.5 of IEEE Std. 7-4.3.2-2003 states that in addition to the system integrity criteria provided by IEEE Std. 603-1991, the digital system shall be designed for computer integrity, test and calibration, and fault detection and self-diagnostics activities. These attributes are further defined in Clause 5.5.1, “Design for computer integrity,” Clause 5.5.2, “Design for test and calibration,” and Clause 5.5.3, “Fault detection and self-diagnostics.” There are no specific acceptance criteria shown in SRP Chapter 7, Appendix 7.1-D, Section 5.5, “System Integrity.”

IEEE Std. 7-4.3.2-2003, Clause 5.5.1, “Design for Computer Integrity”

Clause 5.5.1 of IEEE Std. 7-4.3.2-2003 states that the computer must be designed to perform its safety function when subjected to conditions, either external or internal, that have significant potential for defeating the safety function.

The RadICS platform includes features to provide fault detection and mitigation capabilities. The RadICS platform includes diagnostics and self-testing (see Section 3.7.3 of this SE) that support a high-level of system integrity. However, Radics LLC did not define a specific system architecture or application for the RadICS platform. Instead, Radics LLC defined a generic platform that can be used in a wide range of applications or configurations. Therefore, the NRC staff only evaluated the features provided in the generic platform. This evaluation can be used to support development of future plant-specific logic applications.

The RadICS platform qualification activities discussed in Section 3.6 of this SE, provide suitable evidence that the RadICS platform is capable of maintaining plant safety when subjected to environmental conditions that have the potential to defeat implemented safety functions.

The NRC staff determined that fault detection and mitigation design features provided for the RadICS platform can be used to facilitate performance of safety functions in a reliable manner. Determination of compliance with the criterion of IEEE Std. 7-4.3.2, Clause 5.5.1 requires a plant-specific action item to address system integrity for a plant-specific application (see Section 7.12). Plant specific system requirements must be established to identify safety system preferred failure modes for each safety function performed.

IEEE Std. 7-4.3.2-2003, Clause 5.5.2, “Design for Test and Calibration”

Clause 5.5.2 of IEEE Std. 7-4.3.2-2003 states that test and calibration functions shall not adversely affect the ability of the computer to perform its safety function, and that it shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change. The clause further states that V&V, configuration management, and QA be required for test and calibration functions on separate computers such as test and calibration computers that provide the sole verification of test and calibration data, but that V&V, configuration management, and QA is not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

Online self-diagnosis functions are provided in the RadICS platform to support test and calibration requirements. These are described in Section 6.4 of the RadICS TR and are evaluated in Section 3.7.3 of this SE.

Qualification tests performed for the RadICS platform were conducted with self-diagnosis functions operating in conjunction with the test application performing basic functions. See Equipment Qualification Test Summary Report (Ref. 8) for additional information on these tests. The performance of the RadICS equipment during these tests demonstrated that diagnosis features did not adversely affect the ability of the system to perform its functions. Therefore, the NRC staff determined the diagnosis capabilities provided by the RadICS platform conform to this requirement.

Calibration and test functions performed by the separate MATS computer are described in Section 3.2.4 of this SE. MATS computer and software are non-safety-related and is isolated from the RadICS safety system during normal operations. The MATS functions therefore, cannot affect safety functions performed by the RadICS safety system during operation. The MATS computer does not provide the sole verification of test and calibration data for the RadICS safety system and is therefore not subject to V&V, configuration management, and QA requirements of safety-related systems.

Maintenance activities performed on a RadICS based safety system, including periodic surveillance testing, will be defined based on the plant-specific system requirements. Determination of test and calibration requirements and establishment of surveillance tests necessary to ensure that the identifiable single failures are detected are plant-specific activities See PSAI 7.8.

IEEE Std. 7-4.3.2-2003, Clause 5.5.3, “Fault Detection and Self-Diagnostics”

Clause 5.5.3 of IEEE Std. 7-4.3.2-2003 discusses fault detection and self-diagnostics, and states that if reliability requirements warrant self-diagnostics, then computer programs should contain functions to detect and report computer system faults and failures in a timely manner, and that these self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function.

Section 3.7.3 of this SE provides an evaluation of the RadICS diagnostics and self-test capabilities. These tests and diagnostics provide functions to detect failures in the system

hardware, as well as to detect system failure modes identified in the RadICS FMEDA. See Section 3.5.2.6 of this SE for more information on the RadICS FSC FMEDA.

If errors are encountered during system operation, self-diagnosis features will respond by either providing an alarm or by setting output signals to pre-defined states depending on the severity of the fault identified. Alarms or predefined states are to be defined during plant system development and plant-specific Failure Analysis should be performed for each plant-specific application.

Hardware and software based diagnostic features of the RadICS platform provide an acceptable method of detecting and reporting computer system faults and failures in a timely manner. The RadICS platform is therefore acceptable for providing fault detection in support of safety-related applications. However, because Radics LLC did not define the actions to be taken when Type III faults are detected and did not identify specific self-tests or periodic surveillance testing necessary to detect and address the effects of system failures on plant safety, there may be additional fault-detection and diagnostic function requirements to provide more comprehensive coverage of identified system failures. Therefore, determination of IEEE Std. 7-4.3.2, Clause 5.5.3 compliance is a plant-specific evaluation item. See PSAIs 7.8 and 7.12.

IEEE Std. 7-4.3.2-2003, Clause 5.6, “Independence”

Clause 5.6 of IEEE Std. 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std. 603-1991, data communications between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, “Independence,” provides acceptance criteria for Independence. This guidance states that the regulation at 10 CFR Part 50, Appendix A, GDC 24, “Separation of protection and control systems,” requires the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Establishment of communications among redundant portions of a safety system or between the RadICS safety system and other non-safety systems is a plant plant-specific activity. The base platform architecture identified in the RadICS TR does not specify any direct connections or bi-directional communications between a RadICS platform-based safety system and any other system. Since the RadICS TR does not address a specific application or provide a definitive safety system design, the evaluation of the RadICS platform against the communications independence aspect of this criteria is limited to features and capabilities of its communication interfaces. Section 3.2.3 of this SE describes communications interfaces available within the scope of the RadICS platform. Section 3.10 of this SE contains an evaluation of the Radics LLC communications capabilities with respect to the guidance in DI&C-ISG-04. This evaluation determined that when properly implemented, data communications between safety channels of a RadICS based system or communications between safety and external non-safety systems would not inhibit the performance of the systems safety functions.

The NRC staff finds that the communications capabilities of the RadICS platform provide acceptable design features to enable communications independence when appropriately configured. However, the specific interconnections defined for an application must be determined and addressed during plant application development. See PSAI 7.12 of this SE for plant specific action items.

IEEE Std. 7-4.3.2-2016, Clause 5.7, "Capability for Test and Calibration"

Clause 5.7 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. SRP Chapter 7, Appendix 7.1-D, Section 5.7, "Capability for Test and

Calibration," provides guidance for evaluating and determining acceptability of test and diagnostic software. It states that the reviewer should carefully examine the capability of the software to test itself. It includes guidance on comparing the relative complexity between diagnostics software and operational software and promotes a balance between added complexity of diagnostics and the gain of confidence in the system.

Clause 5.7 of IEEE Std. 7-4.3.2-2016 states that safety system configuration shall not require change or modification to support periodic automated or manual surveillance testing. It also states that measurement and test equipment (M&TE) used for safety systems shall not adversely affect the safety system functionality and that wireless receivers/transmitters on temporarily-connected measurement and test equipment shall be disabled prior to connecting to safety-related equipment.

The NRC staff evaluated the RadICS self-diagnosis and test and calibration capabilities for conformance with these criteria. Section 3.7.3 of this SE describes and evaluates the Self-Diagnostics features of the RadICS platform. The RadICS platform design includes self-diagnostics features to detect failures within the RadICS based safety system during operation. The use of wireless receivers/transmitters on temporarily-connected M&TE is not discussed in the RadICS TR and is therefore not evaluated or approved for use by the NRC staff. There are also no requirements or expectations that RadICS configuration changes would need to be made to support periodic automated or manual surveillance testing.

The level of complexity introduced to the RadICS system by the diagnostic features described in Section 6.4 of the RadICS TR was determined to be commensurate with the safety functions to be performed and the benefits provided by these features justify their inclusion into the RadICS platform design. The NRC staff finds that the RadICS platform complies with the criteria of IEEE Std. 7-4.3.2-2016, Clause 5.7. A plant specific activity to establish conformance with criteria of IEEE Std. 7-4.3.2-2016, Clause 5.7 for diagnostic functions included in plant application logic will need to be performed. See PSAI 7.12.

