

Enclosure 2

Non-Proprietary Documents for RadICS Topical Report

Document Title	Revision Level
2016-RPC003-TR-001, RadICS Topical Report (Nonproprietary Version)	0

NONPROPRIETARY



RPC «RadICS» LLC

RadICS Topical Report

Revision 0

PREPARED BY

M.BURZYNSKI
LICENSING MANAGER

DATE: September 17, 2016

REVIEWED BY

O.SHEVCHENKO
APPLICATION DESIGN BUREAU MANAGER

DATE: September 19, 2016

REVIEWED BY

E.BREZHNEV
QUALITY ASSURANCE MANAGER

DATE: September 19, 2016

REVIEWED BY

A.DITYASHEV
SERVICE SUPPORT DEPARTMENT

DATE: September 19, 2016

REVIEWED BY

D.KOTOV
EQUIPMENT QUALIFICATION AND CALIBRATION
DEPARTMENT MANAGER

DATE: September 19, 2016

REVIEWED BY

E.BULBA
VALIDATION AND COMMERCIAL GRADE
DEDICATION DEPARTMENT MANAGER

DATE: September 19, 2016

REVIEWED BY

O.ODARUSHCHENKO
VERIFICATION DEPARTMENT MANAGER

DATE: September 19, 2016

APPROVED BY:

A.ANDRASHOV
RADICS DIRECTOR

DATE: September 19, 2016



Abstract

The RadICS Topical Report presents design, performance, and qualification information for the RadICS digital safety instrumentation and control (I&C) platform developed by Research and Production Corporation (RPC) Radiy. The RadICS Platform is a generic digital safety I&C platform dedicated to the implementation of Class 1E safety I&C functions in U.S. nuclear power plants (NPPs). The RadICS Platform builds on the digital safety I&C systems developed by RPC Radiy since 1998.

The RadICS Topical Report is the summary licensing document for the RadICS Platform digital safety I&C platform and is organized as follows:

- Chapter 1, Introduction
- Chapter 2, RadICS Development and Operational History
- Chapter 3, Quality Assurance
- Chapter 4, RadICS Commercial Grade Dedication Plan
- Chapter 5, Regulations, Codes, and Standards
- Chapter 6, RadICS Platform
- Chapter 7, RadICS Platform Development Process
- Chapter 8, Electronic Design Development
- Chapter 9, Equipment Qualification and Analysis
- Chapter 10, Diversity and Defense-In-Depth
- Chapter 11, Secure Development and Operational Environment
- Chapter 12, Compliance Summary for Key Regulations, Codes, and Standards
- Appendix A, RadICS Platform Application Guide
- Appendix B, DI&C-ISG-04 Compliance Matrix
- Appendix C, RadICS Electronic Design Documents

*Copyright © 2016 RadICS LLC
All Rights Reserved*

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 2 of 350
--------------	--------------------	-----------	---	---------------



NONPROPRIETARY

Revision History

Revision information for the RadICS Topical Report is listed below. This table will contain a listing and description of changed paragraphs for each succeeding revision.

Revision	Date	Paragraph	Description of Change
0	September 19, 2016	All	Initial Release



Table of Contents

1	Introduction	13
1.1	Background	13
1.2	Objectives of the Report	14
1.3	Scope of the Report	14
1.4	Structure of the RadICS Topical Report	15
1.5	Special Definitions.....	17
1.6	Acronyms and Abbreviations	19
1.7	Chapter 1 References.....	25
2	RadICS Development and Operational History.....	27
2.1	Evolution of RPC Radiy Products.....	27
2.2	Overview of RadICS Platform	28
2.3	RadICS-Based Applications.....	30
2.3.1	Reactor Trip System	30
2.3.2	Engineered Safety Features Actuation System	32
2.3.3	Rod Control System	33
2.4	RPC Radiy Safety I&C Installations	34
2.5	Chapter 2 References.....	36
3	Quality Assurance.....	37
3.1	Introduction	37
3.2	RPC Radiy Quality Assurance Program.....	37
3.2.1	RPC Radiy Organization	37
3.2.2	Quality Management System	43
3.3	RadICS Quality Assurance Program	48
3.3.1	RadICS Organization	48
3.3.2	Quality Assurance Program	52
3.3.3	RadICS NQA-1 Implementation Activities	53
3.3.4	Corrective Action Program	56
3.3.5	10 CFR Part 21 Problem Reporting.....	56
3.3.6	Maintenance Process of NRC Safety Evaluation Report	57
3.4	Chapter 3 References.....	57
4	RadICS Commercial Grade Dedication Plan.....	59
4.1	Commercial Grade Dedication Methodology	59
4.1.1	Definition of the Generic RadICS Platform	59
4.1.2	Compliance with Dedication Guidance	59
4.1.3	RadICS Commercial Grade Dedication Process	62
4.1.4	Maintenance of RadICS Platform Commercial Grade Dedication.....	63
4.2	Chapter 4 References.....	63
5	Regulations, Codes, and Standards.....	65
5.1	Compliance Summary	65
5.2	10 CFR, Code of Federal Regulations	65
5.2.1	10 CFR 50.34(f)(2)(v), Bypass and Operable Status Indication.....	65



5.2.2	10 CFR 50.49, Environmental Qualification.....	65
5.2.3	10 CFR 50.55a(h)(2), Protection Systems.....	65
5.2.4	10 CFR Part 50 Appendix A, General Design Criteria	65
5.2.5	10 CFR Part 50 Appendix B, Quality Assurance Requirements	68
5.3	NRC Regulatory Guides	69
5.3.1	Regulatory Guide 1.22	69
5.3.2	Regulatory Guide 1.28.....	69
5.3.3	Regulatory Guide 1.47	69
5.3.4	Regulatory Guide 1.53.....	69
5.3.5	Regulatory Guide 1.62.....	70
5.3.6	Regulatory Guide 1.75.....	70
5.3.7	Regulatory Guide 1.89.....	70
5.3.8	Regulatory Guide 1.100.....	70
5.3.9	Regulatory Guide 1.105.....	71
5.3.10	Regulatory Guide 1.118.....	71
5.3.11	Regulatory Guide 1.152.....	71
5.3.12	Regulatory Guide 1.153.....	72
5.3.13	Regulatory Guide 1.168.....	72
5.3.14	Regulatory Guide 1.169.....	72
5.3.15	Regulatory Guide 1.170.....	72
5.3.16	Regulatory Guide 1.171.....	73
5.3.17	Regulatory Guide 1.172.....	73
5.3.18	Regulatory Guide 1.173.....	73
5.3.19	Regulatory Guide 1.180.....	73
5.3.20	Regulatory Guide 1.209.....	73
5.4	NUREG-0800, Chapter 7, Branch Technical Positions.....	74
5.4.1	Branch Technical Position 7-8	74
5.4.2	Branch Technical Position 7-11	74
5.4.3	Branch Technical Position 7-12	74
5.4.4	Branch Technical Position 7-14	74
5.4.5	Branch Technical Position 7-17	74
5.4.6	Branch Technical Position 7-18	75
5.4.7	Branch Technical Position 7-19	75
5.4.8	Branch Technical Position 7-21	75
5.5	NRC NUREGs and NUREG/CRs	75
5.5.1	NUREG/CR 6082, Data Communications.....	75
5.6	NRC Digital I&C Interim Staff Guidance Documents.....	75
5.6.1	DI&C-ISG-04.....	76
5.6.2	DI&C-ISG-06.....	76
5.7	Institute of Electrical & Electronics Engineers Standards	76
5.7.1	IEEE Std 7-4.3.2-2003	76
5.7.2	IEEE Std 323-2003.....	76
5.7.3	IEEE Std 338-1987.....	76
5.7.4	IEEE Std 344-2004.....	77
5.7.5	IEEE Std 352-1987.....	77



5.7.6	IEEE Std 379-2000.....	77
5.7.7	IEEE Std 384-1992.....	77
5.7.8	IEEE Std 603-1991.....	78
5.7.9	IEEE Std 730-1998.....	78
5.7.10	IEEE Std 828-2005.....	78
5.7.11	IEEE Std 829-2008.....	78
5.7.12	IEEE Std 830-1998.....	78
5.7.13	IEEE Std 1008-1987.....	79
5.7.14	IEEE Std 1012-2004.....	79
5.7.15	IEEE Std 1028-2008.....	79
5.7.16	IEEE Std 1050-1996.....	79
5.7.17	IEEE Std 1074-2006.....	79
5.8	Instrument Society of America Standards	79
5.8.1	ISA-S67.04-1994	79
5.9	International Electrotechnical Commission Standards.....	80
5.9.1	IEC 60880:2006.....	80
5.9.2	IEC 60987:2007.....	80
5.9.3	IEC 61000.....	80
5.9.4	IEC 61508:2010.....	80
5.9.5	IEC 61513:2001.....	80
5.9.6	IEC 62566:2011.....	81
5.10	U.S. Military Standards	81
5.10.1	MIL-STD-461E	81
5.11	Electric Power Research Institute Technical Reports and Handbooks	81
5.11.1	EPRI TR-107330	81
5.11.2	EPRI TR-106439	82
5.11.3	EPRI Handbook 1011710	82
5.12	American Society of Mechanical Engineers Standards	82
5.12.1	ASME NQA-1-2008	82
5.13	Chapter 5 References.....	82
6	RadICS Platform.....	83
6.1	RadICS Platform Overview	83
6.1.1	RadICS Platform General Attributes.....	85
6.1.2	RadICS Platform Fundamental Safety Approach.....	87
6.1.3	Maintainability and Operability	89
6.1.4	FPGA Based Digital Technology.....	91
6.1.5	Benefits of FPGA Technology	92
6.2	RadICS Chassis-Level Features	93
6.2.1	Theory of Operation	93
6.2.2	RadICS Chassis Configuration	100
6.2.3	Multiple Channels of RadICS	104
6.2.4	Overview of RadICS Chassis Interfaces.....	104
6.2.5	RadICS Hardware Modules.....	108
6.2.6	Hardware Module Specifications	117
6.3	Communications	160



6.3.1	Basic Concepts.....	160
6.3.2	RadICS Communication Hardware Components.....	163
6.3.3	Communication Protocols.....	164
6.4	Platform Diagnostics.....	179
6.4.1	General Diagnostics Concept.....	179
6.4.2	Hardware Self-Diagnostics.....	183
6.4.3	Interfaces and Data Transmission Self-Diagnostics.....	183
6.4.4	FPGA ED Components Self-Diagnostics.....	184
6.5	Redundancy.....	190
6.6	Independence.....	191
6.7	Safety Override Operation.....	191
6.8	PSWD Operation.....	194
6.9	Access Control Features.....	195
6.10	Timing Diagrams and Working Cycles.....	197
6.11	Periodic Testing.....	200
6.12	Download Station.....	201
6.13	Chapter 6 References.....	201
7	RadICS Platform Development Process.....	202
7.1	Overview of Safety Standards Used for RadICS Platform Development Process.....	202
7.2	Standard Requirements in the RadICS Life Cycle.....	204
7.3	RadICS Platform Development Process.....	205
7.3.1	RadICS Safety Life Cycle.....	205
7.3.2	High Level Platform Design.....	211
7.3.3	RadICS Module Electronic Design and Implementation.....	212
7.3.4	RadICS System Integration and Validation.....	219
7.3.5	Project-Specific Application Process.....	219
7.4	RadICS Platform Verification and Validation.....	220
7.4.1	Roles and Responsibilities.....	221
7.4.2	Methods and Tools.....	222
7.4.3	Implementation Activities.....	223
7.4.4	V&V Administrative Requirements.....	227
7.4.5	V&V Documentation Requirements.....	227
7.5	RadICS Configuration Management Process.....	232
7.5.1	Roles and Responsibilities.....	233
7.5.2	Process Controls.....	233
7.5.3	Implementation Activities.....	236
7.6	Requirements for the RadICS Platform and Applications.....	240
7.6.1	Allocation of Requirements.....	241
7.6.2	Documentation of Design Requirements.....	242
7.6.3	Maintainability and User Friendliness Requirements.....	242
7.6.4	Requirements Tracing Tool.....	245
7.7	Development Process Metrics.....	246
7.7.1	Software Quality Metrics Based on Anomaly Reports.....	246
7.7.2	Software Quality Metrics Based on V&V Open Issues.....	246
7.7.3	Software Quality Metrics Based on Test Coverage.....	246



7.8	Development Process Training	247
7.9	Chapter 7 References.....	247
8	Electronic Design Development.....	249
8.1	RadICS Electronic Design Process	249
8.1.1	Development of Electronic Design Architecture Description	250
8.1.2	Development of Function Block Library Detailed Description	251
8.1.3	Development of Function Block Library Code	252
8.1.4	Development of Electronic Design Detailed Description	253
8.1.5	Development of Electronic Design Code	254
8.1.6	Synthesis.....	255
8.1.7	Place and Route.....	255
8.1.8	Bitstream Generation	256
8.2	Application Function Block Library Electronic Design Development.....	257
8.2.1	AFBL Design Activities	257
8.2.2	AFBL Methods of Verification and Validation	258
8.3	FBL and Module Electronic Design and V&V Tools	259
8.3.1	Quartus II	262
8.3.2	HDL Designer	263
8.3.3	Understand.....	263
8.3.4	ModelSim	264
8.3.5	LabView	264
8.3.6	TestComplete	264
8.3.7	TopJTAG Probe	265
8.3.8	Visual Studio	265
8.3.9	PostgreSQL	265
8.3.10	Qt Creator.....	266
8.3.11	GNU Compiler Collection.....	266
8.4	Application Electronic Design Tool	266
8.5	Chapter 8 References.....	267
9	Equipment Qualification and Analysis	268
9.1	Equipment Qualification	268
9.1.1	Equipment to be Tested	268
9.1.2	Equipment Qualification Testing	269
9.1.3	Generic Qualification Envelope	275
9.1.4	Maintenance of Generic Qualification	281
9.2	Equipment Analysis.....	281
9.2.1	Failure Modes, Effects, and Diagnostic Analysis	281
9.2.2	Setpoint Analysis Support	284
9.2.3	Limited Life Parts Analysis	285
9.2.4	Radiation Susceptibility Analysis	285
9.3	Chapter 9 References.....	286
10	Diversity and Defense-In-Depth	288
10.1	Overview	288
10.2	Digital Common Cause Failures	288
10.3	Defense Against Common Cause Failures.....	288



10.3.1	Diversity.....	289
10.3.2	Defense-in-Depth	290
10.4	Chapter 10 References.....	290
11	Secure Development and Operational Environment	291
11.1	RadICS Secure Development Environment.....	291
11.2	Development Environment Vulnerability Assessment	291
11.3	Operating Environment Vulnerability Assessment.....	293
11.4	Secure Development and Operational Environment Controls	294
11.5	Project-Specific Vulnerability Assessments	294
11.6	Chapter 11 References.....	297
12	Compliance Summary for Key Regulations, Codes, and Standards	298
12.1	Quality Assurance	298
12.1.1	Regulatory Guide 1.28.....	298
12.1.2	Regulatory Guide 1.152.....	299
12.2	Technical Requirements.....	300
12.2.1	Regulatory Guide 1.153.....	300
12.2.2	Regulatory Guide 1.152.....	301
12.2.3	DI&C-ISG-04.....	302
12.2.4	NUREG/CR 6082	303
12.3	Software Development Processes	304
12.3.1	Regulatory Guide 1.173.....	305
12.3.2	Regulatory Guide 1.172.....	305
12.3.3	Regulatory Guide 1.171.....	305
12.3.4	Regulatory Guide 1.170.....	305
12.3.5	Regulatory Guide 1.169.....	306
12.3.6	Regulatory Guide 1.168.....	306
12.3.7	Branch Technical Position 7-14	306
12.4	Secure Development and Operating Environment.....	307
12.4.1	Regulatory Guide 1.152.....	307
12.5	Chapter 12 References.....	309
Appendix A:	RadICS Platform Application Guide	311
Appendix B:	DI&C-ISG-04 Compliance Matrix	328
Appendix C:	RadICS Electronic Design Documents.....	343



List of Figures

Figure 2-1: Evolution of RPC Radiy Products.....	27
Figure 2-2: RadICS Platform	29
Figure 2-3: RadICS Platform High Level Representation.....	30
Figure 2-4: Reactor Trip System Configuration.....	31
Figure 2-5: Typical RadICS Reactor Trip System Equipment.....	32
Figure 2-6: RadICS Engineered Safety Features Actuation System Cabinets.....	33
Figure 2-7: RadICS Rod Control System Cabinets	33
Figure 2-8: Typical RCS Architecture Voting Logic Configuration for a PWR Unit	34
Figure 3-1: RPC Radiy Organization Structure.....	38
Figure 3-2: SIL 3 Certification Process.....	45
Figure 3-3: RadICS Organization and Workflow Interfaces.....	50
Figure 3-4: RadICS Product Lifecycle and Organizational Responsibilities	51
Figure 6-1: Typical RadICS Platform Configuration	84
Figure 6-2: Context Diagram of the RadICS Platform.....	85
Figure 6-3: Theory of Operation of RadICS Platform	94
Figure 6-4: RadICS Platform Work Cycle	95
Figure 6-5: RadICS Chassis Design.....	100
Figure 6-6: RadICS Chassis Configuration	101
Figure 6-7: Rear of RadICS Chassis Showing Connectors	102
Figure 6-8: RadICS Chassis Diagram with Internal and External Interfaces	106
Figure 6-9: Maintenance Features of the RadICS Modules	108
Figure 6-10: Typical RadICS Module Architecture	112
Figure 6-11: Data and Signals Exchange Between Different Clock Domains	113
Figure 6-12: Functional Diagram of the LM	120
Figure 6-13: LM Mode Transition Diagram	121
Figure 6-14: Functional Diagram of the AIM.....	130
Figure 6-15: AIM Mode Transition Diagram	131
Figure 6-16: Functional Diagram of the DIM	136
Figure 6-17: DIM Mode Transition Diagram	137
Figure 6-18: Functional Diagram of the AOM.....	142
Figure 6-19: AOM Mode Transition Diagram.....	143
Figure 6-20: Functional Diagram of the DOM.....	149
Figure 6-21: DOM Mode Transition Diagram.....	150
Figure 6-22: Functional Diagram of the OCM	156
Figure 6-23: OCM Mode Transition Diagram	157
Figure 6-24: General Channel Level Protocol.....	175
Figure 6-25: Self-Diagnostics Techniques Classification	180
Figure 6-26: Ways Outputs Can Trip to Safe State.....	182
Figure 6-27: RAD SD Usage for Providing MED SD.....	186
Figure 6-28: PD SD usage for providing MED SD.....	187
Figure 6-29: Approach for Assuring AFBL Integrity.....	189
Figure 6-30: Functional Diagram of SOR Unit	193



Figure 6-31: Functional Diagram of PSWD Unit.....	194
Figure 6-32: RadICS Keyswitch Access Control Features	196
Figure 6-33: Operation Timing Diagram of a Single RadICS Platform	199
Figure 6-34: Operation Timing Diagram for Two RadICS Platforms	199
Figure 7-1: IEC Safety Life Cycle Concept.....	206
Figure 7-2: RadICS Safety Life Cycle	207
Figure 7-3: High-Level RadICS Platform Requirements Documents	212
Figure 7-4: RadICS Platform Development Activities (including V&V).....	226
Figure 7-5: Hierarchy of the Controlled RadICS Configuration Items	234
Figure 7-6: Change Control Work Flow	237
Figure 7-7: RadICS Baseline Configuration Audits	239
Figure 7-8: RadICS Platform and Applications Requirements.....	240
Figure 8-1: RadICS ED Development Lifecycle and Documents.....	250
Figure 8-2: Work Flow of Tools for FBL and ED Development.....	262
Figure 9-1: RadICS QTS Qualification Testing Sequence	270
Figure 11-1: RadICS Project-Specific Lifecycle Security Activities	296
Figure 12-1: Mapping RadICS Documents to BTP 7-14.....	308
Figure A-1: Illustrative Timeline of RadICS Platform Operating Modes.....	311



List of Tables

Table 2-1: RPC Radiy Designed and Manufactured Equipment and Systems Installed in NPPs.....	35
Table 3-1: IEC 61508 SIL Table for Demand Mode.....	46
Table 3-2: RadICS Quality Procedures.....	53
Table 6-1: Qualified Components	103
Table 6-2: Classification of RadICS Chassis and Modules Interfaces	104
Table 6-3: Units Included in RadICS Modules	110
Table 6-4: Summary of Communications Links.....	161
Table 6-5: Safety Features of RadICS Communication Interfaces.....	166
Table 6-6: Faults Detected by RadICS Platform	182
Table 6-7: Timing Requirements for RadICS I/O Modules	198
Table 7-1: Summary of RadICS Life Cycle Development Activities	208
Table 7-2: Generic RadICS ED Task Descriptions	215
Table 7-3: Maintainability and User Friendliness Requirements.....	243
Table 8-1: RadICS Tool Evaluation Criteria.....	260
Table 8-2: RadICS Commercial Development Tools.....	261
Table 9-1: Generic Qualification Envelope for the RadICS Digital Safety I&C Platform.....	276
Table 9-2: Summary of the Predicted Reliability of RadICS Modules	283
Table 12-1: Responses to NUREG/CR-6082 Communications System Questions	303
Table C-1: RadICS Electronic Design Related Documents.....	344



1 Introduction

1.1 Background

The continued safe and economical operation of nuclear power plants (NPPs) requires the modernization of its control and safety systems to cope with obsolescence and age-related degradation. Changes and upgrades made in these systems also affect their digital instrumentation and control (I&C) systems, human-system interface (HSI) systems in the control rooms, and the full-scope simulators.

Nuclear utilities may choose to perform a large-scale modernization of their I&C systems in a single maintenance outage, or they may take several modernization steps spread over a number of outages. The design, manufacturing, and installation tasks to replace existing I&C systems are usually done by external companies and contractors with project supervision by the NPPs technical departments.

Research and Production Corporation (RPC) Radiy has a long history of working with operating NPPs and installing new I&C systems in turn-key projects. RPC Radiy provides a wide variety of I&C solutions ranging from full-scope turn-key modernization projects to reverse engineering and printed circuit board-level, like-for-like replacement as well as solutions to ageing and obsolescence problems, both for safety and non-safety applications. RPC Radiy uses Field Programmable Gate Array (FPGA) technology in its digital platform to implement customized solutions to NPPs I&C systems. RPC Radiy's proven technological expertise has been demonstrated in over 90 systems installed to-date.

RPC Radiy I&C systems have been installed in safety related systems of all operating NPP sites in the Ukraine and Bulgaria. The installed systems include Reactor Trip System (RTS), Reactor Power Control and Limitation System (RPCLS), Engineered Safety Features Actuation System (ESFAS), and Rod Control System (RCS), Switchgear and Electrical Distribution Systems, Nuclear Island Control System, and Turbine Island Control System. In addition, RPC Radiy is supporting Candu Energy Inc. in Canada and the Embalse NPP in Argentina in joint projects to improve and modernize safety systems. A detailed listing of RPC Radiy safety I&C installations is provided in Chapter 2.

RPC Radiy has successfully completed the final independent Functional Safety Assessment performed by *exida*. The certification company confirmed that the RPC Radiy processes and product complied with Safety Integrity Level (SIL) 3 requirements in single or multiple-channel configurations. The SIL 3 certification was performed using International Electrotechnical Commission (IEC) 61508:2010 (Parts 1 - 7) (Reference 1-1).¹

In addition, RPC Radiy has been a strong supporter of industry efforts to promote the use of reliable, diverse, and cost-effective FPGA-based I&C solutions for safety and control systems in NPPs. RPC Radiy has twice hosted for the International Workshop on the Application of Field Programmable Gate Arrays in Nuclear Power Plants, in cooperation with the International Atomic Energy Agency (IAEA) and SunPort SA.

¹ The IEC 61508 Safety Integrity Level rating is different than the Software Integrity Level classification scheme described in IEEE Std 1012-2004.



1.2 Objectives of the Report

RPC Radiy established RadICS as a wholly owned Limited Liability Company (LLC) in July 2012. The RadICS business focus is the design and delivery of I&C systems for NPPs using the RadICS Platform equipment. RadICS is submitting this RadICS Topical Report to the Nuclear Regulatory Commission (NRC) for review and approval of the RadICS Platform design. The RadICS Platform is intended to be used as a digital control system platform solution for safety-related applications in NPPs. It is designed to replace existing analog and computer-based I&C systems currently used in U.S. NPP applications and to be installed as original equipment for new NPP facilities.

RadICS is seeking NRC generic approval for use of the RadICS Platform in nuclear safety I&C systems in any U.S. NPP. The RadICS Platform was originally designed, qualified, and manufactured to meet European nuclear safety and quality standards. In addition, RadICS Platform has been demonstrated to comply with the IEC 61508 SIL 3 certification requirements (Reference 1-2). RadICS is now managed under a quality assurance (QA) program that complies with 10 CFR Part 50 Appendix B (Reference 1-3). The purpose of the RadICS Topical Report is to demonstrate that the RadICS Platform and the associated quality and programmable logic life cycle process comply with NRC requirements. Compliance is demonstrated via the following licensing approach:

- Dedicate the generic RadICS Platform, which was not originally developed under a 10 CFR Part 50 Appendix B QA program, in accordance with the basic requirements for commercial dedication as defined in 10 CFR Part 21 (Reference 1-4). RadICS is employing the commercial dedication processes described in Electric Power Research Institute (EPRI) Topical Report (TR)-106439 (Reference 1-5) and TR-107330 (Reference 1-6) and approved by the NRC (References 1-7 and 1-8).
- Qualify RadICS hardware to meet U.S. standards. The RadICS hardware will be qualified and maintained under the RadICS 10 CFR Part 50 Appendix B quality program (Reference 1-9). If new boards are developed or existing boards modified for obsolescence or other reasons, the new or modified hardware will be appropriately tested and/or analyzed to maintain equipment qualification to U.S. standards.
- Develop project-specific programmable logic in accordance with software life cycle plans that are compliant with NRC Branch Technical Position (BTP) 7-14 (Reference 1-10).
- The RadICS toolset, which issued as design aids and not as a replacement for verification and validation (V&V), are not dedicated but continue to be subject to a configuration management (CM) program.

RadICS has concluded that the RadICS Platform can meet the needs of U.S. nuclear safety I&C applications in NPPs. RadICS will use the RadICS Platform defined in this Topical Report as a basis to provide project-specific systems to utilities and other users. Project-specific systems will be documented and submitted to the NRC by the appropriate licensees, using the appropriate processes, for review and approval for installation.

1.3 Scope of the Report

The RadICS Topical Report focuses on the following topics:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 14 of 350
--------------	--------------------	-----------	---	----------------



- RadICS hardware design, qualification and analysis
- RadICS generic programmable logic and associated development life cycle processes (which includes application-oriented library of re-usable programmable logic components)
- RadICS toolset used to design and implement the system architecture, configure the units and networks, and develop the project-specific programmable logic
- RadICS project-specific development life cycle processes

The RadICS Topical Report also addresses the following interfaces with the RadICS Platform:

- Input connections to field devices but not the field devices
- Output connections to field devices but not the field devices
- Communication independence features of the RadICS Platform that support communication interfaces for export of data to a Monitoring and Tuning System (MATS) or a customer's plant computer system but not the MATS hardware or software or the plant computer system
- Communication independence and data transfer protocol features of the RadICS Platform that support communication with a customer's maintenance laptop computer to adjust setpoints and other predefined calibration factors but not the laptop computer
- Keyswitch interfaces for keyswitch inputs that support RadICS access control features used to support system maintenance activities but not the keyswitch design or location
- Module connections and data protocols for loading electronic design configuration files but not the download station

The RadICS Platform is designed to be functionally and physically similar to currently installed I&C systems. Its platform capabilities include input processing, customizable logic solving, and output processing. The RadICS Platform continuously monitors system status through signals that are received from field sensors. It performs logic computations to create control commands. It also converts control commands to output signals that are applied to field actuators. The RadICS Platform has a modular and scalable design that can be configured to meet the needs of safety I&C applications in NPPs.

The RadICS Platform is a state-of-the-art digital control system platform specifically designed for safety-related control and protection systems in NPP applications. The RadICS Platform features a modular and distributed FPGA-based architecture. The RadICS Platform components are functionally similar to legacy analog measurement and trip modules; however, the RadICS equipment takes advantage of the benefits of digital technology. The FPGA-based architecture supports effective implementation of key nuclear safety design principles: redundancy; independence; predictability and repeatability; and diversity and defense-in-depth (D3). The FPGA-based architecture allows simple programmable logic that avoids the unfavorable aspects of software-based systems

1.4 Structure of the RadICS Topical Report

The RadICS Topical Report has been divided into 12 chapters and 3 appendices:

Chapter 1 - Introduction: This chapter provides an overview of the RadICS Topical Report and identifies the supporting documents that will be submitted for NRC review.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 15 of 350
--------------	--------------------	-----------	---	----------------



Chapter 2 - RadICS Development and Operational History: This chapter provides an overview of RadICS development and operational use in international NPPs where it is currently deployed in a variety of digital safety I&C applications. This information is provided to illustrate the safety I&C developments that led to the RadICS Platform.

Chapter 3 - Quality Assurance: This chapter provides an overview of the quality program and the quality process employed to dedicate the generic RadICS Platform hardware and associated programmable logic used to develop systems for delivery to U.S. customers.

Chapter 4 – RadICS Commercial Grade Dedication Plan: This chapter provides an overview of the commercial grade dedication program used to dedicate the generic RadICS Platform hardware and associated platform programmable logic.

Chapter 5 - Regulations, Codes, and Standards: This chapter identifies the regulatory requirements, design criteria, and guidelines applicable to the RadICS Platform. Compliance with the key guidance documents is summarized in Chapter 12.

Chapter 6 - RadICS Platform: This chapter provides a description of the RadICS Platform operation and how it can be applied in NPP safety-related applications. This chapter also provides descriptions of the hardware and associated generic programmable logic that comprise the RadICS Platform. In addition, details are provided on how digital communications and testability are implemented in the RadICS Platform.

Chapter 7 - RadICS Platform Development Process: This chapter provides a description of the hardware development process, associated planning documents, and component testing process.

Chapter 8 - Electronic Design Development: This chapter provides a description of the RadICS Platform generic programmable logic development life cycle, planning documents, and the verification and validation process. The RadICS programmable logic life cycle processes were examined in more detail as part of the SIL certification. This chapter also describes the separate programmable logic life cycle processes for the implementation of project-specific functionality.

Chapter 9 - Equipment Qualification and Analysis: This chapter provides an overview of the generic equipment qualification program for the RadICS Platform. The RadICS qualification “envelope” is designed to meet or exceed the environmental qualification requirements for NPPs in the U.S. using the EPRI TR-107330 criteria. This chapter also provides a summary of the board-level reliability analysis results and an overview of the response time and setpoint analysis support information.

Chapter 10 - Diversity and Defense in Depth: This chapter provides an overview of the RadICS approach to platform diversity using example applications.

Chapter 11 - Secure Development and Operational Environment: This chapter provides a summary of a RadICS Platform vulnerability analysis and the secure development and operational environment controls provided by RPC Radix.

Chapter 12 - Compliance Summary for Key Regulations, Codes, and Standards: This chapter provides a conformance summary of the RadICS design and development processes for the key regulatory guidance documents.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 16 of 350
--------------	--------------------	-----------	---	----------------



Appendix A - RadICS Platform Application Guide: This appendix provides the project-specific system design guidance for use of the RadICS Platform, including recommended practices and any restrictions.

Appendix B - DI&C-ISG-04 Compliance Matrix: This appendix provides a Digital I&C Interim Staff Guidance (DI&C-ISG)-04 (Reference 1-11) compliance matrix, with the requirement listed, RadICS Platform compliance to each criterion defined.

Appendix C - RadICS Electronic Design Documents: This appendix contains a listing of the RadICS Platform design documents associated with the Electronic Designs for the RadICS Modules and identifies an initial set of documents planned for submittal to NRC to support the review of the RadICS Topical Report.

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

1.5 Special Definitions

RPC Radiy	RPC Radiy is a leading Ukrainian designer and supplier of advanced I&C systems for nuclear power plants. RPC Radiy is the designer and manufacturer of the RadICS Platform equipment. RPC Radiy is the parent company of RadICS LLC. RPC Radiy is the company discussed in the context of the development and manufacture of the RadICS Platform, the RadICS Modules and associated generic Platform Electronic Design (EDs), and the RadICS Platform Functions Block Library.
RadICS	RadICS is a wholly owned LLC established in July 2012. The company's business focus is the design and delivery of I&C systems for NPPs using the RadICS Platform equipment. RadICS is the company discussed in the context of I&C system development using RadICS Platform equipment and the development of the Application ED using the Application Functions Block Library.
RPC Radiy Quality Management System	The RPC Radiy Quality Management System (QMS) governs the design and manufacture of the RadICS Platform equipment. The RPC Radiy QMS is based on International Organization for Standardization (ISO) 9001:2008 (Reference 1-12).
RadICS Quality Assurance Program	The RadICS Quality Assurance Program (QAP) governs the system design, integration, and delivery of I&C systems for NPPs using the RadICS Platform equipment. RadICS QAP is based on 10 CFR Part 50 Appendix B and American Society of Mechanical Engineers (ASME) Nuclear Quality Assurance (NQA)-1-2008 (Reference 1-13) and the NQA-1a-2009 Addenda (Reference 1-14), as endorsed by Regulatory Guide (RG) 1.28 (Reference 1-15).



RadICS Platform	RadICS Platform is used to describe the collective set of equipment that is used to develop I&C systems. The set of equipment includes the RadICS Chassis, the RadICS Modules, the generic Platform ED for the RadICS Modules, the RadICS Platform Functions Block Library, and the associated Radiy Product Configuration Toolset.
RadICS Chassis	Chassis is used to describe the frame and backplane supporting the RadICS Modules, the inter-module connections on the backplane, and the input/output (I/O) module external connections via rear connectors.
RadICS Module	RadICS Module (or just Module) is used to describe the seven types of hardware modules that perform logic processing, input/output functions, and network communications. Discussion of a RadICS Module includes the associated ED on the FPGA. The RadICS Module is the highest level component within the RadICS Platform.
Unit	Unit is used to describe lower level components that are used to build Modules. Units are standardized to maximizes the reuse of proven components and simplify the development of Modules. Units can consist of just hardware or ED or a combination of both.
Electronic Design	ED is used to describe the logic and functionality programmed on the FPGA or Complex Programmable Logic Device on a RadICS Module. There are two levels of logic in the RadICS Logic Module (i.e., Platform ED and Application ED) and only the Platform ED in the I/O Modules.
Platform ED	Platform ED is used to describe the Platform Logic that manages the basic operation of the RadICS Platform. It performs the management of I/O using a defined Work Cycle, interface communication with the Application ED, and the platform self-testing and communication error checking functions. Platform ED is used to refer to the ED as a configuration item and Platform Logic is used to describe what the Platform ED does.
Application ED	Application ED is used incorporate the end user functional requirements for the I&C system functionality. The Application ED is used to execute the user defined functional requirements (e.g., reactor trip and engineered safety feature actuation functions). Application ED is used to refer to the ED as a configuration item and Application Logic is used to describe what the Application ED does.
Function Block Library	Function Block Library (FBL) is used to describe a pre-developed functional blocks used in the implementation of RadICS Platform functions. Functional Blocks are written in Very High Speed Integrated Circuits Hardware Description Language (VHDL). The FBL consists of two parts: Platform FBL (PFBL) and Application FBL (AFBL).



Platform FBL	PFBL refers to the subset of functional blocks used for the development of the Platform ED for the RadICS Modules.
Application FBL	AFBL refers to the subset of functional blocks used for the development of the Application ED for the RadICS Logic Module.
Platform ED Development Life Cycle	Platform ED Development Life Cycle refers to the ED activities performed by RPC Radiy under their QMS to implement the Platform Logic on the RadICS Modules.
Application ED Development Life Cycle	Application ED Development Life Cycle refers to the ED activities performed by RadICS under their QAP to implement the Application Logic on the RadICS Logic Modules in accordance with the end user functional requirements specification.
Form A	Form A means a normally open contact supporting a de-energize to trip function. The contact will open when energizing force is not present.

1.6 Acronyms and Abbreviations

Term	Definition
A	Ampère
A/D	Analog/Digital
AC	Alternating Current
AD	Architecture Description
ADC	Analog-to-Digital Conversion
AECL	Atomic Energy of Canada Limited
AFBL	Application Function Block Library
AFBL SD	Application Logic Functional Block Library Self-Diagnostics
AIM	Analog Input Module
AOM	Analog Output Module
ASME	American Society of Mechanical Engineers
ASPI	Advanced SCSI Programming Interface
BTP	Branch Technical Position
C	Celsius
CCB	Change Control Board
CCF	Common Cause Failure
CDR	Critical Digital Review
CFR	Code of Federal Regulations



Term	Definition
CGD	Commercial Grade Dedication
CM	Configuration Management
CMB	Configuration Management Board
CPLD	Complex Programmable Logic Device
CRAM	Configuration RAM
CRC	Cyclic Redundancy Checks
CRR	Code Review Report
CSA	Canadian Standards Association
D/A	Digital/Analog
DAC	Digital-to-Analog Conversion
DAS	Data Acquisition System
dB	Decibel
dBuV	Signal Level
DC	Direct Current
DD	Detailed Description
DI&C-ISG	Digital Instrumentation and Controls Interim Staff Guidance
DIM	Digital Input Module
DIU	Digital Input Unit
DLS	DownLoad Station
DOM	Digital Output Module
DOU	Discrete Output Unit
DTP ID	Data Transfer Protocol Identification
DTP SD	Data Transmission Protocol Self-Diagnostics
D3	Diversity and Defense-In-Depth
ED	Electronic Design
ED SD	Electronic Design Self-Diagnostics
EEPROM	Electrically Erasable Programmable Read-Only Memory
EPROM	Erasable Programmable Read-Only Memory
EFT	Electrical Fast Transient
EMC	Electromagnetic Compatibility



Term	Definition
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
EQ	Equipment Qualification
ESD	Electrostatic Discharge
ESFAS	Engineered Safety Feature Actuation System
F	Fahrenheit
FBL	Function Block Library
FIT	Fault Insertion Test
FMEA	Failure Mode and Effects Analysis
FMEDA	Failure Modes and Effects Diagnostic Analysis
FPGA	Field Programmable Gate Array
FOIP	Fiber Optic Inter-Chassis Interface
FOMP	Fiber Optic Monitoring Interface
FOTP	Fiber Optic Tuning Interface
FSA	Functional Safety Audit
FSMP	Functional Safety Management Plan
FT	Functional Test
g	Gravity
GDC	General Design Criteria
GHz	Gigahertz
GQA	Global Quality Assurance, Inc.
HBC	Heartbeat Control
HDL	Hardware Description Language
HPD	HDL-Programmed Devices
HSI	Human-System Interface
HW	Hardware
HW SD	Hardware Self-Diagnostics
HWM SD	Hardware Modules Self-Diagnostics
HWU SD	Hardware Unit Self-Diagnostics
Hz	Hertz



Term	Definition
I&C	Instrumentation and Control
I/O	Input/Output
IAEA	International Atomic Energy Agency
ID	Identification
IDR	Input Data Receive
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IERICS	Independent Engineering Review of I&C Systems in Nuclear Power Plants
IF SD	Interface and Data Transmission Self-Diagnostics
IP	Internet Protocol
IPC	Institute for Printed Circuits
ISA	Instrument Society of America
ISO	International Organization for Standardization
IT	Integration Test
JTAG	Joint Test Action Group
kA	Kiloampère
kHz	Kilohertz
kV	Kilovolt
kΩ	Kilohm
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Limited Liability Company
LLS&TS	Logic Level Simulation and Timing Simulation
LM	Logic Module
LSB	Least Significant Bit
LVDS	Low-Voltage Differential Signaling
M	Meter
ma	Milliampère
MATS	Monitoring and Tuning System
MC	Monotony Control



Term	Definition
MED SD	Module ED Self-Diagnostics
MHz	Megahertz
MIL-STD	Military Standard
ms	Millisecond
mV	Millivolt
MΩ	Megohm
NPP	Nuclear Power Plant
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
OBE	Operating Basis Earthquake
OCM	Optical Communication Module
ODT	Output Data Transmission
PAD	Product Architecture Document
PC	Personal Computer
PCB	Printed Circuit Board
PCD	Product Concept Document
PD SD	Packet Data Self-Diagnostics
PLC	Programmable Logic Controllers
PS	Protection System
PSWD	Power Supply and Watchdog
PWR	Pressurized Water Reactor
QA	Quality Assurance
QAP	Quality Assurance Program
QMS	Quality Management System
QTS	Qualification Test Specimen
R&D	Research and Development
Rad	Radiation Absorbed Dose
RAD SD	Random Access Data Self-Diagnostics
RAM	Random Access Memory
RCS	Rod Control System



Term	Definition
RDCS	Rod Drive Control
RDEPSS	Rod Drives Electric Power Supply Subsystem
RFI	Radio Frequency Interference
RG	Regulatory Guide
RMS	Root Mean Square
RPC	Research and Production Corporation
RPCLS	Reactor Power Control and Limitation System
RPCT	Radiy Product Configuration Toolset
RPIS	Rod Position Indication
RPP	Radiy Proprietary Protocol
RR	Review Report
RSCP	RS-232 Interface
RTD	Resistance Temperature Detector
RTL	Register Transfer Level
RTS	Reactor Trip System
RUP	Radiy UDP Based Protocol
RWSP	Radiy Watchdog Interface
SCA	Static Code Analysis
SD	Self-Diagnostics
SER	Safety Evaluation Report
SIL	Safety Integrity Level (from IEC 61508)
SIS	Safety Instrumented System
SOR	Safety Override
SPI	Serial Peripheral Interface
SPIP	SPI Interface
SRP	Standard Review Plan
SRS	Safety Requirements Specification
SSE	Safe Shutdown Earthquake
SSRAM	Synchronous Static Random Access Memory
ST	Switch Time



Term	Definition
STA	Static Timing Analysis
STC	Scientific and Technical Center
TR	Topical Report
TSAP	Test Specimen Application Program
TÜV	Technischer Überwachungsverein (Technical Inspection Association)
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol
UICP	UART Interface
UKTS	Unified Hardware System Equipment (UKTS in Russian)
U.S.	United States of America
V&V	Verification and Validation
V	Volts
VAC	Volts Alternating Current
VDC	Volts Direct Current
VHDL	Very High Speed Integrated Circuits Hardware Description Language
VM	Ventilation Module
VVER	Russian: Voda-Vodyanoi Energetichesky Reaktor (Pressurized Water Reactor)
ZPA	Zero Period Acceleration
Ω	Ohm

1.7 Chapter 1 References

- 1 IEC 61508:2010, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems"
- 2 **exida** Report No. RAD 14-06-037 R002, "Results of the IEC 61508 Functional Safety Assessment for FPGA-Based Safety Controller RadICS," September 15, 2015
- 3 10 CFR Part 50 Appendix B, "Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants"
- 4 10 CFR Part 21, "Reporting of Defects and Noncompliance"
- 5 EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications", Electric Power Research Institute, October 1996
- 6 EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," Electric Power Research Institute, December 1996

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 25 of 350
--------------	--------------------	-----------	---	----------------



- 7 NRC Letter to EPRI dated July 17, 1997, "Review of EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications (TAC No. M94127)"
- 8 NRC Letter to EPRI dated July 30, 1998, "Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute Topical Report, TR-107330, Final Report, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."
- 9 QAPD-001, "RadICS Quality Assurance Program Description"
- 10 Branch Technical Position 7-14, Revision, 5, "Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, March 2007
- 11 DI&C-ISG-04, Revision 1, "Highly Integrated Control Rooms - Digital Communication Systems"
- 12 ISO 9001:2008, "Quality management systems – Requirements"
- 13 ASME NQA-1-2008, "Quality Assurance Program Requirements for Nuclear Facilities"
- 14 ASME NQA-1a-2009, "Quality Assurance Program Requirements for Nuclear Facilities"
- 15 Regulatory Guide 1.28, Revision 4, "Quality Assurance Program Criteria (Design and Construction)"



2 RadICS Development and Operational History

2.1 Evolution of RPC Radiy Products

The first generation of RPC Radiy products, called Unified Hardware System equipment (UKTS in Russian), was introduced in 1995. The main purpose of using UKTS was to replace obsolete NPP equipment that was no longer available in the market. Within the next six years, about 10,000 UKTS modules housed in approximately 700 UKTS cabinets, were manufactured and supplied and installed at to Ukrainian nuclear power plants.

In 1998 RPC Radiy developed a new generation of UKTS-DPI modules and cabinets with digital signal processing, noise-elimination and built-in diagnostics functions. FPGA technology was used for the first time in these modules to implement control logic. More than 50,000 of such modules were installed in NPPs in subsequent years.

The evolution of RPC Radiy products is shown in Figure 2-1.

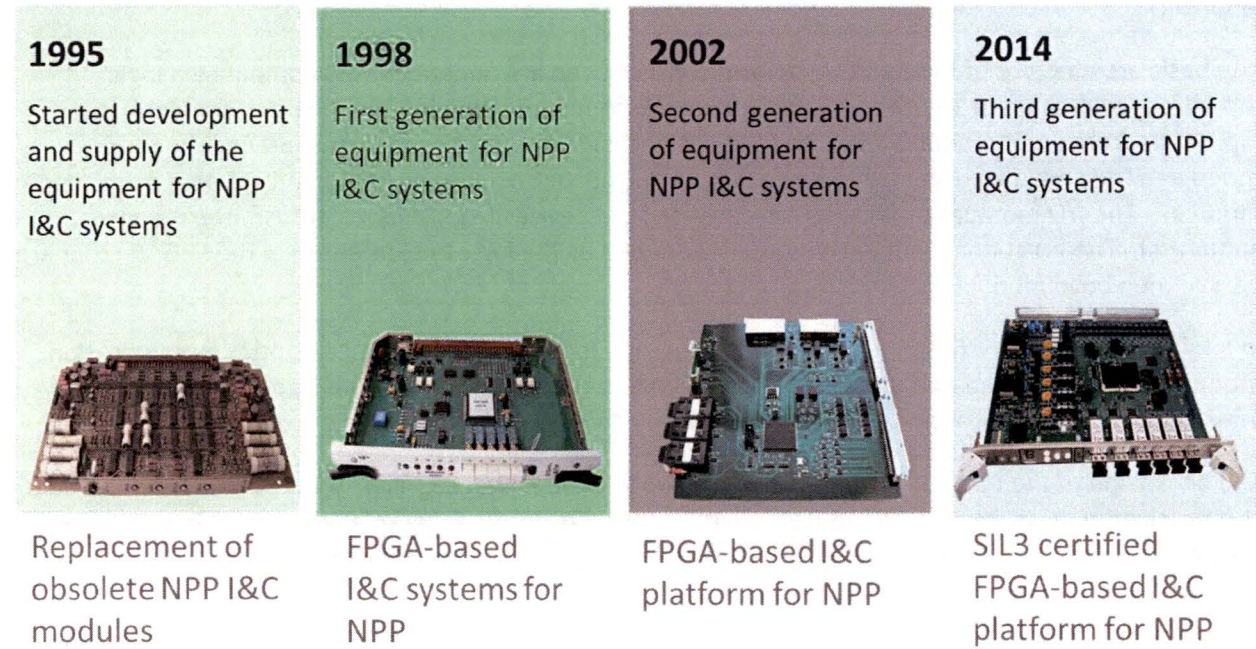


Figure 2-1: Evolution of RPC Radiy Products

The development of a new concept of an FPGA-based I&C platform was initiated in 2002 concurrent with the manufacturing and installation of the UKTS-DPI modules. This new platform, called RADIY Platform, eventually replaced the UKTS-DPI platform, whose main disadvantage was that it was designed for single-purpose applications.



The RADIY Platform is of a modular type and it includes modules such as logic modules, diagnostic modules, and digital and analog I/O modules. RPC Radiy has installed over 70 RADIY Platform-based safety and control systems in operating NPPs. Examples applications include RTS, RPCLS, and ESFAS.

The RPC Radiy latest development is the FPGA-based RadICS Platform. This is a new generation product, designed in 2011 on the basis of an earlier RADIY platform. The RadICS Platform consists of an IEC 61508:2010 (Reference 2-1) SIL 3 chassis level certifiable architecture with a typical response time of less than 10 milliseconds and a comprehensive set of constituent modules.

The Functional Safety Assessments performed by *exida* (Reference 2-2) demonstrated that the RadICS Platform complies with the IEC 61508 SIL 3 certification requirements.

2.2 Overview of RadICS Platform

The RadICS Platform (see Figure 2-2) consists mostly of a set of general-purpose building blocks that can be configured and used to implement project-specific functions and systems. The RadICS Platform is composed of various standardized modules, each based on the use of FPGA chips as computational engines.

The basic architecture of the RadICS Platform consists of an instrument chassis containing a logic module, as well as up to 14 other I/O and fiber-optic communication modules. Logic modules gather input data from input modules, execute user-specific logic, and update the value driving the output modules. They are also responsible for gathering diagnostic and general health information from all I/O modules. The I/O modules provide interfaces with field devices (e.g., sensors, transmitters, and actuators). The functionality of each module is defined by the logic implemented in the FPGA(s) that are part of the above modules.

In addition to the above described general purpose I/O modules, there is a fiber-optic communication module that can be used to expand the I&C system to multiple chassis. It is also possible to provide inter-channel communications via fiber-optic based connections between logic modules.

The backplane of the RadICS Platform provides interfaces to power supplies, process I/Os from the field, communication links, key switch inputs, and indicators. The internal backplane provides interfaces to the various modules installed within each chassis by means of a dedicated, isolated, point-to-point low-voltage differential signaling (LVDS) interface.

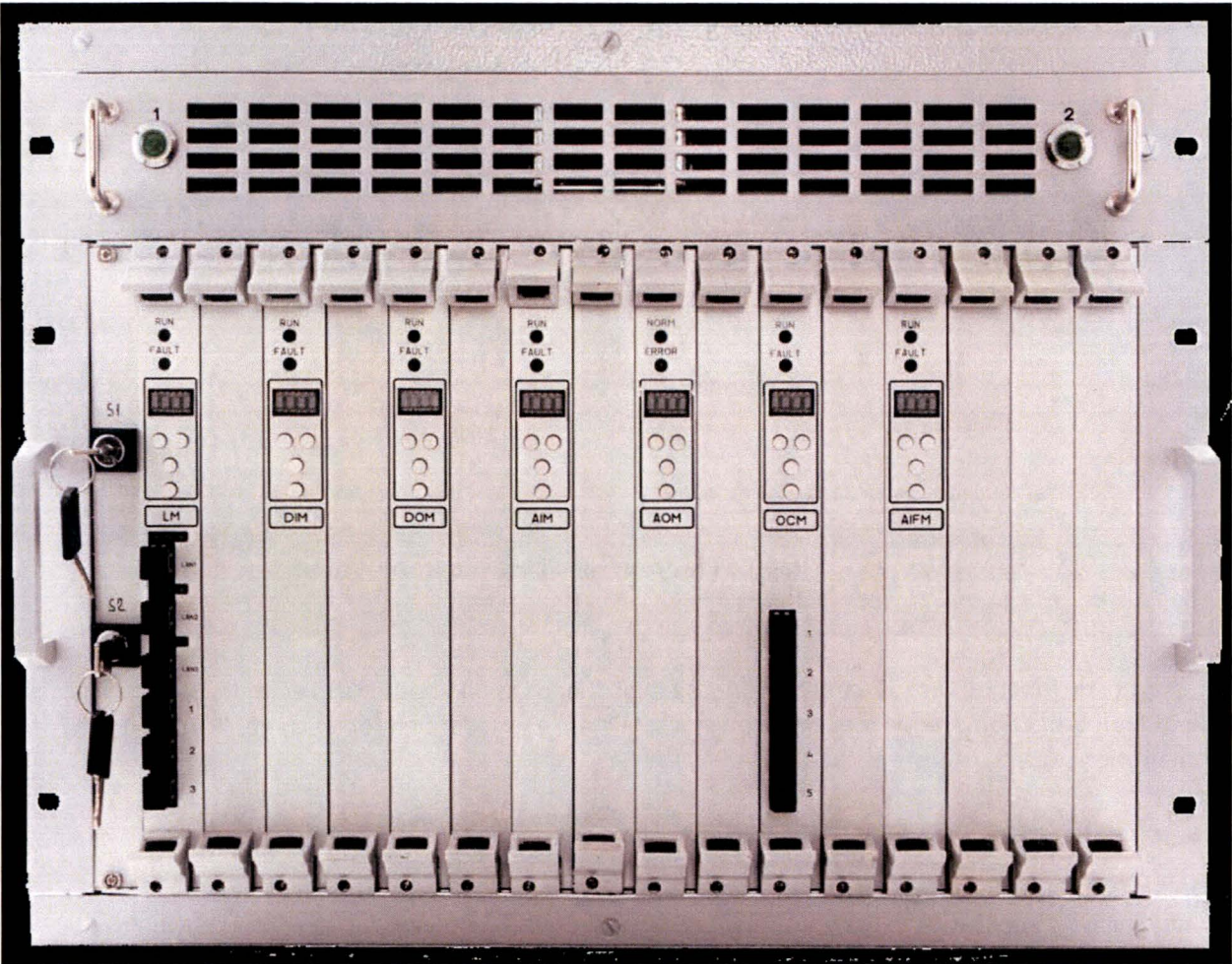


Figure 2-2: RadICS Platform

For application development, RPC Radiy provides a tool called Radiy Product Configuration Toolset (RPCT). This tool can be used to configure logic for various applications using the AFBL.

In addition, the RadICS Platform includes extensive on-line self-surveillance and diagnostics at various levels, including control of FPGA power, watchdog timer, cyclical redundancy check (CRC) calculations, and monitoring of the performance of FPGA support circuits, I/O modules, communications units, and power supplies.

The RadICS Platform can also be represented as a hierarchy with several levels, which could be arranged into two main groups: software and hardware blocks. The RadICS Platform high level representation is shown in Figure 2-3. The non-safety workstations and the HSI software associated with the MATS are not within the scope of the RadICS Platform Topical Report.

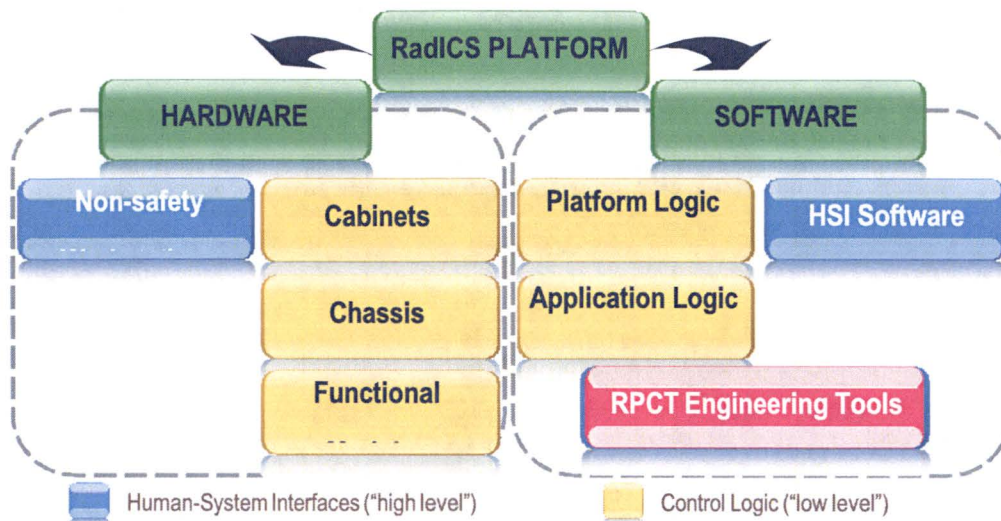


Figure 2-3: RadICS Platform High Level Representation

The diagnostic functions are separated from the logic functions and both are executed concurrently. In case of fault detection, the system is placed in a safe state as predefined for each application during configuration.

2.3 RadICS-Based Applications

FPGA based platforms produced by RPC Radiy are used in the most critical and high-reliability demanding NPP applications such as RTS, ESFAS, and RCS. The following sub-sections provide a description of these systems to provide examples of how the RadICS Platform can be used for specific projects; however, no NRC approval is sought for any specific system architecture or design as part of the RadICS Topical Report review.

2.3.1 Reactor Trip System

RPC Radiy has developed RTSs that have been used to continuously monitor various process variables and generates reactor shutdown signals in case these variables reach their setpoints. These systems have been designed to transmit all the information necessary for surveillance and monitoring of the plant (e.g., the status of command execution, plant conditions, and diagnostic data) to the control room, and on customer's request, to other safety and non-safety systems. The RadICS Platform technology can be used for 3 or 4 redundant channel systems using 2-out-of-3 or 2-out-of-4 voting logic. An example of a 2-out-of-3 voting logic configuration is shown in Figure 2-4.

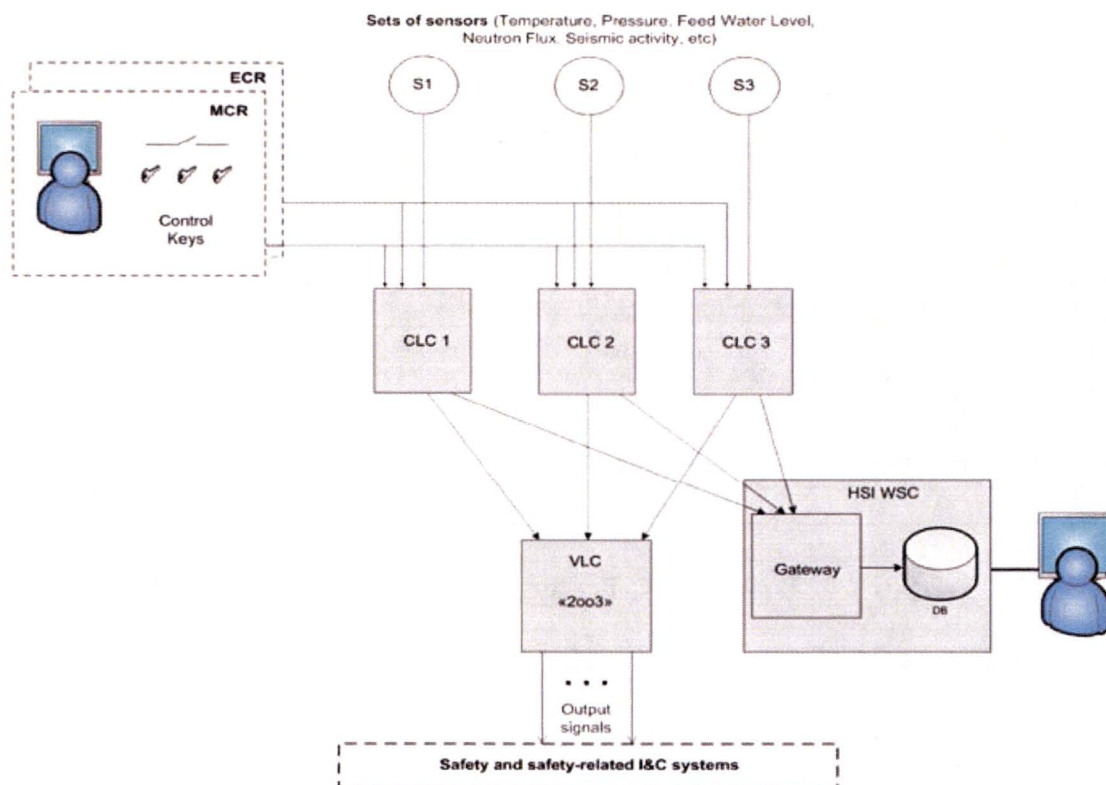


Figure 2-4: Reactor Trip System Configuration

Systems designed with RadICS Platform technology can be designed to correct voting logic when faults are detected, so that system availability is optimized without compromising safety. The RadICS self-diagnostic subsystem includes troubleshooting assistance functions that can be used to support maintenance work for easy localization of faults. In case of failure detection (i.e., failure in a RadICS Module), a system designed with RadICS Platform technology can put itself in the safe state by generating a reactor shutdown signal and the corresponding annunciation signals. RadICS Platform technology has been used to design systems that included manual actuation of shutdown logic from the Main Control Room or Remote Shutdown Station. The RadICS Platform can be adapted to perform equivalent functions in all the major reactor types. A typical set of RadICS Platform equipment is shown in Figure 2-5.



To date there are 30 RPC Radiy designed RTSs in operation at Zaporizhzhе NPP, Rivne NPP, Khmelnytsky NPP, and South Ukraine NPP.

Figure 2-5: Typical RadICS Reactor Trip System Equipment

2.3.2 Engineered Safety Features Actuation System

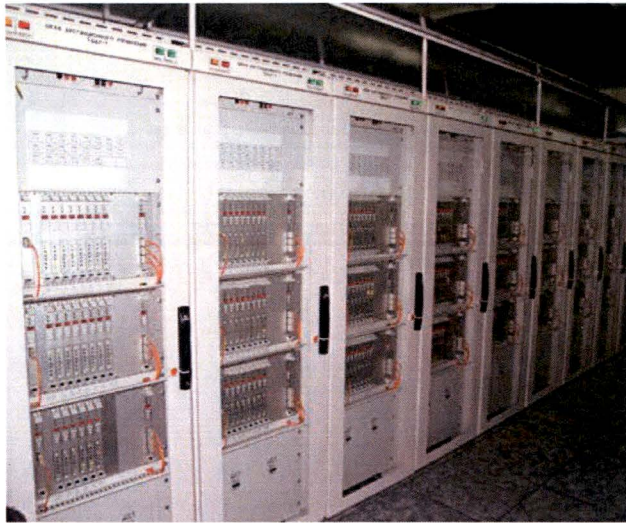
The RadICS Platform technology can be used to design and manufacture ESFAS applications (see Figure 2-6) that have the following main functions:

- Protection, interlocking, and monitoring of actuators
- Manual remote control of actuators
- Acquisition of signal data and other related information
- Signal conditioning and monitoring of safety signals, detectors, and sensor
- Full-scope system self-diagnostics

The following design principles can be applied in the ESFAS using RadICS Platform technology:

- Variety of input signals (e.g., current, voltage, resistance, “dry contact”)
- System expandability to accommodate the need for an increased number of inputs and outputs
- A simple and controlled process for the modification of system logic and control algorithms
- Interfacing capability with other plant control and monitoring systems

A RadICS Platform-based ESFAS can be supplied in two to four channels configurations. In these configurations, a RadICS Platform-based system can meet U.S. Class 1E requirements.

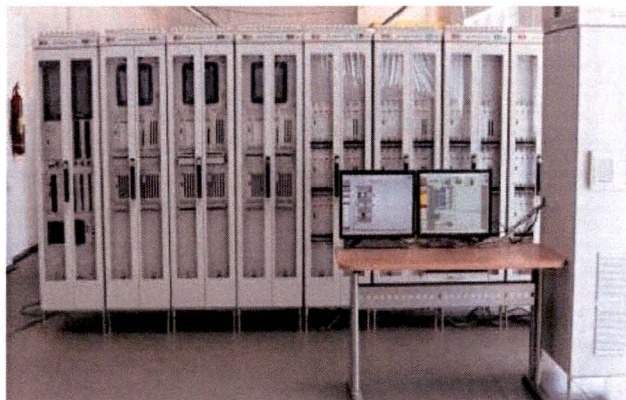


Eighteen ESFASs are presently in operation at Rivne, South Ukraine, and Kozloduy (Bulgaria) NPPs.

Figure 2-6: RadICS Engineered Safety Features Actuation System Cabinets

2.3.3 Rod Control System

A typical RCS (Figure 2-7) using RadICS Platform technology consists of Rod Position Indication (RPIS) and Rod Drive Control (RDCS) sub-systems, electronic equipment power supplies, and Rod Drives Electric Power Supply Subsystem (RDEPSS), designed and manufactured by either RPC Radiy or other suppliers.



The first RPC Radiy supplied RCS has been successfully put in operation in Unit 1 of the South-Ukraine NPP (VVER-1000 PWR- type reactor) in 2013

Figure 2-7: RadICS Rod Control System Cabinets

The function of the RPIS subsystem is to provide an indication of all reactor control and safety rods operation parameters. The RDCS sub-system performs all rod drive control and trip functions.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 33 of 350
--------------	--------------------	-----------	---	----------------



The RDEPSS provides the following functions:

- Uninterruptable electric power supply of Rod Drives in normal operation mode
- Switching off of the rod drives electric power on receipt of a reactor protection signal

A RadICS Platform RCS can have 2, 3, or 4 redundant channels depending on the design basis of the nuclear reactor, and it can be implemented via 1-out-of-2, 2-out-of-3, or 2-out-of-4 voting logic. A typical RadICS Platform RCS architecture in a 1-out-of-2 voting logic configuration for a Pressurized Water Reactor (PWR) unit is shown in Figure 2-8.

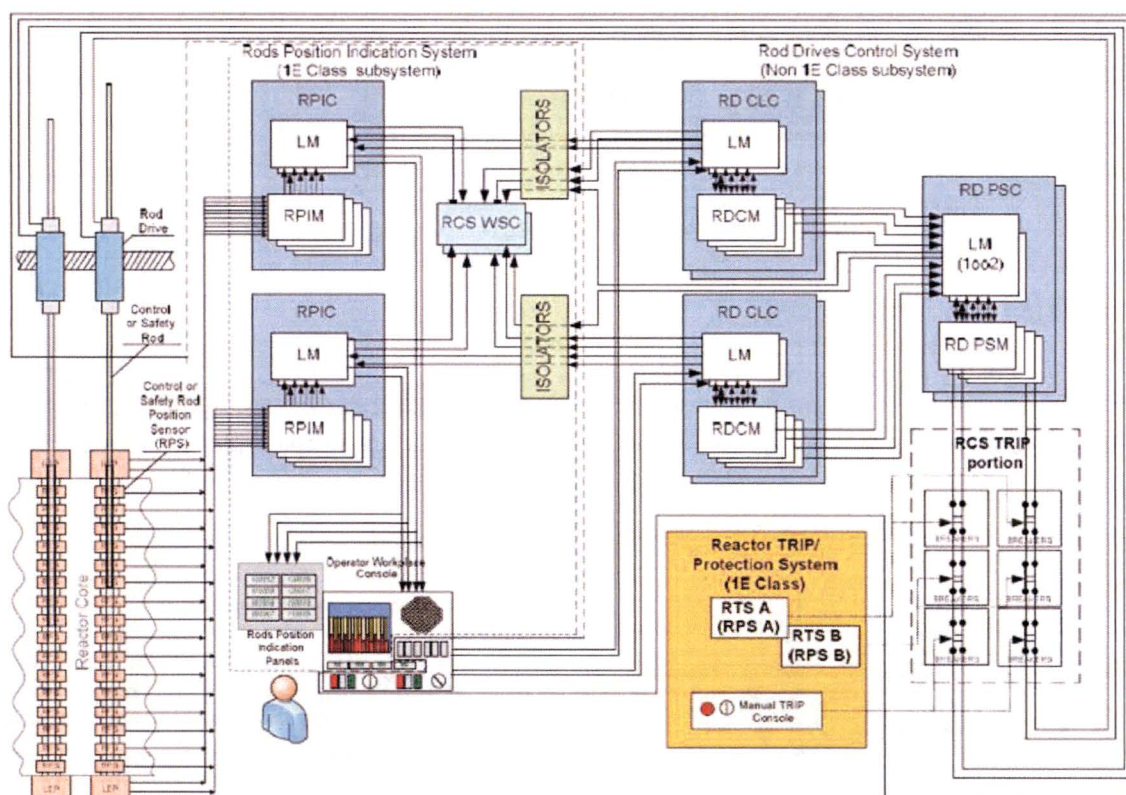


Figure 2-8: Typical RCS Architecture Voting Logic Configuration for a PWR Unit

2.4 RPC Radiy Safety I&C Installations

RPC Radiy FPGA-based I&C systems have been installed in operating NPPs since 1998. A summary of RPC Radiy nuclear I&C references collectively implemented with all technologies is provided in Table 2-1.

**Table 2-1: RPC Radiy Designed and Manufactured Equipment and Systems Installed in NPPs**

Systems Supplied	Nuclear Power Plant	Number of Installed Systems	Installation Years
Reactor Trip System	Zaporozhye NPP; South-Ukraine NPP; Rivne NPP; Khmelnytsky NPP	30	2004-2015
Reactor Power Control and Limitation System	Zaporozhye NPP; South-Ukraine NPP; Rivne NPP; Khmelnytsky NPP	11	2004-2015
Engineered Safety Feature Actuation System	South-Ukraine NPP, Rivne NPP, Kozloduy NPP, Bulgaria	18	2005-2010
Rod Control System	South-Ukraine NPP	1	2013
Fire Alarm System	Zaporozhye NPP; South-Ukraine NPP	11	2008-2014
Power Supply for Rod Control System	Kozloduy NPP, Bulgaria; South-Ukraine NPP	4	2007-2015
UKTS-Based Reactor and Turbine Control System	Rivne NPP; Zaporozhye NPP	15	1998-2004
Switchgear	Rivne NPP; Nuclear Research Institute; Kozloduy NPP; South-Ukraine NPP	1,635	2006-2015
Seismic Sensors	Khmelnytsky NPP; Zaporozhye NPP; Rivne NPP; South-Ukraine NPP	63	2010-2014
Pressure Heat Transportation Pump Motor Speed Measuring Devices	Embalse NPP, Argentina	1	Delivered to Candu Energy, April 2014
Main Control Room and Secondary Control Area Window Annunciators	Embalse NPP, Argentina	1	Delivered to Candu Energy, April 2014

RadICS has a problem reporting and tracking system as described in the RadICS Quality Assurance Manual (Reference 2-3). The RPC Radiy nuclear operating experience has provided ample opportunities to identify latent errors and to validate equipment performance.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 35 of 350
--------------	--------------------	-----------	---	----------------



In addition, operating experience with RPC Radiy digital safety I&C systems has shown no instances where the capability of the safety I&C system to perform its intended safety function(s) was compromised during an anticipated operational occurrence. Specifically, the RPC Radiy systems have not experienced any system failures or common cause failures in more than 400 reactor-years of operation as of December 2015.

2.5 Chapter 2 References

- 1 IEC 61508-2010, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems," International Electrotechnical Commission
- 2 "*exida* Report No. RAD 14-06-037 R002, "Results of the IEC 61508 Functional Safety Assessment for FPGA-Based Safety Controller RadICS," September 15, 2015
- 3 QAPD-001, "RadICS Quality Assurance Program Description"



3 Quality Assurance

3.1 Introduction

RPC Radiy is a leading Ukrainian designer and supplier of advanced I&C systems for NPPs. RPC Radiy offers a full development cycle including design, manufacturing, testing, and equipment installation. RPC Radiy is the designer and manufacturer of the RadICS Platform equipment.

The RPC Radiy QMS governs the design and manufacture of the RadICS Platform equipment. The RPC Radiy QMS is based on ISO 9001:2008 (Reference 3-1). The RPC Radiy QMS is described in Section 3.2.

RadICS is a wholly owned LLC established in July 2012. The company's business focus is the design and delivery of I&C systems for NPPs using the RadICS Platform equipment.

The RadICS QAP governs the system design, integration, and delivery of I&C systems for NPPs using the RadICS Platform equipment. RadICS QAP is based on 10 CFR Part 50 Appendix B (Reference 3-2) and ASME NQA-1-2008 (Reference 3-3) and the NQA-1a-2009 Addenda (Reference 3-4), as endorsed by RG 1.28 (Reference 3-5). The RadICS QAP is described in Section 3.3.

3.2 RPC Radiy Quality Assurance Program

3.2.1 RPC Radiy Organization

RPC Radiy is headquartered in Kirovograd, Ukraine. RPC Radiy provides a full range of design activities. In addition to the RadICS Platform equipment, RPC Radiy designs other hardware components, such as electrical distribution and switchgear cabinets and non-FPGA-based I&C systems. RPC Radiy has a broad range of technical capabilities and high degree of vertical integration: design, procurement, manufacturing, testing, and installation. The RPC Radiy organization structure is shown in Figure 3-1.

3.2.1.1 RPC Radiy Design Bureaus

The RPC Radiy Design Bureaus include the following:

- Design Bureau of I&C Systems performs design of instrumentation and control and electrical systems for NPPs and other industrial facilities,
- Design Bureau of Fire Safety Automatic Control performs design of fire detection and video surveillance systems for NPPs and other industrial facilities,
- Design Bureau of Electrotechnical Equipment designs RTS, ESFAS, RPCLS, and electrical distribution control systems,
- Design Bureau of Physical Processes Analysis develops industrial seismic sensors and seismic detection systems, and
- Design Bureau of Software and Hardware Systems develops new platforms and systems, performs reverse engineering, and supports Radiy activities during international projects.

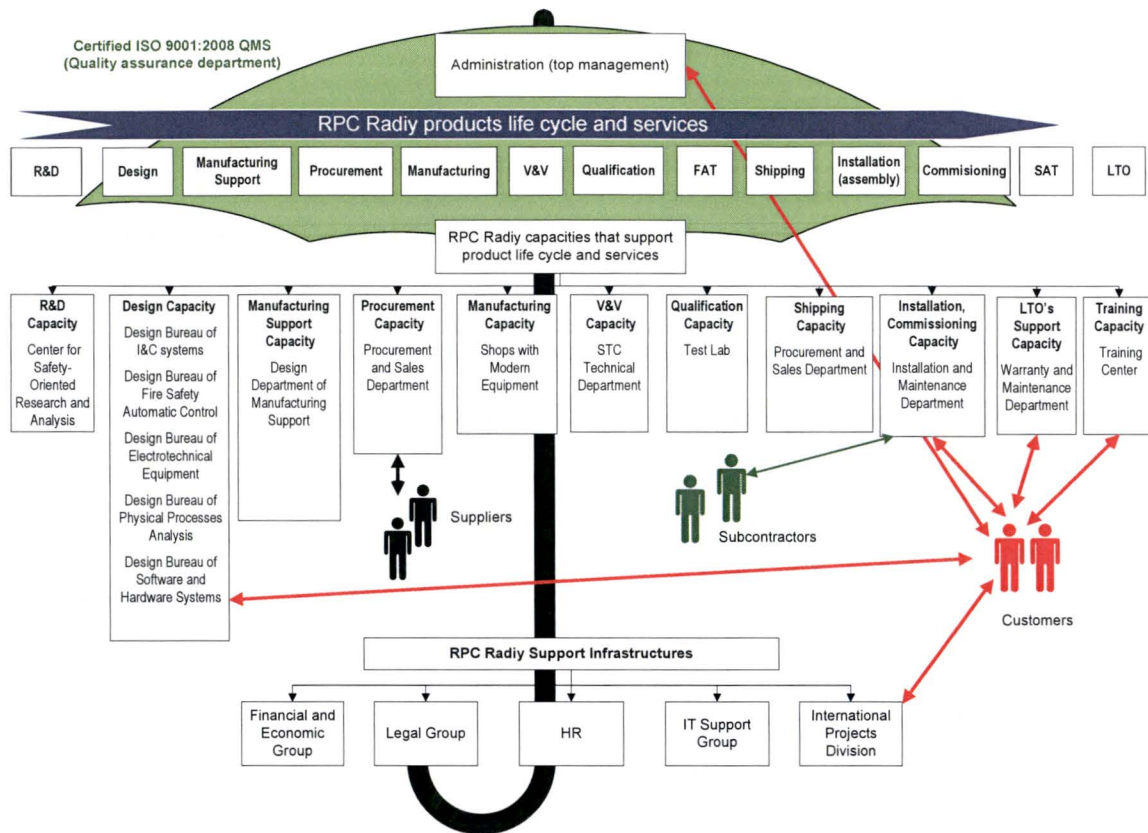


Figure 3-1: RPC Radiy Organization Structure

RPC Radiy has adopted design processes and QMS practices that are in compliance with industry wide safety requirements for I&C systems as described in IEC 61508 (Reference 3-6), as well as specific requirements for nuclear I&C systems as described in the IAEA and IEC standards for nuclear facilities.

RPC Radiy designers have been involved in the development of I&C systems for the nuclear industry since 1995 and with FPGA-based applications since 1998. The RPC Radiy methods are based on the company's experience, continuous improvement processes, and the best international FPGA design practices. RPC Radiy also collaborates with the international NPP community, including the EPRI, to shares FPGA-related experience.

RPC Radiy technical departments and top management support the designers' professional development. Training of designers is performed on a regular basis to achieve the appropriate staff qualification levels. All training activities are performed in accordance with the RPC Radiy QMS.

3.2.1.2 Research and Development (R&D)

RPC Radiy is one of the leading companies in the world providing FPGA-based I&C solutions to the nuclear industry and seeking new applications where FPGA technology can be utilized. The ongoing

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 38 of 350
--------------	--------------------	-----------	---	----------------



investment in Research and Development (R&D) activities leads to continuous improvement of its products.

The Scientific and Technical Center for Safety Infrastructure-Oriented Research and Analysis (STC) is the R&D Department. Some of the STC's main activities are as follows:

- Safety assessment of FPGA based I&C systems and applications,
- Design assessment: evaluating attributes, such as reliability, security, and maintainability of FPGA-based systems hardware and software,
- Development of techniques and tools for multi-version system assessment of safety and diversity,
- Development of V&V techniques for the FPGA-based I&C systems,
- Participation in the development of standards and other normative documents associated with FPGA based I&C systems, support to the development of the RPC Radiy QMS, and
- Certification and licensing support of FPGA based and other I&C systems.

3.2.1.3 Manufacturing Support

The Manufacturing Support department is responsible for the preparation of documentation to be used in the manufacturing of components and assembly units and their interconnecting parts, as well as manufacturing processes such as metal plating, polymeric coating, mounting, handling, rinsing, marking, testing, packing, and associated manufacturing control operations. All manufacturing support activities are performed in compliance with Company Standards, Guides, and Working Instructions/Procedures that are part of RPC Radiy QMS.

3.2.1.4 Procurement

RPC Radiy performs all manufacturing activities in its own production facilities. Certain components, such as printed circuit boards (PCBs) and electronic components, as well as materials, such as metal plates, mounting hardware, and chemical are purchased parts. The selection of these components is performed by RPC Radiy technologists, procurement department personnel, QA staff (quality inspectors and auditors) and using Test Laboratory capabilities (if needed) in accordance with the requirements of generally accepted standards and specifications, which meet the requirements of the ASME NQA-1b-2007 (Reference 3-7) and the guidance in EPRI NP-5652 (Reference 3-8) and EPRI TR-102260 (Reference 3-9).

According to requirements of ISO 9001, ASME NQA-1b-2007, and other related standards, it is necessary to establish a supplies evaluation process to provide reasonable assurance that a commercial grade item will successfully perform its intended safety function. Information required for the evaluation of the RPC Radiy suppliers is obtained via the following methods:

- Testing (Special Tests and Inspections);
- Suppliers' assessment (Commercial Grade Survey),
- Suppliers' inspection (Source Verification), and
- Statistical estimation (Acceptable Supplier/Item Performance Record).

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 39 of 350
--------------	--------------------	-----------	---	----------------



The supplier evaluation and selection process is implemented by the Procurement Department in accordance with established procedures. The capability of a supplier to provide products that conform to the specified technical requirements is evaluated. Suppliers are required to identify all regulatory documents used for products manufacturing and provide them to RPC Radiy, as requested. Product delivery terms are evaluated to the ability of the supplier to deliver products timely in accordance with a plan of delivery. The Procurement Department Head can decide to audit a supplier to confirm the quality of supplied products. Audits are performed in accordance with established procedures by authorized Procurement Department employees. An audit report is provided to the Director of Marketing, Logistics, and Procurement. Based on audit report, the Director of Marketing, Logistics and Procurement makes the decision on further cooperation with subsequent execution of a contract with this supplier and including of this supplier into the List of Approved Suppliers.

The following criteria are used for supplier selection:

1. quality of delivered items:
 - reliability data of suppliers items
 - quantity of unaccepted materials due to noncompliance with requirements
 - acceptable deviations from requirements in various entire scope of delivery
 - quality and completeness of the documentation
 - parts traceability
 - availability of a certified QMS
2. observance of delivery terms:
 - timely delivery of order items
 - compliance with commercial and legal conditions of the contract
 - in case of justified delays, the suppliers' ability and willingness to implement a successful schedule recovery plan
3. price policy and terms of payment:
 - compatibility of terms of payment with the RPC Radiy financial strategy
 - competitive pricing
 - production capability
 - financial health of the company
 - ability and willingness to support their clients during challenging times
4. other requirements:
 - Ability of the suppliers' staff to communicate in a clear and open fashion

All above mentioned activities are performed by the RPC Radiy Procurement and Sales Department on a regular basis, allowing us to maintain an up-to-date list of qualified suppliers.

RPC Radiy has implemented procedures for performing incoming inspection to prevent the usage of counterfeit materials in digital I&C systems. The inspection is used to check the availability of documentation for products that certify the quality, completeness, control, and conformity of product quality to specified regulatory documents. The inspection also checks product packaging and marking. Sampling is used to check product attributes using various test methods (e.g., titrimetric, photometric,



spectroscopic, and gravimetric testing methods) or analysis based on functional testing to controlled parameters.

3.2.1.5 Manufacturing

RPC Radiy has the following manufacturing capabilities and facilities:

- Metal working shop equipped with automated sheet shearing machines, sheet bending presses, turret punch presses, table spot welding machines, and automated welding machines for assembling components and complete cabinets,
- Formed-in-place foam gasket line for polyurethane foam or silicone sealing contours gasket on the doors and different panels of the chassis/racks/cabinets, equipped with automated mixing and dispensing machines,
- Galvanic coating lines,
- Polymeric powder and seal coating lines,
- Automated line for PCB surface mounting (including soldering) equipped with an automatic solder pastes screen printer, inspection conveyor, automatic surface-mount device pick and place machine, inspection conveyor, automatic convection soldering system, and automated X-ray tomography system for soldering quality control,
- Facilities for manual heavy components, as well as production lines for surface mounting of connectors on the PCBs with quality inspection workstations,
- PCB washing and protective coating (including protection against tropical conditions) facilities using Silicone Conformal Coating (Electrolube DCA SSC 3 type),
- Fiber-optical patch cables manufacturing facility equipped with a video fiber microscope, polishing machine, fiber optic curing oven, and universal optical fiber test platform/reflectometer,
- Facilities equipped with special measurement, monitoring, and simulation equipment for calibration of electronic and electric assemblies and systems,
- Facilities for the repair of PCBs, modules, assemblies, and other parts associated with I&C systems. These are equipped with disassembling, demounting, coating, soldering, measurement, monitoring, and simulation equipment, and
- Facilities for the inspection of soldering in PCBs, electronic, and electrical assemblies.

The RPC Radiy manufacturing and inspection facilities comply with the QMS, which complies with applicable ISO, IEC, and Institute for Printed Circuits (IPC) standards.

3.2.1.6 Verification and Validation

RPC Radiy has established a V&V program in full compliance with processes defined in international standards. The following V&V methods are in use:

- Documents review,
- Failure and mode effect analysis (FMEA),
- Static code analysis and code review,
- HDL code functional testing,

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 41 of 350
--------------	--------------------	-----------	---	----------------



- Logic level simulation, timing simulation and static timing analysis (for FPGA ED)),
- Reports review of synthesis, place and route, bitstream generation (for FPGA ED),
- Fault insertion testing (FIT), and
- Integration testing, validation testing.

RPC Radiy prefers the use of proven V&V tools over manual methods to eliminate human error. The above tools are purchased only from well-established vendors, with a good track record of configuration management, V&V, problem notification and resolution, and support and training materials.

The company QMS prescribes that all commercial software tools used for V&V should be tested and evaluated with the issuance of relevant evaluation reports. In addition to commercial software tools, RPC Radiy use in-house developed custom software and hardware tools for V&V activities.

RPC Radiy V&V capabilities are supported by the STC, a department that is technically, administratively, and financially independent from the Design departments. Personnel performing V&V activities have a strong theoretical background and practical experience on design and testing of software and FPGA ED. RPC Radiy practices are in line with those followed by other organizations involved in the design of FPGA-based safety and non-safety I&C solutions for NPPs and in compliance with international standards. STC took an active part in the SIL 3 certification of RadICS Platform.

The V&V process for the RadICS Platform is described in further details in Section 7.4.

3.2.1.7 Qualification Test Laboratory

Equipment qualification (EQ) testing for RPC Radiy I&C systems is performed in the RPC Radiy testing laboratory, which is certified by the National Accreditation Agency of Ukraine² to be in conformance with ISO/IEC 17025:2005 (Reference 3-10). The testing laboratory is equipped with all the necessary certified test equipment. The above test equipment is calibrated in compliance with ISO 10012:2003 (Reference 3-11). The testing laboratory is operated by trained and experienced staff.

The facilities include test benches for seismic qualification and environmental qualification; equipment aging chambers; and I&C systems simulation/modeling facilities. Qualification test capabilities include: radiation exposure and dust resistance (via approved service supplier); pressure, temperature, and humidity resistance; seismic qualification, vibration and other mechanical shock resistance; and electrical insulation, electrical safety, and electromagnetic compatibility. RPC Radiy EQ processes comply with EPRI qualification methods.

3.2.1.8 Storage and Shipping

RPC Radiy storage, packing, and shipment procedures ensure the following:

- Protection against equipment physical and functional damage resulting from mechanical or environmental damage,
- Labelling of parts in compliance with customer requirements,

² Affiliated member of the International Laboratory Accreditation Cooperation



- Packing in containers in compliance with customer requirements and adequate packaging in accordance with the type of equipment and transportation mode, and
- Provision of a complete and detailed packing list.