IEEE Std. 7-4.3.2-2016, Clause 5.8, "Information Displays"

Clause 5.8 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. However, SRP Chapter 7, Appendix 7.1-D, Section 5.8, "Information Displays," notes that, in the past, information displays only provided a display function and, therefore, required no two-way communication. More modern display systems may also have included control functions and, therefore, the NRC staff reviews the capacity for information displays to ensure that incorrect functioning of the information displays does not prevent the safety function from being performed when necessary.

The 2016 version of IEEE Std. 7-4.3.2 provides additional criteria to be considered. Clause 5.8 of IEEE Std. 7-4.3.2-2016 states that safety-related controls and indications shall be dedicated to specific safety divisions.

The RadICS platform scope does not include a safety information display or control components. The criteria of IEEE Std. 7-4.3.2-2016, Clause 5.8 is therefore not applicable to the RadICS Platform. See PSAI 7.12.

IEEE Std. 7-4.3.2-2016 Clause 5.9, "Control of Access"

Clause 5.9 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. For this reason, there is no additional guidance beyond that found in Section 5.9 of SRP Chapter 7, Appendix 7.1-C and RG 1.152, Revision 3.

The 2016 version of IEEE Std. 7-4.3.2 provides additional criteria to be considered however, this criterion is currently not endorsed by the NRC and is instead addressed by the criteria of RG 1.152, Revision 3. The regulatory position Section in RG 1.152, Revision 3, provides guidance on security regarding electronic access to a safety system. SRP acceptance criteria for this guidance can be found in SRP Chapter 7, Appendix 7.1-D, Section 9. The evaluation of the RadICS platform against this guidance is contained in Section 3.13 of this SE.

IEEE Std. 7-4.3.2-2003, Clause 5.10, "Repair"

This clause states that no requirements beyond IEEE Std. 603-1998 are necessary. Therefore, no evaluation was performed for this clause.

IEEE Std. 7-4.3.2-2003, Clause 5.11, "Identification"

Clause 5.11 of IEEE Std. 7-4.3.2-2003 states that (1) identification requirements specific to software systems (i.e., firmware and software identification) shall be used to assure the correct software is installed in the correct hardware component, (2) means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools, and (3) physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std. 603-1991, Clause 5.11. SRP Chapter 7, Appendix 7.1-D, Section 5.11, "Identification," provides acceptance criteria and adds that the identification should be clear and unambiguous. The identification should include the revision level and should be traceable to configuration control documentation that identifies the changes made by that revision for computer Equipment Qualification.

Establishing software/firmware identification requirements and providing the means for retrieving that identification information are directly related to the Radics LLC QAP, in particular, configuration management. Section 3.5.1.7 of this SE contains the evaluation of RadICS configuration management process as it applies to maintaining the configuration of RadICS platform logic. However, the RadICS configuration management process for application logic is outside of the scope of this review. See PSAI 7.12.

RadICS configuration items are managed and controlled in accordance with the Radics LLC configuration management plan. Logic, FBL and ED version management and change control

mechanisms are applied to all configuration items. The configuration information of each hardware and logic component of a RadICS based safety system is securely maintained as RadICS system configuration management records. Logic configuration versions for the assemblage of system logic components are defined in terms of a formally released, configuration-controlled project.

Identification requirements specific to RadICS platform logic are used to assure the correct platform logic and FBLs are installed into the correct RadICS modules. Identification of installed logic can be performed using the RadICS RPCT engineering tool. Physical identification of the RadICS hardware modules will be performed in accordance with the identification requirements in IEEE Std. 603-1991, Clause 5.11. See PSAI 7.12.

Based on the processes reviewed and observed during the regulatory audit for RadICS logic identification, the NRC staff determined the RadICS platform complies with the guidance of IEEE Std. 7-4.3.2-2003, Clause 5.11 for its platform logic. However, assurance that proper hardware and plant application logic configuration is established and maintained is an activity that must be performed during plant application development and implementation. See PSAI 7.12.

IEEE Std. 7-4.3.2-2003, Clause 5.15, “Reliability”

Clause 5.15 of IEEE Std. 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std. 603-1991, when reliability goals are identified, the proof of meeting the goals shall include the software. Guidance is provided in SRP Chapter 7, Appendix 7.1-C, Section 5.15.

As stated in RG 1.152, Revision 3, the NRC does not endorse the concept of quantitative reliability goals as the sole means of meeting regulations for reliability of digital computers in safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system.

Determination of the reliability requirements for a digital safety system is a plant-specific activity that requires an assessment of a full system design, its application, system platform logic, and the safety life cycle processes. Since the RadICS TR does not address a specific plant application, nor establish a specific safety system design, the evaluation against this requirement is limited to consideration of the reliability characteristics of the RadICS digital platform and the quality of its platform logic. Section 3.5.2.7 of this SE includes the NRC staff assessment and evaluation of RadICS Reliability characteristics. While the evaluation indicates the platform satisfies this requirement, a plant-specific evaluation of RadICS system reliability

against specific plant system reliability requirements is necessary to establish full conformance with Clause 5.15. See PSAI 7.12.

3.13 Secure Development and Operational Environment

A secure development environment (SDOE) must be established to ensure that unneeded, unwanted and undocumented code is not introduced into a digital safety system. This SDOE must also protect digital safety systems from unwanted and unauthorized access or changes to the system.

Regulatory Guide 1.152, Revision 3, describes a method that the NRC considers acceptable to comply with the regulatory criteria to promote high functional reliability, design quality, and establish secure development and operational environments for the use of digital computers in SR systems at nuclear power plants. The guidance for secure development and operational environments states that potential vulnerabilities should be addressed in each phase of the digital safety system life-cycle. The overall guidance provides the basis for physical and logical access controls to be established throughout the digital system development process to address the susceptibility of a digital safety system to inadvertent access and modification.

Regulatory positions 2.1 – 2.5 of RG 1.152, Revision 3 identify controls that an applicant should implement during the development activities for safety related digital systems. The RadICS platform was originally developed under a European nuclear quality program, which is described in Section 3.2 of the RadICS TR, and was not specifically designed to conform to the criteria of RG 1.152. However, the RadICS platform was developed for nuclear power plant applications, including safety-related systems, and it includes security features that can be used to prevent or mitigate the effects of inadvertent access during development and operation.

Section 11 of the RadICS TR describes the secure development environment, the RadICS platform vulnerability assessment, and the implementation of SDOE controls. This Section states the following:

> The RadICS platform secure development environment is designed to meet the guidance of RG 1.152 by providing (1) measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded, and unwanted modifications and (2) protective actions taken against a predictable set of undesirable acts that could challenge the integrity, reliability, or functionality of a digital safety system during operations.

Below the NRC staff evaluated the RadICS SDOE to confirm conformance with the criterion of RG 1.152 as follows. For criteria that could not be evaluated, PSAI 7.13 specifies actions to be performed during plant-specific application development.

RG 1.152, Revision 3, Regulatory Position 2.1, “Concepts Phase”

Identification and Description of Secure Operational Environment Design Features

Regulatory Position 2.1 states that digital safety system design features required to establish a secure operational environment for the system should be identified and described as part of an application. Evaluation of a safety system against this part of the regulatory position is, in part, a plant-specific activity that requires an assessment of a completed system design.

Additionally, cyber-security and other security controls applied to the latter phases of the life cycle that occur at a licensee’s site are not part of the 10 CFR Part 50 licensing process and fall under the purview of other licensee programs. See PSAI 7.13.

RPC Radiy and Radics LLC have implemented several design features in the RadICS that are intended to eliminate vulnerabilities associated with company security management and the digital equipment development processes. These design features are listed as security measures and are described in Section 11.1 of the RadICS TR and are evaluated in Section 3.5 of this SE as an integral part of the RadICS development processes.

Assessment of Potential Susceptibilities

Regulatory Position 2.1 states that the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's life cycle that could degrade its reliable operation should be assessed. This assessment should identify the potential challenges to maintaining a secure operational environment for the digital safety system and a secure development environment for development life cycle phases.

RPC Radiy addressed this part of the regulatory position by performing a development environment vulnerability assessment. The results of this vulnerability assessment are documented in the FSC Security Analysis Report (Ref. 36). This analysis identifies the RadICS platform development assets, vulnerabilities and secure controls used to identify and mitigate risks associated with unwanted, unneeded and undocumented functionality being introduced during system development or modification. This RPC Radiy FSC development environment vulnerability assessment includes assessments of: hardware, software and logic, configuration, and network vulnerabilities. The NRC staff concludes that these vulnerability assessments can be used to show conformance with the criteria of RG 1.152, Position 2.1; however, the establishment of a secure environment for application logic development remains a plant specific action. See PSAI 7.13.