RPC Radiy procedures prescribe methods and assign responsibilities for the handling of defective products. Where required to store or ship products that do not meet requirements, these will be properly identified and controlled to avoid unintended use.

3.2.2 Quality Management System

Between 1994 and 2003 the Company has developed, implemented, and put into action the QMS that conformed to the requirements of ISO 9000 series standards. In February 2004, RPC Radiy passed the certification audit by the Ukrainian State Agency "State Regulatory Center of Delivery and Service Quality" of quality certification system "SERTATOM." This certified RPC Radiy compliance with requirements of the national standard DSTU ISO 9001-2001 (Reference 3-12).

In 2008, after analyzing a set of documents, including QMS, the State Committee of the Nuclear Regulations in Ukraine expanded the previously granted the Activity License to authorize RPC Radiy to perform the design and manufacturing activities of certain nuclear products.

In 2009 RPC Radiy introduced an updated QMS that it believes satisfies the requirements of 10 CFR Part 50 Appendix B and ASME NQA-1-2008 to prepare for a broader international presence; however, the QMS is still organized and aligned to ISO 9001:2008.

3.2.2.1 International Certification Activities

Information on the international certification activities is provided to give the NRC some context regarding the effectiveness of the RPC Radiy QMS design and implementation, since it may not be familiar with RPC Radiy and its business operation.

In January 2005, the RPC Radiy QMS was certified in the International Certification System by the TÜV³ Rheinland InterCert for compliance with requirements of international standard ISO 9001:2008. As a result of the successful audit, TÜV Rheinland InterCert issued a certificate confirming that the required production quality controls were established at RPC Radiy. As a result of an additional audit performed by the International Certification Agency TÜV Rheinland InterCert in October 2011, RPC Radiy obtained a new certificate for compliance with standard requirements of ISO 9001:2008. The certificate's scope included design, manufacturing, installation, and maintenance of instrumentation and control systems and the fire alarm system, including systems and equipment important to safety for nuclear power plants. The certificate was updated by TÜV Rheinland InterCert in 2013.

Inputs from other design and manufacturing companies, performing audits to assess RPC Radiy as a potential supplier, also helped improve the RPC Radiy QMS. In 2010, the RPC Radiy QMS was assessed by the former Atomic Energy of Canada Limited (AECL) (now CANDU Energy) Procurement Department to confirm the implementation and effectiveness of the QMS. AECL's Supplier's QMS Audit

³ Technischer Überwachungsverein

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 43 of 350
--------------	--------------------	-----------	---	----------------



was conducted to evaluate the ability of RPC Radiy to supply products which can meet the AECL requirements. RPC Radiy standards were modified and implemented in order to successfully pass the AECL audit. Based on the audit's results, AECL concluded that the RPC Radiy QMS complies with the Canadian Standards Association (CSA) CAN3-Z299 series and subsequently RPC Radiy was included in the official AECL suppliers' list. In order to renew the approved vendor qualification status, CANDU Energy audited RPC Radiy in April 2013 against Canadian Standard CSA N Z299.1 (Reference 3-13) and ISO 9001:2008.

In 2014, the RPC Radiy QMS was assessed by Hungarian nuclear utility MVM Paks Nuclear Power Plant. The audit resulted in a conclusion that RPC Radiy is in full compliance with requirements to perform work such as design, manufacturing, repair, maintenance, expert activities, main contractor activities, and contributions in installation activities related to operation, maintenance, modification, and repair of I&C systems and components classified into the safety categories 2 and 3.

In 2015, RPC Radiy started work with ISO Ingenierie to align the RPC Radiy platform and applications against regulatory requirements in France. The activities include a review of RadICS Platform, as well as a review RadICS Platform, applications, and processes for compliance with IEC standards. The effort is designed to identify an approach for requirements gap analysis and safety case implementation to develop a road map for qualification of RadICS technology in France.

3.2.2.2 International Atomic Energy Agency Mission at RPC Radiy Facilities

The IAEA review mission titled, *Independent Engineering Review of I&C Systems in Nuclear Power Plants (IERICS)*, was established by the Nuclear Power Engineering Section of IAEA to conduct peer reviews of NPP I&C design documents, prototype systems, and systems in actual operation in NPPs. The IERICS review team consists of a group of invited subject matter experts from various IAEA Member States.

The IERICS Mission is based on appropriate IAEA documents, such as Safety Guides and Nuclear Energy Series Reports. The IERICS Mission took place at the RPC Radiy facilities in Kirovograd, Ukraine, in December 2010 and closed-out in March 2011 in the IAEA offices in Vienna, Austria. The subject matter of the above review mission was the RPC Radiy FPGA-based safety I&C RadICS Platform. The IERICS review was based on the IAEA Safety Guide NS-G-1.3 (Reference 3-14) and IAEA Nuclear Energy Series Reports NP-T-1.4 (Reference 3-15), NP-T-1.5 (Reference 3-16), and NP-T-3.12 (Reference 3-17).

The findings of the IERICS Mission were given in the Mission Report IERICS-UKR-2010, *Independent engineering review of instrumentation and control systems (IERICS) in nuclear power plants: IAEA review of the Radiy FPGA-based safety I&C platform and systems for NPPs*. The conclusions of the IERICS Mission included recommendations, suggestions, and an acknowledgement of good practices at RPC Radiy. In particular, the following items were identified as good practices:

- The use of FPGA technology and advanced approaches to the development of an FPGA based platform and systems,
- The design includes extensive on-line self-diagnostics at different system levels,
- Full implementation of the IAEA QMS requirements in the RPC Radiy Quality Management System, and
- Defect reporting program from which other organizations may benefit.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 44 of 350
--------------	--------------------	-----------	---	----------------



The IAEA review team confirmed that extensive, high quality engineering work, in compliance with the relevant sections of the IAEA Safety Guide NS-G-1.3, had been performed by RPC Radiy in the development of FPGA-based I&C systems.

3.2.2.3 IEC Safety Integrity Level Certification

[[]]^{a,c,e} to a critical design review (CDR) based on EPRI TR-1011710 (Reference 3-18). IEC 61508 defines the requirements for suppliers to follow during product development to ensure that their products have a high level of resistance to random hardware and “systematic” design failures. Compliance is evaluated by qualified third party certification agencies which assess and certify that a product has been designed and developed in accordance with the standard.

The IEC 61508 SIL 3 certification process is shown pictorially in Figure 3-2.

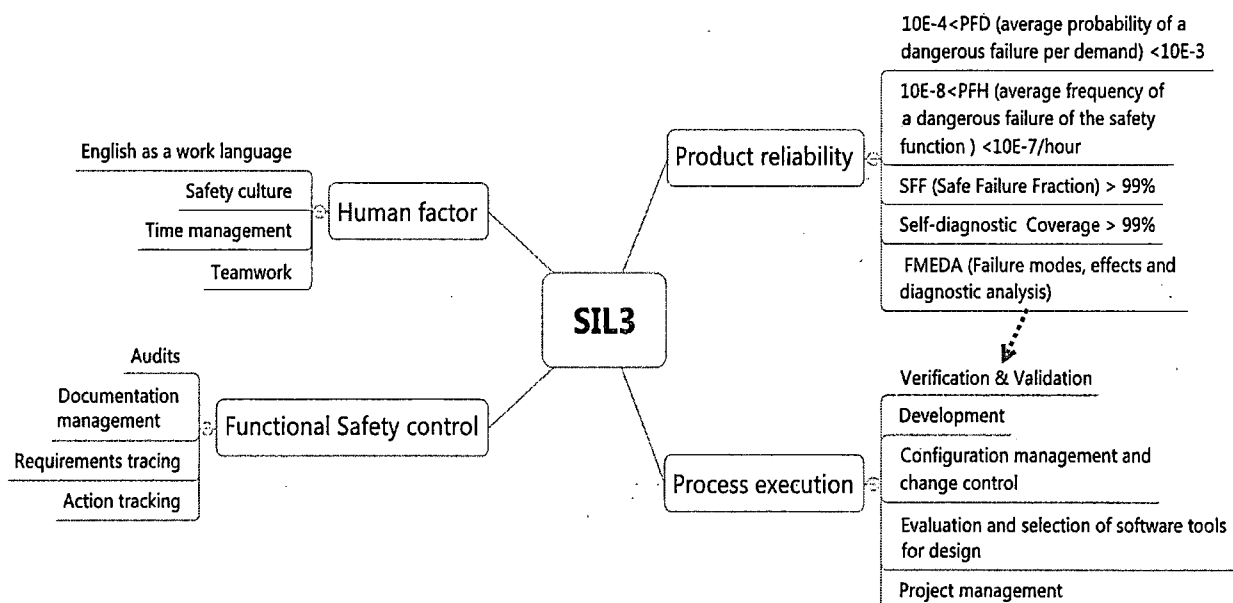


Figure 3-2: SIL 3 Certification Process

exida followed a rigorous process that verified the SIL of the RadICS Platform Hardware and associated ED, as well as its manufacturing and quality control procedures. [[]]

]]^{a,c,e}

The IEC 61508 standard provides means of certifying systems on the basis of four predefined SILs, where SIL 4 would be the most demanding level. SILs are order of magnitude levels of risk reduction. The IEC 61508 establishes three modes of operation:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 45 of 350
--------------	--------------------	-----------	---	----------------



- Low Demand Mode: where the safety function is only performed on demand, and where the frequency of demands is no greater than one per year;
- High Demand Mode: where the safety function is only performed on demand, and where the frequency of demands is greater than one per year;
- Continuous Demand Mode: where the safety function is a part of normal operation.

The SIL table for appropriate measures for a NPP protection system is shown in Table 3-1.

Table 3-1: IEC 61508 SIL Table for Demand Mode

Safety Integrity Level	Average Probability of a Dangerous Failure on Demand of the Safety Function (Low Demand Mode of Operation)	Average Frequency of a Dangerous Failure of the Safety Function, 1/hour (High Demand and Continuous Modes of Operation)	Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$	100,000 to 10,000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$	10,000 to 1,000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$	1,000 to 100
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$	100 to 10

The SIL certification process requires that products developed under a Functional Safety Management Plan (FSMP) to be audited in stages by the independent certification agency. The FSMP describes the process and procedures used to design; verify and validate; and maintain the RadICS Platform. The FSMP defines the specific management responsibilities for the RadICS Platform development project. The FSMP takes all IEC 61508 requirements into consideration and mandates that they be applied throughout the product life cycle.

The SIL certification process outlined in IEC 61508 requires the preparation of a set of documents specific to each of the phases of the product life cycle. These documents must be subject of an independent auditing process and assessment by a Certification Body.

The auditing process starts early in the product development process with an independent Functional Safety Assessment of the readiness of the processes and product(s). Internal Functional Safety Audits (FSAs) are conducted after successful completion of the development process at specific milestones, as described below.

The first internal FSA usually takes place early within the development process, after the functional and safety requirements definition, when V&V plans and product architecture design are available. Other activities that need to be completed before the commencement of this first internal FSA are the safety



concept definition, the section dealing with suppliers and the implementation of a configuration control process.

The objectives of this internal FSA are to verify that:

- The required documents have been approved for use and are under proper configuration
- Control,
- Project QA manual is in place and in line with corporate and project objectives and quality requirements,
- The QA programs of suppliers of materials and services are in line with the project quality requirements as defined in the project QA manual,
- Whether all verification activities associated with this phase of the development process were correctly executed,
- An effective action tracking process was instituted and followed by all members of the team,
- An effective requirements tracing process was instituted and followed by all members of the team,
- The Safety Concept for the product is clearly defined,
- The required competences and accountabilities for the project are clearly identified and the organization is staffed accordingly, and
- An effective Change Management process was instituted and followed by all members of the verification team.

All of the above is consistent with activities as described in the RadICS FSMP.

The objectives of subsequent internal FSAs are:

- To address observations from the previous FSAs,
- To ensure continued compliance with all applicable objectives, as defined for the first internal FSA,
- To ensure that the development process continues to follow the FSMP,
- To verify that only qualified tools are used in the development process,
- To determine whether conditions are met for the commencement of the independent Functional Safety Assessment by the corresponding Certification Body,
- To ensure compliance with the FSMP at each audited project phase,
- Verify that the product release baseline audit has been successfully performed, and
- Verify that fault insertion tests cover the appropriate measures.

The independent Functional Safety Assessment is performed by an external certification agency. The person in the agency, responsible for the independent assessment, prepares the FSMP and various procedures.

The following information is required as input to the independent Functional Safety Assessment:

- IEC 61508,
- The final product functional, safety and performance requirements, and

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 47 of 350
--------------	--------------------	-----------	---	----------------



- The final product safety integrity requirements (requirements for probability rates and reliability indexes).

On completion of the independent Functional Safety Assessment, the certification agency issues the following documents: Functional Safety Assessment Plan, Functional Safety Assessment Report and the certificate of product's compliance.

In 2010, RPC Radiy senior management set as one of the company's goal, to use our RadICS Platform for Safety Instrumented System (SIS) applications under IEC 61508. As a result of the above, the following decisions were made:

- To move from being a turnkey only supplier (supplier of entire systems) to different contractual arrangements where RadICS could be used as a platform for implementation of different safety and non-safety applications and in which RPC Radiy or the client could play the role of the integrator,
- To pursue certification of the RadICS Platform to SIL 3 based on IEC 61508, and
- To contract *exida* Inc. as the independent assessor and certification agency.

In 2011, *exida* performed a preliminary assessment to assist RPC Radiy management in determining the level of effort required to reach SIL 3 certification for the RadICS Platform, assuming a 2-out-of-3 voting logic architecture. The assessment included:

- IEC 61508 Process Gap Analysis (product development and support processes evaluation) and
- System Failure Mode and Effect Analysis (high-level design assessment).

The results of the *exida* assessment formed the basis of a new comprehensive project aimed at enhancing the life cycle processes of the RadICS Platform to the level required for SIL 3 certification.

Changes to the platform development process and detailed planning of associated activities for the upgrading of the RadICS Platform to comply with SIL 3 requirements were implemented during the first phase of the project. Personnel, Document, Functional Safety Management, Configuration Management and Overall V&V plans, along with Safety Requirements Specification and other documents covering all aspects of the life cycle were developed during this phase of the project.

Results of subsequent phases of the certification project showed that all of the *exida* recommendations were taken into account and successfully implemented.

A subsequent assessments performed by *exida*, as well as final independent Functional Safety Assessment in August 2014, confirmed that RPC Radiy processes comply with SIL 3 requirements and the RadICS Platform meets SIL 3 requirements in both multiple and single channel configurations.

3.3 RadICS Quality Assurance Program

3.3.1 RadICS Organization

The RadICS organization is designed to provide for safety-related I&C systems to NPPs using the RadICS Platform equipment. RadICS, based in Kirovograd, Ukraine is responsible for all RadICS-based

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 48 of 350
--------------	--------------------	-----------	---	----------------



application project activities except the manufacturing of the RadICS Platform equipment. The RadICS Platform equipment is manufactured by RPC Radiy, as described in Section 3.2.

The main departments within RadICS that are involved in a RadICS-based application project include:

- [[]] ^{a,c} – Provides customer technical and QA requirements from procurement documents. Provides storage, packaging, and shipping for completed RadICS-based systems [[]] ^{a,c}. Packaging and shipment are performed by [[]] ^{a,c}. All these requirements are included into the purchase order and [[]] ^{a,c}.
- [[]] ^{a,c} – Develops project-specific I&C system designs based on RadICS Platform technology. The systems design work includes the system architecture, the Application EDs, and hardware that implement customer function requirements. The design work is based on using the [[]] ^{a,c}.
- [[]] ^{a,c} – Performs verification activities on the hardware and software design documents prepared by the [[]] ^{a,c}, as specified in the Project Overall V&V Plan. The [[]] ^{a,c} is technically, administratively, and financially independent from the [[]] ^{a,c}.
- [[]] ^{a,c} – Performs commercial grade dedication of RadICS Platform equipment [[]] ^{a,c} the RadICS Platform equipment, including the [[]] ^{a,c}. Performs validation testing of RadICS-based systems developed by [[]] ^{a,c} performs [[]] ^{a,c} of the generic [[]] ^{a,c}. The [[]] ^{a,c} is technically, administratively, and financially independent from the [[]] ^{a,c}.
- [[]] ^{a,c} – Performs required EQ testing or analysis of equipment used for RadICS-based systems.
- [[]] ^{a,c} – Controls the [[]] ^{a,c} and audits implementation of programs and processes. Responsible for independently planning and performing activities to verify the development and effective implementation of the RadICS QA Program. Supports commercial grade dedication activities for commercial grade surveys and source inspections, as specified by the commercial grade dedication plan.
- [[]] ^{a,c} – Performs commissioning, warranty support, customer technical support, spare parts availability control, consideration of claims, and customer complaints.

Figure 3-3 shows the RadICS organization and work flow interfaces for RadICS-based I&C projects.

Figure 3-4 shows the RadICS product lifecycle and organizational responsibilities.



[[

]]^{a,c}

Figure 3-3: RadICS Organization and Workflow Interfaces

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 50 of 350
--------------	--------------------	-----------	---	----------------



II

]]^{a,c}

Figure 3-4: RadICS Product Lifecycle and Organizational Responsibilities

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 51 of 350
--------------	--------------------	-----------	---	----------------



3.3.2 Quality Assurance Program

The RadICS QAP (Reference 3-19) is the top level QA document of the 10 CFR Part 50 Appendix B QA program for the RadICS organization. The QAP 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. The RadICS QAP is based on NEI 11-04A (Reference 3-20).

The RadICS QAP defines specific responsibilities and authority for control of design, documentation, procurement, processes, inspection, testing, nonconformance, corrective action, and QA records. In addition, the RadICS QAP defines requirements for inspection and audits. The RadICS QA Department is responsible for maintaining the RadICS QAP.

The RadICS QAP establishes the quality system document structure, which includes the following:

- RadICS QAP is the upper tier quality requirements document,
- RadICS Quality Procedures implement the QAP requirements for programs and processes,
- RadICS Quality Work Instructions provide standardized methods to accomplish quality-related work, and
- RadICS Forms and Records are used to create the implementation evident for quality-related work.

All RadICS activities for the processes described in the RadICS Topical Report are performed in accordance with the RadICS QAP.

RadICS activities for supplier selection and evaluation comply with the applicable NQA-1-2008/2009a requirements for source (supplier) evaluation and selection and periodic re-evaluation. The RadICS QAP has procedures that control the selection and qualification of suppliers and maintenance of the Qualified Suppliers List. QA evaluators perform supplier evaluations, which include assessment of corrective action history, nonconformance submittals, organization changes, etc. A performance rating is determined based on the evaluation of these criteria and a supplier can be added, retained, or removed from the Qualified Suppliers List. The scope of related activities performed by RadICS includes supplier audits and commercial grade surveys for commercial suppliers. The RadICS QAP provides control for the selection and evaluation of suppliers for calibration and testing services.

The RadICS QAP establishes procurement and dedication control programs designed to detect and prevent usage of counterfeit and fraudulently marketed products in its projects according to requirements of NRC Generic Letter 89-02 (Reference 3-21). The following measures are implemented in RadICS QAP procedures:

- Involvement of engineering staff in the procurement and product acceptance process,
- Implementation of comprehensive source inspection, receipt inspection, and testing programs,
- Establishment of engineering based, programs for review, testing, dedication of commercial-grade products for suitability, and
- Appropriate training in the detection of these items to applicable personnel.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 52 of 350
--------------	--------------------	-----------	---	----------------

The software QA controls applied to the development of Platform and Application EDs for the RadICS Modules are described on Chapter 7. The software QA controls applied to the development of the Platform and AFBL for use in the EDs for RadICS Modules are described on Chapter 8. The secure development environment controls are described in Chapter 11. RadICS has established classification and acquisition process control for software development tools, as described in Section 8.3.

RadICS started to work with Global Quality Assurance, Inc. (GQA) in 2015, to develop a QAP description and a complete set of implementing quality procedures and working instructions to fully align RadICS QAP with 10 CFR Part 50 Appendix B. The RadICS QAP has been developed to be fully compliant with ASME NQA-1-2008/NQA-1a-2009, as endorsed by RG 1.28, Revision 4. This work was performed to support the development of the RadICS Topical Report for submittal to NRC for review and approval.

Table 3-2: RadICS Quality Procedures

Requirements from NQA-1-2008 and Appendix B	Quality Procedures
Criterion I, Organization	
Criterion II, Quality Assurance Program	[[]] ^{a,c}

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 54 of 350
--------------	--------------------	-----------	---	----------------



Requirements from NQA-1-2008 and Appendix B	Quality Procedures
Criterion XII Control of Measuring and Test Equipment	[[]] ^{a,c}
Criterion XIII Handling, Storage and Shipping	[[]] ^{a,c}
Criterion XIV Inspection, Test, and Operating Status	[[]] ^{a,c}
Criterion XV Nonconforming Materials, Parts, or Components	[[]] ^{a,c}
Criterion XVI Corrective Action	[[]] ^{a,c}
Criterion XVII Quality Assurance Records	[[]] ^{a,c}
Criterion XVIII Audits	[[]] ^{a,c}
	[[]] ^{a,c}

A comprehensive training plan was prepared for RadICS personnel on the key elements of the QA Program document and implementing procedures. A qualification and training program was implemented for QA lead auditors and survey personnel using the services of GQA. Initial training of personnel was performed by SunPort (Lausanne, Switzerland) at the RPC Radiy site in April 2015. The RadICS staff has been certified on the following topics:

- Internal/External Auditing topics and techniques
- Organization Safety Culture, Root Cause determination and Problem Solving techniques
- Means to identify and deal with Counterfeit, Fraudulent, and Suspect Items
- Commercial Grade Item Dedication

GQA completed a third party evaluation in August 2016 (Reference 3-23). Evaluation QAP_EVAL-2016 was performed to assess the adequacy of the RadICS Quality Assurance Program documents for meeting 10 CFR Part 50 Appendix B, 10 CFR Part 21, ASME NQA-1-1994, NQA-1-2008, and NQA-1a-2009. The evaluation was performed as a document audit of current policies and quality procedures to assess the RadICS QAP for addressing applicable requirements for control over quality activities for supplying

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 55 of 350
--------------	--------------------	-----------	---	----------------



nuclear safety-related digital instrumentation and control equipment. The scope of the evaluation included the latest approved revisions of the RadICS QAP, 42 Quality Procedures, and 3 significant Work Instructions.

The evaluation found that the RadICS QAP was a comprehensive network of policies, procedures, instructions, and forms that address the nuclear quality assurance requirements in detail. The RadICS QAP also reflect recent regulatory developments, provisions and guidance of impact to nuclear licensees and their suppliers. GQA concluded that the RadICS QAP is comprehensively documented and compliant with stated requirements. Three evaluation comments were submitted for corrective action in accordance with the RadICS QAP.

3.3.4 Corrective Action Program

The RadICS corrective action procedure (Reference 3-24) addresses corrective action for conditions adverse to quality related to the following sources:

- Supplier deficiencies in processes and / or controls as a result of a Commercial Grade Survey (as described in QP 07-4),
- Findings from internal audits (as described in QP 18-1),
- Nonconforming items whose apparent causes resulted in dispositioned rework, replacement or repair (as described in QP 15-1) and for which the dispositioning process has resulted in a decision to investigate the cause of the issue further,
- Customer complaints, returns, or audit findings,
- Software that is assigned a Severity 1 (Critical Error) with a Priority Level 1 (as described in QP-16-2), and
- Trend analysis suggests recurring issues regardless of source.

This procedure acknowledges the implementation of related procedures that correct conditions adverse to quality and prescribes a defined process for attending to significant conditions adverse to quality, regardless of source (e.g., item, audit, programmatic, complaint or trend). The defined process for significant conditions adverse to quality includes causal analysis, taking actions to mitigate or prevent recurrence, and verification of completed corrective actions.

Each corrective action report is evaluated for 10 CFR Part 21 (Reference 3-25) reporting applicability.

3.3.5 10 CFR Part 21 Problem Reporting

RadICS, as the designer and supplier of digital I&C systems to U.S. commercial nuclear licensees, is required to comply with 10 CFR Part 21. The RadICS reporting procedure for defects and noncompliance (Reference 3-26) describes the process for ensuring compliance with the requirements of 10 CFR Part 21. This procedure establishes the requirements for evaluation and reporting of defects and noncompliance in accordance with 10 CFR Part 21. This procedure applies to all materials, components, subassemblies, services, and finished items that are basic components and that have been delivered to a U.S. nuclear customer. The RadICS QA Manager is the Responsible Officer for the effective implementation of this procedure.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 56 of 350
--------------	--------------------	-----------	---	----------------



3.3.6 Maintenance Process of NRC Safety Evaluation Report

RPC Radiy and RadICS periodically update procedures related to the RadICS Platform technology and associated I&C system projects as a result of continuously improve activities after issuance of the NRC Safety Evaluation Report (SER) for the RadICS Digital I&C Platform Topical Report. Additionally, some parts of the RadICS Platform might have to be modified to replace obsolete components or correct identified problems. The overall RadICS Platform and Application Lifecycles might require updates to reflect changes in RPC Radiy or RadICS management structures or quality programs.

RadICS working instructions define a change management process for future changes to the approved RadICS Platform (Reference 3-27). The change management process specifies the criteria and evaluation process to evaluate future platform changes for use. RadICS can use newer Radiy equipment (i.e., RadICS Platform Hardware and ED Modules) and development procedures provided that the specified criteria are met. The change management process is designed to ensure that:

- Changes to the approved RadICS Platform do not modify or eliminate the key design principles, key processing features, or key communication independence features,
- Changes to the RadICS Platform (i.e., Hardware and ED Modules) do not result in more than a minimal increase in the likelihood of occurrence of a malfunction, do not result in more than a minimal increase in the consequences of a malfunction, or do not create a possibility for a malfunction with a different result, and
- Changes to the RadICS or Radiy development procedures do not result in a reduction in the NRC-approved quality methods.

To the extent that product or process changes are confirmed to be within the established criteria in the Topical Report and SER, the RadICS Platform will be considered consistent and current with the Topical Report and SER. Changes that satisfy the criteria can be used for a plant retrofit project. Changes that do not satisfy one or more of the criteria cannot be used for a U.S. plant project without specific NRC review and approval. If changes are required to Topical Report or SER, then RadICS will provide a revision to the Topical Report to reflect those changes to be reviewed and approved by the NRC before allowing products to be developed or systems designed under the new process for installation in the U.S.

RadICS records requirements and periodic reporting obligations are specified for the change evaluations to support a review by independent parties or audits by NRC.

3.4 Chapter 3 References

- 1 ISO 9001:2008, "Quality management systems – Requirements"
- 2 10 CFR Part 50 Appendix B, "Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants"
- 3 ASME NQA-1-2008, "Quality Assurance Program Requirements for Nuclear Facilities"
- 4 ASME NQA-1a-2009, "Quality Assurance Program Requirements for Nuclear Facilities"
- 5 Regulatory Guide 1.28, Revision 4, "Quality Assurance Program Criteria (Design and Construction)"

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 57 of 350
--------------	--------------------	-----------	---	----------------



- 6 IEC 61508:2010, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems"
- 7 ASME NQA-1b-2007, "Quality Assurance Program Requirements for Nuclear Facilities"
- 8 EPRI Report NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety-Related Applications (NCIG-07)," dated June 1, 1988
- 9 EPRI TR-102260, "Supplemental Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items," 1994
- 10 ISO/IEC 17025:2005, "General requirements for the competence of testing and calibration laboratories"
- 11 ISO 10012:2003 "Measurement management systems -- Requirements for measurement processes and measuring equipment"
- 12 DSTU ISO 9001-2001 "Quality management system -- Requirements"
- 13 CSA Z299.1, "Quality Assurance Program - Category 1"
- 14 IAEA Safety Guide NS-G-1.3 "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants"
- 15 IAEA Nuclear Energy Series Report No.NP-T-1.4, "Implementing Digital I&C Systems in Modernization of Nuclear Power Plants"
- 16 IAEA Nuclear Energy Series Report No.NP-T-1.5, "Protecting Against Common-Cause Failures in Digital I&C Systems"
- 17 IAEA Nuclear Energy Series Report No.NP-T-3.12, "Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants"
- 18 EPRI Technical Report 1011710, "Handbook for Evaluating Critical Digital Equipment and Systems," Electric Power Research Institute, November 2005
- 19 QAPD-001, "RadICS Quality Assurance Program Description"
- 20 Nuclear Energy Institute Letter to NRC dated June 6, 2013, "Issuance of NEI 11-04A, Revision 0, Nuclear Generation Quality Assurance Program Description"
- 21 NRC Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products"
- 22 EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996
- 23 Global Quality Assurance letter to RadICS dated August 26, 2016, "Evaluation of the RadICS Quality Assurance Program Description"
- 24 RadICS Procedure QP QP 16-1, "Corrective Action"
- 25 10 CFR Part 21, "Reporting of Defects and Noncompliance"
- 26 RadICS Procedure QP 15-2, "Reporting of Noncompliance in accordance with 10 CFR Part 21"
- 27 RadICS Work Instruction WI 03-7/2, "RadICS Technology Change Evaluation Process"



4 RadICS Commercial Grade Dedication Plan

The RadICS Platform is the third-generation digital safety I&C platform developed by RPC Radiy in accordance with European nuclear safety standards for such systems. The basic U.S. licensing strategy to demonstrate that the generic RadICS Platform and the associated quality and software life cycle processes comply with U.S. nuclear safety requirements is described in Chapter 1.

4.1 Commercial Grade Dedication Methodology

RadICS has developed a Commercial Grade Dedication Plan for the RadICS Platform (References 4-1 through 4-9). This plan outlines the various steps to be followed to dedicate the RadICS Platform. The results of the dedication will be documented in a Commercial Grade Dedication Report for the RadICS Platform with the plan is fully implemented.

4.1.1 Definition of the Generic RadICS Platform

The generic RadICS Platform software is described in Chapter 6. The development of the RadICS Platform is described in Chapters 7 and 8. The EQ plan for the RadICS Platform is described in Chapter 9.

4.1.2 Compliance with Dedication Guidance

EPRI NP-5652 (Reference 4-10) provides the upper tier framework for the technical basis for acceptance and the specific methods used to establish acceptance. NRC conditionally endorsed EPRI NP-5652 in Generic Letter 89-02 (Reference 4-11). EPRI TR-106439 (Reference 4-12) is based on the NRC-endorsed guidance in EPRI NP-5652 and tailors the guidance for the commercial grade dedication (CGD) of digital equipment. NRC approved EPRI TR-106439 (Reference 4-13). NRC also states in RG 1.152 (Reference 4-14) that EPRI TR-106439 contains adequate guidance to meet the requirements in IEEE Std 7-4.3.2-2003, Section 5.4.2 (Reference 4-15).

It is important to understand how this guidance relates to the use of testing in the acceptance review. Testing can be used to support acceptance in three distinct ways, each with its own set of rules.

Method 1 – Special Tests and Inspections - EPRI NP-5652 Section 3.1.2 states that “Method 1 should be used when the purchaser desires to verify critical characteristics after the item is received.” Method 1 testing is performed during the commercial grade dedication process. EPRI NP-5652 Section 2.5 specifies that this work must be performed in accordance with a 10 CFR Part 50, Appendix B program (Reference 4-16).

Method 2 - Commercial Grade Survey - EPRI NP-5652 Section 3.2.2 states that “Method 2 should be used when the purchaser desires to accept commercial grade items based on the merits of a supplier's commercial quality controls. These controls may constitute quality programs, procedures, or practices.” EPRI NP-5652 Section 3.2.3 states that “Two basic criteria must be met when conducting a commercial grade survey. The purchaser must confirm that the selected commercial grade item's critical characteristics are controlled under the scope of commercial quality system activities. The purchaser must also be reasonably assured that

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 59 of 350
--------------	--------------------	-----------	---	----------------



the commercial supplier's activities adequately control the commercial grade items supplied." EPRI NP-5652 Table 3-1 lists typical supplier controls that can be surveyed using Method 2, which includes testing. Similarly, EPRI TR-106439 Figure 3-2 shows a review of vendor testing as an element of the dedication process. EPRI NP-5652 Section 2.5 specifies that the review for acceptance of vendor testing must be performed in accordance with a 10 CFR Part 50, Appendix B program; however, the vendor testing itself is not performed in accordance with a 10 CFR Part 50, Appendix B program.

Method 3 - Source Verification - EPRI NP-5652 Section 3.3.1 states that "Method 3 involves the verification of critical characteristics by witnessing quality activities before releasing the item for shipment." EPRI NP-5652 Section 2.5 specifies that the verification for acceptance of vendor testing must be performed in accordance with a 10 CFR Part 50, Appendix B program; however, the vendor testing itself is not performed in accordance with a 10 CFR Part 50, Appendix B program.

Method 4 - Item/Supplier Performance Record - EPRI NP-5652 Section 3.4.1 states that "Method 4 allows the purchaser to accept commercial grade items based upon a confidence in the supplied item achieved through proven performance of the item. It also allows the purchaser to take credit for item performance based upon historical verification gained from the successful utilization of Methods 1, 2, or 3 or pertinent industry-wide performance data."

NRC Generic Letter 89-02 places two limitations of the use of EPRI NP-5652:

1. Acceptance Method 2, "Commercial-Grade Survey of Supplier", should not be employed as the basis for accepting items from suppliers with undocumented commercial quality control programs or with programs that do not effectively implement their own necessary controls. Likewise, Method 2 should not be employed as the basis for accepting items from distributors unless the survey includes the part manufacturer(s) and the survey confirms adequate controls by both the distributor and the part manufacturer(s).
2. Acceptance Method 4, "Acceptable Supplier/Item Performance Record," should not be employed alone unless:
 - a. The established historical record is based on industry-wide performance data that is directly applicable to the item's critical characteristics and the intended safety-related application; and
 - b. The manufacturer's measures for the control of design, process, and material changes have been adequately implemented as verified by audit (multi-licensee team audits are acceptable).

RadICS performed an initial assessment of the historical development records for the RadICS Platform as part of the CGD planning effort and made two broad conclusions. First, RadICS concluded that

[[]]^{a,c,f} would be needed to satisfy the U.S. regulatory requirements for [[]]^{a,c,f} and are

described in Chapter 9. Second, RadICS concluded that the RadICS [[]]

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 60 of 350
--------------	--------------------	-----------	---	----------------



]]^{a,c,t} will be evaluated using Method 2.

Method 3 will not be used by RadICS for the RadICS Platform CGD effort. A Method 3 process, if used, would be akin to a licensee observing a factory acceptance test for a RadICS system they purchased.

Method 4 was [[

]]^{a,c,t}. RadICS has only used the RadICS Platform operating experience to demonstrate satisfactory performance with the platform technology.

The sources of guidance related to dedicating a commercial grade digital safety I&C platform are EPRI TR-106439 and EPRI TR-107330 (Reference 4-17). Implementation of this guidance for dedication of the generic RadICS Platform is described below.

The Commercial Grade Dedication Plan for RadICS Platform is based on established guidance:

- EPRI TR-106439 for the CGD of the RadICS Platform developed to the RPC Radiy QMS and IEC Requirements
- EPRI TR-107330 for the EQ tests to be performed on the RadICS Platform

RG 1.152 recognizes the acceptability of EPRI TR-106439 for CGD. The RadICS Module EDs will be treated as the "legacy software" described in Section 7.6 of EPRI TR-107330.

4.1.2.1 EPRI TR-106439 Guidance

EPRI TR-106439 will be used to structure the CGD effort. Compliance with EPRI TR-106439 process will be demonstrated using a checklist, which provides a mapping that shows where the elements of the dedication process are addressed in licensing documentation.

The RadICS Commercial Grade Dedication Plan will use a combination of three acceptance methods described in EPRI TR-106439 to verify the adequacy of the generic RadICS Platform:

- Method 1: Special Tests and Inspections of the RadICS Platform equipment

[[

]]^{a,c,t}

- Method 2: Commercial Grade Survey of RadICS Modules [[
]]^{a,c,t}

Critical characteristics will be based on three sets of U.S. benchmarks:

- The RadICS Module ED development process, which is based on IEC Standards, will be evaluated for dependability critical characteristics developed from applicable NRC review guidance for safety system software development defined in NRC BTP 7-14 (Reference 4-18), IEEE Standard 7-4.3.2-2003, and other endorsed IEEE standards.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 61 of 350
--------------	--------------------	-----------	---	----------------



- The RadICS Platform design characteristics will be evaluated for performance and dependability critical characteristics developed from NUREG/CR-6082 (Reference 4-19), DI&C-ISG-04 (Reference 4-20), and IEEE Std 603-1991(Reference 4-21).
- The RadICS Platform design characteristics will be evaluated for selected physical critical characteristics developed from EPRI TR-107330.

[[

]]^{a,c,t}

EPRI TR-106439 envisions the approach of using the historical development records as a basis for acceptance in a commercial grade dedication review. [[

]]^{a,c,t}

- Method 4: Acceptable Performance Record of the RadICS Platform

The review of the performance record will be based on the RPC Radiy operating experience to demonstrate satisfactory performance with the RadICS Platform technology. [[

]]^{a,c,t}

4.1.2.2 EPRI TR-107330 Guidance

EPRI TR-107330 will be used to define the qualification test methods (including the operability and prudence tests) and the critical characteristics to demonstrate acceptable performance during the qualification tests. Testing will demonstrate that the RadICS Platform functioned correctly during and/or after exposure to the series of stress tests outlined in EPRI TR-107330. The operability and prudence test acceptance criteria will be important critical characteristics for performance in the CGD evaluation of the RadICS Platform.

4.1.3 RadICS Commercial Grade Dedication Process

The RadICS process for CGD is dedication is defined in a RadICS quality procedure (Reference 4-22), which requires the following:

- Writing a Dedication Plan that includes a detailed checklist with the acceptance activities to be performed to demonstrate compliance with EPRI TR-106439.
- Performing these activities and completing the checklist according to the approved Plan.
- Reporting the results in a Dedication Report.

The RadICS Platform CGD Report will contain the completed checklist and will be issued after the completion of the qualification tests for the RadICS Platform equipment.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 62 of 350
--------------	--------------------	-----------	---	----------------



The RadICS Platform CGD Report will define the qualification boundary of the RadICS Platform. The RadICS Platform can be used to implement safety-related I&C systems within the defined qualification boundary defined in Chapter 9. It is also expected that I&C systems implemented with the RadICS Platform will address the project-specific actions items identified in the NRC safety evaluation report for the RadICS Platform Topical Report. Any safety-related system beyond that included in the baseline dedication will require additional evaluation for the new application boundary.

The RadICS Platform CGD Report will maintained as an auditable record for the RadICS Platform CGD effort, as required by 10 CFR 21.21(c)(2) (Reference 4-23).

4.1.4 Maintenance of RadICS Platform Commercial Grade Dedication

The RadICS Platform hardware and associated Module EDs will be qualified and maintained under the RadICS 10 CFR Part 50 Appendix B quality program (Reference 4-24). If new boards are developed or existing boards modified for obsolescence or other reasons, the new or modified hardware will be appropriately tested and/or analyzed to maintain dedication and EQ to U.S. standards. Changes to the RadICS Platform are evaluated in accordance with the same process that formed the basis for the original CGD acceptance, as controlled by RadICS procedures.

All future modifications to the RadICS Platform will continue to be performed under the RPC Radiy QMS, as described in Chapter 3. The RadICS Platform dedication assessment will be updated to address future modifications to the platform.

Documentation supporting the commercial grade item dedication is maintained as a configuration item.

The RadICS Platform CGD maintenance controls satisfy the requirements of IEEE Std 7-4.3.2 Section 5.4.2.3.

4.2 Chapter 4 References

- 1 RadICS Platform Commercial Grade Dedication Plan for LM, Document 2015-RTS001-CGDP-LM-101
- 2 RadICS Platform Commercial Grade Dedication Plan for DIM, Document 2015-RTS001-CGDP-DIM-003
- 3 RadICS Platform Commercial Grade Dedication Plan for DOM, Document 2015-RTS001-CGDP-DOM-102
- 4 RadICS Platform Commercial Grade Dedication Plan for AIM, Document 2015-RTS001-CGDP-AIM-103
- 5 RadICS Platform Commercial Grade Dedication Plan for AOM, Document 2015-RTS001-CGDP-AOM-104
- 6 RadICS Platform Commercial Grade Dedication Plan for OCM, Document 2015-RTS001-CGDP-OCM-106
- 7 RadICS Platform Commercial Grade Dedication Plan for Chassis, Document 2015-RTS001-CGDP-CH-107
- 8 RadICS Platform Commercial Grade Dedication Plan for I/O Connections Protection Module, Document 2015-RTS001-CGDP-CH-131



- 9 RadICS Platform Commercial Grade Dedication Plan for Ventilation Module, Document 2015-RTS001-CGDP-CH-132
- 10 EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07)," July 1988
- 11 Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products"
- 12 EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, Electric Power Research Institute, October 1996
- 13 Letter from NRC to EPRI dated July 17, 1997, "Review of EPRI Topical Report TR-106439, 'Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications'"
- 14 Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
- 15 IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
- 16 10 CFR Part 50 Appendix B, "Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants"
- 17 EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," Electric Power Research Institute, December 1996
- 18 NUREG-0800, Chapter 7, NRC Branch Technical Position 7-14, Revision 5, "Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, March 2007
- 19 NUREG/CR 6082, "Data Communications," August 1993
- 20 DI&C-ISG-04, Revision 1, "Highly Integrated Control Rooms - Digital Communication Systems"
- 21 IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations"
- 22 RadICS Procedure QP 07-3, "Commercial Grade Dedication Procedure"
- 23 10 CFR 21.21, "Notification of failure to comply or existence of a defect and its evaluation"
- 24 QAPD-001, "RadICS Quality Assurance Program Description"



5 Regulations, Codes, and Standards

5.1 Compliance Summary

A summary of NRC regulatory requirements and acceptance criteria for I&C systems important to safety is found in Standard Review Plan (SRP) Table 7-1 (Reference 5-1). RadICS reviewed this table and other sources to define the scope of the regulatory requirements and acceptance criteria that applied to the generic RadICS Platform. Several of the items listed in SRP Table 7-1 apply to project-specific safety I&C systems. Compliance with project-specific regulatory requirements cannot be assessed in the context of a generic digital safety I&C platform that does not include the specific applications. The results of the screening performed by RadICS are documented in this Chapter.

5.2 10 CFR, Code of Federal Regulations

The following regulations were assessed for applicability to the RadICS Platform design.

5.2.1 10 CFR 50.34(f)(2)(v), Bypass and Operable Status Indication

Project-specific applications of the RadICS Platform will comply with the requirement of 10 CFR 50.34(f)(2)(v), *Bypass and Operable Status Indication*, to provide automatic indication of the bypassed and operable status of safety systems. The generic RadICS Platform supports indications in the main control room and hardwired discrete outputs can be provided, as described in Chapter 6. The specific means for complying with 10 CFR 50.34(f)(2)(v) must be assessed on a project-specific basis.