Remote Access

Regulatory Position 2.1 states that remote access to the safety system should not be allowed. In RG 1.152, remote access is defined as the ability to access a computer, node, or network resource that performs a safety function or that can affect the safety function from a computer or node that is located in an area with less physical security than the safety system (e.g., outside the protected area).

Evaluation of a safety system against this part of the regulatory position is a plant-specific activity that requires an assessment of a completed system design. The RadICS platform design partially addresses this part of the regulatory position by incorporating design features that limit connectivity between RadICS safety systems and other external systems. Section 3.2.3.2 of this SE describes external communications interfaces of the RadICS platform and Section 3.10 of the SE evaluates these interfaces for regulatory compliance. These interfaces include features that can be credited to restrict remote accessibility for RadICS systems. See PSAI 7.13.

RG 1.152, Revision 3, Regulatory Position 2.2, "Requirements Phase"

Definition of Secure Operational Environment Functional Requirements

Regulatory Position 2.2 states that the functional performance requirements and system configuration for a secure operational environment; interfaces external to the system; and requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance should be defined. The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements.

The conformance of a safety system with this part of the regulatory position was not evaluated because defining and establishing requirements for external communication interfaces is a plant-specific activity that requires an assessment of the safety system design. See PSAI 7.13.

Verification of SDOE Requirements

Regulatory Position 2.2 states that the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system's SDOE features.

Section 11.4 of the RadICS TR identifies secure development and operational environment controls that are included in the RadICS platform design. The identified controls include: communications, platform diagnostics, and access control design features. These SDOE features have been implemented in accordance with the platform development processes described and evaluated in Section 3.5 of this SE. These development processes provide a framework for establishing correctness, completeness, accuracy, testability, and consistency attributes and were determined by the NRC staff to be acceptable. Application specific SDOE features may also be identified during system requirements development activities. Such features would need to be included as application design requirements and would need to be incorporated into the application logic during the application development process. See PSAIs 7.2 and 7.13.

Use of Predeveloped Software (Logic) and Systems

Regulatory Position 2.2 states that the requirements specifying the use of pre-developed software and systems (e.g., reused software and COTS systems) should address the reliability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).

The RadICS platform modules and electronic designs, which include PFBL and AFBL libraries are developed and maintained by RPC Radiy, which is not an 10 CFR Part 50, Appendix B supplier.

RadICS modules, including platform logic designs are commercially dedicated by Radics LLC for use in nuclear applications. Section 4 of the RadICS TR describes the process for performing commercial grade dedication of RadICS Modules including methods used during commercial grade dedication to address safety system reliability. Section 3.4 of this SE provides an evaluation of the Radics LLC commercial grade dedication processes.
The RadICS platform logic is pre-developed and is subject to application specific safety system reliability requirements. See Section 3.5.2.7, "Reliability Analysis," of this SE. Application ED logic will be developed by Radiy LLC under its QA program and in accordance with a licensee's 10 CFR Part 50, Appendix B QA processes. See PSAI 7.2 for more information on vendor oversight activities to be performed during application development. The NRC staff concludes that the Radiy LLC CGD processes can be used show conformance with the criteria of RG 1.152 Position 2.2; however, reliability requirements are plant specific and therefore must be verified during application logic development. See PSAI 7.13.

Prevention of the Introduction of Unnecessary Requirements

Regulatory Position 2.2 states that the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code should be prevented during the requirements phase.

Evaluation of a safety system against this part of the regulatory position is a plant-specific activity that requires an assessment of a completed system design. See PSAI 7.2 for more information on V&V activities to be performed during application development including the development of system requirements specifications and PSAI 7.13 for establishing conformance with this criterion. RPC Radiy partially addresses this part of the regulatory position by requiring an independent reviewer check the requirements specifications in order to detect and correct the insertion of requirements that have an undesirable effect on the secure operational environment of the system. This ensures that the secure operational environment features of the RadICS Platform are not compromised by changes or the introduction of new functions or products to the platform design. The NRC staff concludes that these secure operational environment features can be used show compliance with the criteria of RG 1.152 Position 2.2; however, the additional plant specific actions must be taken to ensure that unnecessary requirements are not included in the application logic. See PSAI 7.13.

3.12.3 RG 1.152, Revision 3, Regulatory Position 2.3, “Design Phase”

System Features: Translation of SOE Requirements into Design Configuration Items

Regulatory Position 2.3 states that the safety system design features for a secure operational environment identified in the system requirements specification should be translated into specific design configuration items in the system design description.

Evaluation of a safety system against this part of the regulatory position is a plant-specific activity that requires an assessment of a completed system design. See PSAI 7.2 for more information on V&V activities to be performed during application development including development of a system design description. Radics LLC partially addresses this part of the regulatory position by using requirements traceability methods to confirm the traceability of the RadICS platform SDOE features from requirements to design specifications. See Section 3.5.2.5 of this SE for evaluation of the Radiy requirements traceability processes. See PSAI 7.13.

Physical and Logical Access Controls

Regulatory Position 2.3 states that physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life cycle.

RPC Radiy partially addresses this part of the regulatory position because the physical, logical and administrative access control features established for platform logic development are based on the results of the completed FSC security analysis. Evaluation of a specific safety system against this part of the regulatory position is a plant-specific activity that requires an assessment of a completed system design. See PSAI 7.2 for more information on V&V activities to be performed during application development including performance of an application development environment vulnerability assessment.

The NRC staff reviewed the platform FSC security analysis report (Ref. 36) and determined the vulnerability assessments provided can be used show conformance with the criteria of RG 1.152, Position 2.3 for platform logic physical and logical access control functions; however, the implementation of physical and logical access controls into application logic remains a plant specific action. See PSAI 7.13.

The RadICS platform secure development environment ensures that no unintended electronic design logic is included in the platform and related documentation during electronic design development, and that unintended changes to the platform logic installed in the system are prevented.

RPC Radiy implements configuration control measures to: detect unauthorized changes to controlled documents (e.g., specifications, design descriptions and test reports); control access to the document control system and the electronic design development and storage environment; independently verify that the content of production copies of electronic designs match the controlled master copies, label controlled media and storage devices, and identify electronic design versions that are under development, approved for production, and retired. The RadICS platform TR states that security measures that are designed to eliminate credible vulnerabilities associated with company security management and the digital equipment development process have been implemented. However, the review of the application logic secure development environment controls implemented in a RadICS platform-based system is a plant-specific activity. See PSAI 7.13 for further information on this activity.

The programming ports used to modify RadICS FPGA or CPLD logic on system modules are inaccessible during normal system operation. [

] generate a signal that can be used to initiate an alarm in the main control room. Configuration of this alarm is a PSAI. See PSAI 7.2.

The NRC staff finds that the RadICS platform contains secure operational environment features that can be used to support the plant specific safety applications. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criterion to be a plant specific action. See PSAI 7.13.

Prevention of the Introduction of Unnecessary Design Features

Regulatory Position 2.3 states that measures should be taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.

RadICS development processes partially address this part of the regulatory position by requiring an independent review of the electronic design specifications in order to detect and correct the insertion of design features that could have an undesirable effect on the secure operational environment of the system. Requirements traceability methods are used to verify that the secure operational environment features from the requirement phase are correctly translated into the design, and to ensure that unauthorized functionality is not introduced into the design. The NRC staff finds that RadICS processes for verifying the translation of SDOE design features is acceptable and can be used to support the plant specific application of the RadICS

platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criterion to be a plant specific action. See PSAI 7.13.

3.12.4 RG 1.152, Revision 3, Regulatory Position 2.4, "Implementation Phase"

Transformation from System Design Specification to Design Configuration Items

Regulatory Position 2.4 states that the developer should ensure that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete.

RadICS development processes partially address this part of the regulatory position by using requirements traceability methods. Requirements traceability methods are used to verify that the secure operational environment features from design specification to design configuration items.

The NRC staff finds that RadICS processes for verifying the translation of SDOE design specifications is acceptable and can be used to support the plant specific application of the RadICS platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers these criteria to be a plant specific action. See PSAI 7.13.

Implementation of Secure Development Environment Procedures and Standards

Regulatory Position 2.4 states that the developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system.

RPC Radiy addresses this part of the regulatory position through implementation of development environment control procedures and by implementing physical, logical and administrative controls to construct and maintain a secure development environment that minimizes the potential for unintended modifications to the system.