5.2.2 10 CFR 50.49, Environmental Qualification

10 CFR 50.49, *Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants*, identifies specific requirements for qualification of electric equipment important to safety. RG 1.89 describes methods acceptable to the NRC for complying with 10 CFR 50.49. RadICS Platform equipment will not be installed in harsh environments. The qualification of the RadICS Platform for mild environments is described in Chapter 9.

5.2.3 10 CFR 50.55a(h)(2), Protection Systems

As required in 10 CFR 50.55a(h), *Protection Systems*, the RadICS Platform complies with IEEE Std 603-1991. Compliance with applicable portions of IEEE Std 603-1991 for the RadICS Platform is addressed in Chapter 12. The specific means for complying with 10 CFR 50.55a(h)(2) on a system level must be assessed on a project-specific basis.

5.2.4 10 CFR Part 50 Appendix A, General Design Criteria

The applicable General Design Criteria (GDC) from 10 CFR Part 50 Appendix A are discussed below.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 65 of 350
--------------	--------------------	-----------	---	----------------



5.2.4.1 General Design Criterion 1, Quality Standards, and Records

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

The RadICS quality assurance program that governs all RadICS activities is compliant with 10 CFR Part 50 Appendix B and ASME NQA-1-2008 and the NQA-1a-2009 Addenda, as described in Chapter 3. The alignment of the RadICS QAP to GDC 1 is described in Chapter 12.

5.2.4.2 GDC 2, Design Bases for Protection Against Natural Phenomena

The basic requirement is that structures, systems, and components important to safety shall be designed to withstand the effects of a range of natural phenomena without loss of capability to perform their safety functions. The RadICS Platform is intended for use in Class 1E safety I&C applications. The generic qualification program for RadICS Platform that would support compliance with GDC 2 for a specific project is described in Chapter 9. The licensee for a project-specific application of the RadICS Platform will address the correspondence of the generic qualification envelope for the RadICS Platform with the site-specific qualification bounding envelopes.

5.2.4.3 GDC 4, Environmental and Dynamic Effects Design Bases

The basic requirement is that structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. The generic qualification program for RadICS Platform that would support compliance with GDC 4 for a specific project is described in Chapter 9. The licensee for a project-specific application of the RadICS Platform will address the correspondence of the generic qualification envelope for the RadICS Platform with the site-specific qualification bounding envelopes.

5.2.4.4 GDC 13, Instrumentation and Control

The RadICS Platform standard input boards enable the design of systems using the RadICS Platform technology that can monitor a wide range of variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. The RadICS Platform features that would support compliance with GDC 13 for a specific project are described in Chapter 6. The specific means for complying with GDC 13 must be assessed on a project-specific basis.

5.2.4.5 GDC 20, Protection System Functions

The RadICS Platform features that would support compliance with GDC 20 for a specific project are described in Chapter 6. The standard RadICS Platform hardware described in Chapter 6, the hardware development process described in Chapter 7, and the development life cycle processes for RadICS Electronic Designs (EDs) described in Chapters 7 and 8 are the foundations for designing and

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 66 of 350
--------------	--------------------	-----------	---	----------------



implementing project-specific safety I&C systems that accomplish the GDC 20 safety functions. The specific means for complying with GDC 20 must be assessed on a project-specific basis.

5.2.4.6 GDC 21, Protection Systems Reliability and Testability

The RadICS Platform features that would support compliance with GDC 21 for a specific project are described in Chapter 6. The RadICS Platform is designed for high functional reliability. A summary of the board/device-level hardware reliability is provided in Chapter 9. The RadICS ED logic is designed to be highly reliable. The RadICS Platform ED life cycle processes are described in Chapters 7 and 8 have been assessed as part of the Functional Safety Assessments performed by *exida* that demonstrated that the RadICS Platform complies with the IEC 61508 SIL 3 certification requirements (Reference 5-2). The RadICS Application ED development life cycle process is described in Chapter 7. The in-service testing and periodic testing features of RadICS are described in Chapter 6. The standard RadICS Module hardware and associated Platform ED described in Chapter 6 can be readily employed in system architectures with redundant and independent divisions that comply with the single failure criterion. The specific means for complying with GDC 21 must be assessed on a project-specific basis.

5.2.4.7 GDC 22, Protection System Independence

The RadICS Platform features that would support compliance with GDC 22 for a specific project are described in Chapter 6. RadICS systems have the requisite independence of divisions to ensure that a fault in one independent division does not propagate and affect other redundant divisions. Representative RadICS Platform single division and four division architectures are described in Chapter 2. RadICS Platform interdivisional (i.e., coincidence voting) communications also comply with NRC DI&C-ISG-04 recommendations, as described in Appendix B.

The RadICS Platform has the requisite independence to ensure that a postulated fault in a connected non-safety I&C system does not propagate and affect the safety I&C system. As described in Chapter 6, this is accomplished by a one-way (broadcast only) communication link from the safety I&C system to the non-safety I&C system. In addition, RadICS Platform outputs can be connected to non-Class 1E systems. The Class 1E / non-Class 1E isolation capability of these outputs is verified through qualification testing, which is described in Chapter 9.

RadICS Platform hardware is qualified for a mild operating environment, with a generic qualification envelope as described in Chapter 9. Operation within this envelope will not result in loss of the protection function.

The in-service testing and periodic testing features of the RadICS Platform are described in Chapter 6. With appropriate redundancy in an actual system, maintenance and testing activities will not result in loss of the protection function.

D3 should be addressed in the context of a suite of safety and non-safety I&C systems at a NPP. The RadICS Platform can be used to employ signal diversity, as described in Chapter 10.

The design and implementation of RadICS Platform digital communications described in Chapter 6 enables independence to be maintained between redundant divisions and between the safety I&C

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 67 of 350
--------------	--------------------	-----------	---	----------------



system and non-safety I&C systems. The interdivisional communications provisions that address the guidance in DI&C-ISG-04 are described in Appendix B.

The specific means for complying with GDC 22 must be assessed on a project-specific basis. D3 will be addressed in the context of the project-specific suite of safety and non-safety I&C systems.

5.2.4.8 GDC 23, Protection System Failure Modes

The RadICS Platform features that would support compliance with GDC 23 for a specific project are described in Chapter 6. Modes of operation of the RadICS Platform are described in Chapter 6, which also explains the behavior of the RadICS Platform when failures are detected. As discussed in Chapter 9, board-level failure mode and effects analyses (FMEAs) are documented in a separate report. The specific means for complying with GDC 23 must be assessed on a project-specific basis.

5.2.4.9 GDC 24, Separation of Protection and Control Systems

The RadICS Platform features that would support compliance with GDC 24 for a specific project are described in Chapter 6. The design and implementation of RadICS Platform digital communications described in Chapter 6 enables separation to be maintained between the safety I&C system and non-safety I&C systems. These communications provisions that address the guidance in DI&C-ISG-04 are as described in Appendix B. The specific means for complying with GDC 24 must be assessed on a project-specific basis.

5.2.4.10 GDC 25, Protection System Requirements for Reactivity Control Malfunctions

The RadICS Platform features that would support compliance with GDC 25 for a specific project are described in Chapter 6. The specific means for complying with GDC 25 must be assessed on a project-specific basis.

5.2.4.11 GDC 29, Protection Against Anticipated Operational Occurrences

The RadICS Platform features that would support compliance with GDC 29 for a specific project are described in Chapter 6. The RadICS Platform is designed for high functional reliability. A summary of the board/device-level hardware reliability is provided in Chapter 9. Operating experience with RPC Radiy systems described in Chapter 2 has shown no instances where the RPC Radiy systems have experienced any system failures or common cause failures that affected the capability of the safety I&C system to perform its intended safety function(s) during an anticipated operational occurrence. The specific means for complying with GDC 29 must be assessed on a project-specific basis. Specifically, the RPC Radiy systems have not experienced any system failures or common cause failures in more than 400 reactor-years of operation as of December 2015.

5.2.5 10 CFR Part 50 Appendix B, Quality Assurance Requirements

The RadICS QAP that governs all RadICS activities is compliant with 10 CFR Part 50 Appendix B, Quality Assurance Requirements for Nuclear Power Plants and Fuel Reprocessing Plants, and ASME NQA-1-2008

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 68 of 350
--------------	--------------------	-----------	---	----------------



and the NQA-1a-2009 Addenda, as described in Chapter 3. The alignment of the RadICS QAP to 10 CFR Part 50 Appendix B is described in Chapter 12.

5.3 NRC Regulatory Guides

The following NRC RGs were assessed for applicability to the RadICS Platform design.

5.3.1 Regulatory Guide 1.22

The RadICS Platform features that would support compliance with RG 1.22, *Periodic Testing of Protection System Actuation Functions*, for a specific project are described in Chapter 6. The specific means for complying with RG 1.22 must be assessed on a project-specific basis.

5.3.2 Regulatory Guide 1.28

RG 1.28, Revision 4, *Quality Assurance Program Criteria (Design and Construction)*, endorses Part I and Part II requirements included in NQA-1-2008 and the NQA-1a-2009 Addenda for the implementation of a quality assurance program during the design and construction phases of NPPs and fuel reprocessing as an acceptable method for complying with the requirements of Appendix B to 10 CFR Part 50, subject to the specified additions and modifications. The RadICS QAP that governs all RadICS activities is compliant with 10 CFR Part 50 Appendix B and ASME NQA-1-2008 and the NQA-1a-2009 Addenda, as described in Chapter 3. The alignment of the RadICS QAP to RG 1.28 is described in Chapter 12.

5.3.3 Regulatory Guide 1.47

The RadICS Platform features that would support compliance with RG 1.47, Revision 1, *Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System*, for a specific project are described in Chapter 6. RG 1.47 provides supplemental guidance for implementing IEEE Std 603-1991 to satisfy the NRC regulatory requirements with respect to the bypassed and inoperable status indication for NPP safety systems. Project-specific applications of the RadICS Platform will comply with the requirement to provide automatic indication of the bypass or inoperable status of portions of the protection system. In project-specific applications, compliance with RG 1.47 requires further determinations that bypass or inoperable status is also provided for the following:

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

The specific means for complying with RG 1.47 must be assessed on a project-specific basis.

5.3.4 Regulatory Guide 1.53

RG 1.53, Revision 2, *Application of the Single-Failure Criterion to Safety Systems*, endorses IEEE Std 379-2000 with qualifications. The standard RadICS Platform hardware described in Chapter 6 can be implemented in system architectures with redundant and independent channels, divisions, and trains that comply with the single failure criterion. Representative RadICS Platform system architectures are

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 69 of 350
--------------	--------------------	-----------	---	----------------



described in Chapter 2. The specific means for complying with RG 1.53 must be assessed on a project-specific basis.

5.3.5 Regulatory Guide 1.62

The RadICS Platform features that would support compliance with RG 1.62, Revision 1, *Manual Initiation of Protection Actions*, for a specific project are described in Chapter 6. The specific means for complying with RG 1.62 must be assessed on a project-specific basis.

5.3.6 Regulatory Guide 1.75

RG 1.75, Revision 3, *Criteria for Independence of Electrical Safety Systems*, endorses IEEE Std 384-1992 with qualifications. The standard RadICS Platform hardware described in Chapter 6 is designed to establish and maintain the independence of safety-related equipment, circuits, and auxiliary supporting features by physical separation and electrical isolation. In a project-specific application, this is accomplished by physically separating the redundant divisions of the safety system.

Representative RadICS Platform system architectures are described in Chapter 2. These typical architectures include the interdivisional communication interfaces that are needed to support voting logic. As described in Chapter 6, interdivisional communications is accomplished using fiber optic links that maintain the electrical isolation between divisions and RadICS Logic Module features that maintain the required logical data isolation between divisions.

Electrical independence between Class 1E and non-Class 1E digital systems also is established by means of fiber optic links. As described in Chapter 6, data isolation is assured by implementing logical data isolation in the Class 1E systems as well as providing only one-way (broadcast only) communication links from the Class 1E system to the non-Class 1E system.

The alignment of the RadICS Platform to RG 1.75, Revision 3, is described in Chapter 12. The specific means for complying with the system level independence requirements in RG 1.75 must be assessed on a project-specific basis.

5.3.7 Regulatory Guide 1.89

RG 1.89, Revision 1, *Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants*, describes methods acceptable to the NRC for complying with 10 CFR 50.49 with regard to qualification of electric equipment important to safety for service in NPPs. These methods ensure the equipment can perform its safety function during and after a design basis accident. This RG endorses IEEE Std 323-1974. Platform equipment will not be installed in harsh environments. The qualification of the RadICS Platform for mild environments is described in Chapter 9.

5.3.8 Regulatory Guide 1.100

RG 1.100, Revision 3, *Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants*, endorses IEEE Std 344-2004. Chapter 9 describes the seismic qualification testing of the RadICS

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 70 of 350
--------------	--------------------	-----------	---	----------------



Platform and the use of RG 1.100, Revision 3, and EPRI TR-107330 (corrected version) in the seismic qualification test plan. The alignment of the RadICS Platform to RG 1.100, Revision 3, is described in Chapter 12. The licensee for a project-specific application of the RadICS Platform will address the correspondence of the generic qualification envelope for the RadICS Platform with the site-specific qualification bounding envelopes.

5.3.9 Regulatory Guide 1.105

RG 1.105, Revision 3, *Setpoints for Safety-Related Instrumentation*, endorses Instrument Society of America (ISA) Standard ISA-S67.04-1994 with qualifications.

As described in Section 5.2.3, EPRI TR-107330, Section 4.2.4 requires the qualifier to provide information about the qualified hardware to support an application specific setpoint analysis per ISA-S67.04-1994. Chapter 9 describes the approach RadICS used for preparing the setpoint analysis support documentation for the RadICS Platform. This documentation provides sufficient design specification data for a setpoint analysis to be performed on a project-specific RadICS system. The specific means for complying with RG 1.105 must be assessed on a project-specific basis.

5.3.10 Regulatory Guide 1.118

RG 1.118, Revision 3, *Periodic Testing of Electric Power and Protection Systems*, endorses IEEE Std 338-1987 with qualifications. As provided in IEEE Std 338, automatic testing provisions for programmable digital computer-based systems are subject to the testing provisions of this standard and IEEE Std 7-4.3.2-2003. The RadICS Platform features that would support compliance with RG 1.118 for a specific project are described in Chapter 6. The specific means for complying with RG 1.118 must be assessed on a project-specific basis.

5.3.11 Regulatory Guide 1.152

RG 1.152, Revision 3, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 7-4.3.2-2003 with qualifications. Compliance of the RadICS Platform EDs with IEEE Std 7-4.3.2-2003 is described in Chapter 12.

The RadICS ED life cycle processes applied by RPC Radiy and RadICS provide protection against unauthorized, unintended, and unsafe modifications to the EDs, thereby promoting integrity and reliability during operation and maintenance.

As described in Chapter 6, the generic RadICS Platform has been designed as the foundation for project-specific digital safety I&C systems that will implement nuclear safety functions. The design of the generic RadICS Modules and associated Platform ED life cycle processes applied through the factory test phase also accomplish computer security functions by: (a) providing inherent protection against unauthorized, unintended, and unsafe modifications to the system, and (b) implementing design requirements that promote integrity and reliability during operation and maintenance in the event of inadvertent operator actions or undesirable behavior of connected equipment.

The secure development and operating environment for the RadICS Platform is described in Chapter 11.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 71 of 350
--------------	--------------------	-----------	---	----------------



RG 1.152 Annex C identifies that EPRI TR-106439 contains adequate guidance for the evaluation and acceptance of commercial grade digital equipment for nuclear safety applications. The CGD program for the RadICS Platform is described in Chapter 4.

Compliance with RG 1.152 for the RadICS Platform is described in Chapter 12. The specific means for complying with the application of RG 1.152 on a system level must be assessed on a project-specific basis.

5.3.12 Regulatory Guide 1.153

RG 1.153, Revision 1, *Criteria for Safety Systems*, endorses IEEE Std 603-1991 and the correction sheet of January 30, 1995. The RadICS Platform features that would support compliance with RG 1.153 for a specific project are described in Chapter 12.

5.3.13 Regulatory Guide 1.168

RG 1.168, Revision 2, *Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 1012-2004 and IEEE Std 1028-2008. IEEE Std 828-2005 describes a structured approach to software V&V. IEEE Std 1028-2008 described methods to perform software reviews and audits. The RPC Radiy and RadICS approaches to software V&V is described in Chapters 7 and 8. The RPC Radiy and RadICS approaches to software V&V is described in Chapters 7 and 8. The RadICS approach to software reviews is described in Section 7.4.3. The RPC Radiy and RadICS approaches to software audits are described in Sections 7.3.1, 7.5.3.3, and 11.4. The alignment of the RPC Radiy and RadICS configuration management programs to RG 1.168, Revision 2, is described in Chapter 12.

5.3.14 Regulatory Guide 1.169

RG 1.169, Revision 1, *Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 828-2005. IEEE Std 828-2005 describes a structured approach to software configuration management. The RPC Radiy and RadICS approaches to software configuration management are described in Section 7.5. The alignment of the RPC Radiy and RadICS configuration management programs to RG 1.169, Revision 1, is described in Chapter 12.

5.3.15 Regulatory Guide 1.170

RG 1.170, Revision 1, *Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 829-2008. IEEE Std 829-2008 describes a structures approach to software test documentation. Section 7.5.4.2 describes the RPC Radiy and RadICS approaches to Platform and Application ED V&V test documentation. The alignment of RPC Radiy and RadICS software test documentation to RG 1.170, Revision 1, is described in Chapter 12.



5.3.16 Regulatory Guide 1.171

RG 1.171, Revision 1, *Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 1008-1987. IEEE Std 1008-1987 describes a structured approach for performing software unit testing. RadICS Platform software testing is described in Chapters 7 and 8. The alignment of RadICS software testing to RG 1.171, Revision 1, is described in Chapter 12.

5.3.17 Regulatory Guide 1.172

RG 1.172, Revision 1, *Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 830-1998. IEEE Std 830-1998 is a recommended practice for writing software requirements specifications; however, as a recommended practice, it does not identify and specific requirements. The RadICS Platform and Application requirements documents are described in Chapter 7. The alignment of the RPC Radiy and RadICS software requirements specifications to RG 1.172, Revision 1, is described in Section 12.

5.3.18 Regulatory Guide 1.173

RG 1.173, Revision 1, *Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 1074-2006, which provides a structured approach for developing a software life cycle program. The life cycle processes for the RadICS Platform and Application ED are described in Chapters 7 and 8. The alignment of the RadICS Platform and Application ED lifecycles to RG 1.173, Revision 1, is described in Chapter 12.

5.3.19 Regulatory Guide 1.180

RG 1.180, Revision 1, *Guidelines for Evaluating Electromagnetic and Radio- Frequency Interference in Safety-Related Instrumentation and Control Systems*, endorses IEC 61000, Military Standard (MIL-STD)-461E, IEEE Std 1050-1996, IEEE Std C62.41-1991, and IEEE Std C62.45-1992 with qualifications. Chapter 9 describes the use of RG 1.180, Revision 1, in the electromagnetic and radio-frequency interference qualification test plan. The alignment of the RadICS Platform to RG 1.180, Revision 1, is described in Chapter 12. The licensee for a project-specific application of the RadICS Platform will address the correspondence of the generic qualification envelope for the RadICS Platform with the site-specific qualification bounding envelopes.

5.3.20 Regulatory Guide 1.209

RG 1.209, *Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants*, endorses IEEE Std 323-2003 with qualifications. Chapter 9 describes the use of RG 1.209 in the RadICS EQ program. The RG also notes that NRC has approved EPRI TR-107330 as an acceptable method for addressing mild-environment qualification of programmable logic controllers (PLCs) that is considered equivalent to and consistent with RG 1.209. The alignment of the RadICS Platform to RG 1.209 is described in Chapter 12. The licensee for a project-specific

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 73 of 350
--------------	--------------------	-----------	---	----------------



application of the RadICS Platform will address the correspondence of the generic qualification envelope for the RadICS Platform with the site-specific qualification bounding envelopes.

5.4 NUREG-0800, Chapter 7, Branch Technical Positions

The following NRC Branch Technical Positions (BTPs) were assessed for applicability to the RadICS Platform design.

5.4.1 Branch Technical Position 7-8

BTP 7-8, Revision 5, *Guidance on Application of Regulatory Guide 1.22*, provides additional review guidance regarding the use of RG 1.22 for digital systems. The RadICS Platform periodic testing features that would support compliance with BTP 7-8 for a specific project are described in Chapter 6.

5.4.2 Branch Technical Position 7-11

BTP 7-11, Revision 5, *Guidance on Application and Qualification of Isolation Devices*, provides additional review guidance regarding the use of RG 1.75 for I&C systems. As described in Chapter 6, the RadICS Platform uses the following types of qualified isolation devices: Module features described in Section 6.6 and fiber optic cables. Electrical isolation testing is described in Chapter 9. The alignment of the RadICS Platform to the review guidance in BTP 7-11 is described in Chapter 12.

5.4.3 Branch Technical Position 7-12

BTP 7-12, Revision 5, *Guidance on Establishing and Maintaining Instrument Setpoints*, provides additional review guidance regarding the use of RG 1.105 for I&C systems. EPRI TR-107330, Section 4.2.4 requires the qualifier to provide information about the qualified hardware to support an application specific setpoint analysis per ISA-S67.04-1994. Chapter 9 describes how RadICS, as both vendor and qualifier, applied this approach and prepared a setpoint analysis support document for the generic RadICS Platform. This documentation is intended to provide sufficient design specification data for a project-specific setpoint analysis to be performed. Compliance of actual system setpoints with BTP 7-12 will be addressed by the licensee on a project-specific basis.

5.4.4 Branch Technical Position 7-14

BTP 7-14, Revision 5, *Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems*, provide a structured approach for developing software using a series of plan. The alignment of the RadICS Platform and Application ED documents to BTP 7-14 is described in Chapter 12.

5.4.5 Branch Technical Position 7-17

BTP 7-17, Revision 5, *Guidance on Self-Test and Surveillance Test Provisions*, provides additional review guidance regarding the use of RGs 1.22, 1.118, and 1.152 for digital I&C systems. The RadICS Platform self-diagnostic test and surveillance test provisions are described in Chapter 6. The alignment of the RadICS Platform to the review guidance in BTP 7-17 is described in Chapter 12. The use of RadICS

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 74 of 350
--------------	--------------------	-----------	---	----------------



Platform automatic test features as credit for performing Technical Specification surveillance test functions must be assessed on a project-specific basis.

5.4.6 Branch Technical Position 7-18

BTP 7-18, Revision 5, *Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems*, provides additional review guidance regarding the use of RG 1.152 for the CGD of digital I&C systems. The alignment of the RadICS Platform to the review guidance in BTP 7-18 is described in Chapter 12.

5.4.7 Branch Technical Position 7-19

BTP 7-19, Revision 6, *Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems*, provides guidance for the evaluation of D3 analyses performed on safety-related I&C systems to assess vulnerabilities to digital common cause failures. The licensee for a project-specific application of the RadICS Platform will address D3 in the context of the project-specific suite of safety and non-safety I&C systems. RadICS systems have the capability to implement signal diversity. The RadICS Platform features that would support compliance with BTP 7-19 for a specific project are described in Chapter 10. The D3 assessment for an actual system will be addressed by the licensee on a project-specific basis.

5.4.8 Branch Technical Position 7-21

BTP 7-21, Revision 5, *Guidance on Digital Computer Real-Time Performance*, provides review guidance to verify that system timing requirements calculated from the design basis events and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system design and implementation. Chapter 6 describes how the RadICS Platform addresses the review guidance in BTP 7-21. The alignment of the RadICS Platform to the review guidance in BTP 7-21 is described in Chapter 12.

5.5 NRC NUREGs and NUREG/CRs

The following NRC NUREG document was assessed for applicability to the RadICS Platform design.

5.5.1 NUREG/CR 6082, Data Communications

Section 2 of NUREG/CR-6082, *Data Communications*, has 15 questions intended to help focus reviews of data communication systems. An evaluation the RadICS Platform for those questions is provided in Chapter 12.

5.6 NRC Digital I&C Interim Staff Guidance Documents

The following NRC DI&C-ISG documents were assessed for applicability to the RadICS Platform design.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 75 of 350
--------------	--------------------	-----------	---	----------------



5.6.1 DI&C-ISG-04

DI&C-ISG-04, Revision 1, *Highly Integrated Control Rooms - Digital Communication Systems*, provides criteria for the evaluation of communication independence features used for interdivisional communication. An evaluation of the RadICS Platform for the DI&C-ISG-04 communication independence criteria is provided in Chapter 12. Alignment with the DI&C-ISG-04 guidance for RadICS Platform communication features is described in Appendix B.

5.6.2 DI&C-ISG-06

The documents submitted by RadICS for the NRC generic review of the RadICS Platform are consistent with the guidance in DI&C-ISG-06, Revision 1, *Licensing Process*, which lists the documents expected for a project-specific review. Many of the listed documents do not apply to the generic Tier 3 review of a digital safety I&C platform. Alignment with the DI&C-ISG-06 guidance for supporting documents is described in Appendix C.

5.7 Institute of Electrical & Electronics Engineers Standards

The following IEEE standards were assessed for applicability to the RadICS Platform design.

5.7.1 IEEE Std 7-4.3.2-2003

IEEE Std 7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, is endorsed by RG 1.152 with the exception of Annexes B to F. Conformance with the requirements of IEEE Std 7-4.3.2-2003 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 NPPs. The alignment of the RadICS Platform and Application ED development processes to IEEE Std 7-4.3.2-2003 is described in Chapter 12.

5.7.2 IEEE Std 323-2003

IEEE Std 323-2003, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, is endorsed by RG 1.209 with qualifications. An earlier version, IEEE Std 323-1974 is endorsed by RG 1.89. Chapter 9 described the use of IEEE Std 323-2003 for environmental qualification testing of the RadICS Platform. The alignment of the RadICS Platform to IEEE Std 323-2003 is described in Chapter 12. The licensee for a project-specific application of the RadICS Platform will address the correspondence of the generic qualification envelope for the RadICS Platform with the site-specific qualification bounding envelopes.

5.7.3 IEEE Std 338-1987

IEEE Std 338-1987, *Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems*, is endorsed by RG 1.118 with qualifications. Chapter 6 provides the coverage of self-diagnostic tests and periodic surveillance testing provisions of the RadICS Platform that can be used to

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 76 of 350
--------------	--------------------	-----------	---	----------------



comply with IEEE Std 338-1987. The specific means for complying with IEEE Std 338-1987 must be assessed on a project-specific basis.

5.7.4 IEEE Std 344-2004

IEEE Std 344-2004, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, is endorsed by RG 1.100 with qualifications. Chapter 9 described the use of IEEE Std 344-2004 for RadICS Platform seismic qualification testing of RadICS Platform. The alignment of the RadICS Platform seismic qualification testing to IEEE Std 344-2004 is described in Chapter 12.

5.7.5 IEEE Std 352-1987

Chapter 9 describes the use of IEEE Std 352-1987, *Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*, for the generic board/module-level FMEAs.

5.7.6 IEEE Std 379-2000

IEEE Std 379-2000, *Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, is endorsed by RG 1.53 with qualifications. The standard RadICS Modules components described in Chapter 6 can be implemented in redundant and independent system architectures that comply with the single failure criterion. Representative RadICS Platform system architectures are described in Chapter 2. The specific means for complying with IEEE Std 379-2000 must be assessed on a project-specific basis.

5.7.7 IEEE Std 384-1992

IEEE Std 384-1992, *Standard Criteria for Independence of Class 1E Equipment and Circuits*, is endorsed by RG 1.75 with qualifications. The standard RadICS Platform hardware components and associated EDs described in Chapter 6 are designed for establishing and maintaining the independence of safety-related equipment and circuits, and auxiliary supporting features by physical separation and electrical isolation. In a project-specific application, this is accomplished by physically separating the redundant channels, divisions, and trains of the safety system.

Example RadICS Platform system architectures are described in Chapter 2. These typical architectures include the interdivisional communication interfaces that are needed to support voting logics. Communications between redundant divisions and trains are isolated and designed to retain the required independence. Interdivisional communications is accomplished using fiber optic data links that maintain the electrical isolation between divisions.

The typical RadICS Platform system architectures described in Chapter 2 also include Class 1E to non-Class 1E communications interfaces. Electrical isolation between the Class 1E system and the non-Class 1E system is accomplished using fiber optic data links and one-way (broadcast only) communications from the Class 1E system to the non-Class 1E system.



The alignment of the RadICS Platform to IEEE 384-1992 is described in Chapter 12.

The specific means for complying with the system level independence requirements in IEEE 384-1992 must be assessed on a project-specific basis.

5.7.8 IEEE Std 603-1991

IEEE Std 603-1991, *Criteria for Safety Systems for Nuclear Power Generating Stations*, with the January 30, 1995 correction sheet, is incorporated by reference in 10 CFR 50.55a(h) and endorsed by RG 1.153. The generic RadICS Platform and project-specific RadICS systems can be configured comply with IEEE Std 603-1991 for projects using the RadICS Platform technology. The RadICS Platform features that would support compliance with IEEE Std 603-1991 for a specific project are described in Chapter 12.

5.7.9 IEEE Std 730-1998

The RPC Radiy QMS and RadICS ED QAP documentation complies with the intent of IEEE Std 730-1998, *IEEE Standard for Software Quality Assurance Plans*, as described in Chapters 7 and 8.

5.7.10 IEEE Std 828-2005

IEEE Std 828-2005, *IEEE Standard for Software Configuration Management Plans*, is endorsed by RG 1.169. IEEE Std 828-2005 describes a structured approach to software configuration management. The RPC Radiy and RadICS approaches to software configuration management are described in Section 7.5. The alignment of the RPC Radiy and RadICS configuration management programs to IEEE Std 828-2005 is described in Chapter 12.

5.7.11 IEEE Std 829-2008

IEEE Std 829-2008, *IEEE Standard for Software Test Documentation*, is endorsed by RG 1.170. IEEE Std 829-2008 describes a structured approach to software test documentation. Section 7.4.5.2 describes the RPC Radiy and RadICS approaches to Platform and Application ED V&V test documentation. The alignment of RPC Radiy and RadICS software test documentation to IEEE Std 829-2008 is described in Chapter 12.

5.7.12 IEEE Std 830-1998

IEEE Std 830-1998, *IEEE Recommended Practice for Software*, is endorsed by RG 1.172. IEEE Std 830-1998 is a recommended practice for writing software requirements specifications; however, as a recommend practice, it does not identify and specific requirements. The RadICS Platform and Application requirements documents are described in Chapter 7. The alignment of the RPC Radiy and RadICS software requirements specifications to IEEE Std 830-1998 is described in Chapter 12.



5.7.13 IEEE Std 1008-1987

IEEE Std 1008-1987, *IEEE Standard for Software Unit Testing*, is endorsed by RG 1.171. IEEE Std 1008-1987 describes a structured approach for performing software unit testing. RadICS Platform software testing is described in Chapters 7 and 8. The alignment of RadICS software testing to IEEE Std 1008-1987 is described in Chapter 12.

5.7.14 IEEE Std 1012-2004

IEEE Std 1012-2004, *IEEE Standard for Software Verification and Validation Plans*, is endorsed by RG 1.168 with qualifications. The 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.

5.7.15 IEEE Std 1028-2008

IEEE Std 1028-2008, *IEEE Standard for Software Reviews and Audits*, is endorsed by RG 1.168 with qualifications. The RPC Radiy and RadICS approaches to reviews and audits comply with the intent of IEEE Std 1028-2008, as described in Chapters 7 and 8.

5.7.16 IEEE Std 1050-1996

IEEE Std 1050-1996, *Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, is endorsed by RG 1.180 with qualifications. The use of IEEE Std 1050-1996 for the RadICS Platform qualification test specimen grounding and shielding is described in Chapter 9 and the RadICS Equipment Qualification Plan (Reference 5-3). The system level aspects of complying with IEEE Std 338-1987 must be assessed on a project-specific basis.

5.7.17 IEEE Std 1074-2006

IEEE Std 1074-2006, *IEEE Standard for Developing Software Life Cycle Processes*, is endorsed by RG 1.173, Revision 1, and provides a structured approach for developing a software life cycle program. The life cycle processes for the RadICS Platform and Application EDs are described in Chapters 7 and 8. The alignment of the RadICS Platform and Application ED lifecycles to IEEE Std 1074-2006 is described in Chapter 12.

5.8 Instrument Society of America Standards

The following ISA standard was assessed for applicability to the RadICS Platform design.

5.8.1 ISA-S67.04-1994

ISA-S67.04-1994, *Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants*, is endorsed by RG 1.105 with qualifications. As described in Section 5.2.3, EPRI TR-107330, Section 4.2.4 requires the qualifier to provide information about the qualified hardware to support an application specific setpoint analysis per ISA-S67.04-1994. Chapter 9 describes the approach RadICS, as both vendor

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 79 of 350
--------------	--------------------	-----------	---	----------------



and qualifier, used to prepare the setpoint analysis support documentation for the RadICS Platform. This documentation will provide sufficient design specification data for a setpoint analysis to be performed on a project-specific RadICS system. The specific means for complying with ISA-S67.04-1994 must be assessed on a project-specific basis.

5.9 International Electrotechnical Commission Standards

The following IEC standards were assessed for applicability to the RadICS Platform design.

5.9.1 IEC 60880:2006

IEC 60880:2006, *Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions*, introduces the concept of software lifecycle and details the concept of system safety lifecycle of digital systems given in IEC 61513 to the software portion of the I&C system and details the I&C validation stage in IEC 61513:2001 to the software portion of the system and introduces software-specific issues to the validation process. The life cycle processes for the RadICS Platform ED were established according to the guidance provided in IEC 60880:2006 and were documented in dedicated development plans, which are described in Chapter 7.

5.9.2 IEC 60987:2007

IEC 60987:2007, *Nuclear Power Plants – Instrumentation and Control Important to Safety – Hardware Design Requirements for Computer-Based Systems*, sets out the general requirements for the hardware development life-cycle of computer-based systems. The life cycle processes for the RadICS Platform ED were established according to the guidance provided in IEC 60987:2007 and were documented in dedicated development plans, which are described in Chapter 7.

5.9.3 IEC 61000

Chapter 9 describes the use of IEC 61000, *Electromagnetic Compatibility*, series standards endorsed by RG 1.180, Revision 1, for the electromagnetic interference (EMI)/radio frequency interference (RFI) qualification testing of the RadICS Platform.

5.9.4 IEC 61508:2010

IEC 61508:2010, *Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems*, provides a means of certifying systems on the basis of predefined SILs. The use of IEC 61508:2010 is described in Section 3.2.2.3.

5.9.5 IEC 61513:2001

IEC 61513:2001, *Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – General Requirements for Systems*, establishes the relationship between NPP safety objectives, requirements for the overall architecture of I&C systems, and requirements of the individual systems

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 80 of 350
--------------	--------------------	-----------	---	----------------



important to safety. The life cycle processes for the RadICS Platform ED were established according to the guidance provided in IEC 61513:2001 and were documented in dedicated development plans, which are described in Chapter 7.

5.9.6 IEC 62566:2011

IEC 62566:2011, *Nuclear Power Plants – Instruments and Control Important to Safety – Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions*, establishes requirements for each stage of the hardware description language (HDL)-Programmed Devices (HPD) lifecycle (requirements specification, design, implementation, verification, integration and validation) to develop highly reliable HPDs for use in I&C systems of NPPs performing safety category A functions. The life cycle processes for the RadICS Platform ED were established according to the guidance provided in IEC 62566:2011 and were documented in dedicated development plans, which are described in Chapter 7.

5.10 U.S. Military Standards

The following U.S. MIL-STD was assessed for applicability to the RadICS Platform design.

5.10.1 MIL-STD-461E

Chapter 9 describes the use of MIL-STD-461E, *DOD Interface Standard Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment*, as endorsed by RG 1.180, Revision, for the EMI/RFI qualification testing of the RadICS Platform.

5.11 Electric Power Research Institute Technical Reports and Handbooks

The following EPRI documents were assessed for applicability to the RadICS Platform design.

5.11.1 EPRI TR-107330

In RG 1.209, NRC noted that it has accepted EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants* (dated December 1996), as an acceptable method for addressing mild-environment qualification of PLCs that is considered equivalent to, and consistent with, the RG.

The use of EPRI TR-107330 for the RadICS Platform qualification program is described in Chapter 9. The RadICS Platform ED will be treated as the 'legacy software' described in Section 7.6 of EPRI TR-107330. Compensatory measures for legacy software are identified in EPRI TR-106439. The use of EPRI TR-107330 for the RadICS Platform CGD program is described in Chapter 4.



5.11.2 EPRI TR-106439

In RG 1.152 Annex C, NRC identifies that EPRI TR-106439, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications* (dated October 1996), contains adequate guidance for the evaluation and acceptance of commercial grade digital equipment for nuclear safety applications. The use of EPRI TR-106439 for the RadICS Platform CGD program is described in Chapter 4.

5.11.3 EPRI Handbook 1011710

The purpose of EPRI TR-1011710, *Handbook for Evaluating Critical Digital Equipment and Systems*, is to provide practical guidance to nuclear utility engineers on how to conduct generic and project-specific CDR. The CDR can be used to gain assurance that a given critical digital system or platform has the necessary properties and will function as expected. It is a structured way to investigate and document the potential for unacceptable behavior to occur in service, due to deficiencies in the digital system specification, design, configuration, operation, maintenance, or documentation, or due to misapplication.

The use of EPRI Handbook 1011710 for the RadICS Platform CGD program is described in Chapter 3.

5.12 American Society of Mechanical Engineers Standards

The following ASME Standard was assessed for applicability to the RadICS Platform design.

5.12.1 ASME NQA-1-2008

The use of NQA-1-2008, *Quality Assurance Program Requirements for Nuclear Facilities*, and the NQA-1a-2009 Addenda to meet 10 CFR Part 50 Appendix B is described in Chapter 3. The alignment of the RadICS QAP to ASME NQA-1-2008 is described in Chapter 12.

5.13 Chapter 5 References

- 1 NUREG-0800, NRC Standard Review Plan, Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety," Revision 5, March 2007
- 2 *exida* Report No. RAD 14-06-037 R002, "Results of the IEC 61508 Functional Safety Assessment for FPGA-Based Safety Controller RadICS," September 15, 2015
- 3 RadICS Equipment Qualification Test Plan, Document 2016-RTS002-EQTP-004



6 RadICS Platform

6.1 RadICS Platform Overview

RadICS Platform is a new generation product that was designed in 2010-2011. It is based on more than 10 years of RPC Radiy experience with digital I&C platform design, production, operation, and maintenance. The RadICS Platform is composed of multiple types of Modules, based on the use of FPGA chips as computational, processing, and system-internal control engines for each of the Modules. In terms of its high level functionality and flexibility, the RadICS Platform is essentially a safety PLC, except that the internal logic is performed by FPGAs instead of microprocessors.

The typical safety-related I&C systems channel configuration, based on the RadICS Platform consists of one seismic-resistant Chassis, which contains Logic Module (LM) and up to 14 other RadICS Modules (i.e., I/O and optical communication) in any combination of their types. The basic set of I/O Modules types comprises Analog Input Module (AIM), Discrete Input Module (DIM), Discrete Output Module (DOM), and Analog Output Module (AOM). The Optical Communication Module (OCM) can be used to extend the system to multiple Chassis configuration. It is also possible to provide interchannel links between 2, 3, or 4 channels via fiber-optic communications directly between their LMs for coincidence voting. The RadICS Platform offers a fast response time (≤ 10 milliseconds).

LM performs input Modules data acquisition, execution of user configured logic, drives the output Modules, and processes diagnostic data from all I/O Modules installed in the RadICS Platform Chassis. The I/O Modules provide interfaces with other devices (e.g., detectors, sensors, actuators, signalization devices). The functionality of each Module is driven by the logic implemented in the ED onboard the FPGA(s).

The seismically-resistant Chassis for RadICS Platform provides protected external interfaces to process I/Os, two independent power supply units (links), communications links, local inputs/outputs (from/to the built-in-Chassis/cabinet detectors/sensors/keys or indicators). Internal Chassis interfaces facilitate connections to the various Modules that are installed within the Chassis by means of dedicated, isolated, point-to-point high-speed LVDS communication lines.

The RadICS Platform is configured using the RPCT and the RadICS AFBL.

A typical RadICS Platform configuration is shown in Figure 6-1.

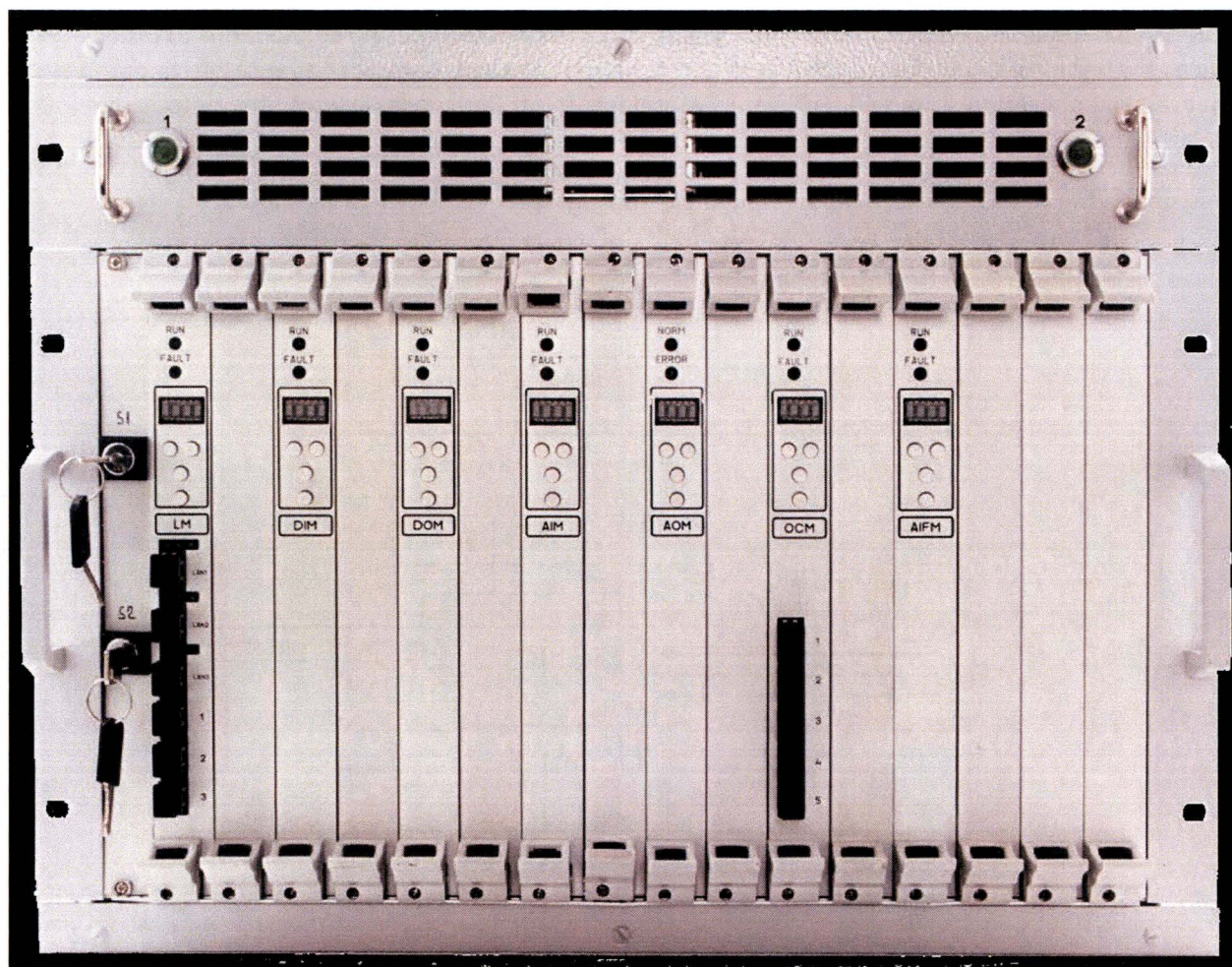


Figure 6-1: Typical RadICS Platform Configuration

The RadICS Platform is itself a single rack-mount Chassis containing all required inputs, outputs and logic processing so that it operates as a single-channel device in de-energize to trip applications. Like a safety PLC, the RadICS Platform functionality is organized on two levels: the generic platform level logic and the customizable application level logic. The RadICS Platform can be configured in two to four channels configurations. In these configurations, a RadICS Platform system can meet U.S. Class 1E requirements.

In normal operation, the RadICS Platform operates in “on-line” mode and performs the safety function defined at the application level. Self-diagnostics are performed by both the application and platform levels, although they are aimed at different types of faults. Failures detected by either level that are potentially unsafe are converted to safe failures.



In the on-line mode, no reconfiguration, no tuning, and no potentially unsafe connections to other devices are permitted. Monitoring of the RadICS Platform is possible through non-interfering one-way broadcast of application state and hardware status data. In off-line mode, in which the outputs are in the safe state, diagnostic equipment may be connected, and tuning and reconfiguration are possible.

The scope of the RadICS Platform addressed in the Topical Report is shown in Figure 6-2.

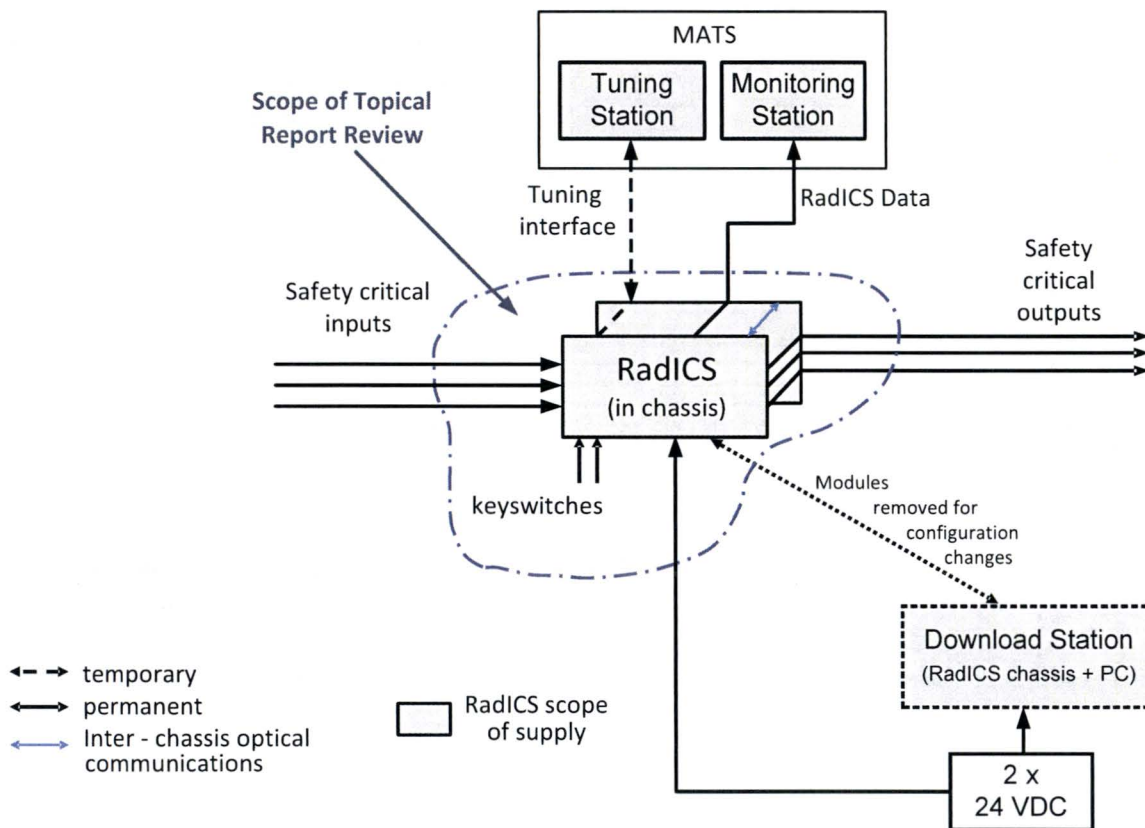


Figure 6-2: Context Diagram of the RadICS Platform

6.1.1 RadICS Platform General Attributes

The RadICS Platform has been designed to comply with international nuclear safety I&C requirements. The applicable regulations, regulatory guidance, industry standards, and other guidance applicable to digital safety I&C systems are documented in Chapter 5. The resulting RadICS Platform has the following general attributes:

- Fail-safe: The RadICS Platform assures that, in case of detected failure meeting certain criteria, the outputs associated with a Logic Module achieve a pre-defined safe position.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 85 of 350
--------------	--------------------	-----------	---	----------------



- **Fault-tolerance:** RadICS supports system architectures that can meet the redundancy requirements of the single failure criterion. In addition, RadICS LMs can automatically correct its voting logic in case faults are detected, so that system availability is optimized without compromising safety. The criteria establish that no single failure will result in loss of any of the safety functions. The RadICS Platform system architecture is dictated by reliability requirements imposed on the application by the end user's requirements.
- **Diversity:** RadICS supports system architectures that employ signal diversity to defend against common cause failures (CCF). The RadICS Platform also can be deployed as a diverse system as part of an application-level D3 strategy. The RadICS Platform architectural and technological features provide the RadICS-based integrated I&C systems with a large degree of diversity.
- **Functional isolation:** RadICS Platform equipment and communications design prevents propagation of failures between redundant equipment in separate divisions. In addition, communication paths to non-safety I&C systems are electrically isolated with one-way communications from the RadICS Platform to the non-safety I&C system. This prevents faults in a non-safety I&C system from affecting the RadICS Platform.
- **Determinism:** For all processing, the same inputs produce the same outputs within a guaranteed response time
- **Self-diagnostic testing:** Self-diagnostic testing is used to check correct operation of the RadICS Modules and associated ED during startup and normal operation. The startup self-diagnostic tests check for correct operation before the RadICS Platform is released for normal operation. Other self-diagnostic tests are performed during normal operation to check for correct operation of the RadICS Modules. Self-diagnostic testing features check the integrity of the Application Logic each work cycle. Error checking is performed on all digital communications.
- **Ease of use:** Operation and maintenance are simplified by hardware, interfaces, and data transmission, and FPGA electronic designs self-diagnostics.
- **Flexibility:** Architecture flexibility and scalability to tailor general system design to customer needs in terms of number inputs received and actuators to be controlled.
- **Modularity:** The RadICS Platform can be delivered either in standard Chassis to be integrated into existing cabinets (for refurbishment purposes) or in new cabinets.
- **Scalability:** The RadICS Platform has been deployed internationally in a wide variety of safety I&C applications, including RTS, RPCLS, and ESFAS.
- **High quality development process for electronic design:** The software life cycle processes used to develop the generic RadICS Platform baseline and developing the project-specific Application ED are based on recognized standards and include independent V&V.
- **Secure development and operational environment:** The software life cycle processes used for the RadICS Platform establishes a secure development and operational environment for managing the generic RadICS Platform baseline and developing the project-specific Application Logic through the factory test phase. These processes protect against unauthorized, unintended, and unsafe modifications to the system, and support implementation of design requirements that promote integrity and reliability during operation and maintenance in the event of inadvertent operator actions or undesirable behavior of connected equipment.



6.1.2 RadICS Platform Fundamental Safety Approach

The RadICS Platform was designed to meet several high-level principles of safety.

- **De-energize to trip**

The RadICS Platform uses the de-energized state as the safe state for each RadICS Module:

- The fault status of the RadICS Platform input Modules is reported to the RadICS LM. For the Faulted mode, the RadICS LM processes such inputs as either opened contact for DIMs or zero voltage/current for AIMs, as specified in the Application Logic.
- All outputs are set to the open contact or zero voltage and zero current state as the safe state.
- All failures of power supplies lead either to the safe state, or if they result in no effect upon first failure (e.g., first failure of a redundant power supply). These failures are annunciated and flagged to the Application Logic, which can then handle the failure condition in accordance with the end user's functional specifications.

- **Automatic Transitions to the Safe State**

The RadICS Platform will drive all safety output Module outputs to the safe state for the first-occurrence of the following:

- Power is off or a critical failure has occurred
- Power is initially turned on
- Startup self-diagnostic tests have not finished successfully
- Platform diagnostic results require it
- Application Logic requires it (which may include the use of RadICS Platform diagnostics reported to the Application Logic through function blocks)
- Set Safety Override (SOR) keyswitch has been used
- Human Action to Leave the Safe State

The RadICS Platform requires human intervention to release outputs from the safe state and pass them to the control of the Application Logic:

- At completion of startup (also requires that there be no detected failures)
- After the SOR has been activated for any reason
- After any failure that causes a safe-state transition

- **Safety Modules Only**

The RadICS Platform detects the presence of non-safety Modules during the self-diagnostics at startup, and will maintain the safe state if any is detected.



- **IEC 61508 Safety Integrity Level 3 Capability by Design** ^{4,5}

The RadICS Modules are implemented using common Units to the extent possible:

- The RadICS Modules are designed with redundant components where needed to permit self-diagnostic tests and data redundancies are used to permit detection of data corruption with very high probability
- Watchdogs are incorporated on every Module
- CRCs are used on all communications and safety-critical data
- External communications links are all treated as 'black-channel'
- Communications ports are monitored and blocked except when specifically required (e.g., tuning)
- RadICS Modules perform the self-diagnostics and take safe-state action. This involves Application Logic where feasible (i.e., it is competent to take such action) to incorporate end user's functional requirements.
- Application ED is created using the RadICS Platform FBL
- Failure Modes, Effects, and Diagnostics Analysis (FMEDA) is used to confirm the failure rates and safe failure fractions

- **Application Logic Functionality**

- The Application Logic is implemented in the Application ED using the assembler provided that verifies logic for fundamental errors such as referencing non-existent I/O channels, loop-backs, etc.
- The Application ED is validated after every reconfiguration of the RadICS Platform Application ED.
- Tuning is a controlled activity: a TUNING keyswitch is required to activate the tuning port and the provided Tuning Personal Computer (PC) requires a password.
- The RadICS Platform is isolated from the field during tuning, and the end user performs a functional test of the tuning changes before returning the RadICS Platform to online status.

⁴ IEC standard IEC 61508 defines SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a given SIL. The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. In order to achieve a given SIL, the device must meet targets for the maximum allowed probability of dangerous failure and a minimum acceptable safe failure fraction. The concept of 'dangerous failure' is rigorously defined for the system in question, normally in the form of requirement constraints whose integrity is verified throughout system development.

⁵ The IEC concept for SIL (Safety Integrity Level) is different from and not to be confused with the IEEE SIL (Software Integrity Level) concept used in IEEE Std 1012 (Reference 6-1).

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 88 of 350
--------------	--------------------	-----------	---	----------------



- **Controlled Scope**

The operational interfaces of the product are clearly defined and designed to minimize the potential for unsafe events:

- Configuration and calibration changes are performed outside the in-service RadICS Platform Chassis.
- After every configuration change to the Application ED or to the hardware configuration, the RadICS Platform must be revalidated. Configuration self-diagnostic checks are performed during system startup, as described in Section 6.2.6.
- Tuning changes are made only when the RadICS Platform trip outputs are isolated from the field (i.e., the field 'sees' a safe state). After every change to tuning parameters, the effects of the changes must be tested by the end user before reconnecting the field outputs. This means the MATS Tuning PC is not an online tool.
- The monitoring interface to the MATS is one-way broadcast (i.e., non-interfering). Thus, the MATS is also non-interfering. The MATS is supplied by the end user, to meet the end user's Human Factors requirements.
- The RadICS Platform blocks all inward communications with the only exception being tuning inputs when put into TUNING mode by the keyswitch.

6.1.3 Maintainability and Operability

The RadICS Platform has a number of features that support maintenance and operation of RadICS Platform-based systems.

- **On-line Monitoring**

On-line monitoring provides continuous indication of the results of platform diagnostics, RadICS Platform operating mode, presence and state of keyswitches, selected field input and/or Application Logic signals, the current operational Application ED tuning values, and proposed tuning values as they are set by the MATS Tuning PC. RadICS Platform monitoring data sent over to the MATS via a one-way data link. Thus, the plant operators in the control room can be informed of failures detected by the RadICS Platform system and can initiate system maintenance. They can also monitor all access to the system and check entered tuning values for human errors. The MATS also permits the plant operators to confirm the post-tuning testing. All these features lead to maintainers approaching the system with good diagnostic information and verification by control room staff to detect errors before they can adversely affect the plant.

- **Operational Parameter Tuning Capability**

Operational parameters may need to be adjusted during a reactor operating cycle or between cycles. The RadICS Platform provides the ability to tune these parameters via the Fiber Optic Tuning Interface using the MATS. Tuning is normally locked out, and is enabled only by a keyswitch. In the TUNING mode, parameters that are specified in the Application ED can be adjusted by connecting a MATS Tuning PC with special software to the RadICS Platform. The

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 89 of 350
--------------	--------------------	-----------	---	----------------



RadICS Platform outputs are isolated from the field (i.e., safe state) for tuning. The end user performs functional tests to confirm the tuning values before restoring the system to normal operation. The RadICS Platform also checks tuning values for 'reasonableness' and basic validity. The Application Logic can also be engineered to perform other specified checks. Tuning parameters are stored in electrically erasable programmable read-only memory (EEPROM) on the RadICS LM, so they are retained even after power is lost and restored.

- **Minimized Maintenance Error**

The RadICS Platform design incorporates features to minimize the potential for maintain or operator error that could lead to unsafe operation of the product. This includes:

- A non-interfering local status display on every RadICS Module
- Comprehensive diagnostics relayed to the MATS
- Detection of some maintenance errors (e.g., wrong module in a slot)
- Hot-swap capability
- Validated maintenance documentation
- User SOR

- **Hardware Protection**

Protective devices are used at all RadICS Module interfaces:

- Diodes and/or voltage limiters are used as appropriate to protect devices that interface to the field
- Fiber optics interfaces are used where practical
- All interfaces between a Module and the Chassis backplane are galvanically isolated, including power connections

- **Checking of User Configuration and Tuning Values**

Configuration of the Application ED is an offline activity using offline tools. The offline configuration tool checks for detectable errors in coding such as loopbacks, references to Modules in the wrong slot, or the wrong kind of Module. Actual installation errors such as using the wrong slot are detected online at startup. Tuning is normally locked out, and is enabled only by a keyswitch. The RadICS Platform outputs are isolated from the field (i.e., safe state) for tuning; and the end user performs functional tests to confirm the tuning values before restoring the system to normal operation. The RadICS Platform also checks tuning values for 'reasonableness' and basic validity.

- **User Safety Override**

The LM and output Modules have SOR Units which allows the user to force the RadICS Platform into the safe state. The SOR Unit overrides all outputs of the Application and Platform ED to drive the outputs to the safe state.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 90 of 350
--------------	--------------------	-----------	---	----------------



- **Hot Swappable Modules**

The RadICS Platform design permits removing and replacing a Module while the Chassis is powered up (hot swap) or powered down. It is expected that the maintainer follows the appropriate procedures to ensure that maintenance activity does not affect the RadICS Platform operation in a way not foreseen by the Application ED.

All RadICS Modules have been designed to be hot-swappable to prevent damage due to maintenance error. The normal procedure is to power down the RadICS Platform Chassis before performing maintenance; however, all Modules are hot-swappable, so no damage will occur to a Module even if it is extracted or inserted at power. Plant safety is assured when a hot swap action is performed, since any Module that has been removed will be identified as failed. The LM will make the identification for a hot swap of an I/O Module in its Chassis. The output Modules in the Chassis and other LMs in the system (e.g., other divisions) will make the identification if a LM is removed from a Chassis. The LMs will use the diagnostic information to take the appropriate actions, as specified in the end user's functional requirements for the Application Logic.

Removal of the LM will force all output Modules to the safe state. When a replacement LM is inserted and completes its startup sequence, the LM will return to normal operation. The LM may be held in RUN (SAFE) mode until the SOR is reset unless it is hard-wired to be automatic. Removal of any I/O Module will also force all output Modules to the safe state.

- **Authentication of the RadICS Module Version**

Nuclear standards specifically require authentication of the version of installed software. The hardware version of every RadICS Module is inscribed on the back side of the Module printed circuit board. The ED version installed in the RadICS Module FPGA can be displayed on the 4-character display of the Module.

The RadICS Platform features that support maintenance and operation facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment, which satisfy the repair requirements of IEEE Std 603-1991 Section 5.10 (Reference 6-2). The RadICS Module version authentication features satisfy the identification requirements of IEEE Std 7-4.3.2-2003 Section 5.11 (Reference 6-3).

6.1.4 FPGA Based Digital Technology

The RadICS Platform is composed of various standardized Modules, each based on the use of FPGA chips as computational engines.

FPGA-based I&C systems have been developed and applied to applications in the aerospace and process industries since the early 1990s. Although the use of FPGAs in nuclear power plants has lagged behind in the past, compared to other industries, due to quite conservative approaches, there are an increasing number of FPGA installations in operating nuclear power plants worldwide, most of them provided by RPC Radly.



FPGA technology is an alternative to microprocessor based technologies and other types of programmable devices. FPGAs are semiconductor-based programmable devices which can be configured to perform custom-designed functions. It includes two entities: an FPGA chip which is a hardware component that can be tested against hardware qualification requirements, and the electronic design, represented by a set of instructions in HDL to be configured into the FPGA hardware and that can be verified against functional requirements.

There are two main FPGA chip architectures: fine-grained and coarse-grained. The coarse-grained FPGAs have very large logic blocks (macrocells) with sometimes two or more sequential logic elements, and the fine-grained ones have very simple logic blocks.

Another architectural difference is the technology used to manufacture the FPGA chips. The most common technologies are:

- EPROM/EEPROM/Flash based chips are re-writable types (they allow reprogramming of the FPGA) and non-volatile (no data or logic is lost in case of power losses)
- SRAM based chips are re-writable, but volatile
- Anti-fuse based chips are non-rewritable and non-volatile (one-time programmable)

The RadICS Platform uses SRAM-based FPGAs for the Modules and complex programmable logic devices (CPLDs) for the watchdogs.

The development process of FPGA applications typically consists of requirement specification, design, implementation, and integration along with the associated V&V activities.

The objective of the requirements specification phase is to define precisely all the requirements that apply to the FPGA platform and associated application. These requirements are usually derived by following a top-down approach whereby each system component is allocated functional and safety requirements and interfaces among them are defined.

The most critical phase of the FPGA overall development process is the design phase. Errors made in this phase will dramatically affect all subsequent stages. The development process includes architectural and detailed design activities. The development process for the RadICS Module EDs is described in Chapters 7 and 8.

6.1.5 Benefits of FPGA Technology

The application of FPGA technology has significant advantages that can be utilized both in I&C modernization projects of existing nuclear power plants and in I&C designs for new nuclear power plants. These advantages are the following:

- Design, development, implementation, and operation simplicity and transparency
- Easy portability of algorithms and possibility of re-programming, if algorithms or technology may change in the future, but the hardware stays the same
- Reduction of vulnerability of the digital I&C system to cyber-attacks or malicious acts due to the absence of any system software or operating systems



- Faster and more deterministic performance due to capability of executing logic functions and control algorithms in a parallel mode; due to advantage of native hardware parallelism, FPGAs are able to process more data, provide faster input and output response times and execute more instructions per clock cycle than digital signal processors
- Possibility to segregate safety functions and non-safety functions on the same integrated circuit
- Diversity with the potential to comply with strict requirements that include, but are not limited to, design, equipment, functional and software diversity
- More reliable, testable and error-free end-product due to reduction in the complexity of the V&V and implementation processes
- More direct qualification process for FPGA-based safety systems due to the simplicity and transparency of system architecture and its design process
- Resilience to obsolescence due to the portability of the HDL code between different versions of FPGA chips produced by the same or different manufacturers: even if the FPGA migrates to the next generation, the HDL code remains unchanged

6.2 RadICS Chassis-Level Features

6.2.1 Theory of Operation

Figure 6-3 illustrates the operation of RadICS Platform and shows the operation of the LM and I/O Modules. Adding more I/O Modules does not change the fundamental operation. This figure shows that there are two levels of logic in the LM (i.e., Application and Platform) and only the Platform level in the I/O Modules.

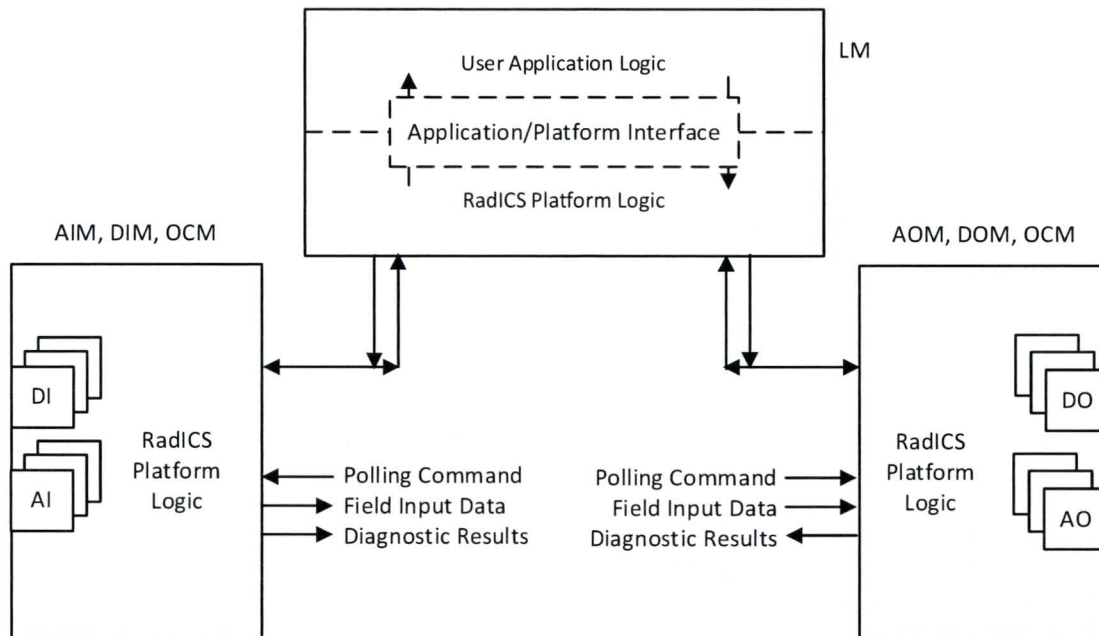


Figure 6-3: Theory of Operation of RadICS Platform

After initialization, the RadICS Platform operates with a standard Work Cycle that is performed cyclically. The basic RadICS Platform Work Cycle includes four Phases:

- Input Data Receive – Request and receive input data for the current Work Cycle from I/O Modules and perform Application Logic test code
- Application Logic Processing and Configuration – Process Application Logic and preparation (i.e., configuration) of communication messages
- Output Data Transmission – Transmit Application Logic processing results to the output Modules
- Switch Time – Allows period of time for output Modules to complete switching

The standard RadICS Platform Work Cycle is illustrated in Figure 6-4.

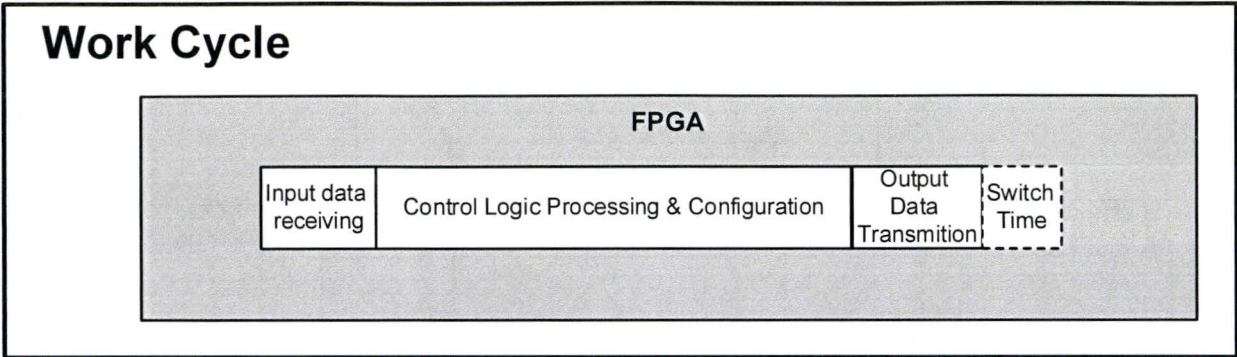


Figure 6-4: RadICS Platform Work Cycle

The Work Cycle is controlled by the LM, as described in Section 6.2.6.1.2. The other RadICS Modules operate in response to commands from the LM, as described in Sections 6.2.6.2 through 6.2.6.5.

All RadICS Modules include a number of common elements plus the specialized hardware for their specific purpose. The common hardware elements include:

FPGA	executes all platform control logic (plus Application Logic in the LM) plus extensive diagnostics
CPLD	acts as watchdog, monitors power supplies and FPGA; can force the Module into FAULTED mode, which drives the safe state
Power supply	Each Module taps the two +24 Volts Direct Current (VDC) supply lines on the backplane, and develops all needed voltages.
Clocks	Each Module has several independent clocks to provide for self-checking
LVDS	communications on the private backplane lines between Modules (LM \leftrightarrow I/O)
Display	status display on the front of each Module, for maintainer
SOR	Safety Override (on output Modules only): allows a temporary override to force safe state outputs at a system level

These standard features are described further in Section 6.2.5.

6.2.1.1 Chassis

The RadICS Chassis distributes two +24 VDC supplies to every slot. Each Module taps both these supplies for redundancy and develops its own voltages needed to operate all the Units within the Module. This includes the various voltages needed by the FPGA. Any voltages needed by the I/O channels are galvanically isolated on a channel basis.



All RadICS Modules communicate via the backplane, using direct individual lines from each I/O slot to the LM slot. I/O Modules have no direct communication with each other; rather they each have one direct individual line to the LM slot.

6.2.1.2 Input/Output Modules

Each I/O Module operates autonomously. Each I/O Module constantly performs self-diagnostic tests on its own common hardware, individual I/O channel hardware, and on its ability to communicate with the LM. The self-testing is interrupted⁶ on the individual channel hardware for those modules where diagnostic cycle is longer than the Work Cycle (i.e., DOM and DIM) when the I/O Module receives a command from the LM. The LM polls the I/O Modules to provide it with field data and self-diagnostic results (in the case of an AIM or DIM) or to set outputs and return diagnostic results (in the case of a DOM and AOM). The I/O Module diagnostics resume once the LM command is executed.

To permit exhaustive self-diagnostics as required by IEC 61508 (Reference 6-4), the individual input or output channels on the I/O Modules have sufficient hardware redundancy so that random hardware failures can be detected by the self-diagnostics. Similarly, data handling in the FPGA involves high-order CRC checks so that the vast majority of functional and memory faults and communications errors are also detected. A separate CPLD acts as a watchdog to detect FPGA failures or failures affecting the FPGA that it cannot detect and puts the Module into FAULTED mode (safe state) if that occurs or the FPGA reports a critical failure to the watchdog.

For input Module channel faults, the I/O Module will continue to operate, but the I/O Module will signal to the LM that the failed channel's data is bad. The 4-character display on the front of the Module will display a fault code instead of RUN and the diagnostic result is reported to the Application Logic. For total Module failure, such as a failure affecting the FPGA, the Module will shut down; this will also be detected by the LM, and reported to the Application Logic.

6.2.1.3 Optical Communication Module

The OCM is used to extend the capacity and capabilities of the RadICS Platform (i.e., to allow Application Logic running in one chassis LM to use data derived from I/O in other chassis). Each chassis LM can execute logic related to I/O within its own chassis as well share selected data with logic in another chassis. The OCM provides five optically-coupled SIL 3 black-channel links to these expansion chassis by linking an OCM in each pair of chassis.

Failures within one chassis are detectable in another chassis in the following ways:

- A critical fault in an OCM will cause it to stop updating OCMs in other chassis; consequently, an unfaulted chassis will see a communications timeout on the OCM communicating with the faulted chassis.

⁶ Interrupted in this context does not mean an interrupt of software execution, because there is no software; instead it means the test logic is momentarily disabled and the command response logic is enabled.



- A critical fault in any I/O module except OCM results in setting all modules within that chassis to the safe state, in which case an OCM will continue updating OCMs in other chassis and additional actions from the Application Logic are needed.
- Communications errors between the OCMs will result in error codes set by both OCMs
- User level values can be communicated (e.g., each signal needed in other chassis can be accompanied by 'health' signals, so if an analog input in one chassis fails, the health signal can inform logic in the LM of another chassis that the analog input value is untrustworthy).

The OCM also includes five RS-232/485 channels for communications to external devices, but these are reserved for future use.

6.2.1.4 Logic Module

The LM includes two separately designed logic configurations: the RadICS Platform Logic and the end user Application Logic. Both levels of logic are protected by the same CRC checks and timing checks by the watchdog, as described for the I/O Modules.

6.2.1.5 Operation Modes Overview

The following text provides an overview of the operation modes for all Modules.

POWERED-OFF	<p>This mode represents removal of power from the Module or the RadICS Platform as a whole, whether by human action or by loss of the power sources.</p> <p>The RadICS Platform is powered off when both 24 VDC supplies are removed. In the powered-off state, all the RadICS Platform outputs are in their safe state.</p>
STARTUP	<p>In this mode, the FPGA acquires its configuration from EEPROM and this is verified by a CRC check. The FPGA then starts normal operation, including executing the Application Logic, and performs all the self-diagnostic tests applied in RUN mode plus some extra tests.</p> <p>Any critical failures (i.e., Type I or II) result in exit to FAULTED mode. If no failures are detected, the Modules exit to RUN (SAFE) or RUN mode (depending on the Module), but it is possible for the operator to trigger exit to CONFIGURATION mode.</p> <p>When the RadICS Platform is powered up, there is a [[]]^{a,c,e} second period of operation in STARTUP mode during which all outputs are held in the safe state and the RadICS Platform executes all standard self-diagnostic tests plus some extra startup tests. At the end of STARTUP mode, all Application Logic is initialized, and ready to run.</p>

**RUN (SAFE)**

In this mode, all the Application Logic is up and running, but the outputs are overridden by the SOR and maintained in the safe state. Operator intervention is required to advance to RUN mode. This mode does not exist for input Modules since they do not have field outputs or SOR Units. RUN mode self-diagnostic tests are executed.

At the end of a successful STARTUP mode period (i.e., no safety-critical failures detected), the RadICS Platform will allow the SOR to be reset and until the SOR is reset, the RadICS Platform operates in RUN (SAFE) mode. In RUN (SAFE) mode, the Application Logic executes normally, setting the internal values of the outputs, but all outputs are subjected to the SOR, which sets the final outputs to the safe state.

Transition out of RUN (SAFE) mode into RUN mode occurs when the Reset-SOR input is closed and all conditions that set the SOR have cleared. There are two options to implement this: 1) manual reset by the operator using a momentary contact keyswitch or 2) installed wiring that holds the reset circuit closed, thus providing an automatic transition from STARTUP mode (i.e., momentarily to RUN (SAFE) mode, and then to RUN mode).

RUN

In this mode, all the Application Logic is up and running and controls the outputs. RUN mode self-diagnostic tests are executed.

TUNING

In this mode, parameters which the Application Logic design provided for can be adjusted by connecting a MATS Tuning PC with special software to the RadICS Platform.

TUNING mode requires the use of a TUNING key and an end user supplied contact that when closed, indicates that the safety load of the RadICS Platform (i.e., the final actuator) is held in the safe state (controlled by what is called the ARMING key). This permits the end user to fully test the tuning changes under safe conditions, since the output contacts can be opened or closed without affecting plant safety.

FAULTED

In this mode, all outputs are forced to the safe state. This mode results from discovery of a critical failure. The only exit from this mode is via powering off the RadICS Platform.



CONFIGURATION

This mode has two functions: configuration and calibration.

- Configuration: Changes to the Application Logic or configuration of the RadICS Platform have to be made in a Chassis equipped for this purpose, called the Download Station (DLS). All Modules also store authentication data in EEPROM which includes version information. This information is sent to the MATS when online. To change or download this data, one uses this mode and the DLS.
- Calibration: Analog Modules (AIM and AOM) use this mode to perform hardware calibration. Calibration can be done in the in-service Chassis; however, the application designer must design logic to ensure safety during calibration. Calibration can also be performed when the Modules are removed from the Chassis by using the DLS.

The Application Logic can be designed to detect whether a module is in CONFIGURATION mode and ensure safety. Input signal ports are provided to detect this state and to engage the SOR.

6.2.1.6 Human-Machine Interface

The RadICS Platform consists of functionally dedicated Modules (i.e., each Module performs one kind of I/O) inserted into the slots of the RadICS Chassis. All empty slots are populated with fixed blanks to protect the Chassis interior from dirt and accidental insertion of tools. IEC 61508 requires that the designer “consider” human factors issues. Chassis-related human factor features include:

- Labelling to identify slot allocation
- Visually verifiable tie-down clamps
- Blanks covering all unused slots
- Front mounted fiber optic connectors for LM and OCM
- Rear-connected I/O

The labelling of each slot minimizes the likelihood of a maintenance technician inadvertently inserting a wrong type of Module into any active slot. The RadICS Platform will detect such error via its startup self-diagnostics even if such a mistake is made, as described in Section 6.2.6.1.2. These self-diagnostics would detect an incorrect replacement made during a hot swap when the module goes through the STARTUP Mode.

The tie-down clamps exert a positive pressure on the Modules to ensure they stay inserted during a seismic event. The full insertion of a Module and complete clamp-down are visually verifiable because the clamp rotates to a position in contact with the Module faceplate when correctly closed, and rests at a noticeable angle.

To ensure that Modules can be inserted into active slots only, a permanent dummy plate covers unused Module slots. Even if this feature did not exist, an I/O Module that was inserted would have no effect on the system, since the slot was not enabled in the specific RadICS Platform configuration.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 99 of 350
--------------	--------------------	-----------	---	----------------



There are fiber-optic connectors on the LM and OCM, which can be used to communicate with LMs in other Chassis. All I/O cables are rear-connected. There is normally no need for access during system operation, so the rear connections eliminate many potential maintenance errors.

The RadICS Platform human-machine interface features satisfy the identification requirements of IEEE Std 603-1991 Section 5.11.

6.2.2 RadICS Chassis Configuration

The RadICS Chassis has 2 slots for LMs⁷ and 14 slots for other I/O Modules. The mechanical design of the RadICS Chassis (hereinafter referred to as Chassis) is a metal box consists of 16 physical slots for Modules, backplane for providing connections between Modules and power supply for the Modules, and two fans (with associated control board). Each of the slots for Modules is equipped with rails for proper and safe installation. There are 16 physical slots for special electromagnetic protection Modules for external interfaces (see Figure 6-5). Each Module locks into place with a lever at top and bottom. Electrical connection of each of the Modules is accomplished by insertion of the Module into the Chassis socket.

[[

]]^{a,c,e}

Figure 6-5: RadICS Chassis Design

The Chassis is configured by installation of the various types of Modules in accordance with the following configuration constraints:

⁷ The mechanical and electrical design allows for two LM, but only one LM is used at present.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 100 of 350
--------------	--------------------	-----------	---	-----------------



- Two LM Slots are reserved for LMs in the Chassis (i.e., slots F1 and F2). The qualified configuration will use only one LM, in slot F1
- Modules for Input Signals (i.e., DIM and AFM) may be installed in any slot from #1 to #14
- Modules for Output Signals (i.e., DOM and AOM) may be installed in any slot from #1 to #14
- Modules for Optical Communication (i.e., OCM) may be installed in any slot from #1 to #14
- Any slot (except F1 for the LM) may be left empty

Special coding pegs are provided for I/O Modules to prevent a RadICS Module from being inserted into the wrong slot.

The Chassis configuration is shown in Figure 6-6.

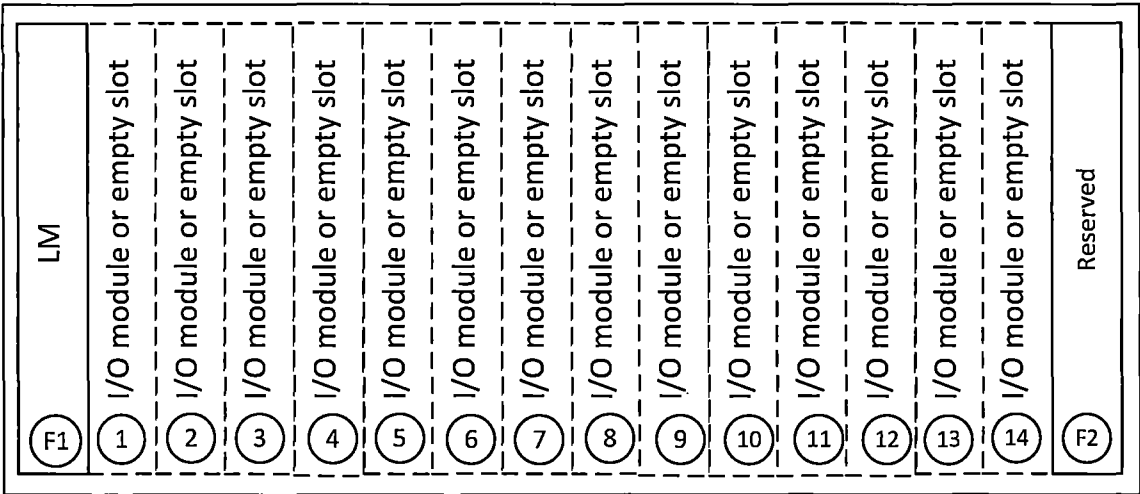


Figure 6-6: RadICS Chassis Configuration

The RadICS Platform Chassis connectors are located on the rear of the Chassis, as shown in Figure 6-7.



[[

]]^{a,c,e}

Figure 6-7: Rear of RadICS Chassis Showing Connectors

The [[
]]^{a,c,e} are XR1 and XR2 at the top of the Chassis. The [[
]]^{a,c,e} is XN1 at the far right.

This figure also shows the connectors for individual Modules. Connector XM1 is for the [[
]]^{a,c,e} and appears on the right in the rear view. Two connectors (XA1 and XA2) are used for the AIM, AOM, DIM, and DOM. [[

]]^{a,c,e}

OCM port connectors XA1 – XA5 are used for RS-232 interfaces and XB1 – XB5 are used for RS-485 interfaces. Connector XM2 is not used.
Table 6-1 summarizes the qualified hardware components and the programmable logic configuration items that are included in the RadICS Platform to be qualified.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 102 of 350
--------------	--------------------	-----------	---	-----------------

**Table 6-1: Qualified Components**

Part Number	Description
A007.C00.V00.R00	Chassis Hardware
A001.C00.V01.R00	Logic Module Hardware
A001.FV00.FR01.CV01.CR00	LM Platform Electronic Design
A003.C00.V00.R00	Analog Input Module Hardware
A008.C00.V00.R00	I/O Interface Protection Module for AIM, AOM and DIM (Top)
A008.C01.V00.R00	I/O Interface Protection Module for AIM, AOM and DIM (Bottom)
A003.FV00.FR02.CV01.CR00	AIM Platform Electronic Design
A004.C00.V00.R00	Discrete Input Module Hardware
A004.FV00.FR01.CV01.CR00	DIM Platform Electronic Design
A002.C00.V02.R00	Analog Output Module Hardware
A002.FV00.FR02.CV01.CR00	AOM Platform Electronic Design
A006.C00.V00.R00	Discrete Output Module Hardware
A006.FV00.FR01.CV01.CR00	DOM Platform Electronic Design
A008.C02.V00.R00	DOM Interface Protection Module (Top)
A008.C03.V00.R00	DOM Interface Protection Module (Bottom)
A005.C00.V00.R00	Optical Communication Module Hardware
A008.C06.V00.R00	OCM Interface Protection Module
A005.FV00.FR02.CV01.CR00	OCM Platform Electronic Design
A014.C00.V00.R00	Ventilation Module Hardware
A011.FV00.FR00.CV00.CR00	Ventilation Module Electronic Design

The allocation of Modules to the slots is verified at startup to match the configuration defined in the Application ED. The LM compares information received from the I/O Modules with the expected configuration. The LM will prevent continued operation of the system by transitioning to the FAULTED mode.

All RadICS Modules can be removed or inserted while power is off. The Modules are also designed to be hot-swappable to prevent damage due to maintenance error.



6.2.3 Multiple Channels of RadICS

The basic set of Modules that can be used to create application with a choice of higher level redundant architectures that include 1-out-of-2, 2-out-of-3, and 2-out-of-4 configurations. The single channel Chassis is a common high level building block that is used for all of these configurations. Multiple Chassis can be used to extend a single channel configuration for scalability by connections between the OCMs for scalability expansion within a division and between LMs for coincidence voting in multi-division systems.

6.2.4 Overview of RadICS Chassis Interfaces

Four standard interfaces are used in the RadICS Platform:

- External Interfaces are used to communicate with another Chassis or specific device
- Internal Interfaces are used for on-board communications within a Module or for Module to Module communications within a Chassis
- Online Interfaces are interfaces that can directly influence a safety-critical system during normal operation
- Offline Interfaces are interfaces used for a safety-critical system configuration when it is out of operation

Table 6-2 shows a list of all existing interfaces of the Chassis and Modules including their classification.