During the regulatory audit, the NRC staff reviewed Radiy procedures used to implement the secure development environment and found them to be adequate means of establishing the secure platform development environment. The NRC staff finds that RPC Radiy secure platform development environment controls and procedures meet the criterion of regulatory position 2.4 and are, therefore, acceptable.

Establishment of a secure development environment for application logic development remains a plant specific activity which must be performed during application logic development. See PSAI 7.13.

Accounting for Hidden Functions in the Code

Regulatory Position 2.4 states that hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system should be accounted for.

Radics LLC addresses this part of the regulatory position by performing various V&V activities. An independent V&V team is used to check the system electronic designs and FBLs. The independent V&V team verifies the electronic designs by performing functional and structural unit testing, which would detect and correct the insertion of functions and vulnerable features that would have an undesirable effect on the secure operational environment of the system. The NRC staff evaluated the V&V processes and activities used for RadICS platform development. See Sections 3.5.1.6 and 3.5.2.2 of this SE for more information on this evaluation.

The NRC staff finds that Radics LLC processes for detecting and addressing errors in the platform and logic implementation are acceptable and can be used to support the plant specific application of the RadICS platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criterion to be a plant specific action. See PSAI 7.13.

3.12.5 RG 1.152, Revision 3, Regulatory Position 2.5, "Test Phase"

Validation of Secure Operational Environment Design Configuration Items

Regulatory Position 2.5 states that the secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items.

The conformance of a safety system with this part of the regulatory position was not evaluated because it is an activity that requires an assessment of the plant-specific safety system design. See PSAI 7.13.

Configuration of Secure Operational Environment Design Features

Regulatory Position 2.5 states that the developer should correctly configure and enable the design features of the secure operational environment. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity.

The compliance of a safety system with this part of the regulatory position was not evaluated because it is an activity that requires an assessment of the plant-specific safety system design. See PSAI 7.13.

4.0 SUMMARY

The NRC staff determined the RadICS platform, consisting of modules described in the RadICS TR, their design features, the platform logic embedded in electronic boards and the processes used to produce them are sufficient to support compliance with the applicable regulatory requirements for a plant-specific use for safety-related I&C systems. This determination is applicable for use of the RadICS platform in safety-related applications provided that each plant-specific use satisfies the limitations and conditions delineated in Section 5.0 of this SE and the system is properly installed and used. The NRC staff further concludes that the RadICS platform can be used in safety-related systems to provide reasonable assurance of adequate protection of public health, safety and security based on the technical evaluation provided in

Section 3.0 of this SE. On this basis, the NRC staff determined the RadICS platfrm is acceptable for use in safety-related I&C systems.

5.0 LIMITATIONS AND CONDITIONS

For each generic open item and plant-specific action item that applies to the applicant's or licensee's use of the RadICS platform, an applicant or licensee referencing this SE should demonstrate that applicable items have been satisfactorily addressed. The applicable items provide limitations and conditions for the RadICS platform's use, as reviewed by the NRC staff and documented within this SE.

6.0 GENERIC OPEN ITEMS

On the basis of its review of the RadICS platform, the NRC staff has identified the following generic, open items:

6.1 Qualified Platform Components – This SE is limited to components of the RadICS platform listed in Table 3.2-1 of this SE. Use of other components for safety-related applications is not approved by the NRC and may be subject to additional evaluation and qualification testing.

7.0 PLANT-SPECIFIC ACTION ITEMS

The following plant-specific actions should be performed by an applicant or licensee referencing the RadICS topical report for a safety-related system based on the RadICS platform.

7.1 RadICS Platform Changes – An applicant or licensee referencing the topical report should demonstrate that the RadICS platform used to implement the plant-specific system is unchanged from the generic platform addressed in this SE. Otherwise, the licensee should clearly and completely identify any modification or addition to the generic RadICS platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes. In addition, the applicant must verify that modules, features, and or functions that require configuration are properly configured and tested to meet system requirements.

7.2 Application Logic Development Process – An applicant or licensee referencing the topical report should provide oversight to ensure the development of its Application Logic is performed in accordance with an acceptable process that is equivalent to the processes described in Sections 7 and 8 of the RadICS TR and evaluated in Section 3.5 of this SE.

7.3 System Cycle Time – The applicant or licensee must perform timing analyses and functional testing of the application logic implementation and system configuration to demonstrate that response time performance satisfies application specific requirements established in the plants safety analysis report.

7.4 Plant-Specific Equipment Environmental Qualification – The applicant or licensee must demonstrate that the generic qualification envelope established for the RadICS platform

bounds the corresponding plant-specific environmental conditions for the location(s) in which the equipment is to be installed.

7.4.1 Temperature and Humidity – The applicant or licensee should ensure that specific equipment configuration of RadICS components to be installed is consistent with that of the RadICS equipment used for environmental qualification tests. See Section 3.6.1 of this SE for boundary conditions established for the RadICS platform during temperature and humidity testing.

7.4.2 Class 1E to Non-Class 1E Isolation – The applicant or licensee should ensure that all RadICS interfaces between 1E and Non-1E circuits do not exceed the maximum test voltages to which the RadICS equipment is qualified to operate. See Section 3.6.2 of this SE for boundary conditions established for the RadICS platform during isolation testing.

7.4.3 Electro-Magnetic Compatibility – The applicant or licensee should ensure that specific equipment configuration of RadICS components to be installed is consistent with that of the RadICS equipment used for EMC qualification tests. See Section 3.6.3 of this SE for boundary conditions established for the RadICS platform during EMC testing.

7.4.4 Seismic Qualification – An applicant or licensee referencing the topical report must demonstrate that the qualified seismic withstand capability of the RadICS platform bounds the plant-specific seismic withstand requirements. See Section 3.6.4 of this SE for boundary conditions established for the RadICS platform during Seismic testing.

7.5 Failure Modes and Effects Analysis – An applicant or licensee referencing the topical report must perform a system-level FMEA to demonstrate that the application-specific use of the RadICS platform identifies each potential failure mode and determines the effects of each. The RadICS FMEDA (evaluated in Section 3.5.2.6 of this SE) is intended to be used as input data to support a system-level FMEA and reliability analysis for an NPP-specific RadICS Platform system. The FMEA should demonstrate that single-failures, including those with the potential to cause a non-safety system action that results in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions, as applicable.

The applicant or licensee should ensure system failure states identified in the FMEA are consistent with system requirements and should review how errors and failures are indicated and managed upon being detected.

7.6 Application Specific System Reliability – An applicant or licensee referencing the topical report should perform a system-level evaluation of the degree of redundancy, diversity, testability, and quality provided in a RadICS platform-based safety system to determine if the degrees provided are commensurate with the safety functions being performed. An applicant or licensee should confirm that a resultant RadICS platform-based system

continues to satisfy any applicable reliability goals that the plant has established for the system.

This plant-specific action should consider the effect of possible failures, system-level design features provided to prevent or limit the failures' effects, and any application-specific inclusion of a maintenance bypass functionality to support plant operations.

7.7 Setpoint Methodology – An applicant or licensee referencing the topical report must perform an analysis of accuracy, repeatability, thermal effects and other necessary data for use in determining the contribution of the RadICS platform to instrumentation uncertainty in support of setpoint calculations.

7.8 System Testing and Surveillance – Because a combination of surveillance, RadICS diagnostics and automatic self-tests are necessary to provide comprehensive coverage of platform failures, the applicant or licensee referencing the topical report must establish periodic surveillance testing necessary to detect system failures for which automatic detection is not provided. The applicant or licensee must also define appropriate surveillance intervals to provide acceptable comprehensive coverage of identifiable system failure modes.

7.9 Diversity and Defense-In-Depth Analysis – An applicant or licensee referencing the topical report must perform a plant-specific D3 analysis for safety protection system applications of the RadICS platform. If the RadICS platform internal diversity features are to be credited as a means of mitigating logic CCF consideration, then the following additional PSAIs should be performed by the licensee.

7.9.1 Self-Diagnostics Design Requirements – The licensee must establish requirements for validation testing of Type III self-diagnostics features to ensure plant safety requirements are satisfied.

7.9.2 Plant Specific Fail-Safe Behavior Requirements Definition – Fail Safe state requirements shall be established by the licensee for all RadICS system outputs to ensure plant safety is achieved when RadICS system logic failures (e.g., Type I, II, or III faults) are detected by system self-diagnostic functions.

7.9.3 Conservation of Existing Diversity Measures – The applicant or licensee must confirm that diversity attributes of the existing protection system are preserved in the upgraded system. This diversity may be expressed in the signal selection and protection system functional algorithms established and accepted for the plant design.