Table 6-2: Classification of RadICS Chassis and Modules Interfaces

Interfaces/Type	External	Internal	Online	Offline
24 VDC Power Supply Interface	+	-	+	-
I/O Interface	+	-	+	-
Fiber Optic (RUP) Interface	+	-	+	-
Fiber Optic (RPP) Interface	+	-	+	-
Fiber Optic (RUP) Interface*	+	-	-	+
Safety Override Interface	+	-	+	-
RS-232/485 Interface	+	-	+	-
Address Interface (on-board jumpers)	-	+	+	-
Tuning Access Interface	+	-	+	-
LVDS Interface	-	+	+	-
Active Serial Programming Interface (ASPI) Interface	+	-	-	+
Joint Test Action Group (JTAG) Interface	+	-	-	+



Interfaces/Type	External	Internal	Online	Offline
Serial Peripheral Interface (SPI) Interface	+	-	+	-
Universal Asynchronous Receiver/Transmitter (UART) Interface	+	-	-	+
Watchdog Interface (voltage diagnostic data only)	-	+	+	-
Synchronous Static Random Access Memory (SSRAM) Interface	-	+	+	-
Real Time Interface	+	-	+	-

* - for tuning purpose

Figure 6-8 shows a high level block diagram of the Chassis and its associated external and internal interfaces.



[[

]]^{a,c,e}

Figure 6-8: RadICS Chassis Diagram with Internal and External Interfaces

6.2.4.1 RadICS Chassis External Interfaces

All external interfaces of the single channel Chassis are galvanically-isolated interfaces to components outside this Chassis. The Chassis external interfaces are:

- 24 VDC Power Supply Interface is used to provide [[]]^{a,c,e} to the Chassis. This power interface is safety related.
- I/O Interfaces are provided via connectors on the backplane for the field I/O connections to the I/O Modules and LM. [[

]]^{a,c,e}



- LM-to-MATS interface uses a [[]]^{a,c,e} using the Radiy User Datagram Protocol (UDP)-based interface protocol (RUP) for communications via fiber optical medium. This communication interface is safety related.
- Tuning interface with MATS Tuning PC uses [[]]^{a,c,e} using the proprietary Radiy Tuning Interface (RUP) via fiber optical medium. This communication interface is not safety critical.
- Tuning Access Interface provides a safety related [[]]^{a,c,e} to de-energize RUP Fiber Optic Interface. This communication interface is safety related.
- Safety Override Interface uses a safety related [[]]^{a,c,e}. The LM, AOM, and DOM are equipped with the SOR. When set the SOR will override the normal Application Logic outputs and put the affected Module outputs into the safe state. This communication interface is safety related.
- UART, ASPI, and JTAG Interfaces are special interfaces for [[]]^{a,c,e}. These communication interfaces are safety related.
- Inter-Chassis link uses the Radiy Proprietary Protocol (RPP) Fiber Optic Interface for safety critical communications that can be used to expand a RadICS Chassis up to a total of [[]]^{a,c,e} using OCM OPTO Units within a single division and with up to [[]]^{a,c,e} (e.g., four 2-out-of-4 voting channels) using the LM OPTO Units for connections between LMs in different divisions.

6.2.4.2 RadICS Chassis Internal Interfaces

The single channel Chassis also has internal interfaces that facilitate connections to the various Modules that are installed within the Chassis. These interfaces are at two levels: [[]]^{a,c,e}

- [[]]^{a,c,e} and is safety critical.
- [[]]^{a,c,e} This interface is not safety critical, because the [[]]^{a,c,e}. The [[]]^{a,c,e} is a non-safety interface to [[]]^{a,c,e}. The slot reserved for the LM has [[]]



function does not impact safety critical operation. The ^{a,c,e} on a local display unit located on the front panel of the Module. The ^{a,c,e} does not impact safety critical operation.

6.2.5 RadICS Hardware Modules

The RadICS Modules are implemented using common sub-modules or “Units” to the extent possible.

Module	Highest level Module within the RadICS Platform (e.g., LM, DIM, etc.)
Unit	Low to intermediate level module mounted on one or more Modules (e.g., LVDS transceiver, clock unit, etc.)

6.2.5.1 RadICS Module-Related Features

The aspects of each Module which relate to maintainability are all mounted on the faceplate of the Module as shown in Figure 6-9, with the deliberate exception of the JTAG connector, which is mounted so as to be inaccessible while the Module is installed in the Chassis.

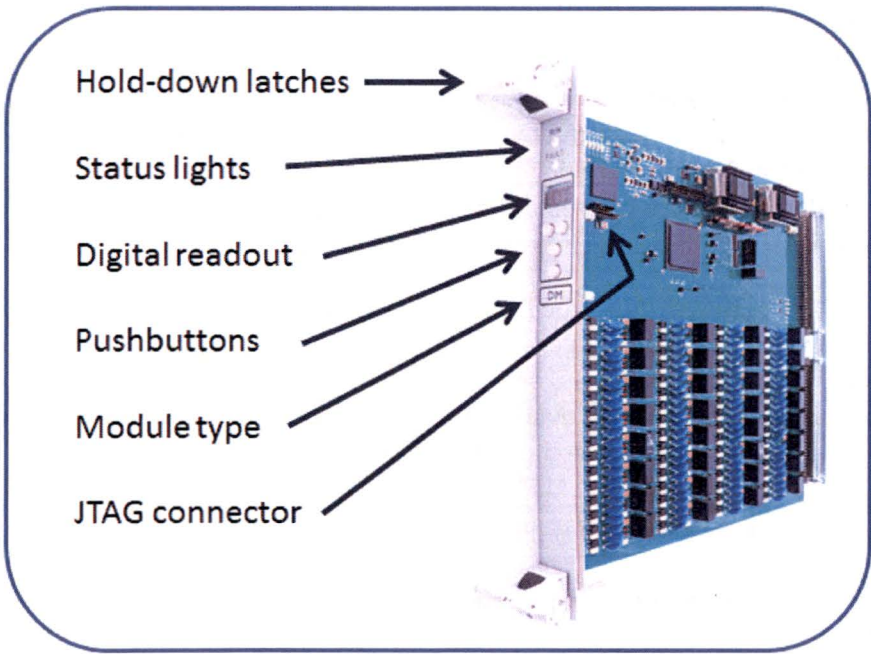


Figure 6-9: Maintenance Features of the RadICS Modules

This figure shows an enlargement of the hold-down latches in the closed/locked position.



There are RUN and FAULT status lights on every Module. The RUN light is on when the Module is running normally. The FAULT light illuminates if there is a failure within the RadICS Module detected by the self-diagnostics (i.e., this does not illuminate if the Platform or Application ED detect a field failure, such as a failed transmitter). The FAULT indication persists until power is removed, so a maintainer can respond to a maintenance order and expect to immediately identify the failed Module.

The digital readout provides two functions: more detailed display of a fault indication, mode status, and status indication used during configuration (downloading of a new electronic design) or during calibration (applicable only to certain Modules). The FAULT readout indication persists until power is removed or until a more serious failure is detected, in which case the more serious failure is displayed.

The pushbuttons allow a maintenance technician to navigate through the menu and to scroll all available fault codes. The pushbuttons also allow entry into CALIBRATION or CONFIGURATION mode (these modes are considered to be indistinguishable for safety purposes since the Module is treated as offline in either mode) only if the correct sequence of buttons is pushed in the first 20 seconds following application of power. After this time window, the pushbuttons are only read in CALIBRATION or CONFIGURATION mode.

Each Module carries a Module-type label that the maintenance technician must match against the slot label. This labelling reduces the likelihood of a maintenance error such as mixing up two Modules of different type when re-inserting them. Special coding pegs are provided for I/O Modules to prevent a RadICS Module from being inserted into the wrong slot. In any case the RadICS Platform will detect incorrectly located Modules during the STARTUP Mode self-diagnostic period.

The JTAG and ASPI connectors are not on the faceplate, but rather on the Module PCB, where they cannot be accessed except by removing the Module from the Chassis. Removal of the Module from the Chassis will cause the RadICS Platform to drive all safety outputs to the safe state. Since the ASPI connector (for FPGAs) and the JTAG connector (for CPLDs) are the only means to change the ED configuration of the Module, the system is protected from such errors whether accidental or intentional.

The normal procedure is to power down the RadICS Chassis before performing maintenance; however, all Modules are hot-swappable, so no damage will occur if a Module is extracted or inserted at power. Plant process safety is assured if this sort of action is performed, since any Module that has been removed will be identified as failed. Removal of the LM will force all output Modules to the safe state. When a replacement LM is inserted and completes its startup sequence, the LM will return to normal operation. The LM may be held in RUN (SAFE) mode until the SOR is reset unless it is hard-wired to be automatic. Removal of any I/O Module will also force all output Modules to the safe state.

6.2.5.2 RadICS Module Design Features

The RadICS Modules are designed with redundant components where needed to permit self-diagnostic tests. Data redundancies are used to permit detection of data corruption with very high probability. Watchdogs are incorporated on every Module. CRCs are used on all communications and safety-critical data. External communications links are all treated as 'black-channel'. Communications ports are monitored and blocked except when specifically required (e.g., tuning). The Modules perform self-

The general high level safety concept for the RadICS Modules employed to meet the target SIL (from IEC 61508) is that, no matter what configuration of Modules is used, an individual Module is designed such that failures that are both dangerous and undetected are limited to less than 10 percent. The RadICS Platform design target is to attempt to meet the same target for each Unit.

The interfaces to Units that are used on more than one Module are standardized. This design strategy maximizes the reuse of proven components and simplifies inter-operation of Modules. The ED of each Module performs self-diagnostics of the Units on the Module. The Units used to compose each Module are identified in Table 6-3.

Unit\Module	LM	DIM	DOM	AIM	AOM	OCM
[[
]] ^{a,c,e}
Communication Units						
[[



Unit\Module	LM	DIM	DOM	AIM	AOM	OCM
]] ^{a,c,e}

Figure 6-10 illustrates the typical Module architecture. The key differences between the various Modules are highlighted in the notes below the figure.



[[

]]^{a,c,e}

Figure 6-10: Typical RadICS Module Architecture

The purpose of each Unit is described below.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 112 of 350
--------------	--------------------	-----------	---	-----------------



6.2.5.2.1 FPGA Unit

The FPGA Unit is used to provide input data acquisition, perform the main functions of Module (e.g., data processing, Application Logic execution, etc.), diagnostics, output data conditioning, and data exchange with other Modules (within and beyond the Chassis). The ED of the FPGA is customized to perform the functionality of the specific Module type to meet both functional and integrity requirements specified for the Module.

A CRC check is applied to data transferred from the ASPI during STARTUP mode and a failure of this test prevents the LM from entering RUN mode.

6.2.5.2.2 Clock Unit

Clock Units are used to generate three separate clocks. Each clock has its own reference quartz oscillator: [[

]]^{a,c,e}, as shown in Figure 6-11. [[

]]^{a,c,e}

[[

]]^{a,c,e}

Figure 6-11: Data and Signals Exchange Between Different Clock Domains

Operation of the clock diagnostics is explained in Section 6.8.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 113 of 350
--------------	--------------------	-----------	---	-----------------



6.2.5.2.3 EEPROM Unit

The EEPROM Unit is used for storing different information that is needed for Module operation. The EEPROM Unit performs write/read by frames, data integrity checks, frames numeration checks, and data identification. EEPROM Units are divided into four categories according to the type of data stored:

- [[
]]^{a,c,e}
- [[
]]^{a,c,e}
- [[
]]^{a,c,e}
- [[
]]^{a,c,e}

All four types of EEPROM are used in the LM. Only the Service EEPROM is used on the DIM, DOM, AIM, AOM, and OCM.

[[
]]^{a,c,e}

6.2.5.2.4 Input Units

The Input Units are used to provide input data acquisition and directly interact with the I/O Interfaces. The Analog-to-Digital Conversion (ADC) Unit is galvanically isolated with active diagnostics and provides receiving one analog input signal that can be multiplied by installing a jumper. The DIU Unit is galvanically isolated with active diagnostics and provides for receiving discrete input signals and monitoring of the transmission path.

[[
]]^{a,c,e}

DIU Unit self-diagnostics are performed continuously to check the state of input switch for stuck on/off conditions. Diagnostic test results are reported to the LM and Application ED.

6.2.5.2.5 Output Units

The Output Units are used to provide output data conditioning and directly interact with I/O Interfaces. The Discrete Output (DOU) Unit is galvanically isolated with active diagnostics and provides for transmitting discrete output signals and monitoring of the transmission path. The Digital-to-Analog Conversion (DAC) Unit is galvanically isolated with active diagnostics and provides analog output signal



conditioning. Safe state of the output Unit is open output discrete signal for DOU and 0 V and 0 mA for DAC.

DOU Unit self-diagnostics are performed continuously to check the state of output switch for stuck on/off conditions. Diagnostic test results are reported to the LM and Application ED.

[[
]]^{a,c,e}

6.2.5.2.6 Safety Override Unit

The SOR Unit is used to provide a trip into the safe state of Modules by de-energizing the field-effect transistors in the Output Units, irrespective of Output Unit control signals from the FPGA Unit. The SOR Unit directly interacts with the Safety Override Interface. SOR performs the function to put the Output Units in the safe state independent of FPGA status or commands from it. The SET-SOR switch is used set the SOR. When the SOR is set, all application safety outputs are overridden and placed in the safe state by the RadICS Platform. The RESET-SOR switch is used to reset the SOR provided that no safety critical failures have been detected. The SOR allows the maintenance technician to quickly set all safety outputs to the safe state for any reason, and to restore the system when the work is complete. The use of the SOR Unit must be integrated with the user-specific actuation logic for energize-to-trip applications.

6.2.5.2.7 Power Supply and Watchdog Unit

The 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 galvanically isolated with the active diagnostics and used for power supply, watchdog timer, and voltage control with the active diagnostics. The PSWD Unit controls each output voltage, after its conversion, on operating range overrun deviations, as well as executes the FPGA operability control functions. The PSWD Unit receives a heartbeat signal from the FPGA Unit and [[

]]^{a,c,e}

Operation of the PSWD Unit is described in Section 6.8.

6.2.5.2.8 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. The LM identifier uniquely identifies LMs in the system for use with the MATS Tuning PC and for reporting different kinds of information to the MATS. [[



]]^{a,c,e}

6.2.5.2.9 Active Serial Programming Interface Unit

The 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, which includes FLASH memory, is used for writing, storing and reading of FPGA configuration. Access to the FLASH memory is provided only during project-specific manufacturing.

[[

]]^{a,c,e}

6.2.5.2.10 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. The Indication Board Unit can also indicate different kinds of service information for each Module type (e.g., unique LM identifier, identifier, onboard temperature, slot number, etc.). The Indication Board Unit can also be used to transition a Module to CONFIGURATION mode.

6.2.5.2.11 Synchronous Static Random Access Memory Unit

The SSRAM Unit is used for storing different temporary information needed for the Application Logic in the LM. The SSRAMU stores Application Logic netlist data, which is read from the AppNetlist EEPROM data in STARTUP and uploaded to SSRAM. Then it will be read each Work Cycle from SSRAM and processed.

[[

]]^{a,c,e}

6.2.5.2.12 Communication Units

The Communication Units are used to provide the data and data exchange within and between Chassis. The Communication Units use different protocols: RPP, RUP, and RS-232 based Protocol (RS-232). The LAN Unit is used for communication with peripheral devices (e.g., MATS). The OPTO Unit is used for optical transceiving with the same Unit in another Module of the same type. The LVDS Unit is used for point-to-point communication between two Modules within one Chassis. The RS-232/485 Unit is used for one-way communication with peripheral devices.



6.2.5.2.13 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. The Real Time Unit transmits real-time data received from an information technology system or the same data from timekeeping chip if original signal is lost to FPGA Unit.

The Real Time Unit does not affect any safety function performed by the LM. The time signal is not used by any safety function. The Real Time Unit uses of a dedicated data format that is distinct from formats used by safety critical logic and data so that safety logic would detect corruption of safety data by the time signal. The Real Time Unit is galvanically isolated.

6.2.5.3 Ventilation Module

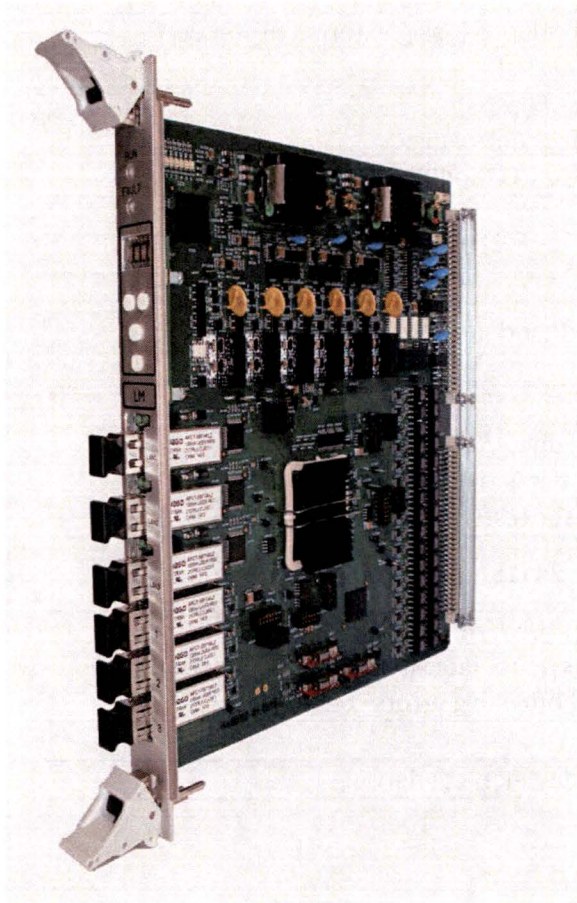
The RadICS Platform has Ventilation Module (VM) that is used for driving chassis fans. The VM performs only one function (i.e., driving fans) and does not exchange data with other RadICS Modules. The VM is controlled by a CPLD that processed data received from fans (e.g., indication of voltage and speed) and external devices (e.g., control switches and alarms indications). The VM can detect fan failures; however, this capability is not critical, since an unexpected fans stop will cause chassis internal temperatures to increasing, which are detected by other monitoring features, as described in Sections 6.2.5.2.7 and 6.8.

6.2.6 Hardware Module Specifications

The RadICS Hardware Modules are described in the following sections, which describe the technical specifications, operation, and failure detection and prevention for each Module.

6.2.6.1 Logic Module

The LM is used for data exchange with Modules in Chassis and Units within Module and execution of Application Logic specified by the end user's functional requirements.



LM Product Highlights

- Dedicated FPGA chip for user configurable control logic
- Integrity checks on each communication line
- 14 LVDS full duplex lines for communication with OCM and I/O Modules
- 3 galvanic-isolated discrete inputs (2 available, 1 reserved)
- 6 fast discrete outputs with embedded diagnostics of the outputs state
- 3 fiber optical lines for internal system communications
- 1 input for MATS Tuning PC programming access key signal
- 3 Fast Ethernet (100 BASE-FX) optical communication lines
- Hot swappable

6.2.6.1.1 LM Technical Specifications

The technical specifications for the LM are:

FPGA capacity	capacity to handle > 500 application blocks 260,000 logic elements for Platform ED
Memory	8,121 Kilobit (FPGA internal) 2,048 Kilobit (four external EEPROMs) 512 K*36 bits (external SSRAM)
Discrete inputs	24 VDC, 10 milliamp maximum, Form A "dry" contact with galvanic isolation between inputs
Discrete inputs overvoltage protection	up to 150 VDC continuous
Access key signal input	discrete signal (24 VDC, 0 to 10 milliamp) receiver with optic-isolation
Discrete outputs	"dry" contact: up to 48 V, 0.5 amp (AC/DC), galvanic-isolated by optic-relays



Discrete outputs overvoltage protection	up to +60 VDC/VAC continuous (using external protection elements installed in Chassis)
Control logic processing cycle	up to 5 milliseconds (for Chassis) up to 2.5 milliseconds for control logic up to 2.5 milliseconds for I/O Modules signals/data processing
Diagnostic cycle	up to 5 milliseconds
Ethernet / protocol	100 BASE-FX IP/UDP
LVDS line speed	100 Megabit/second
LVDS line protocol	proprietary protocol with integrity checking (CRC), galvanic- isolated Tx / Rx
Fiber optical lines speed	100 Megabit/second
Self-diagnostic functions	independent watchdog unit, I/O error detection, checksum analysis, active diagnostics with internal fault detection, continuous self-diagnostic tests, power supply fault detection
Power supply / consumption	2 independent inputs – 24 (18 – 36) VDC / 0.8 amp
Indications	2 status LED indicators (RUN/FAULT) 4-character dot matrix symbol-indicator for current operational mode, service info, and providing errors codes
Operating temperature	0 to 60 °C
Operating humidity	5 to 95% relative humidity, non-condensing

The functional diagram of the LM is shown in Figure 6-12.



[[

]]^{a,c,e}

Figure 6-12: Functional Diagram of the LM

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 120 of 350
--------------	--------------------	-----------	---	-----------------



6.2.6.1.2 LM Operation

The LM operation requirements are to:

1. Exchange data with other Modules within the Chassis and with LMs in other Chassis (e.g., channel voting),
2. Process and execute Application Logic specified by the end,
3. Transmit RadICS Platform diagnostic and Application ED processing data to the MATS, and
4. Provide means to change tuning values.

The LM operating modes and possible modes transitions are shown in Figure 6-13.

[[

]]^{a,c,e}

Figure 6-13: LM Mode Transition Diagram

In the POWERED-OFF mode the LM does not perform any functions. All Hardware Units are de-energized; all outputs are in the safe state; no data transmitted or received; and configuration and tuning changes are not allowed. The LM can transition to the STARTUP mode if the Module is energized.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 121 of 350
--------------	--------------------	-----------	---	-----------------



In STARTUP mode the LM performs the following functions:

1. [[

a,c,e

All functions of RUN mode are then performed, but a [[
]]^{a,c,e}. All data (i.e., self-diagnostics results, Application Logic values,
tuning values, presence/absence of all keys) are transmitted via Fiber Optic Interface to the MATS as in
RUN mode. In the [[
]]^{a,c,e}. After [[
]]^{a,c,e}, the LM will transition into [[

]]^{a,c,e} The LM can transition to the
[[
]]^{a,c,e} if the Module is de-energized.

In RUN (SAFE) mode the LM performs the following functions:

1. [[

]]^{a,c,e}

The LM can transition to the POWERED-OFF mode if the Module is de-energized. The LM can transition
to the [[
]]^{a,c,e}.
The LM will transition into [[



]]^{a,c,e}. The LM will also transition into [[
]]^{a,c,e}

In RUN mode the LM performs the following functions:

1. All Hardware Units are energized [[
]]^{a,c,e}
3. Module performs the following sequence of actions:
 - a. Input Data Receiving Phase:
 - [[

- b. Application Logic Processing and Configuration Phase:
 - [[

- c. utput Data Transmission Phase:
 - [[

- d. witch Time Phase:
 - [[

4. Performed periodically or constantly during all processes described above:
 - a. [[

]]^{a,c,e}



The LM can transition to the POWERED-OFF mode if the Module is de-energized. The LM will transition to the [[

]]^{a,c,e}. The LM will transition to the [[
]]^{a,c,e} are present. The LM will transition into [[
]]^{a,c,e}

In TUNING mode the LM performs the following functions:

1. [[

]]^{a,c,e}

4. The following actions are performed periodically or constantly during all processes described above:
a. [[

]]^{a,c,e}

5. MATS Tuning PC tests the password.

The LM can transition to the POWERED-OFF mode if the Module is de-energized. The LM will transition to the [[

]]^{a,c,e}. The LM will transition into [[
]]^{a,c,e}

In FAULTED mode the LM performs the following functions:

1. [[

]]^{a,c,e}

The LM can only transition to the [[

]]^{a,c,e}.

In CONFIGURATION mode the LM performs the following functions:

1. [[

]]^{a,c,e}

In CONFIGURATION Mode the LM can transition to the POWERED-OFF mode if the Module is de-energized. The LM will transition into [[

]]^{a,c,e}

6.2.6.1.3 LM Failure Detection and Prevention

The LM is designed to detect the following failures that are potentially dangerous unless revealed by self-diagnostics and reported to the Application Logic:

- [[

]]^{a,c,e}

The safety concept for the LM includes the following features:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 125 of 350
--------------	--------------------	-----------	---	-----------------



- [[

]]^{a,c,e}, as described in Section 6.4.2.

- [[

]]^{a,c,e}, as described in Section 6.4.

- [[

]]^{a,c,e}, as described in Section 6.4.3.

- [[



]]^{a,c,e}, as

described in Section 6.4.4.1.

- [[]]^{a,c,e}

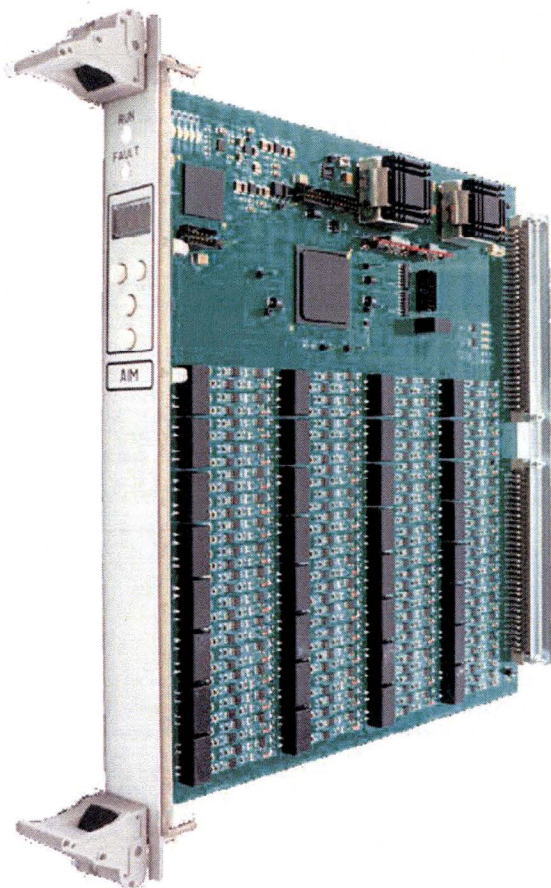
Module type	Fault type I	Fault type II	Fault type III
Input Modules (AIM, DIM, OCM)	[[]] ^{a,c,e}	[[]] ^{a,c,e}	[[]] ^{a,c,e}
Output Modules (DOM, AOM)	[[]] ^{a,c,e}	[[]] ^{a,c,e}	[[]] ^{a,c,e}
LM	[[]] ^{a,c,e}	[[]] ^{a,c,e}	[[]] ^{a,c,e}

† DBAL = Decided by Application Logic (i.e., Application Logic has to specify how to handle faults of I/O Modules).

Once an error condition has been detected, the error state continues to be reported on the Indication Board Unit and via the MATS until either power is removed or a higher level error is detected.

6.2.6.2 Analog Input Module

The AIM is used for the acquisition of analog signals (0 V to +5.1 V) and the conversion to engineering units. The AIM has 32 independent input channels.



AIM Product Highlights

- Enhanced I/O diagnostics
- 32 independent analog input channels
- 18-bit analog/digital (A/D) conversion in each analog input channel
- 2 LVDS full duplex lines (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Built-in calibration
- Hot swappable

6.2.6.2.1 AIM Technical Specifications

The technical specifications for the AIM are:

Input analog signal range	0 to +5.1 V (0 to 20 milliamp using external resistor installed in connection/junction box) Differential input impedance: not less than 1 MΩ.
A/D conversion resolution	18 bits / 400 kilo samples per second (kSPS)
Common mode rejection ratio	> 86 dB
Overall accuracy	0.1% of full scale for 0 to +5.1 V 0.15% of full scale for 4 to 20 milliamp
Input channel isolation	all input channels are galvanic-isolated up to 500 V _{RMS} AC or 707 VDC field-to-Chassis and channel-to-channel
Overvoltage protection	±60 VAC/VDC continuous (using external protection elements installed in Chassis)
Information package exchange cycle	5 milliseconds



Diagnostic package exchange cycle	5 milliseconds
LVDS line speed	100 Megabit/second
LVDS line protocol	proprietary protocol with integrity checking (CRC), galvanic-isolated Tx / Rx
Self-diagnostic functions	independent watchdog unit, I/O error detection, checksum analysis, active diagnostics with internal fault detection, continuous self-diagnostic tests, power supply fault detection
Power supply / consumption	2 independent inputs – 24 (18-36) VDC / 0.85 amps
Indications	2 status LED indicators (RUN/FAULT); 4-character dot matrix symbol-indicator for providing current operational mode, service information, and errors codes
Operating temperature	0 to 50 °C (32 to 122 °F)
Operating humidity	0 to 95% relative humidity, non-condensing

The functional diagram of the AIM is shown in Figure 6-14.



[[

]]^{a,c,e}

Figure 6-14: Functional Diagram of the AIM

6.2.6.2.2 AIM Operation

The AIM operation requirements are to:

- 1 Acquire analog signals from field sensors;
- 2 Filter and scale the analog signals; and
- 3 Perform data exchange with the LM.

The AIM operating modes and possible modes transitions are shown in Figure 6-15.



[[

]]^{a,c,e}

Figure 6-15: AIM Mode Transition Diagram

In the POWERED-OFF mode the AIM does not perform any functions. All Hardware Units are de-energized, no data transmitted or received, configuration changes are not allowed. The AIM can transition to the STARTUP mode if the Module is energized.

In STARTUP mode the AIM performs the following functions:

1. [[

]]^{a,c,e}

All functions of RUN mode are then performed, but a [[
]]^{a,c,e}. The AIM can transition to the RUN mode if the Module is energized. In the [[
]]^{a,c,e} After [[



]]^{a,c,e}, the AIM will transition into RUN mode or into [[
]]^{a,c,e}

In RUN mode the AIM performs the following functions:

- 1 All Hardware Units are energized
- 2 [[]]^{a,c,e}
- 3 Module performs two [[]]^{a,c,e} of actions:
 - a. Data Processing:
 - Input data acquisition from ADC Units
 - Scaling and filtering of input data
 - Comparison of processed input data
 - b. Data Transmission/Receiving:
 - Data transmission
 - [[]]

- Data receiving]]^{a,c,e}
 - [[]]

-]]^{a,c,e}
- 4 Performed periodically or constantly during all processes described above:
 - a. [[]]

]]^{a,c,e}

The AIM can transition to the POWERED-OFF mode if the Module is de-energized. The AIM will transition into [[]]^{a,c,e}

In FAULTED mode the AIM performs the following functions:

1. [[]]

]]^{a,c,e}

The AIM can only transition to the [[]]^{a,c,e}.

In CONFIGURATION mode the AIM performs the following functions:

1. [[]]



]]^{a,c,e}

In CONFIGURATION Mode the AIM can transition to the [[
]]^{a,c,e}. The AIM will transition into [[
]]^{a,c,e}

6.2.6.2.3 AIM Failure Detection and Prevention

The AIM is designed to detect deviations from the specified accuracy, execution of analog-to-digital conversion, or response time for the signals transmitted to LM. The data with detected errors are flagged as invalid. The safety concept for the AIM includes the following features:

- [[

]]^{a,c,e}, as described in Section 6.4.2.
- [[

]]^{a,c,e}, as described in Section 6.4.
- [[

]]^{a,c,e}, as described in Section 6.4.3.

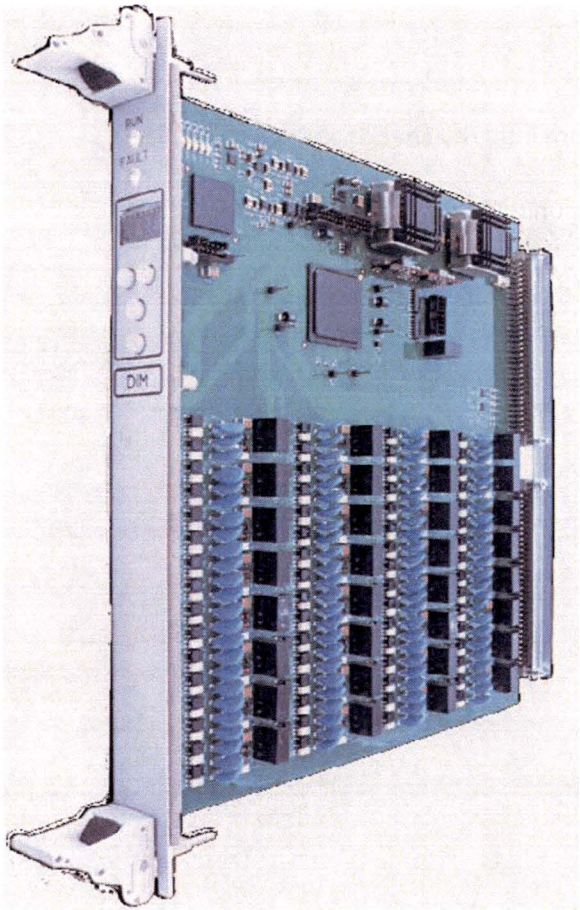
]]^{a,c,e}

Once an error condition has been detected, the error state continues to be reported on the Indication Board Unit and via the MATS until either power is removed or a higher level error is detected.



6.2.6.3 Discrete Input Module

The DIM is used for the acquisition of discrete dry contact signals via DIU Units and transmission to LM via LVDS Transceiver Unit. The DIM has 32 independent input channels.



DIM Product Highlights

- Enhanced input diagnostics
- 32 independent discrete input channels (“dry” contact type)
- 2 LVDS (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Hot swappable

6.2.6.3.1 DIM Technical Specifications

The technical specifications for the DIM are:

Internal power supply for each independent discrete input	24 VDC / 10 milliamp maximum (Form A “dry” contact)
Input channel isolation	all input channels are galvanic-isolated up to 500 V _{RMS} AC or 707 VDC field-to-Chassis and channel-to-channel



Input channel isolation method	Optic relay
Overvoltage protection	150 VDC continuous (using external protection elements installed in Chassis)
Information package exchange cycle	5 milliseconds
Diagnostic package exchange cycle	5 milliseconds
LVDS line speed	100 Megabit/second
LVDS line protocol	proprietary protocol with integrity checking (CRC), galvanic-isolated Tx / Rx
Self-diagnostic functions	independent watchdog unit, I/O error detection, checksum analysis, active diagnostics with internal fault detection, continuous self-diagnostic tests, power supply fault detection
Power supply / consumption	2 independent inputs – 24 (18-36) VDC / 0.6 amps
Indications	2 status LED indicators (RUN/FAULT); 4-character dot matrix symbol-indicator for providing current operational mode, service information, and errors codes
Operating temperature	0 to 60 °C
Operating humidity	5 to 95% relative humidity, non-condensing

The functional diagram of the DIM is shown in Figure 6-16.



[[

]]^{a,c,e}

Figure 6-16: Functional Diagram of the DIM

6.2.6.3.2 DIM Operation

The DIM operation requirements are to:

- 1. Acquire discrete dry contact signals and
- 2. Perform data exchange with the LM.

The DIM operating modes and possible modes transitions are shown in Figure 6-17.



[[

]]^{a,c,e}

Figure 6-17: DIM Mode Transition Diagram

In the POWERED-OFF mode the DIM does not perform any functions. All Hardware Units are de-energized, no data transmitted or received, configuration changes are not allowed. The DIM can transition to the STARTUP mode if the Module is energized.

In STARTUP mode the DIM performs the following functions:

1. [[

]]^{a,c,e}

All functions of RUN mode are then performed, but a [[

]]^{a,c,e}. In the [[

]]^{a,c,e}. After [[

]]^{a,c,e}, the DIM will transition into RUN mode [[

]]^{a,c,e}

In RUN mode the DIM performs the following functions:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 137 of 350
--------------	--------------------	-----------	---	-----------------



- 1. All Hardware Units are energized.
- 2. [[]]^{a,c,e}
- 3. Module performs the following sequence of actions:
 - a. Data Processing
 - b. Input data acquisition [[]]^{a,c,e}:
 - c. Data Transmission/Receiving:
 - Data transmission
 - [[]]

- 4. Performed periodically or constantly during all processes described above:
 - a. [[]]

]]^{a,c,e}

The DIM can transition to the POWERED-OFF mode if the Module is de-energized. The DIM will transition into [[]]

In FAULTED mode the DIM performs the following functions:

- 1. [[]]
-]]^{a,c,e}

The DIM can only transition to the [[]]

In CONFIGURATION mode the DIM performs the following functions:

- 1. [[]]

]]^{a,c,e}

In CONFIGURATION Mode the DIM can transition to the POWERED-OFF mode if the Module is de-energized. The DIM will transition into [[]]



6.2.6.3.3 DIM Failure Detection and Prevention

The DIM is designed to input data updates that are slower than the specified time or data corruption for the signals transmitted to LM. The safety concept for the DIM includes the following features:

- [[

]]^{a,c,e}, as described in Section 6.4.2.

• [[
]]^{a,c,e}, as described in Section 6.2.5.2.4.
• [[
]]^{a,c,e}, as described in Section 6.4.

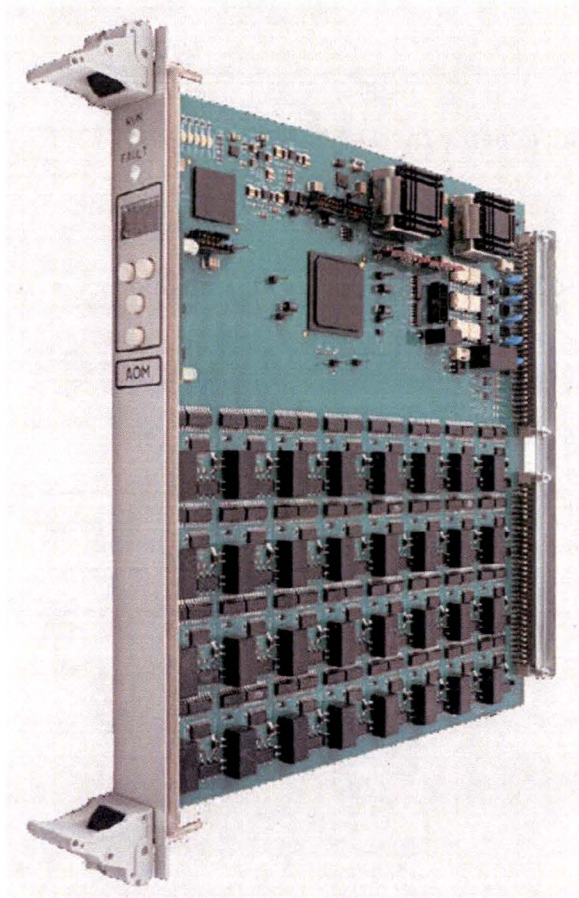
- [[
]]^{a,c,e}, as described in Section 6.4.3.

]]^{a,c,e}

Once an error condition has been detected, the error state continues to be reported on the Indication Board Unit and via the MATS until either power is removed or a higher level error is detected.

6.2.6.4 Analog Output Module

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



AOM Product Highlights

- Enhanced diagnostics of output channels
- 32 independent analog output channels
- 16-bit analog/digital (A/D) conversion in each channel
- 2 LVDS full duplex lines (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Built-in calibration
- Hot swappable

6.2.6.4.1 AOM Technical Specifications

The technical specifications for the AOM are:

Output range	0 to +5 V / 4 to 20 milliamp / ± 10 V / 0 to 5 milliamp
D/A conversion resolution	16 bits
Output signal value accuracy	0.15% of full scale
Maximum output load	up to 1.2 kilo ohm (k Ω) for current output minimum of 1 k Ω for voltage output
Internal power supply on each output channel	± 15 V / ± 35 milliamp
Output analog channel isolation	all output channels are galvanic-isolated up to 500 V _{RMS} AC or 707 VDC field-to-Chassis and channel-to-channel
Overvoltage protection	± 60 VAC/VDC continuous (using external protection elements installed in Chassis)
Output signal update cycle	5 milliseconds



Diagnostic package exchange cycle	Up to 250 milliseconds
LVDS line speed	100 Megabit/second
LVDS line protocol	proprietary protocol with integrity checking (CRC), galvanic-isolated Tx / Rx
Self-diagnostic functions	independent watchdog unit, I/O error detection, checksum analysis, active diagnostics with internal fault detection, continuous self-diagnostic tests, power supply fault detection
Power supply / consumption	2 independent inputs – 24 (18-36) VDC / 0.8 amps
Indications	2 status LED indicators (RUN/FAULT); 4-character dot matrix symbol-indicator for providing current operational mode, service information, and errors codes
Operating temperature	0 to 50 °C (32 to 122 °F)
Operating humidity	0 to 95% relative humidity, non-condensing

The functional diagram of the AOM is shown in Figure 6-18.



[[

]]^{a,c,e}

Figure 6-18: Functional Diagram of the AOM

6.2.6.4.2 AOM Operation

The AOM operation requirements are to:

- 1. Perform data exchange with the LM,
- 2. Process data received from LM, and
- 3. Condition control signals for DAC Units.

The AOM operating modes and possible modes transitions are shown in Figure 6-19.



[[

]]^{a,c,e}**Figure 6-19: AOM Mode Transition Diagram**

In the POWERED-OFF mode the AOM does not perform any functions. All Hardware Units are de-energized, no data transmitted or received, configuration changes are not allowed. The AOM can transition to the STARTUP mode if the Module is energized.

In STARTUP mode the AOM performs the following functions:

1. [[

]]^{a,c,e}



All functions of RUN mode are then performed, but a [[
]]^{a,c,e}. The AOM can transition to the [[
]]^{a,c,e}. In the [[
]]^{a,c,e}. After [[
]]^{a,c,e}, the AOM will transition into [[
]]^{a,c,e}

In RUN (SAFE) mode the AOM performs the following functions:

1. All HW Units are energized [[

]]^{a,c,e}

The AOM can transition to the POWERED-OFF mode if the Module is de-energized. The AOM can transition to the RUN mode [[

]]^{a,c,e}. The AOM will transition into [[
]]^{a,c,e}

In RUN mode the AOM performs the following functions:

1. All Hardware Units are energized.
2. [[
]]^{a,c,e}
3. Module performs the following sequence of actions:
 - a. Data Processing:
 - [[

]]^{a,c,e}

- b. ata Transmission/Receiving:
 - Data transmission
 - [[

]]^{a,c,e}

- Data receiving
 - [[

]]^{a,c,e}

4. Performed periodically or constantly during all processes described above:
 - a. [[



]]^{a,c,e}

The AOM can transition to the POWERED-OFF mode if the Module is de-energized. The AOM can transition to the [[

]]^{a,c,e}. The AOM will transition into
]]^{a,c,e}

[[

In FAULTED mode the AOM performs the following functions:

1. [[

]]^{a,c,e}

The AOM can only transition to the [[]]^{a,c,e}.

In CONFIGURATION mode the AOM performs the following functions:

1. [[

]]^{a,c,e}

In CONFIGURATION Mode the AOM can transition to the POWERED-OFF mode if the Module is de-energized. The AOM will transition into [[

]]^{a,c,e}

6.2.6.4.3 AOM Failure Detection and Prevention

The AOM is designed to detect deviations between the signals received from LM and actually conditioned output signals that exceed the specified accuracy or an output data conditioning process that exceeds the specified response time. The safety concept for the AOM includes the following features:

- [[

]]^{a,c,e}, as described in Section 6.4.2.

- [[

]]^{a,c,e}, as described in Section 6.4.2.

- [[

]]^{a,c,e}, as described in Section 6.4.