If the RadICS protection system is to be used for performing a reactor trip function then the applicant or licensee must also ensure that the RadICS system is diverse from anticipated transients without scram (ATWS) systems as required by 10 CFR Part 50.62.

7.10 Communications (DI&C-ISG-04) – The NRC staff determined that the RadICS platform includes features to support satisfying various sections and clauses of DI&C-ISG-04. An applicant or licensee referencing the topical report must evaluate the RadICS platform-based system to verify it fully satisfies the criteria of DI&C ISG-04 as applicable. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with its direct and indirect consequences. The applicant or licensee should also develop procedures to control the use of the MATS to ensure that safety logic module are removed from service prior to enabling the MATS tuning access interface.

7.11 IEEE Std. 603 – The NRC staff determined that the RadICS platform is capable of satisfying various sections and clauses of IEEE Std.603-1991. An applicant or licensee referencing the topical report should identify the approach taken to satisfy each applicable clause of IEEE Std.603-1991 with consideration of the plant-specific design basis.

This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events including direct and indirect consequences. Therefore, an applicant or licensee should demonstrate that the plant-specific and application-specific use of the RadICS platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

7.12 IEEE Std. 7-4.3.2 – The NRC staff determined that the RadICS platform is capable of satisfying various sections and clauses of IEEE Std. 7-4.3.2-2003. An applicant or licensee referencing the topical report should identify the approach taken to satisfy each applicable clause of IEEE Std. 7-4.3.2-2003 with consideration of the plant-specific design basis.

This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events including direct and indirect consequences. Therefore, the applicant or licensee should demonstrate that the plant-specific and application-specific use of the RadICS platform satisfies the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.

7.13 Secure Development and Operational Environment – An applicant or licensee referencing the topical report for a safety-related plant-specific application should ensure that a secure development and operational environment has been established for its plant-specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.”

8.0 REFERENCES

1. RadICS License Topical Report Submittal and Request for Safety Evaluation, September 20, 2016 (ADAMS Package Accession No. ML16274A376).
2. Radics LLC Submittal of Digital I&C Platform Topical Report Support Documents, December 3, 2016, Tool Selection and Evaluation Report, Radics LLC Product Safety

Manual, Radics LLC Functional Safety Management Audit Plan (ADAMS Package Accession No. ML16344A238).

3. NRC RadICS TR Acceptance Review Letter, April 5, 2017 (ADAMS Accession No. ML16281A459).
4. Radics LLC Digital I&C Platform Topical Report Supplemental Information, September 15, 2017 (ADAMS Package Accession No. ML17275A198).
5. Phase 1 RAIs from NRC to Radics LLC, March 1, 2018 (ADAMS Accession No. ML18058B946).
6. Radics LLC Responses to the Request for Additional Information, April 13, 2018 (ADAMS Package Accession No. ML18107A173).
7. Submittal of RadICS Digital I&C Platform Topical Report Supplemental Information Update, Updated discussion on Diversity and Defense-In-Depth, August 2, 2018 (ADAMS Package Accession No. ML18219A841).
8. Submittal of Phase 2 Documents for RadICS Digital I&C Platform Topical Report, Equipment Qualification Test Summary Report, Commercial Grade Dedication Summary Reports for all RadICS Modules, August 10, 2018 (ADAMS Package Accession No. ML18227A197) (EQ Test Summary Report ADAMS Accession No. ML18227A167).
9. Regulatory Audit Report for the RadICS Digital Platform Licensing Topical Report, May 21, 2018 (ADAMS Accession No. ML18130A894).
10. Radiy FPGA-based Safety Controller Functional Safety Management Plan, September 13, 2016 (ADAMS Accession No. ML16274A350).
11. Radiy FPGA-based Safety Controller Functional Safety Management Plan Phase 3 Extension, August 29, 2016 (ADAMS Accession No. ML16274A354).
12. Commercial Grade Dedication Plan for Digital Input Module, Rev. 4, August 19, 2016 (ADAMS Accession No. ML16274A365).
13. Commercial Grade Dedication Plan for Logic Module, Rev. 1, September 7, 2016 (ADAMS Accession No. ML16274A366).
14. Commercial Grade Dedication Plan for Digital Output Module, Rev. 1, September 7, 2016 (ADAMS Accession No. ML16274A367).
15. Commercial Grade Dedication Plan for Analog Input Module, Rev. 2, September 7, 2016 (ADAMS Accession No. ML16274A378).
16. Commercial Grade Dedication Plan for Analog Output Module, Rev. 1, September 7, 2016 (ADAMS Accession No. ML16274A379).
17. Commercial Grade Dedication Plan for Optical Communication Module, Rev. 1, September 7, 2016 (ADAMS Accession No. ML16274A380).
18. Commercial Grade Dedication Plan for Chassis, Rev. 1, September 7, 2016 (ADAMS Accession No. ML16274A381).
19. Commercial Grade Dedication Plan for Input/Output Connections Protection Module, Rev. 1, September 7, 2016 (ADAMS Accession No. ML16274A382).
20. Commercial Grade Dedication Plan for Ventilation Module, Rev. 1, September 7, 2016 (ADAMS Accession No. ML16274A383).

21. Commercial Grade Dedication Report for Digital Input Module, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A171).

22. Commercial Grade Dedication Report for Logic Module, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A169).

23. Commercial Grade Dedication Report for Digital Output Module, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A172).

24. Commercial Grade Dedication Report for Analog Input Module, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A170).

25. Commercial Grade Dedication Report for Analog Output Module, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A168).

26. Commercial Grade Dedication Report for Optical Communication Module, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A174).

27. Commercial Grade Dedication Report for Chassis, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A179).

28. Commercial Grade Dedication Report for Input/Output Connections Protection Module, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A177).

29. Commercial Grade Dedication Report for Ventilation Module, Rev. 0, July 27, 2018 (ADAMS Accession No. ML18227A180).

30. RadICS Overall Verification and Validation Plan, Rev. 3, September 9, 2016 (ADAMS Accession No. ML16274A352).

31. Radiy FPGA-based Safety Controller Integration Test Plan, Rev. 3, September 1, 2016 (ADAMS Accession No. ML16274A363).

32. Radiy FPGA-based Safety Controller Safety Validation Test Plan, Rev. 4, August 26, 2016 (ADAMS Accession No. ML16274A356).

33. Radiy FPGA-based Safety Controller Configuration Management Plan, Rev. 3, August 29, 2016 (ADAMS Accession No. ML16274A351).

34. Radiy FPGA-based Safety Controller Safety Requirements Specification, Rev. 3, September 1, 2016 (ADAMS Accession No. ML16274A355).

35. RadICS Product Safety Manual (D11.1), Rev. 2.3, February 28, 2016 (ADAMS Accession No. ML16344A248).

36. Radiy FPGA-based Safety Controller Security Analysis Report, Rev. 1.1, June 7, 2013 (ADAMS Accession No. ML16274A353).

37. RadICS Product Architecture Document (D5.1), Rev. 3, September 2, 2016 (ADAMS Accession No. ML16274A362).

38. RadICS Equipment Qualification Test Plan, 2016-RTS002-EQTP-004, Rev. 0, September 20, 2016 (ADAMS Accession No. ML16274A364).

39. RadICS Tool Selection and Evaluation Report, Rev. 2.0M, November 12, 2014 (ADAMS Accession No. ML16344A247).

40. RadICS Functional Safety Management Audit Plan, Rev. 1.1M, December 3, 2012 (ADAMS Accession No. ML16344A249).

Appendix A: Comments on Draft Safety Evaluation for RadICS Topical Report and NRC Staff Responses