- [[

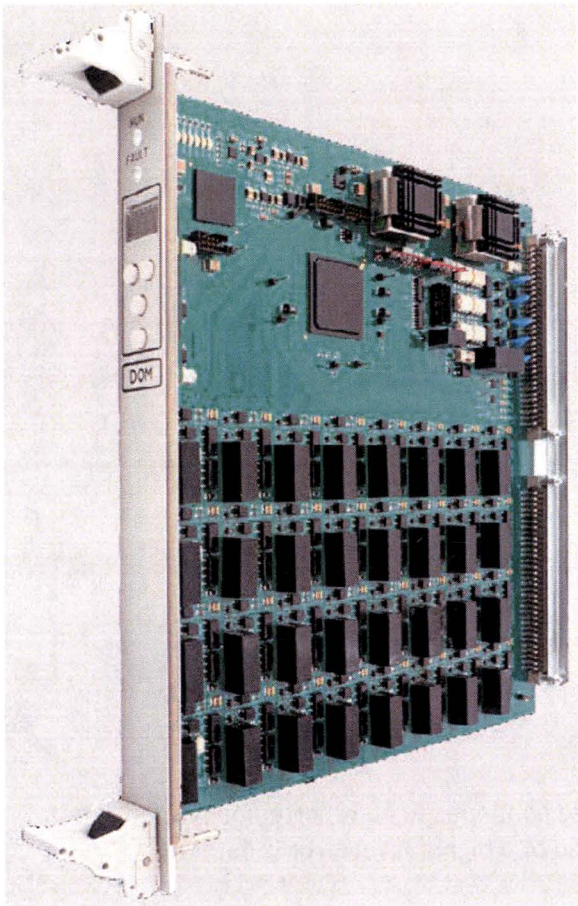
-]] ^{a,c,e}, as described in Section 6.4.3.
[[

]] ^{a,c,e}

Once an error condition has been detected, the error state continues to be reported on the Indication Board Unit and via the MATS until either power is removed or a higher level error is detected.

6.2.6.5 Discrete Output Module

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



DOM Product Highlights

- Enhanced active output diagnostics
- 32 independent digital form-A optic-relay isolated output channels (switching up to 48 VDC / 0.5 amp)
- 2 LLVDS (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Fuse and Overvoltage protected outputs
- Hot swappable

6.2.6.5.1 DOM Technical Specifications

The technical specifications for the DOM are:

Output channel load voltage / current (maximum switching voltage / current)	up to 48 VDC, 0.5 A, Form A contact
Output channel isolation	all output channels are galvanic-isolated up to 500 V _{RMS} AC or 707 VDC field- to-Chassis and channel-to-channel
Output channel isolation method	Optic relay
Output overvoltage protection	up to ±60 VDC/VAC continuous (using external protection elements installed in Chassis)
Information package exchange cycle	5 milliseconds
Diagnostic package exchange cycle	Up to 5 milliseconds



LVDS line speed	100 Megabit/second
LVDS line protocol	proprietary protocol with integrity checking (CRC), galvanic-isolated Tx / Rx
Self-diagnostic functions	independent watchdog unit, I/O error detection, checksum analysis, active diagnostics with internal fault detection, continuous self-diagnostic tests, power supply fault detection
Power supply / consumption	2 independent inputs – 24 (18-36) VDC / 0.4 amps
Indications	2 status LED indicators (RUN/FAULT); 4-character dot matrix symbol-indicator for providing current operational mode, service information, and errors codes
Operating temperature	0 to 60 °C
Operating humidity	5 to 95% relative humidity, non-condensing

The functional diagram of the DOM is shown in Figure 6-20.



[[

]]^{a,c,e}

Figure 6-20: Functional Diagram of the DOM

6.2.6.5.2 DOM Operation

The DOM operation requirements are to:

- 1. Driving of discrete dry contact signals and
- 2. Perform data exchange with the LM.



The DOM operating modes and possible modes transitions are shown in Figure 6-21.

[[

]]^{a,c,e}

Figure 6-21: DOM Mode Transition Diagram

In the POWERED-OFF mode the DOM does not perform any functions. All Hardware Units are de-energized, no data transmitted or received, configuration changes are not allowed. The DOM can transition to the STARTUP mode if the Module is energized.

In STARTUP mode the DOM performs the following functions:

1. All Hardware Units are energized [[



]]^{a,c,e}

All functions of RUN mode are then performed, but a [[
]]^{a,c,e}. In the [[
]]^{a,c,e}. After [[
]]^{a,c,e}, the DOM will transition into [[
]]^{a,c,e}

In RUN (SAFE) mode the DOM performs the following functions:

1. [[

]]^{a,c,e}

The DOM can transition to the POWERED-OFF mode if the Module is de-energized. The DOM can transition to the [[

]]^{a,c,e}. The DOM will transition into [[
]]^{a,c,e}. The LM will also transition into [[

]]^{a,c,e}

In RUN mode the DOM performs the following functions:

1. All Hardware Units are energized.
2. [[
]]^{a,c,e}
3. Module performs the following sequence of actions:
 - a. Data Processing:
 - [[
 - b. ata Transmission/Receiving:
]]^{a,c,e}
 - Data transmission
 - [[
 - Data receiving
]]^{a,c,e}
 - [[

]]^{a,c,e}



4. Performed periodically or constantly during all processes described above:

a. [[

]]^{a,c,e}

The DOM can transition to the POWERED-OFF mode if the Module is de-energized. The DOM will transition into [[

]]^{a,c,e}. The DOM will transition into
]]^{a,c,e}

[[

In FAULTED mode the DOM performs the following functions:

1. [[

]]^{a,c,e}

The DOM can only transition to the POWERED-OFF mode [[

]]^{a,c,e}

In CONFIGURATION mode the DOM performs the following functions:

1. [[

]]^{a,c,e}

In CONFIGURATION Mode the DOM can transition to the POWERED-OFF mode if the Module is de-energized. The DOM will transition into [[

]]^{a,c,e}

6.2.6.5.3 DOM Failure Detection and Prevention

The DOM is designed to detect deviations between the signals received from LM and actually conditioned output signals that exceed the specified accuracy or an output data conditioning process that exceeds the specified response time. The safety concept for the DOM includes the following features:

• [[

]]^{a,c,e}, as described in Section 6.4.2.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 152 of 350
--------------	--------------------	-----------	---	-----------------



- [[]]^{a,c,e}, as described in Section 6.4.
- [[]]

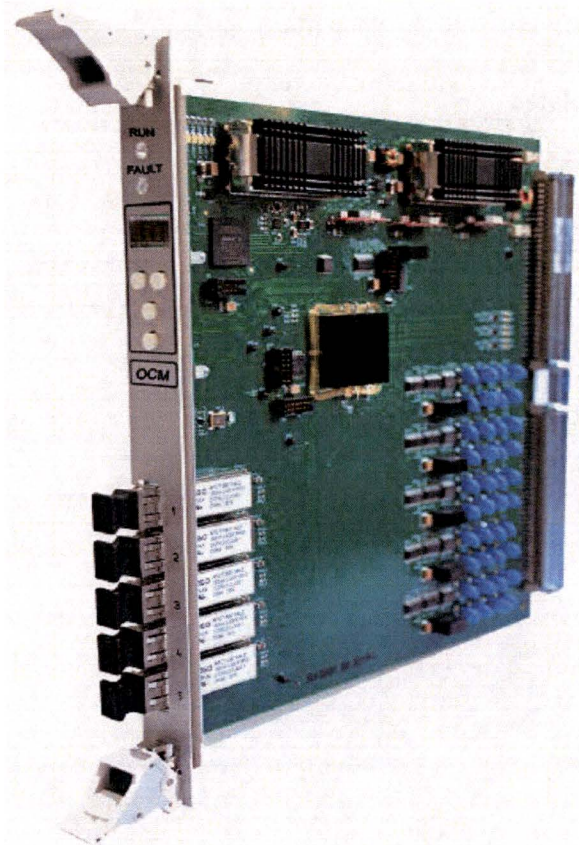
- [[]]^{a,c,e}, as described in Section 6.4.3.

]]^{a,c,e}

Once an error condition has been detected, the error state continues to be reported on the Indication Board Unit and via the MATS until either power is removed or a higher level error is detected.

6.2.6.6 Optical Communication Module

The OCM is intended for receiving and transmitting data via Fiber Optic (RPP) Interface that is used to extend the RadICS Platform to additional chassis, and for transmitting data via RS-232/485 Interfaces in a way that can be customized to be compatible with old systems. A pair of OCMs, which include OPTO Units, act as the isolating data transceivers between different Chassis (point to point communication). The OCM has five independent Optical Transceiver Units. Each of them performs transceiving data from/to other Chassis with OCMs. The OCM also has five independent RS-232/485 Transmitter Units to transmit data to older style monitoring systems.



OCM Product Highlights

- 5 fiber optical lines
- 2 LVDS lines (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Hot swappable
- 5 RS-232 or RS-485 serial communication interfaces

6.2.6.6.1 OCM Technical Specifications

The technical specifications for the OCM are:

Fiber optical lines type	optic full duplex
LVDS lines type	hardwired full duplex
Fiber optical lines speed	100 Megabit/second
LVDS lines speed	100 Megabit/second
RS-232 interfaces speed	up to 115,200 Bauds
RS-485 interfaces speed	up to 10 Megabit/second
RS-232/RS-485 interfaces protection	up to 28 V _{RMS} (line to line) up to 120 V _{RMS} (line to ground) power cross condition
Information package exchange cycle	5 milliseconds
Diagnostic package exchange cycle	5 milliseconds
Fiber optical line protocol	proprietary protocol with integrity checking (CRC), galvanic-isolated Tx / Rx



LVDS line protocol	proprietary protocol with integrity checking (CRC), galvanic-isolated Tx / Rx
Isolation	all lines are galvanic-isolated
Self-diagnostic functions	independent watchdog unit, checksum analysis, active diagnostics with internal fault detection, continuous self-diagnostic tests, power supply fault detection
Power supply / consumption	2 independent inputs – 24 (18-36) VDC / 0.4 amps
Indications	2 status LED indicators (RUN/FAULT); 4-character dot matrix symbol-indicator for providing current operational mode, service information, and errors codes
Operating temperature	0 to 60 °C
Operating humidity	5 to 95% relative humidity, non-condensing

The functional diagram of the OCM is shown in Figure 6-22.



[[

]]^{a,c,e}

Figure 6-22: Functional Diagram of the OCM

6.2.6.6.2 OCM Operation

The OCM operation requirements are to:

1. Perform data exchange via optical communications with other OCM Modules.
2. Perform data exchange with LM.
3. Perform information integrity check for each received data packet.
4. Provide data for external sinks via RS-232/485 Interface.

The OCM operating modes and possible modes transitions are shown in Figure 6-23.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 156 of 350
--------------	--------------------	-----------	---	-----------------



[[

]]^{a,c,e}

Figure 6-23: OCM Mode Transition Diagram

In the POWERED-OFF mode the OCM does not perform any functions. All Hardware Units are de-energized, no data transmitted or received, configuration changes are not allowed. The OCM can transition to the STARTUP mode if the Module is energized.

In STARTUP mode the OCM performs the following functions:

- 1. [[

]]^{a,c,e}

All functions of RUN mode are then performed, but a [[
]]^{a,c,e}. In the [[
]]^{a,c,e}. After [[
]]^{a,c,e}, the OCM will transition into RUN mode or into
[[
]]^{a,c,e}

In RUN mode the OCM performs the following functions:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 157 of 350
--------------	--------------------	-----------	---	-----------------



1. All Hardware Units are energized.
2. [[]]^{a,c,e}
3. Module performs the following sequence of actions:
 - a. Data receiving from LM and transmission to field:
 - Data receiving:
 - [[]]
 - Data transmission (identically for each of five OPTO Units):
 - [[]]
 - b. Data receiving from field and transmission to LM:
 - Data receiving (identically for each of five OPTO Units):
 - [[]]
 - Data transmission
 - [[]]
4. [[]]
5. Performed periodically or constantly during all processes described above:
 - a. [[]]

The OCM can transition to the POWERED-OFF mode if the Module is de-energized. The OCM will transition into [[]]

In FAULTED mode the OCM performs the following functions:

1. [[]]

The OCM can only transition to the [[]]

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 158 of 350
--------------	--------------------	-----------	---	-----------------



In CONFIGURATION mode the OCM performs the following functions:

1. [[

]]^{a,c,e}

In CONFIGURATION Mode the OCM can transition to the POWERED-OFF mode if the Module is de-energized. The OCM will transition into [[

]]^{a,c,e}

6.2.6.6.3 OCM Failure Detection and Prevention

The OCM is designed to detect incorrect data received (based on CRC) from LM or other OCMs. The data with detected errors are flagged as invalid. The safety concept for the OCM includes the following features:

- [[

]]^{a,c,e} as described in Section 6.4.2.

- [[

]]^{a,c,e}, as described in Section 6.4.

- [[

]]^{a,c,e}, as described in Section 6.4.3.

- [[



II^{a,c,e}

Once an error condition has been detected, the error state continues to be reported on the Indication Board Unit and via the MATS until either power is removed or a higher level error is detected.

6.3 Communications

The RadICS Platform includes various interfaces and protocols, including fiber optic interfaces and LVDS protocol for inter-Module and inter-Chassis connectivity purposes. The RadICS Platform communication features contribute to the predictability and repeatability of the design and satisfy the system integrity requirements of IEEE Std 603-1991 Section 5.5 and IEEE Std 7-4.3.2-2003 Sections 5.5.1 and 5.6. Additional aspects of the RadICS Platform communication independence features comply with DI&C-ISG-04, Revision 1 guidance regarding inter-divisional communication.

6.3.1 Basic Concepts

Physical and functional Independence of communication channels is achieved by selecting appropriate system architectures and data communication protocols. The implementation of radial (point-to-point) architecture in RadICS Platform interchannel communication links provides the RadICS Platform with the capability to maintain failure-free data exchange between I&C components even when one of the channels has failed. Additional measures designed to achieve the desired physical and functional independence are the application of fiber-optic communication lines for data exchange between I&C components and the separation of safety and control functions from information and diagnostic functions.

Three types of communication categories are defined for the RadICS Platform.⁸ They are as follows:

- White Channel - Communication channel in which all hardware and software components are designed implemented and validated according to IEC 61508. Implication: trusted safety channel
- Grey Channel - Communication channel with some evidence of design or validation according to IEC 61508. Implication: an untrusted channel which has some known design features which reduce the diagnostics needed to be able to trust the channel (e.g., point-to-point wiring rules out aliasing as a source of error)
- Black Channel - Communication channel without available evidence of design or validation according to IEC 61508. Implication: totally untrusted channel; all safety measures have to be taken by functions connected to the two ends of the channel

In the RadICS Platform architecture, all communications with other Modules within the same Chassis are based on dedicated slot-to-slot (point-to-point) connections between predefined specific slot locations. I/O Modules can communicate only with the LM within the same Chassis. Physically the Chassis and LVDS channel will support a LM Module in slot F1. This eliminates the need for any slot specific

⁸ IEC 61784-3:2010 has a description of white, grey and black channels (Reference 6-5)



addressing for I/O Modules. The LM also has a dedicated slot so that it does not require any additional address information to communicate with any other Modules within the same Chassis.

Each set of point to point communication paths between an I/O Module and the Chassis LM uses four physical lines to provide fully independent full duplex differential communications in both directions for each link. This link is the LVDS interface. The backplane communications is safety-related and designed as a SIL 3 black-channel.

The RadICS Platform architecture design eliminates the need for slot addresses since all communications within the Chassis take place using dedicated point to point connections between slot positions so that only two Modules have access to those signal paths. The participants in these communications are therefore uniquely identified without the possibility of cross interference, except by multiple physical short circuits between particular physical lines, which are nearly impossible to occur and would be detected if it occurred. Additional within-Chassis communications communication checking measures are implemented in the Platform ED. For example, inserted messages are detected by invalid sequence numbers and potentially protocol or media access violations. Corruptions and collisions would be detected by the packet level CRC. The communication error checking techniques are described in Section 6.4.3.

The FPGA Unit acquires input data, executes Module logic functions (e.g., data processing, Application Logic, etc.), performs diagnostics, and conditions output data. [[

]]^{a,c,e}

In general, all communications interfaces are treated as safety critical using the measures summarized below (the broadcast link to the MATS is not safety critical, but uses all of the measures below except acknowledgement). Table 6-4 summarizes all the links, the protocol used, and the safety criticality according to IEC 61508.

Table 6-4: Summary of Communications Links

Communication Link	Protocol	Safety Criticality
LM ↔ I/O Modules via backplane LVDS	RPP	[[]] ^{a,c,e}
OCM ↔ OCM via fiber optic cable	RPP	[[]] ^{a,c,e}
LM ↔ LM via fiber optic cable (to extend theRadICS capabilities (e.g., I/O expansion or processing expansion)	RPP	[[]] ^{a,c,e}



Communication Link	Protocol	Safety Criticality
LM \leftrightarrow OCM via fiber optic cable (to extend the RadICS capabilities (e.g., I/O expansion or processing expansion))	RPP	[[]] ^{a,c,e}
PSWD \leftrightarrow FGPA	RSWP	[[]] ^{a,c,e}
LM \rightarrow MATS via fiber optic cable (broadcast)	RUP	[[]] ^{a,c,e}
MATS Tuning PC \leftrightarrow LM via fiber optic cable (temporary connection)	RUP	[[]] ^{a,c,e}
UART interface used to download configuration data to and from EEPROM via FPGA in CONFIGURATION mode (temporary connection with Module removed from Chassis)	RPU	[[]] ^{a,c,e}
SPI interface used to download configuration data to EEPROM and to upload tuning parameter changes to Tuning EEPROM in TUNING mode	RSPE ⁹	[[]] ^{a,c,e}

Several additional measures are utilized for communications to support the RadICS fundamental safety approach.

- CRCs are used on all communications and safety-critical data. External communications links are all treated as 'black-channel'.
- Communications ports are monitored and blocked except when specifically required (e.g., tuning).
- The interface to the MATS is one-way broadcast (i.e., non-interfering), rated at SIL 2. Thus the MATS is also non-interfering. (Note: The MATS is supplied by the end user, to meet project-specific Human Factors requirements.)
- The RadICS Platform blocks all inward communications with the only exception being tuning inputs when put into TUNING mode by the keyswitch.
- Implementation of the lower levels of the transmission path between two OCMs is not relevant to analysis of safety communications based upon the black channel concept, since all necessary integrity measures are included as a part of the safety application level of the protocol.
- All communication links between OCMs are configured as point to point data exchanges with only one data source and one data sink.

⁹ RSPE – Radiy SPI-based Protocol for EEPROM



6.3.2 RadICS Communication Hardware Components

The basic RadICS communications interfaces and dedicated hardware Modules are described in Sections 6.2.4.2, and 6.2.6.6, and 6.3. This section describes how the board level communication components work. There are four board level communication components:

- OPTO Unit
- LVDS Unit
- LAN Unit
- RS-232/485 Unit

The primary purpose of these components is to enable data exchange within and between the RadICS Chassis as well as external devices. Several different communication protocols are utilized, as described in Section 6.3.3.

- Radiy Proprietary Protocol – RPP
- Radiy UDP based Protocol – RUP
- RS-232 based Protocol – RS-232
- Radiy Protocol for UART Interface (RPU)
- Radiy SPI-based Protocol for EEPROM (RSPE)
- Radiy Watchdog Interface Channel Level Protocol (RSWP)

Diagnostics of the components are performed through RadICS Platform ED by analyzing the data and the transmission protocols which are transmitted through each component. The fiber optic RUP Interface is de-energized, if the TUNING key is not in Tuning position and RadICS Platform is not in TUNING mode. All external communications links are optically isolated and the output to the monitoring station is non-interfering (one-way broadcast).

6.3.2.1 *Optical Transceiver Unit*

The OPTO Unit is used for optical transceiving with the same Unit in another Module of the same type. The OPTO Unit uses standard optical transceiving interface with associated optical isolation. The OPTO Unit converts electric signals to optical signals and vice versa, provides galvanic isolation for optical signals, and for signal transmission outside the Chassis. The OPTO Unit consists of a receiver and transmitter that provide full duplex communication, which may be maintained with other similar Units, located in other Modules or external to the system. All communication links of the OPTO Unit are executed according point-to-point principle between two different Modules. Every communication link has its own identification (i.e., address) to allow for detection of an incorrect connection between two devices. Each communication link identifier is unique within the whole system (i.e., not just one chassis). The OPTO Unit is safety related.

The OPTO Unit is considered a black-channel device so all data sent via this Unit is subject to the communications protocol for the link in question, which includes complete data validation by ED. The error detection methods are described in Section 6.4.



6.3.2.2 LVDS Transceiver Unit

The LVDS Unit is used for point-to-point communication between two Modules within one Chassis. LVDS provides galvanic isolation and converts the unidirectional discrete electric signal in the form of a differential signal using two symmetrical links. LVDS consists of a receiver and transmitter, providing full-duplex operation that may be supported with other similar Units, located in other Modules of the same Chassis. All communication links of LVDS are implemented on point-to-point principle between two different Modules. The given type of communication in RadICS Platform is used for data exchange between LM with I/O Modules and Optical Communication Modules within the Chassis. The LVDS Unit is safety related.

The LVDS Unit is considered a black-channel device so all data sent via this Unit is subject to the communications protocol for the link in question, which includes complete data validation by the RadICS Platform ED. The error detection methods are described in Section 6.4.

6.3.2.3 LAN Transceiver Unit

The LAN Unit is used for communication with a peripheral device (e.g., MATS or MATS Tuning PC). It uses RUP to transmit data to the MATS. When the LAN Unit is designated for use with a MATS Tuning PC, the Unit is in de-energized state except in the TUNING Mode. Dedicated protocols are used for specific purposes: RUP for the Tuning interface and RUP for the one-way broadcast to the MATS. A fiber-optic cable is used to galvanically isolate the LM from the external Unit. The LAN Unit is safety related.

The LAN Unit is considered a black-channel device so all data sent via this Unit is subject to the communications protocol for the link in question, including rejection of incoming transmissions where not allowed. The error detection methods are described in Section 6.4.

6.3.2.4 RS-232/485 Transmitter Unit

The RS-232/485 Unit is used for one-way communication with a peripheral device (e.g., data acquisition system). The RS-232/485 Unit uses the RS-232/485 Interface to transmit data. Dedicated protocols are used for specific purposes: RS-232/485 Interface (RPP). The RS-232/485 Unit is safety related.

The RS-232/485 Unit is considered a black-channel device so all data sent via this Unit is subject to the communications protocol for the link in question, including rejection of incoming transmissions where not allowed. The error detection methods are described in Section 6.4.

6.3.3 Communication Protocols

RadICS uses several types of data communication:

- Client-server (safety-related point-to-point as in the I/O Module response to interrogation by the LM)
- Broadcast (non-safety related as in the on-line reporting of plant data and RadICS Platform status to MATS)

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 164 of 350
--------------	--------------------	-----------	---	-----------------



- Transformational (as in a transceiver used for communication between LMs in the same division (safety-related) or between LM and MATS Tuning PC (non-safety related))

In all cases, two things are specified for the communications link to meet IEC 61508 requirements:

- Sequence of operations
- Data packet construction, including validation data and demonstration that it is of adequate capability to detect errors for the SIL target

Safety features of all communication interfaces used in the RadICS Platform are listed in Table 6-5.

Table 6-5: Safety Features of RadICS Communication Interfaces

[[

Interface ¹ (Channel Level Protocol)	Interface Features					
	Transport Level Protocol	CRC	Numerator	ID check	Timeout/ Acknowledgement	Others

Interface ¹ (Channel Level Protocol)	Interface Features					
	Transport Level Protocol	CRC	Numerator	ID check	Timeout/ Acknowledgement	Others

The RadICS Platform data transmission protocols are divided into two levels:

- Transport Level Protocols – intended to transmit (transport) fixed amounts of any data and to provide Channel Level Protocol organization; data integrity checks are part of protocol service data.
- Channel Level Protocols – intended to organize a data exchange channel with defined data structure; consist of multiple frames of Transport Level Protocols; data integrity check means can be present as part of data.

6.3.3.1 Transport Level Protocols

Transport Level Protocols are:

- RPP (Radiy Proprietary Protocol) – is basic for all in-Chassis and inter-Chassis communications
- RUP (Radiy UDP-based Protocol) – is used for communication with MATS and MATS Tuning PC
- RS-232 (Radiy RS-232-based Protocol) – is basic for communications with other equipment via RS-232 interface
- RPU (Radiy Protocol for UART Interface) – is basic for data exchange via UART interface with the DLS
- RSPE (Radiy SPI-based Protocol for EEPROM) – is basic for data exchange between FPGA and EEPROM

6.3.3.1.1 Radiy Proprietary Protocol

RPP is basic protocol for data exchange within Chassis and for inter-Chassis data exchange.

RPP has the following message structure:

[[

Field	Size (Words)	Offset	Description

]]^{a,c,e}

RPP has error detection methods based on the requirements in IEC 61508 Part 2, clause 7.4.11.

Error Type	Inherent Defenses	Added Defenses
Corruption	-	[[]] ^{a,c,e}
Unintended repetition	-	[[]] ^{a,c,e}
Incorrect sequence	Backplane: Lack of any storage mechanism in the black channel.	[[]] ^{a,c,e}
Loss	-	[[]] ^{a,c,e}
Unacceptable delay	-	[[]] ^{a,c,e}
Insertion	Point-to-point: there is no other signal source in any channel	[[]] ^{a,c,e}
Masquerade	Point-to-point: there is no other signal source in any channel	[[]] ^{a,c,e}
Addressing		[[]]

6.3.3.1.2 Radiy UDP-based Protocol

RUP is basic protocol for data exchange with external devices (e.g., MATS, MATS Tuning PC, etc.).

RUP has the following message structure:

[illegible]

Page 170 of 350



RUP has error detection methods based on the requirements in IEC 61508 Part 2, clause 7.4.11.

Error Type	Inherent Defenses	Added Defenses
Corruption	-	[[]] ^{a,c,e}
Unintended repetition	-	[[]] ^{a,c,e}
Incorrect sequence	Incorrect sequence of frames or transmission sessions is not crucial. Numerator affects only CRC to add dynamically changing parameter in case of static data.	[[]]
Loss	-	[[]]
Unacceptable delay	-	[[]] ^{a,c,e}
Insertion	-	[[]]
Masquerade	-	[[]]

6.3.3.1.3 Radiy RS-232-based Protocol

RS-232 is a one-way protocol and used for communications with old equipment via RS-232 interface. RS-232 uses standard UART protocol as a base without parity bit and bitrate of data transceiving is constant. The data bits are sent within each byte least significant bit (LSB) first. This standard is also referred to as "little endian". The data bytes are also sent within each word LSB first.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 171 of 350
--------------	--------------------	-----------	---	-----------------



RS-232 has the following message structure:

[[

[illegible]

11^{a,c,e}

6.3.3.1.4 RPU Radiy Protocol for UART Interface

RPU is basic for data exchange via UART interface with the DLS to download/upload data to/from FPGA internal RAM for further downloading/uploading to/from EEPROM.

RPU has the following message structure:

[[

	Offset (bytes)	Items	Descriptions	Size (Bytes)

]]^{a,c,e}



RPU has error detection methods based on the requirements in IEC 61508 Part 2, clause 7.4.11.

Error Type	Inherent Defenses	Added Defenses
Corruption	-	[[] ^{a,c,e}
Unintended repetition	Repetition is not dangerous. Same data will be re-stored in same addresses two or more times.	-
Incorrect sequence	Order in which data will be stored is not crucial. It is only crucial to store whole data package.	[[] ^{a,c,e}
Loss	-	[[]
Unacceptable delay	-	[[] ^{a,c,e} oss]]
Insertion	Point-to-point: there is only one source.	[[]
Masquerade	Point-to-point	[[] ^{a,c,e}

6.3.3.1.5 Radiy SPI-based Protocol for EEPROM

RSPE is basic for data exchange between FPGA and EEPROM.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 173 of 350
--------------	--------------------	-----------	---	-----------------



RSPE has the following message structure:

[[

	Offset (bytes)	Items	Descriptions	Size (Bytes)

]]^{a,c,e}

The read process is very simple. The RadICS Module FPGA specifies the frame number it wants to read. The frame number is transformed into an absolute EEPROM address offset. The EEPROM data frame includes the data and a CRC-64 checksum calculated that includes the frame address. Data integrity checks are performed during frame downloading, which include checks of the embedded frame address. RSPE has error detection methods based on the requirements in IEC 61508 Part 2, clause 7.4.11.

Error Type	Inherent Defenses	Added Defenses
Corruption	-	[[]] ^{a,c,e}
Unintended repetition	Repetition is not dangerous. Same data will be re-stored in same addresses two or more times.	-
Incorrect sequence	Order in which data will be stored is no crucial. It is only crucial to store whole data package.	[[]] ^{a,c,e}
Loss	CRC-64 calculated and uploaded to EEPROM with data will be used during the downloading process for integrity checking.	-
Unacceptable delay	See discussion for RPU Transport and SPIP Channel protocols.	[[]]
Insertion	Point-to-point: EEPROM and FPGA are hard-wired. No connector is present.	-
Masquerade	Point-to-point: EEPROM and FPGA are hard-wired. No connector is present.	-

6.3.3.2 Channel Level Protocols

Channel Level Protocols are protocols for each interface specified in Table 6-5. They all are based on Transport Level Protocols. The Channel Level Protocol is a sequence of Transport Level Protocol frames. The general approach to a channel level protocol is shown in Figure 6-24.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 174 of 350
--------------	--------------------	-----------	---	-----------------

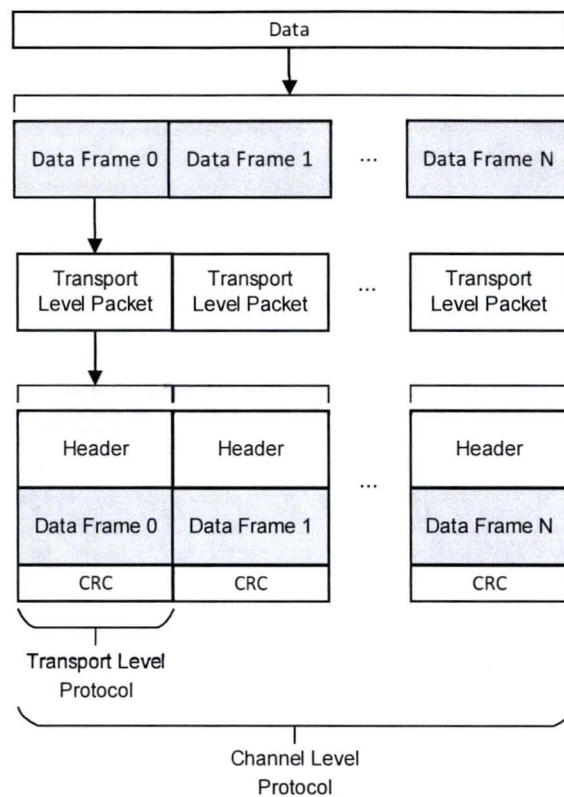


Figure 6-24: General Channel Level Protocol

The Channel Level Protocols are described below, except for the proprietary Altera protocols used to configure the RadICS Modules.

6.3.3.2.1 LVDS Interface Channel Level Protocol

LVDS Interface Protocol is based on RPP and is a sequence of RPP frames. It has all the functionality of RPP with the following additional error detection methods:

Error Type	Inherent Defenses	Added Defenses
Unacceptable delay		[[]] ^{a,c,e}

6.3.3.2.2 Fiber Optic Inter-Chassis Interface Channel Level Protocol

FOIP is based on RPP and is a sequence of RPP frames. It has all the functionality of RPP with the following additional error detection methods:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 175 of 350
--------------	--------------------	-----------	---	-----------------



Error Type	Inherent Defenses	Added Defenses
Unacceptable delay		[[]] ^{a,c,e}
Insertion	Point-to-point: there is no other signal source in any channel	[[]]
Masquerade	Point-to-point: there is no other signal source in any channel	[[]] ^{a,c,e}

6.3.3.2.3 Fiber Optic Monitoring Interface Channel Level Protocol

FOMP is based on RUP and is a sequence of RUP frames. It has all the functionality of RUP with the following additional error detection methods:

Error Type	Inherent Defenses	Added Defenses
Unintended repetition	Repetition is not dangerous. Same data will be re-stored in same addresses two or more times.	[[]] ^{a,c,e}
Unacceptable delay	No acknowledgement mechanism to prevent any control from MATS	[[]] ^{a,c,e}
Insertion	-	[[]] ^{a,c,e}
Masquerade	-	[[]] ^{a,c,e}

6.3.3.2.4 Fiber Optic Tuning Interface Channel Level Protocol

FOTP is based on RUP and is a sequence of RUP frames. It has all the functionality of RUP with the following additional error detection methods:

Error Type	Inherent Defenses	Added Defenses
Unintended repetition	Repetition is not dangerous. Same data will be re-stored in same addresses two or more times.	[[]] ^{a,c,e}
Unacceptable delay	-	[[]] ^{a,c,e}

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 177 of 350
--------------	--------------------	-----------	---	-----------------



Error Type	Inherent Defenses	Added Defenses
Corruption	-	[[]] ^{a,c,e}
Insertion	-	[[]] ^{a,c,e}

6.3.3.2.7 SPI Interface Channel Level Protocol

SPIP is based on RSPE and is a sequence of RSPE frames. It has all the functionality of RSPE with the following additional error detection methods:

Error Type	Inherent Defenses	Added Defenses
Incorrect sequence	-	[[]]
Unacceptable delay	Protocol delay is not dangerous because there are other mechanisms for delay checking. It is critical to read all the data stored in EEPROM without delays in STARTUP Mode. There are special mechanisms to control such delays outside the communication protocol (i.e., DiagData Controller - Fault Processing Block) and to trip the Module to FAULTED Mode (Level I fault).	-

6.3.3.2.8 UART Interface Channel Level Protocol

UICP is based on RPU and is a sequence of RPU frames. It has all the functionality of RSPE with the following additional error detection methods:

Error Type	Inherent Defenses	Added Defenses
Unintended repetition	Repetition is not dangerous. Same data will be re-stored in same addresses two or more times	[[]] ^{a,c,e}
Incorrect sequence	Is not dangerous. Order in which data will be stored is not crucial. It is only crucial to store whole data package. During STARTUP Mode, data is read and checked for integrity using CRC-64 calculated (including frame number). Important to write data to proper address with correct CRC-64.	[[]]



6.4 Platform Diagnostics

Each RadICS Module of RadICS Platform has built-in self-diagnostics capabilities. Automated tests are executed continuously during system operation. These tests include data integrity checking that is performed on each of the following general processes: data transmission, data reading/writing, and data processing.

Each RadICS I/O Module has its own diagnostic controller that gathers the internal diagnostic data and sends it to the LM. The LM diagnostic controller gathers the internal LM diagnostic data and sends it and the I/O Module diagnostic information to the MATS through a one-directional transmission line.

When a failure is detected, a generalized fault signal is sent to the MATS interface and other user specified alarm systems. These alarms allow maintenance personnel to quickly determine the place, time, character, and hazard degree of the failure.

The RadICS Platform self-diagnostic testing features are designed to be independent from the executing control functions. Performance of the self-diagnostic testing, as well as failures of self-diagnostic testing features, do not affect the performance of the rest of the RadICS Platform system, and do not deteriorate its performance. The self-diagnostic test results can have an effect on the RadICS Platform operation (e.g., Type I fault detection will transition a RadICS Module to FAULTED Mode).

Self-diagnostics are performed by both the Application and Platform ED levels and are aimed at different types of faults. Failures detected by either level that are potentially unsafe are converted to safe failures. The RadICS Modules perform the self-diagnostics and take safe-state action. This involves Application Logic where feasible (i.e., it is competent to take such action) to allow the end user to specify the actions taken in the event of certain failures. The Modules are designed with redundant components where needed to permit self-diagnostic tests and data redundancies are used to permit detection of data corruption with very high probability. The RadICS Platform detects the presence of non-safety Modules during the self-diagnostics at startup, and will maintain the safe state if any such Modules are detected.

Continuous automatic monitoring, as well as failures of the RadICS Platform diagnostic features do not affect the operation of the rest of the RadICS Platform system, and do not deteriorate its performance. This is attained due to the diagnostic features independent of the features executing control functions.

The RadICS Platform built-in self-diagnostics support the predictability and repeatability of the design, which satisfy the system integrity requirements of IEEE Std 603-1991 Section 5.5 and IEEE Std 7-4.3.2-2003 Sections 5.5.1, 5.5.3, and 5.6. The RadICS Platform built-in self-diagnostics capabilities facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment, which satisfy the repair requirements of IEEE Std 603-1991 Section 5.10.

6.4.1 General Diagnostics Concept

Techniques for safety integrity and functional safety assurance that are used in RadICS Platform can be divided into three main groups:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 179 of 350
--------------	--------------------	-----------	---	-----------------



- Hardware Self-Diagnostics
- Interfaces and Data Transmission Self-Diagnostics
- Platform EDs Self-Diagnostics

All self-diagnostic parts are integrated with each other. Figure 6-25 illustrates the self-diagnostics technique classification.

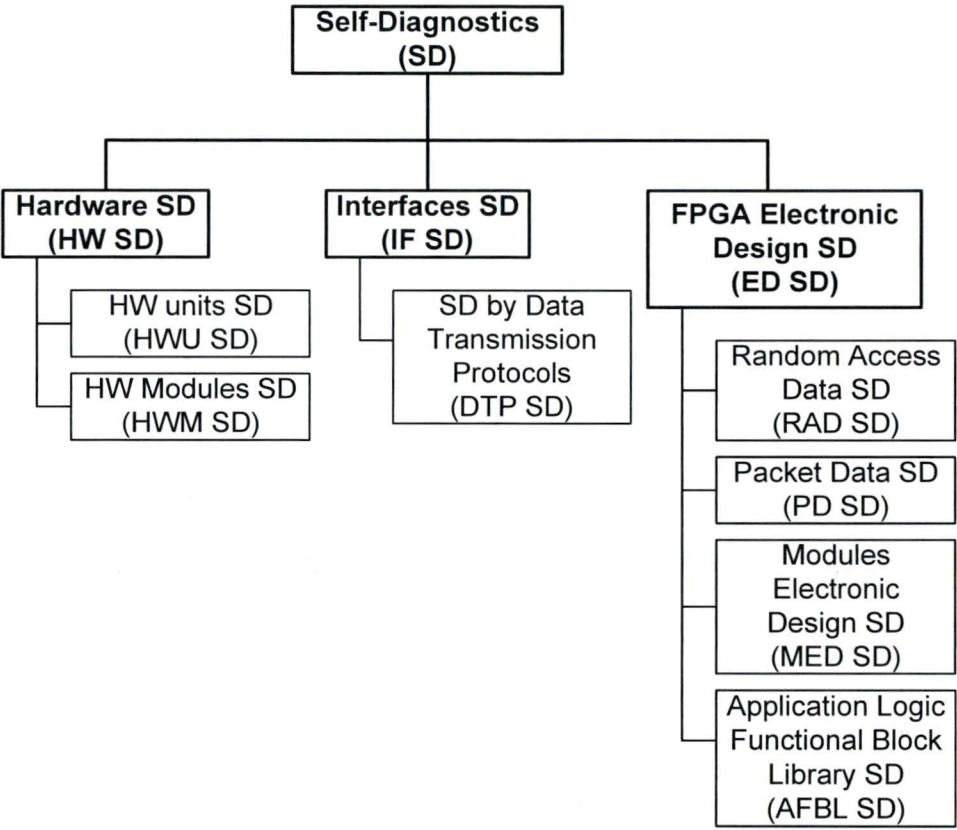


Figure 6-25: Self-Diagnostics Techniques Classification

HW SD includes the following:

- [[

]]^{a,c,e}

IF SD includes the following:

- [[

]]^{a,c,e}



Electronic Design Self-Diagnostics (ED SD) includes the following:

- [[

]]^{a,c,e}

Faults detected by self-diagnostics can be divided into three types at a Module level and at a system level.

At the Module level:

- Watchdog-detected Level Faults (Type I) – Platform control logic could not guarantee trip to safe state (e.g., a self-diagnostic test detects an FPGA fault). [[
]]^{a,c,e}
- Critical Level Faults (Type II) – Hardware or part of ED cannot properly perform its functions [[

]]^{a,c,e}

- User-defined Level Faults (Type III) – User defines criticality of detected errors and their processing algorithm (performed by Application Logic). Platform and Application ED can guarantee trip to safe state (e.g., an out-of-range input, a failed input channel, or a failed input Module (whatever the cause) in which case the Application Logic decides how serious the failure is).

At the system level:

- Input Module Faults – If an input Module suffers a Type III Fault, the Application Logic in the LM can decide (by Application Logic) how to manage it, as specified by the end user's functional requirements).
- Logic Module Faults – If the LM suffers a Type I or Type II fault, the error must be treated as a product level Type I fault and all outputs are driven to the safe state.
- Output Module Faults – If an output Module detects a Type I fault, it is de-energized and the LM will trip to the safe state when it detects the loss of communication with the de-energized output Module. If an output Module detects a Type II fault, it will drive its outputs to the safe state and report this to the LM. If an output Module detects a Type III fault, the Application Logic in the LM can decide (by Application Logic) how to manage it, as specified by the end user's functional requirements).

So, there are three ways to trip a RadICS system into a safe state. Each of them can perform trip of outputs. Figure 6-26 illustrates this safety feature.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 181 of 350
--------------	--------------------	-----------	---	-----------------

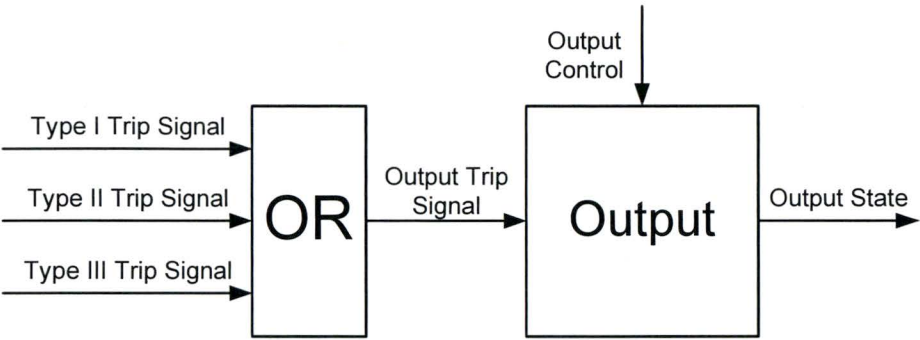


Figure 6-26: Ways Outputs Can Trip to Safe State

Table 6-6 lists faults detected by the RadICS Platform.

Table 6-6: Faults Detected by RadICS Platform

Fault Type	Detected Fault
Type I	<div><ul style="list-style-type: none">• [[</div> <div>]]^{a,c,e}</div>



DTP SD, due to the specific structure of each protocol, allow implementation of reliable IF SD. Each transmitted data packet includes the following data:

- [[

]]^{a,c,e}

The identification information in the transmitted data packets, which carries source and sink of information (i.e., Module type, protocol, protocol version, optical communication descriptor, etc.) allows for verification that the information was generated by a proper source, has an appropriate format, and sent to the correct will be accepted.