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
1	Page 5 / Line 10	Clarification	Change RPC--Radiy to RPC Radiy	Accepted
2	Page 5 / Lines 16-21	Clarification	Change Radics LLC TR to RadICS TR in four places	Accepted
3	Page 5 / Line 36	Clarification	Change RPC-Radiy to Radics LLC	Accepted
4	Page 5 / Line 36	Clarification	Change Kirovograd to Kropyvnytskyi. Formal name changed by local government.	Accepted
5	Page 5 / Line 38	Clarification	Change RPC-Radiy's to RPC Radiy's	Accepted
6	Page 6 / Line 2	Editorial	Change date to March 1, 2018	Accepted
7	Page 6 / Line 3	Editorial	Change reference to 5	Accepted
8	Page 6 / Lines 7-8	Clarification	Change sentence to read: The NRC staff conducted an audit of the RadICS platform development documents at the Kinectrics, Inc. ~~Radics LLC~~ facilities in Toronto, Canada on April 2 through 5, 2018.	Accepted
9	Page 10 / Line 38	Clarification	Change RADIY to Radics	Accepted
10	Page 10 / Line 44	Clarification	Change Radiy to RPC Radiy	Accepted
11	Page 10 / Line 46	Clarification	Change ISO 9001:2008 to ISO 9001:2015	Accepted Revision 0 still refers to ISO 9001:2008. The current ISO should be reflected in the -A version.
12	Page 11 / Line 18	Clarification	Change Radics LLC to RadICS	Accepted
13	Page 11 / Line 46	Clarification	Change Radics LLC to RadICS	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
14	Pages 14-15 / Table 3.2.-1	Clarification	Add hardware identifier numbers to Table 3.2-1 This change makes the SER consistent with the information in Table 1 of the "EQ Summary Report 2016-RTS002-EQTSR-040" (ML18227A167).	Accepted – Confirmed all hardware numbers to be correct.
15	Pages 16 / Lines 9-10	Clarification	Change Radics LLC to RadICS-based in two places	Accepted
16	Page 17 / Figure 3.2.2.1	Clarification	Reverse the order of the Diagnostics and Application Logic blocks to better represent the software architecture and the relationship to RPCT.	Accepted
17	Page 22 / Lines 9-10	Clarification	Change Radiy chassis to RadICS chassis in two places	Accepted
18	Page 24 / Lines 5-6	Clarification	Change RadICS platform chassis to RadICS chassis in two places	Accepted
19	Page 24 / Line 14	Clarification	Change sentence to read: … types of programmable logic~~;~~ RadICS platform FPGA logic, self-diagnostics FPGA and CPLD logic, …	Accepted
20	Page 24 / Line 23	Clarification	Change sentence to read: … data between modules via the chassis backplane bus, performing self-testing, and processing … The information is consistent with RadICS Topical Report Section 6.4.	Accepted
21	Page 24 / Line 36	Clarification	Change Radiy LLC to RPC Radiy	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
22	Page 25 / Line 16	Clarification	Change sentence to read: The logic development processes for ~~both~~ the FPGA and CPLD platform … The information on the CPLD library was provided to NRC in Enclosure 3 to Radics LLC submittal dated August 2, 2018 (ML18219A841), RadICS Digital I&C Platform Topical Report Supplemental Information Update," that updated discussion on Diversity and Defense-In-Depth.	Accepted
23	Page 25 / Line 26	Clarification	Change sentence to read: Application Logic, FPGA and CPLD Platform function block libraries are different and distinct … The information on the CPLD library was provided to NRC in Enclosure 3 to Radics LLC submittal dated August 2, 2018 (ML18219A841), RadICS Digital I&C Platform Topical Report Supplemental Information Update, that updated discussion on Diversity and Defense-In-Depth.	Accepted
24	Page 25 / Line 40	Clarification	Change RadICS LLC to Radics LLC	Accepted
25	Page 25 / Line 46	Clarification	Change RadICS QA program to Radics LLC QA program	Accepted
26	Page 26 / Line 14	Clarification	Change RadICS to Radics LLC	Accepted
27	Page 28 / Lines 1-2	Clarification	Change RadICS QA program to Radics QA Program Document (QAPD)	Accepted
28	Page 28 / Line 2	Clarification	Change RadICS to Radics LLC	Accepted
29	Page 28 / Line 3	Clarification	Change QAP [QA program] to QAPD	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
30	Page 31 – Line 20	Clarification	Change RadICS to Radics	Accepted
31	Page 31 / Line 35	Clarification	Change RadICS to Radics LLC	Accepted
32	Page 34 – Line 12	Clarification	Change Radics LLC to RadICS	Accepted
33	Page 34 – Line 18	Clarification	Change Radics LLC to RadICS	Accepted
34	Page 34 – Line 35	Clarification	Change Radics LLC to RPC Radiy	Accepted
35	Page 34 – Line 41	Clarification	Change Radics LLC to RadICS	Accepted
36	Page 34 / Line 50	Editorial	Change SFMP to FSMP	Accepted
37	Page 35 – Line 4	Clarification	Change Radics LLC to RadICS	Accepted
38	Page 35 / Line 19	Clarification	Change SIL 4 to software integrity level 4	Accepted
39	Page 36 – Line 23	Clarification	Change RadICS to Radics LLC	Accepted
40	Page 36 – Line 24	Clarification	Change Radics to Radiy	Accepted
41	Page 36 – Line 25	Clarification	Change Radiy to Radics	Accepted
42	Page 39 – Line 31	Clarification	Change Radics LLC to RPC Radiy	Accepted
43	Page 39 – Line 32	Clarification	Change Radics to RadICS and Radics LLC to RPC Radiy	Accepted
44	Page 39 / Line 35	Editorial	Change 3.5.1.2. to 3.4.1.2	Not Accepted - There is no Section 3.4.1.2 in the SE. The RadICS SIL scheme is described in Section 3.5.1.2, “Development Plan,” of the SE.
45	Page 39 / Line 39	Clarification	Change FBL to HW	Not Accepted – Figure 1 in the FSMP identifies an FBL Development team. This part of the SE is addressing software, logic, and FBL development

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
				processes and not hardware development processes.
46	Page 40 / Line 5	Clarification	Change SIL 4 to software integrity level 4	Accepted
47	Page 40 / Line 30	Clarification	Change sentence to read: The security vulnerability assessments described in Chapter 11 ~~Sections 11.2 and 11.3~~ replace the security analyses …	Accepted: These sections include "vulnerability assessments" in their titles but it is OK to abstract to the term security assessment as suggested.
48	Page 40 / Line 33	Clarification	Change RadICS to Radics LLC	Accepted
49	Page 40 / Line 41	Clarification	Change SIL 4 to software integrity level 4	Accepted
50	Page 41 / Line 43	Editorial	Change 4.1.2.3 to 3.2.2.3	Accepted
51	Page 42 – Line 4	Clarification	Change Radics LLC to RadICS	Accepted
52	Page 42 – Line 32	Clarification	Change Radics LLC to RadICS	Accepted
53	Page 44 / Lines 4-5	Clarification	Change sentence to read: … qualification test team ~~and a metrology test team which are~~ that is under authority of the project	Not Accepted – Both the FSC safety validation test plan and the FSC Safety Validation test plan include descriptions of a metrology test team as stated. If this is not accurate, then Radiy should explain why.
54	Page 46 – Line 38	Clarification	Change Radics LLC FSC to RadICS	Accepted
55	Page 47 / Line 28	Clarification	Change RadICS to Radics LLC	Accepted
56	Page 48 – Line 23	Clarification	Change Radics LLC to RPC Radiy	Accepted
57	Page 49 / Line 47	Clarification	Change third bullet to read: Analog Input (Deviation more than 2% of span)	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
58	Page 51 / Line 48	Clarification	Change sentence to read: The following specification documents were provided to or audited by the NRC to support evaluation of the RadICS Safety Requirements Specification (SRS) documentation …	Accepted
59	Page 53 / Line 35	Clarification	Change sentence to read: The qualification program developed for the ~~Radics LLC Radics LLC~~ RadICS QTS addressed …	Accepted
60	Page 53 / Line 39	Clarification	Change Radics LLC RadICS platform to RadICS platform	Accepted
61	Page 53 / Line 43	Clarification	Change Kinetrics to Kinectrics	Accepted
62	Page 54 / Line 28	Clarification	Add new bullet: Chassis and Module Connections This change makes the SER consistent with the information on page 9 of the "EQ Summary Report 2016-RTS002-EQTSR-040" (ML18227A167).	Accepted
63	Page 54 / Lines 32-36	Clarification	Change sentence to read: Table 9-1 of the RadICS topical report (Reference 1) specifies the qualification envelope for temperature and humidity to be 40 to 140 ~~122~~ Deg. F (4.4 to 60 ~~50~~ Deg. C) and 10 to 90% relative humidity (non-condensing). Environmental test levels are specified to be 34.9 ~~35~~ to 148.5 ~~140~~ Deg. F (1.6 ~~1.7~~ to 64.7 ~~60~~ Deg. C) and 5 to 95% relative humidity (non-condensing), thus encompassing the platform temperature and humidity specifications. This change makes the SER consistent with the information on page 24 of the "EQ	Not Accepted: This data is changed in R1 of the TR which has not been submitted for evaluation. Staff cannot rely on information in a document that has not been submitted for review. The only docketed revision has the original data.

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
			Summary Report 2016-RTS002-EQTSR-040" (ML18227A167).	
64	Page 55 / Line 8	Editorial	Change 17330 to 107330	Accepted
65	Page 58 / Line 41	Clarification	Change first bullet in Section 3.6.3.4 to read: IEC 61000-4-4, "Power Leads: Test Voltage Level: 2~~1~~ kV maximum" This change makes the SER consistent with the information in Section G.13 of the "EQ Summary Report 2016-RTS002-EQTSR-040" (ML18227A167).	Not Accepted: This data is changed in R1 of the TR which has not been submitted for evaluation. Staff cannot rely on information in a document that has not been submitted for review. The only docketed revision has the original data.
66	Page 60 / Lines 23-29	Clarification	Change sentence to read: Table 9-1, "Generic Qualification Envelope for the RadICS Digital Safety I&C Platform," of the RadICS platform TR specifies the seismic qualification requirements to be 5 triaxial OBE tests with a Required Response Spectrum (RRS) curve given as Figure 4-5 in EPRI TR-107330 with a peak acceleration of 9.8 g between 4.5 and 16 Hz and minimum zero period acceleration (ZPA) of 4.9 g followed by one triaxial SSE test with a RRS curve given as Figure 4-5 in EPRI TR-107330 with a peak acceleration of 14 g between 4.5 and 16 Hz and minimum ZPA of 7 g. This change makes the SER consistent with the information on pages 25 and 54-57 of	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
			the “EQ Summary Report 2016-RTS002-EQTSR-040” (ML18227A167).	
67	Page 61 / Lines 18-23	Clarification	Change the paragraph to read: ~~Section 5.2.1 of the RadICS platform TR states that “input acceleration levels used for Cabinet Seismic Resistance Test is set high enough to cover the floor response spectrum range of power plants in the U.S.” Due to the generic applicability of this safety evaluation, the NRC staff was not able to confirm the accuracy of this statement for all U.S. plants thus, a~~An applicant referencing this safety evaluation will need to confirm that RadICS platform equipment seismic qualification levels are within plant specific design basis seismic conditions for SSE and OBE earthquakes. This information was not provided in the RadICS Topical Report and appears to be a copy error from the recently issued SER for the MELTAC Topical Report.	Accepted
68	Page 61 / Lines 26-31	Clarification	Change the paragraph to read: <u>The acceleration envelope established for RadICS equipment exceeded the acceleration</u> ~~Acceleration~~ levels specified for generic plant SSE in EPRI TR-107330. ~~greater than the acceleration envelope established for RadICS equipment. Because the RadICS platform equipment was not tested to acceleration levels greater than 7 g, it does not meet the criteria for generic seismic qualification at plant sites~~	Not Accepted – The test report does not show that acceleration levels called for by EPRI 107330 (Figure 4-5) were achieved. Therefor the platform is qualified to the acceleration levels achieved by the test which were less than the acceleration levels called for by EPRI 107330.

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
			~~having greater than 7 g postulated plant specific SSE acceleration levels.~~ This change makes the SER consistent with the information on pages 25 and 54-57 of the "EQ Summary Report 2016-RTS002-EQTSR-040" (ML18227A167).	Revised wording to simplify and state safety conclusion without referring to the 7G limit.
69	Page 62 / Lines 4-10	Clarification	Change the paragraph to read: Based on review of the RadICS seismic test results and supporting analysis, the NRC staff determined that the RadICS platform ~~does not~~ fully ~~satisfy~~ satisfies the guidance criteria of EPRI TR-107330 because seismic withstand performance requirements were ~~not~~ demonstrated for the maximum acceleration level of 14 g for a generic SSE. ~~However, t~~ The NRC staff finds that seismic qualification of the RadICS platform has been acceptably demonstrated for OBE and SSE events up to acceleration levels shown in the OBE and SSE test results spectra in the RadICS Equipment Qualification Test Report (Reference 8). This change makes the SER consistent with the information on pages 25 and 54-57 of the "EQ Summary Report 2016-RTS002-EQTSR-040" (ML18227A167).	Not Accepted – The test report does not show that acceleration levels called for by EPRI 107330 (Figure 4-5) were achieved. Therefor the platform is qualified to the acceleration levels achieved by the test which were less than the acceleration levels called for by EPRI 107330 (Figure 4-5). No changes will be made to SE unless additional test data is provided by Radiy.
70	Page 62 / Lines 43-45	Clarification	Change the paragraph to read: The second is 10 CFR 50.36(c)(1)(ii)(A), which provides basis for timing requirements ~~commitments~~ by requiring the inclusion of the limiting safety systems settings for nuclear reactors in the plant technical specifications, "so	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
			chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded." Radics LLC did not make any commitments on this matter.	
71	Page 63 / Line 20	Clarification	Change Radics to Radics LLC	Accepted
72	Page 65 / Lines 21-24	Clarification	Change the sentence to read: The NRC staff determined that design features, operation of the RadICS system, and PSAI 7.3 ~~Radics LLC's commitments to perform timing analysis and tests~~ provide sufficient confidence that provide sufficient confidence that RadICS based safety systems will operate deterministically to meet the recommendations of BTP 7-21 and is therefore acceptable. Radics LLC did not make any commitments on this matter. This information was not provided in the RadICS Topical Report and appears to be a copy error from the recently issued SER for the MELTAC Topical Report.	Accepted
73	Page 65 / Lines 36-37	Clarification	Change the sentence to read: … all safety ~~discrete~~ outputs to ~~fail-~~safe states.	Accepted
74	Page 66 / Line 2	Clarification	Change the paragraph to read: Type III – User defined level faults. The user defines criticality of detected errors and their processing algorithm. The responses to Type III faults are not addressed by the RadICS platform design. Methods to identify and mitigate these faults must be	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
			implemented within application design during plant specific development activities	
75	Page 66 / Line 24	Clarification	Change Radics LLC to RadICS	Accepted
76	Page 69 / Lines 33-41	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
77	Page 70 / Lines 13-15	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
78	Page 70 / Lines 19-21	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
79	Page 70 / Lines 24-26	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
80	Page 70 / Lines 29-50	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
81	Page 71 / Lines 1-13	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
82	Page 71 / Lines 35-47	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
83	Page 71 / Lines 45-47	Clarification	Delete the sentences: Therefore, if a licensee chooses to credit internal diversity between features of the Quartus II tool, a separate diversity assessment would need to be performed as an application specific action item. See PSAI 7.9. This information was identified as implicit attributes of the FPGA and CPLD configuration tool that was not explicitly defined nor verified for the RadICS Platform diversity strategy in Enclosure 3 to Radics LLC submittal dated August 2, 2018	Accepted – Though it is a true statement, it can be deleted as requested. The PSAI still stands and must be addressed by an applicant referencing this TR.

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
			(ML18219A841), "RadICS Digital I&C Platform Topical Report Supplemental Information Update," that updated discussion on Diversity and Defense-In-Depth.	
84	Page 72 / Lines 2-3	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
85	Page 72 / Lines 5-11	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
86	Page 72 / Lines 9-11	Clarification	Delete the sentences: Therefore, a licensee activity should be performed to determine sufficient separation is established when this defensive measure is to be credited. See PSAI 7.9.1. Separation is achieved on the modules because the FPGA and CPLD are discrete and separate components, as described in RadICS Topical Report Section 6.8. The communication protocol, between the FPGA and CPLD is described in RadICS Topical Report Section 6.3.3.2.6.	Accepted
87	Page 72 / Lines 13-28	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
88	Page 72 / Line 30	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
89	Page 72 / Lines 32-44	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
90	Pages 73-76 / Table 3.8-1 (Items 1 – 6)	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
91	Page 76 – Item 6	Clarification	Radics LLC expected a determination on the logic diversity for the three domains (Electronic Design safety functions, self-test and diagnostic functions, and the PSWD functions). The inherent diversity for different timing or order of execution based on the parallel processing of these diverse functions using three separate clock domains. This information was provided to NRC in Enclosure 3 to Radics LLC submittal dated August 2, 2018 (ML18219A841), "RadICS Digital I&C Platform Topical Report Supplemental Information Update," that updated discussion on Diversity and Defense-In-Depth.	Revised: Deleted the last sentence of this item. Since this table is provided for information only, there is no need to include safety determinations here. Also added the following statement to add credit to the logic diversity level based on the RadICS design features. "[ ]."
92	Page 77 / Lines 5-6	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 1)	Accepted
93	Page 80 / Line 2	Clarification	Change sentence to read: … provide communications between LMs or OCMs in different safety divisions … This information was provided to NRC in the response to	Accepted – Change as recommended.

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
			RAI-P1-02 in Radics LLC submittal dated April 13, 2018 (ML18107A173), “Response to Request for Additional Information for RadICS Topical Report.”	
94	Page 80 / Lines 48-49	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
95	Page 82 / Lines 24-27	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
96	Page 82 / Lines 32-39	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
97	Page 83 / Lines 1-9	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
98	Page 83 / Lines 35-36	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
99	Page 83 / Lines 39-40	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
100	Page 83 / Lines 46-47	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
101	Page 83 / Line 48	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
102	Page 84 / Line 2	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
103	Page 84 / Line 5	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
104	Page 84 / Line 16	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
105	Page 85 / Lines 5-7	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
106	Page 87 / Lines 9-18	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
107	Page 87 / Lines 28-29	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
108	Page 88 / Lines 49-50	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
109	Page 89 / Lines 7-8	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
110	Page 89 / Lines 10	Clarification	Change Radiy to Radics	Accepted
111	Page 89 / Lines 44-47	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
112	Page 90/ Lines 2-4	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
113	Page 90 / Lines 46-47	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
114	Page 91 / Lines 18-19	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
115	Page 101 / Line 34	Clarification	Change Radiy LLC to Radics LLC	Accepted
116	Page 101 / Line 39	Clarification	Change RPS Radiy to RPC Radiy	Accepted
117	Page 101 / Lines 43-44	Clarification	Change ISO 9001:2008 to ISO 9001:2015 in two places	Accepted:Revision 0 still refers to ISO 9001:2008. The current ISO should be reflected in the -A version.
118	Page 102 / Line 2	Clarification	Change RadICS to Radics LLC	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
119	Page 102 / Line 7	Clarification	Change Radiy to Radics	Accepted
120	Page 102 / Line 14	Clarification	Change QAP policy to QA policy	Accepted
121	Page 102 / Line 15	Clarification	Change sentence to read: The Radics LLC Appendix B based QAP policy is established in the RadICS QAPD ~~Description (QAPD) document,~~ (QAPD-001), which …	Accepted
122	Page 102 / Line 17	Clarification	Change QAP to QAPD	Accepted
123	Page 102 / Line 28-29	Clarification	Change QAP to QAPD in two places	Accepted
124	Page 104 / Line 32	Clarification	Change Radics LLC to RadICS platform	Accepted
125	Page 104 / Line 35	Clarification	Change Radics LLC based to RadICS platform-based	Accepted
126	Page 105 / Line 34	Clarification	Change sentence to read: … should be established ~~as~~ during plant-specific application development.	Accepted
127	Page 105 / Line 34	Clarification	Add sentence at end of paragraph: See PSAI 7.10.	Accepted
128	Page 110 / Line 20	Clarification	Change Radics LLC to RadICS	Accepted
129	Page 111 / Line 6	Clarification	Change QAP to QAPD	Accepted
130	Page 111 / Line 7	Clarification	Change RadICS to Radics LLC	Accepted
131	Page 111 / Line 22	Clarification	Change QAP to QAPD	Accepted
132	Page 111 / Lines 24-25	Clarification	Change QAP to QAPD in two places	Accepted
133	Page 113 / Line 1	Clarification	Change Radiy to Radics	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
134	Page 113 / Line 19	Clarification	Change integrity level (Level 4) to software integrity level 4	Accepted
135	Page 113 / Line 26	Clarification	Change SIL 4 to software integrity level 4	Accepted
136	Page 114 / Line 6	Clarification	Change sentence to read: IEEE Std. 828-2005 ~~and IEEE Std. 1042-1987 are~~ is endorsed by RG 1.169. IEEE Std 1042 is no longer endorsed by RG 1.169.	Accepted
137	Page 114 / Line 11	Clarification	Change sentence to read: The NRC evaluated the Radics LLC configuration management program, described in Section 7.5 of the RadICS TR, and determined it to be compliant with the criteria of IEEE Std. 828-2005 ~~and IEEE Std. 1042-1987~~ as endorsed by RG 1.169. IEEE Std 1042 is no longer endorsed by RG 1.169.	Accepted
138	Page 114 / Line 39	Clarification	Change Radics LLC component to RadICS	Accepted
139	Page 116 / Line 12	Editorial	Change 106430 to 106439	Accepted
140	Page 116 / Line 23	Clarification	Change Radics LLC component to RadICS-	Accepted
141	Page 119 – Line 26	Clarification	Change Radics LLC to RadICS	Accepted
142	Page 119 / Lines 40-41	Clarification	Change sentence to read: However, because Radics LLC did not define the actions to be taken when Type III faults are detected …	Accepted
143	Page 121 – Line 1	Clarification	Change Radics LLC to RadICS	Accepted
144	Page 121– Line 7	Clarification	Change Radics LLC to RadICS	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
145	Page 122– Line 27	Clarification	Change Radics LLC to RadICS	Accepted
146	Page 122 – Line 30	Clarification	Change Radics LLC to RadICS	Accepted
147	Page 122 / Line 38	Clarification	Change Radics LLC to RadICS	Accepted
148	Page 123 / Lines 20-21	Clarification	Change Radics LLC to RadICS system	Accepted
149	Page 128 / Lines 5-8	Proprietary	Deemed Proprietary by RPC Radics LLC (Note 2)	Accepted
150	Page 131 / Line 7	Clarification	Change RADICS to RadICS	Accepted
151	Page 131 / Line 19	Clarification	Change Section 8 to Sections 7 and 8	Accepted
152	Page 133 / Lines 10-14	Clarification	Change paragraph to read: Self-Diagnostics Design Requirements – The licensee must establish requirements for validation ~~enabling and~~ testing of Type III ~~necessary~~ self-diagnostics features to ensure plant safety requirements are satisfied. ~~to ensure used to identify and address postulated control or protection logic common cause failures within the RadICS safety system.~~ This information was provided to NRC in Enclosure 3 to Radics LLC submittal dated August 2, 2018 (ML18219A841), “RadICS Digital I&C Platform Topical Report Supplemental Information Update,” that updated discussion on Diversity and Defense-In-Depth.	Accepted

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
153	Page 133 / Lines 16-20	Clarification	Change paragraph to read: Plant Specific Fail-Safe Behavior Requirements Definition – Fail Safe state requirements shall be established by the licensee for all components actuated by the RadICS Platform ~~safety functions~~ to ensure plant safety is achieved when RadICS system logic failures (e.g., Type I, II, or III faults) are detected by system self-diagnostic functions. This information was provided to NRC in Enclosure 3 to Radics LLC submittal dated August 2, 2018 (ML18219A841), "RadICS Digital I&C Platform Topical Report Supplemental Information Update," that updated discussion on Diversity and Defense-In-Depth.	Revised - The intent of this PSAI is to require licensees to define the required fail-safe states for the RadICS outputs and not the fail-safe state of the components that are actuated by the RadICS system. Reworded PSAI to clarify this position.
156	Page 133 / Lines 22-34	Clarification	Change paragraph to read: Conservation of Existing Diversity Measures – The applicant or licensee must confirm that installation of a RadICS protection system is diverse from for the system for reducing the risk from anticipated transients without scram, as required by 10 CFR 50.62 and existing diversity attributes of the existing protection system are preserved in the upgraded system. This diversity may be expressed in the signal selection and protection system functional algorithms established and accepted for the plant design. ~~The applicant or licensee should confirm that functional diversity that has~~	Revised: Added the following sentence to identify ATWS diversity requirements. "If the RadICS protection system is to be used for performing a reactor trip function then the applicant or licensee must also ensure that the RadICS system is diverse from anticipated transients without scram (ATWS) systems as required by 10 CFR Part 50.62."

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
			~~been added to safety systems based on operating experience (e.g., requiring both under voltage and shunt trip features for reactor trip breakers) is retained. For example, the applicant or licensee should confirm that the additional diversity that has been included in plant I&C designs to establish compliance with 10 CFR 50.62 is maintained in the revised safety system design.~~ This information was provided to NRC in Enclosure 3 to Radics LLC submittal dated August 2, 2018 (ML18219A841), "RadICS Digital I&C Platform Topical Report Supplemental Information Update," that updated discussion on Diversity and Defense-In-Depth.	

Note 1 - The basis for withholding the proprietary information was provided in Research and Production Corporation Radics LLC letter to NRC dated August 2, 2018, "Submittal of RadICS Digital I&C Platform Topical Report Supplemental Information Update (Docket Number 99902032)." (ADAMS Accession No. ML18219A747)

Note 2 - The basis for withholding the proprietary information was provided in Research and Production Corporation Radics LLC letter to NRC dated April 13, 2018, "Response to Request for Additional Information for RadICS Topical Report (CAC NO.: MF8411; EPID: L-2016-TOP-0010)." (ADAMS Accession No. ML18107A238)