The numerator information in the packet allows for verification that all the received data packets refer to the same data transmission cycle. The numerator also introduces a dynamic parameter even in case of static data and allows finding static errors. Numerator monotony control allows for detection of missed data transmissions.

[[

]]^{a,c,e}

DTP SDs are implemented by ED SD facilities, as interfaces themselves are not able to implement necessary activities. DTP SD is assured by using the following techniques:

- [[

]]^{a,c,e}

In such a way each interface is covered by diagnostics to provide safety integrity and functional safety.

6.4.4 FPGA ED Components Self-Diagnostics

The RadICS Platform ED SD directly receives, processes, and conditions data for RadICS Platform operation. ED SD includes:

- Random access data self-diagnostics (RAD SD)
- Packet data self-diagnostics (PD SD)
- Modules electronic design self-diagnostics (MED SD)
- AFBL self-diagnostics (AFBL SD)
- Data Transmission Protocols (DTP SD)
- EEPROM data compatibility check



6.4.4.1 Random Access Data and Packet Data Self-Diagnostics

RAD SD is intended for random access data integrity diagnostics while transmission, storing, reading, and writing. The following characteristics are included in RAD SD:

- [[

]]^{a,c,e}

PD SD is intended for the packet data integrity self-diagnostics while transmission, storing, reading, and recording. The following characteristics are included in PD SD:

- [[

]]^{a,c,e}

6.4.4.2 Module Electronic Design Self-Diagnostics

MED SD includes several self-diagnostics techniques:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 185 of 350
--------------	--------------------	-----------	---	-----------------



- [[

]]^{a,c,e}

Application of RAD SD or PD SD to all the data within the ED provides self-diagnostics coverage for all PFBL elements that were used for the creation of the ED creating and through which data are transmitted (e.g., memory, multiplexer, controllers, etc.). The following characteristics are included in RAD SD or PD SD:

- [[

]]^{a,c,e}

Figure 6-27 shows how RAD SD is used for data path diagnostic coverage.

]]^{a,c,e}

Figure 6-27: RAD SD Usage for Providing MED SD

[[

]]^{a,c,e}. By this method, diagnostics on “stuck at” state of components and data paths are provided even with static input data.

DP2 diagnostics component implements the following functions:

- [[



]]^{a,c,e}

DP4 diagnostics component implements the following functions:

- [[

]]^{a,c,e}

Figure 6-28 shows how PD SD is used for data path diagnostic coverage.

[[

]]^{a,c,e}

Figure 6-28: PD SD usage for providing MED SD

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 187 of 350
--------------	--------------------	-----------	---	-----------------



DP5 and DP6 diagnostic components implement the following functions:

- [[

[[

]]^{a,c,e}



6.4.4.3 Application Logic Functional Block Library Self-Diagnostics

[[

]]^{a,c,e}

Figure 6-29: Approach for Assuring AFBL Integrity

6.4.4.4 Data Transmission Protocols

DTP SD is implemented by ED SD facilities, as interfaces themselves are not able to implement the necessary SD activities. DTP SD is assured by using the following techniques:

- [[

)]]^{a,c,e}



By using these methods each interface is covered by diagnostics to provide safety integrity and functional safety.

6.4.4.5 *EEPROM Data Compatibility Check*

A unique ID (i.e., 64-bit hash code) is stored in the Tuning, Application Netlist, and Configuration EEPROMs. These unique IDs are read during STARTUP mode and compared to ensure match for the chassis, as a safety critical function. They continue to be compared during other modes but these comparisons are not treated as safety critical.

6.5 *Redundancy*

The RadICS Platform modular architecture is convenient for building redundant systems. RadICS Platform provides for three kinds of redundancy management:

- Architecture-based active redundancy management: Safety I&C systems typically are comprised of several separate, independent divisions (typically three or four). Output signals from each division are issued through output boards into the hardware voting logic.
- Hardware-based active redundancy management: Redundancy is built into the hardware for inputs, outputs, and power supplies.
 - For inputs, the ADC Unit provides redundancy of input analog signal results after analog-to-digital conversion and Analog signal is also transmitted to redundant Unit for scaling and filtration and analog-to-digital conversion.
 - For outputs, the safety concept is based on 1-out-of-2 taken twice redundancy for de-energize to trip, plus testing of individual switches. To open the discrete output, all four switches are opened; however, at least one in each pair must open. Once a safety condition is detected by the application or the platform, all four outputs are de-energized.
 - For power supplies, the PSWD Unit receives redundant 24 VDC power supply and is used for its converting into the voltage levels (for example into +1.2 V, +3.3 V, etc.), necessary for all RadICS Module operation.
- Logic-based active redundancy management: The degree and architecture of redundancy is dictated by reliability requirements imposed on the application. The RadICS Modules can be configured as single channels, voting logic configurations, such as 2-out-of-3, 3-out-of-4, or variations of these configurations. Redundancy is also achieved by allocating the same functionality to main and standby processing units at the PCB level. The general design principle of this reconfiguration, and of the redundant architecture, is to comply with the single failure criterion provided in IEEE Std 379-2000 (Reference 6-6). This feature also improves system reliability and availability without degrading safety.

The criteria establish that no single failure will result in loss of any of the safety functions. RadICS Platform-based systems can be configured to meet these requirements using the standard RadICS

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 190 of 350
--------------	--------------------	-----------	---	-----------------



Modules, which will satisfy U.S. requirements for single failure tolerance defined in IEEE Std 603-1991 Section 5.1, RG 1.53 (Reference 6-7), and IEEE Std 379-2000.

6.6 Independence

The RadICS Platform and applications meet independence requirements by incorporating features to ensure, physical and functional separation between redundant devices performing safety functions. By implementing these design features, the RadICS Platform systems maintain their required safety functions in the presence of a single fault in any of their components.

The RadICS Platform design incorporates the following features: galvanic isolation and shielding of input, output and power supply circuits in each channel using electrical or optical isolation devices; physical separation (using distance, barriers, or both of them) between redundant channels, independent redundant power supplies, physical and functional separation of devices performing safety and non-safety functions.

Physical and functional independence of communication channels is achieved by selecting appropriate system architectures and data communication protocols. The implementation of radial (point-to-point) architecture in our interchannel communication links provides us with the capability to maintain failure-free data exchange between I&C components even when one of the channels has failed. Additional measures designed to achieve the desired physical and functional independence are the application of fiber-optic communication lines for data exchange between I&C components and the separation of safety and control functions from information and diagnostic functions. The interface to the MATS is one-way broadcast via a fiber optic link controlled by the RadICS Platform.

These independence features also satisfy U.S. requirements for independence defined in IEEE Std 603-1991 Section 5.6, RG 1.75 (Reference 6-8), and IEEE Std 384-1992 (Reference 6-9).

Physical and functional independence of functional elements on the Module FPGA is established for each channel and each monitoring element during the development of the ED AD for each RadICS Module. The functional elements include bond wires and pin-out and their own separated inputs and outputs that are not routed through another channel for functional element. The Project ED Design Procedure specifies that for each FPGA design element that requires physical and functional independence, create a logical design partition for that design element and assign the design partition to a LogicLock location constraint. These constraints are implemented using the Quartus II development tool.

The RadICS Platform independence features satisfy the independence requirements of IEEE Std 603-1991 Section 5.6 for the RadICS Platform equipment. The RadICS Platform isolation features also satisfy IEEE Std 384-1992, as endorsed by RG 1.75, Revision 3. The RadICS Platform communication independence features satisfy the system independence requirements of IEEE Std 7-4.3.2-2003 Section 5.6.

6.7 Safety Override Operation

The SOR is a supplementary safety function of the RadICS Platform that permits a temporary override to safe-state values of the safety-critical outputs of the system when the SOR is set and allows a return to

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 191 of 350
--------------	--------------------	-----------	---	-----------------



normal operation when the SOR is reset. The SOR may be used under administrative control to manually set RadICS Modules to a safe state while a maintainer is working in the rack. It can also be activated by the Application Logic, as specified by the end user's functional requirements.

The SOR can be set (i.e., outputs are set to the safe state) under any of several conditions, and can be reset only by operator (or hardwired) action when all setting conditions are clear.

The SOR is quite different from the FAULTED mode. In FAULTED mode, RadICS is irrevocably driven to the safe state, and this can be recovered only by powering down and powering-up the RadICS Chassis or LM. In contrast, the SOR can be reset by the operator as long as the setting conditions have been cleared. Every Module that contains output channels (e.g., LM, AOM, and DOM) includes the SOR capability.

The Set-SOR function always takes precedence over the reset SOR function.

The SOR is set globally (i.e., it affects all output Modules) under any of the following conditions:

- By RadICS Platform Logic during STARTUP mode
- By Application Logic, as specified by the end user's functional requirements
- By external hardware setting 2-out-of-3 of the Set-SOR input contacts to the LM and every DOM/AOM
- By external hardware setting 2-out-of-3 of the Set-SOR input contacts to the LM only. The LM communicates this to all output Modules.

The SOR is set locally (i.e., to affect only the specific output Module) under any of the following conditions:

- By Application Logic, as specified by the end user's functional requirements
- By external hardware setting 2-out-of-3 of the Set-SOR input contacts to 1 or more DOM/AOM

The SOR is reset globally under either of the following conditions:

- By closing the Reset-SOR input contacts to LM and all I/O output Modules one-time (momentary contact) and closing Set-SOR input contacts to LM and all I/O output Modules on continuing basis (continuous contact) or Set-SOR contacts stay closed (if setting SOR was performed by RadICS Platform ED).
- By closing the Reset-SOR input contact to the LM and closing Set-SOR input contacts if none of the SOR-setting conditions is currently set.

The SOR is reset locally under all of the following conditions:

- By closing the Reset-SOR input contacts and closing Set-SOR input contacts to the specific DOM/AOM or DOMs/AOMs if none of the global SOR-setting conditions is currently set, none of the local SOR-setting conditions is currently set, and the LM SOR is not set.

Figure 6-30 shows the functional diagram of the SOR Unit.



[[

]]^{a,c,e}**Figure 6-30: Functional Diagram of SOR Unit**

The set safety override inputs are normally “high” because the Set-SOR keyswitch is closed. When the operator opens the Set-SOR keyswitch, the safety override inputs drop and the flip-flop resets to open the power switch and de-energize the output Units connected to it. Similarly, a Set-SOR from the FPGA will also open the power switch and de-energize the output Units connected to it.

The 2-out-of-3 Set-SOR switch logic is used to provide immunity from spurious operation.

The use of the SOR feature can be remotely monitored from the control room and therefore there is an independent check that authorized access to the system is following safe practices.

The RadICS Platform SOR facilitates testing and timely replacement and repair of malfunctioning equipment, which satisfies the test, calibration, and repair requirements of IEEE Std 603-1991 Sections 5.7 and 5.10.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 193 of 350
--------------	--------------------	-----------	---	-----------------



6.8 PSWD Operation

The PSWD Unit receives redundant 24 VDC power supplies and converts them into the voltage levels necessary for Module operation. PSWD Unit can detect a failure of either 24 VDC source and use the operating one. PSWD Unit applies overvoltage protection for the voltages converted from the 24 VDC supplies. PSWD Unit provides diagnostics for power supply failures to the FPGA.

[[

]]^{a,c,e}

Figure 6-31 provides the functional diagram of the PSWD.

[[

]]^{a,c,e}

Figure 6-31: Functional Diagram of PSWD Unit



[[

]]^{a,c,e}

The Voltage Supervisor and Watchdog CPLD performs the following critical functions:

- [[

]]^{a,c,e}

PSWD design feature ensures that the critical PSWD Unit functions can be performed independently of FPGA failures. Every RadICS Module has a PSWD Unit.

The RadICS Platform PSWD Unit supports the predictability and repeatability of the design, which satisfies the system integrity requirements of IEEE Std 603-1991 Section 5.5 and IEEE Std 7-4.3.2-2003 Section 5.5.1.

6.9 Access Control Features

The RadICS Platform has the following features to fulfill the access control requirements:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 195 of 350
--------------	--------------------	-----------	---	-----------------



- RadICS Platform Chassis and cabinets with access control keys and alarm features
- Using unique identifiers for RadICS Modules to prevent substitution by malicious intention or by mistake

The keyswitches associated with a RadICS Chassis are shown in Figure 6-32. All of these contribute to preventing and detecting failures and maintenance errors.

The TUNING keyswitch is typically mounted on the RadICS Chassis and is connected directly to a dedicated contact input on the LM. The ARMED Keyswitch operates a dry contact supplied by end user is used by the RadICS Platform. It may be driven by any secure means (e.g., keyswitch). The dry contact is used to indicate that the end user downstream safety logic is secured in safe state. The ARMED key contact is connected to a designated input on LM. The keyswitches can be mounted anywhere that is convenient to the end user and consistent with their functions.

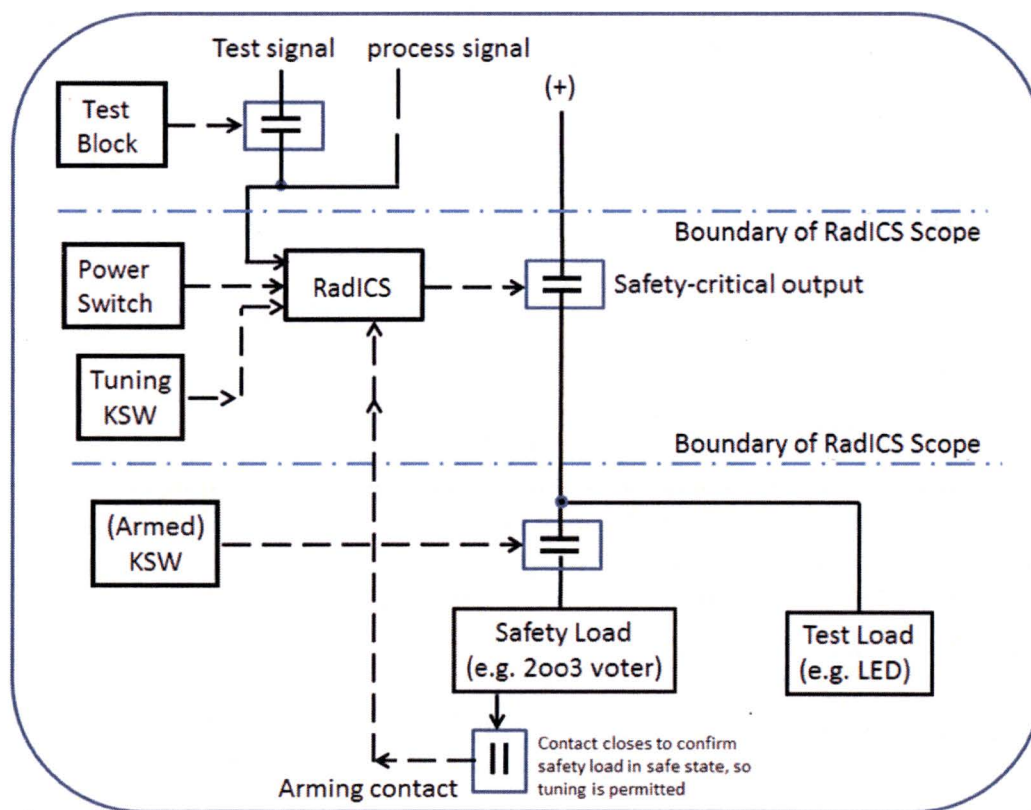


Figure 6-32: RadICS Keyswitch Access Control Features

The TUNING keyswitch is typically controlled by the control room staff. This keyswitch must be present and turned to the “tune” position for the RadICS Module to provide power internally to the designated



tuning port used to connect the MATS Tuning PC. The RadICS Platform logic reads this port only when the keyswitch is in the “tune” position. The tuning activity is signaled to the MATS in the control room.

The ARMED keyswitch is used to permit complete testing of single or multiple safety functions within the RadICS Platform system. The keyswitch is used to force all safety field outputs of the RadICS Platform to the safe state regardless of the state of the RadICS outputs. A contact from this logic is provided to the RadICS Platform to indicate the safety load is in the safe state. The end user uses the ARMED keyswitch to place the RadICS Platform field outputs in the safe state whenever tuning the RadICS Platform Application ED and to test the effects of the tuning changes before putting the RadICS Platform channel back online. The ARMED keyswitch circuit allows for complete testing by varying the input parameters through their complete range from non-trip conditions into trip conditions while the plant equipment is in the safe state at all times.

To enable the vendor to configure the RadICS Platform (i.e., to define the Application Logic to be implemented in the Module ED), there is an additional JTAG connector interface at the LM PCB. This interface is inaccessible when the Module is installed in a Chassis and it only allows configuration of the Application ED in an off-line mode. Removal of the Module from the Chassis will cause the RadICS Platform to drive all safety outputs to the safe state. Since the JTAG connector is the only means to change the Application ED configuration of the Module, the system is protected from such errors whether accidental or intentional.

The software used in configuring process of the RadICS Platform contains password protection features, as well as functions to check the successful completion of the configuration process.

The RadICS Platform control of access features satisfy the control of access requirements of IEEE Std 603-1991 Section 5.9.

6.10 Timing Diagrams and Working Cycles

The RadICS Platform performs initialization when the platform transitions from POWERED-OFF mode to STARTUP mode. Initialization time should take not more than $[[\quad]]$ ^{a,c,e}. After initialization, Work Cycles are performed cyclically. During a Work Cycle, all functions of the RadICS Platform are performed. A Work Cycle duration is $[[\quad]]$ ^{a,c,e}.

A RadICS Platform Work Cycle consists of the following Phases:

Input Data Receive (IDR)	Receive input data from the I/O Modules for the current Work Cycle and perform application test logic code.
Application Logic Processing and Configuration (AppLPrc and CFG)	Application Logic processing and generation of I/O Module data packets
Output Data Transmission (ODT)	Transmission of Application Logic processing results to the output Modules.
Switch Time (ST)	Switching time for the output Modules.



The timing allocations provided for each Phase are:

- $[[\quad]]^{a,c,e}$ is allocated to receive and transmit the data from the input Modules (i.e., AIM and DIM) to the LM. This time is allocated to implement a full cycle of input data processing (i.e., hardware operation, data processing, and transmission to LM). Application test logic code is performed during this time.
- $[[\quad]]^{a,c,e}$ are allocated for Application Logic processing in the LM. This time is allocated to execute Application ED (i.e., process input data and form output data).
- $[[\quad]]^{a,c,e}$ is allocated to transmit the results of Application Logic processing from LM to the output Modules (i.e., AOM, DOM, and OCM). This time is allocated to read the results of Application Logic processing from the LM output memory and transmit the data to the output Modules.
- $[[\quad]]^{a,c,e}$ is allocated for output Module switching. This time is allocated for switching of the output elements of the output Modules (e.g., field-effect transistors, relay, etc.).

The AFBL SD testing described in Section 6.4.4.3 is performed in all Phases except the Application Logic Processing and Configuration Phase.

The Work Cycle time parameters are different for each I/O Module because of differences in Module hardware and functionality, as shown in Table 6-7.

Table 6-7: Timing Requirements for RadICS I/O Modules

Module	Time Allocation	Parameters
AIM	$[[\quad]]$	$]^{a,c,e}$
DIM	$[[\quad]]$	$]^{a,c,e}$
AOM	$[[\quad]]$	$]^{a,c,e}$
DOM	$[[\quad]]$	$]^{a,c,e}$



Module	Time Allocation	Parameters
OCM	[[]] ^{a,c,e}

The operation timing diagram of a single RadICS Platform is shown in Figure 6-33.

[[

]]^{a,c,e}

Figure 6-33: Operation Timing Diagram of a Single RadICS Platform

The operation timing diagram for communication between two RadICS Platforms is shown in Figure 6-34.

[[

]]

Figure 6-34: Operation Timing Diagram for Two RadICS Platforms



Figure 6-34 demonstrates that one OCM-OCM communication between chassis adds to response time up to 5 milliseconds. If a signal passes through more than two chassis, then the timing can be calculated individually by keeping in mind that an OCM receives data from the LM in the ODT Phase and transmits data to the LM during the IDR phase.

The RadICS Platforms operate asynchronously with each other. Because of small variations in the platform clocks, it is possible that data from the sending platform may not be updated for the next Work Cycle of the receiving platform. This case can occur if the receiving platform is running slightly faster than the sending platform. In this case, the receiving platform may still have the old input data, which is outdated. It will take a second Work Cycle until updated (valid) data are processed. Consequently, the

]]^{a,c,e}

The RadICS Platform Work Cycle features support the predictability and repeatability of the design and satisfy the system integrity requirements of IEEE Std 603-1991 Section 5.5 and IEEE Std 7-4.3.2-2003 Section 5.5.1. The Work Cycle features also address the BTP 7-21 review guidance regarding allocation of system timing requirements to the digital computer portion of the system.

6.11 Periodic Testing

The RadICS Platform has extensive self-diagnostic testing features. These tests are supplemented by the following periodic tests that are typically performed during a refueling outage.

[[

]]^{a,c,e}. The RadICS Platform should run uninterrupted during this and

[[

]]^{a,c,e}

Test injection signals should be used to drive the input variables to the end of the instrumentation range at the safe end of the instrumentation range (i.e., apply conditions that do not trip the safety setpoint). The injection signal should be gradually increased (or decreased) until the setpoint trips to verify it meets requirements. The injection signal should be reduced (or increased) to below (or above) the trip setpoint to verify that the

]]^{a,c,e}. The injection signal should be driven to the high (or low) end of the instrumentation range to check the calibration of the signal.

[[



]]^{a,c,e}

The RadICS Platform periodic testing requirements satisfy the test and calibration requirements of IEEE Std 603-1991 Section 5.7.

6.12 Download Station

The DLS is physically a RadICS Platform Chassis that is identical to the in-service RadICS Platform Chassis that is installed as part of the safety-related I&C system. The DLS is used for:

- Downloading Application ED to the LM
- Calibrating an AIM
- Calibrating an AOM

The only configuration requirement for the DLS LM is that its Application Logic accept and require at least one of every type of RadICS Module used in the installed system. The DLS must accept such a Module in at least one slot so it can be calibrated. The convenient approach is to use the same configuration as the in-service RadICS Platform Chassis.

The RadICS Platform DLS satisfies the test and calibration requirements of IEEE Std 603-1991 Section 5.7.

6.13 Chapter 6 References

- 1 IEEE Std 1012-2004, "IEEE Standard for Software Verification and Validation Plans"
- 2 IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations"
- 3 IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
- 4 IEC IEC 61508-2010, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems," International Electrotechnical Commission
- 5 IEC 61784-3:2010, "Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions"
- 6 IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems"
- 7 Regulatory Guide 1.53, Revision 2, "Application of the Single-Failure Criterion to Safety Systems"
- 8 Regulatory Guide 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems"
- 9 IEEE Std 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits"



7 RadICS Platform Development Process

7.1 Overview of Safety Standards Used for RadICS Platform Development Process

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 IAEA Safety Standards reflect international consensus on what constitutes a high level of safety, and form the basis for the IAEA safety review services and assistance. They are intended for use by all organizations involved in the nuclear industry, including operating organizations, regulatory bodies, designers, and suppliers. Safety Guide IAEA NS-G-1.3, *Instrumentation and Control systems important to safety in nuclear power plants*, provides guidance on the design of I&C systems important to safety in NPPs, including all I&C components, from sensors to actuators and final elements, operator interfaces, and auxiliary equipment (Reference 7-1). This guide supplements Safety Standards Series No. NS-R-1, *Safety of Nuclear Power Plants: Design*, which establishes the design requirements for ensuring the safety of NPPs (Reference 7-2).

Safety Guide IAEA NS-G-1.3, *Software for Computer Based Systems Important to Safety in Nuclear Power Plants*, provides guidance on the collection of evidence and preparation of documentation to be used in the safety demonstration for the software for computer based systems important to safety in NPPs, for all phases of the system life cycle (Reference 7-3).

The IEC uses IAEA safety guides (mainly NS-R-1, NS-G-1.3, and NS-G-1.1) as guidelines for development of I&C systems important to safety. IEC standards provide guidance for the implementation in the design of basic safety principles.

IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, (Reference 7-4) outlines industry best practices to be followed during the entire lifecycle of programmable electronic systems in order to reduce the risk of systematic failures to an acceptable level. IEC 61508:2010 addresses all aspects of the lifecycle of electrical/electronic/programmable devices in safety-related applications, regardless of the technology (FPGA or other).

IEC 61513:2001, *Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems*, (Reference 7-5) establishes the relationship between NPP safety objectives, requirements for the overall architecture of I&C systems, and requirements of the individual systems important to safety. This standard uses the main principles of IEC 61508:2010 to introduce requirements applicable to computer-based I&C systems and equipment that are used to perform functions important to NPP safety.

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*, (Reference 7-6) addresses computer-based I&C software. IEC 60880:2006 addresses the following topics:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 202 of 350
--------------	--------------------	-----------	---	-----------------



- Introduces the concept of software lifecycle and details the concept of system safety lifecycle of digital systems given in IEC 61513 to the software portion of the I&C system
- Recommends good practices related to activities, such as: development of safety applications software, software verification processes, software modification, qualification and configuration control procedures, and tools application requirements
- Prescribes the adoption of I&C software development principles, such as: top-down design methods; the “V” model for software development; modularity; verification of each phase and clear and unambiguous documentation contents
- Details the I&C validation stage in IEC 61513:2001 to the software portion of the system and introduces software-specific issues to the validation process

IEC 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*, (Reference 7-7) sets out the general requirements for the hardware development life-cycle of computer-based systems. IEC 60987:2007 addresses the following topics:

- establishes requirements for the I&C systems hardware and aims at ensuring consistency between system and hardware requirements
- establishes requirements hardware development, including V&V

Taken together, IEC 61508, IEC 61513, IEC 60880, and IEC 60987 include requirements for the whole lifecycle of digital I&C systems and products. These standards are not I&C technology specific and are suitable for identification of requirements as applicable to FPGA based I&C systems at a general level.

Considering the growing trend of programmable devices in the nuclear industry, in 2006, IEC subcommittee 45A dealing with I&C for nuclear facilities, decided to create a new standard to establish requirements for the development processes to be applied to FPGA-based I&C systems performing Category A functions (equivalent to the U.S. safety-related functions). The first edition of IEC 62566, *Nuclear power plants – Instruments and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*, (Reference 7-8) was issued in 2011. IEC 62566:2011 addresses the following topics:

- Establishes requirements for each stage of the HPD lifecycle (requirements specification, design, implementation, verification, integration and validation) to develop highly reliable HPDs for use in I&C systems of NPPs performing safety category A functions
- Describes activities and guidelines to be followed in addition to requirements in IEC 61513:2001, for the system integration and validation of HPDs
- Adapts the basic safety principles from IEC 61508:2010 for the development of HDL-Programmed Devices
- Clarifies IEC 60880:2006 requirements taking into account FPGA specific features

Before IEC 62566 was published, RPC Radiy was already using many of the requirements in the development of the equipment dedicated as the RadICS Platform. RPC Radiy designers have analyzed and used many good practices that have been successfully applied in other safety critical domains (e.g., aerospace). These goods practices are described in RTCA/DO 254, *Design Assurance Guidance for*

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 203 of 350
--------------	--------------------	-----------	---	-----------------



Airborne Electronic Hardware, (Reference 7-9) an aerospace standard that highlights the processes and other non-technical aspects specific to FPGA-based systems.

Adherence to the above standards and the adoption of the best practices in the industry enables RPC Radiy to develop modern, safe, and reliable digital I&C systems.

The RadICS QAP and procedures are in line with the requirements and recommendations found in international and domestic regulatory documents and the RadICS staff is fully trained to follow them throughout the product life cycles, as described in Chapter 3.

7.2 Standard Requirements in the RadICS Life Cycle

All regulatory documents requirements and recommendations can be divided into two categories:

- Process oriented requirements: These describe processes, organizations, documentation, and concepts to be followed in order to achieve the desired safety levels and provide recommendations on how to avoid common mistakes and meet all established requirements.
- Mandatory safety and functional requirements: These are the main I&C safety and functional requirements that define the way the I&C system will operate and describe the NPP I&C mandatory features.

Between 1995 and 2011, RPC Radiy modernized their existing digital safety I&C technology, as described in Chapter 2. The equipment dedicated as the RadICS Platform is the third generation of nuclear I&C equipment developed by RPC Radiy. The RadICS Platform development life cycle defined in this chapter was designed to comply with international engineering practice for software for nuclear safety applications. As described in Chapter 4, the generic RadICS Platform is being commercially dedicated to demonstrate how the RadICS Platform ED life cycle processes comply with U.S. nuclear safety requirements. As described in Chapter 3, the dedication of the generic RadICS Platform is now maintained under a QAP that complies with 10 CFR Part 50 Appendix B.

The following equipment and software was developed for the RadICS Platform:

- Standardized Class 1E hardware Modules based on FPGA technology. The LM performs input module data acquisition, executes Application ED, and drives the output modules and process diagnostic data from all I/O Modules installed in the chassis. The I/O Modules provide interfaces with other devices (e.g., detectors, sensors, actuators, signalization devices). The functionality of each Module is driven by the ED implemented in the onboard FPGA(s).
- Standardized Class 1E EDs (i.e., programmable logic) for the FPGAs that perform the standardized functionality of the RadICS Modules
- A Class 1E FBL is used to standardize design activities, minimize the potential for human errors, and reduce the design time and cost of a RadICS Platform system while maintaining high quality. The FBL consists of pre-developed functional blocks used in the implementation of functions of a wide complexity range. Functional Blocks are written in VHDL. The FBL consists of two parts:
 - The RadICS PFBL which includes functional blocks used for the ED of the RadICS Modules (e.g., transceivers, diagnostic elements, etc.)
 - The RadICS AFBL which includes functional blocks used in the Application ED (e.g., logical, mathematical functions, time functions, etc.)

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 204 of 350
--------------	--------------------	-----------	---	-----------------



- A non-Class 1E set of tools integrated in a software development environment called RPCT. This tool can be used to configure EDs for various applications using the AFBL.

All ED associated with the RadICS Platform was developed or procured according to the RPC Radiy QMS. The RadICS Platform Class 1E ED originally was developed under the life cycle process that was established based on the guidance of the IEC 61508:2010. As described in Chapter 4, the generic RadICS Platform is being commercially dedicated to demonstrate how the RadICS Platform ED life cycle processes comply with U.S. nuclear safety requirements. As described in Chapter 3, the dedications of the generic RadICS Platform is now maintained under a QA program that complies with 10 CFR Part 50 Appendix B.

The RPCT tools were developed by RPC Radiy. RadICS also uses commercial off-the-shelf tools, as discussed in Section 8.3.

7.3 RadICS Platform Development Process

The RadICS Platform development process consists of three stages: high level system/platform design, Module ED development and implementation, and system integration and validation (including EQ for the RadICS Platform development).

The RadICS Platform safety life cycle model is described in Section 7.3.1. The RadICS Platform high-level design stage is described in Section 7.3.2. The Module ED and implementation stage is described in Section 7.3.3. The system integration and validation stage is described in Section 7.3.4. The RadICS project-specific system high-level design stage is described in Section 7.3.5.

The RadICS Platform EQ process is described in Chapter 9.

7.3.1 RadICS Safety Life Cycle

The RadICS Platform safety life cycle is based on the development model used in the IEC standards. The IEC model covers the complete cradle-to-grave life of a safety product or a safety system, as shown in Figure 7-1. The shaded parts apply to the design of a product, such as the RadICS Platform, that will be used in NPP safety-related systems.

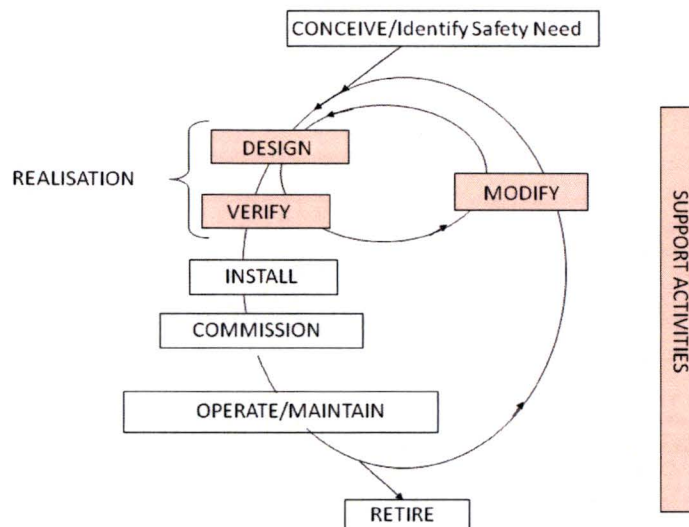


Figure 7-1: IEC Safety Life Cycle Concept

The RadICS Platform safety life cycle expands the design and verify phases to better define the pairing of design activities with the V&V activities for all the levels of design. It should be recognized that the V-model representation does not show well parallelism in the design process and looping required by V&V results. The overall RadICS Platform development lifecycle is shown in Figure 7-2. The figure also provides an overall context for the RadICS Platform development tasks. The product/system portion of the life cycle highlights the tasks that are largely independent of the use of FPGA technology. Similarly, the hardware portion of the life cycle recognizes that the RadICS Platform is built from hardware that has many design aspects that are unrelated to the use of FPGA technology. The Electronic Design portion of the lifecycle captures the development activities that are directly related to the use of FPGA technology. Support activities are activities and support services that have to be available for the complete life cycle and are not associated with any individual life cycle phase.

The activities in the RadICS Platform safety life cycle may not necessarily be continuous. For example, A4 starts early with planning of the all V&V activities, as documented in the Overall V&V Plan. After the Safety Requirements Specification (SRS) is written, the Validation Test Plan and Specification are prepared. The Test Specification may have to be modified after the Product Architecture Document (PAD) is issued. The Validation Test Report must wait until almost the end of the project.

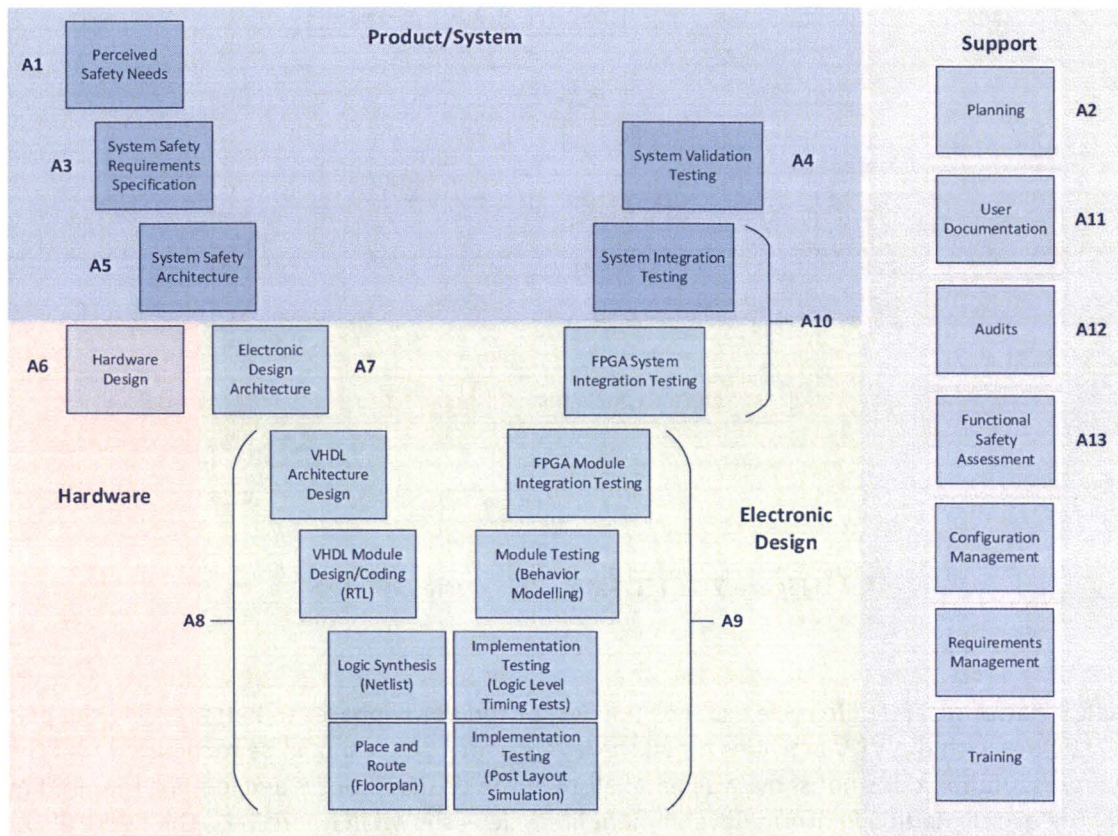


Figure 7-2: RadICS Safety Life Cycle

The RadICS Platform development activities tagged with the A label in the figure are described in Table 7-1. The RadICS Platform V&V process is described in Section 7.4. The RadICS Platform configuration management process is described in Section 7.5. The RadICS Platform requirements management process is described in Section 7.6. The use of quality metrics for RadICS projects is described in Section 7.7. The RadICS training activities are described in Section 7.8.

The process controls for the RadICS FBL development are described in Chapter 8.



Table 7-1: Summary of RadICS Life Cycle Development Activities

Label	Title	Description
A1	Perceived Safety Needs	<p>This Activity identifies the safety needs of the target or market industries and clients, and describes the RadICS product that will meet those needs and which RPC Radiy is willing to provide. The [[</p> <p>]]^{a,c,e}</p>
A2	Planning	<p>This Activity plans the work activities, the documentation required, configuration management, training, resourcing, and all the other support activities that must be present from [[</p> <p>]]^{a,c,e}</p>
A3	System Safety Requirements Specification	<p>This Activity starts the formal engineering work of designing the product. [[</p> <p>]]^{a,c,e}</p> <p>Validation is based on these requirements.</p>
A4	Validation Planning and Validation	<p>This Activity is executed in two parts: planning and testing. The planning part generates the Validation Test Plan and the Test Specification from the SRS. The testing part produces the Test Specification and the Validation Test Report near the end of the project realization phase.</p> <p>[[</p> <p>]]^{a,c,e} The Overall V&V Plan serves as the umbrella "Test Plan" for all other Test Plans and numerous Test Specifications. The Overall V&V Plan [[</p> <p>]]^{a,c,e}</p>



Label	Title	Description
A5	System Safety Architecture Design	<p>This Activity implements the requirements from A3. [[</p> <p style="text-align: right;">]]^{a,c,e}</p> <p>High-level integration (and testing) is based on the details of the architecture. [[</p> <p style="text-align: center;">]]^{a,c,e}</p> <p>Note: Software is used here in the sense of VHDL.</p>
A6	Hardware Design	<p>In this Activity, the architecture requirements for hardware, from A5, are applied to design and build the chassis and to design and populate PCBs [[</p> <p style="text-align: right;">]]^{a,c,e}</p>
A7	Electronic Design Architecture	<p>In Activity A5, the FPGA ED Safety Requirements Specifications and FPGA ED Safety Design are developed. [[</p> <p style="text-align: right;">]]^{a,c,e}</p> <p>This information is included in the ED Detailed Description (DD) document. Activity A7 is performed following the FPGA Electronic Design Development Procedure.</p>



Label	Title	Description
A8	Detailed Design and Coding	<p>A8 involves VHDL Detailed Design and VHDL module design and coding. [[]]^{a,c,e}</p> <p>Activity A8 is performed following the FPGA Electronic Design Development Procedure.</p> <p>Note: For VHDL design and test purposes, a “component” is a module or low-level integration of related modules</p>
A9	Electronic Design Functional Tests	<p>A9 is the lowest level of ED testing and includes [[]]^{a,c,e}</p> <p>Activity A9 is performed following the FPGA Electronic Design Development Procedure.</p>
A10	Integration Testing	<p>During A10, integration tests [[]]^{a,c,e}</p>
A11	User Documentation	<p>The prime output of A11 is the Product Safety Manual. [[]]^{a,c,e}</p>
A12	Audits	<p>This “phase” is an on-going support activity which is intended to verify at suitable intervals in the process, as defined in the [[]]^{a,c,e}</p>
A13	Functional Safety Assessment	<p>This phase is conducted by [[]]^{a,c,e}</p>



7.3.2 High Level Platform Design

A set of high-level design documents are produced during the RadICS Platform design process.

The Product Concept Document (PCD) is prepared by a multi-disciplinary team. It defines what product looks like, how it is to be used, and how it is positioned in the market.

The SRS is prepared by the safety and design teams. It applies integrity requirements from IEC 61508 and high-level functional requirements. It is developed as a black-box requirements document. The SRS is reviewed by personnel with the appropriate qualifications using safety requirements checklist to ensure the consistency and completeness of the document review. The checklist is used as a verification step for completeness and is maintained as a project record. The SRS is reviewed by a multi-discipline team. The results of the team review are documented in meeting minutes and all action items are tracked to closure.

The PAD defines the modularization of the design. It defines all interfaces and how possible failures are detected and mitigated. It documents how the SRS requirements are met. This RadICS PAD describes architecture of RadICS Platform. As specified in RadICS FSMP, PAD implements high level requirements presented in RadICS PCD and RadICS SRS. While PCD and SRS are the black-box documents, PAD is white-box and defines the internal structure of the product, providing design solutions for the requirements, and allocating the parts of the solution to the hardware, software, and FPGA/VHDL subsystems of the product.

The architectural design defines all functional blocks and their interfaces, as well as other information required for the detailed design development process. Reliability, traceability, and design verifiability requirements are defined at this stage.

The RadICS PAD identifies the overall system architecture in sufficient detail to illuminate potential failure modes and their impact on the safety of the system, and to document the requirements for counter-measures such as high-effectiveness diagnostics, and preventative design measures. It also identifies known safety integrity measures that can help to mitigate the impact of any dangerous failure modes and their effectiveness. It provides a top level view of the architecture on a qualitative basis.

The PAD is verified by conducting a System FMEA and the FMEDA. An FMEDA is one of the analyses that are performed to achieve functional safety certification of a device per IEC 61508. The FMEDA generates failure rates and the safe failure fraction. The FMEDA is maintained throughout the RadICS Platform lifecycle to reflect changes that come from downstream review or design changes. The FMEDA is used in the development of validation test cases, as described in Section 7.4.3.

The output of the architectural design requirements definition process is the textual or graphical description of the design partitioning of the above requirements among the system components. Upon completion of this design activity, a design review is performed, which may result in creating a modified design partitioning or correction of the initial requirements.

The PAD also provides software safety functional and software safety integrity requirements required to implement the safety concept. The identification of separate hardware and software requirements is

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 211 of 350
--------------	--------------------	-----------	---	-----------------



required by IEC 61508. The separation of requirements allows for separation of the hardware and ED white box testing.

The interrelation between these system documents is shown in Figure 7-3.

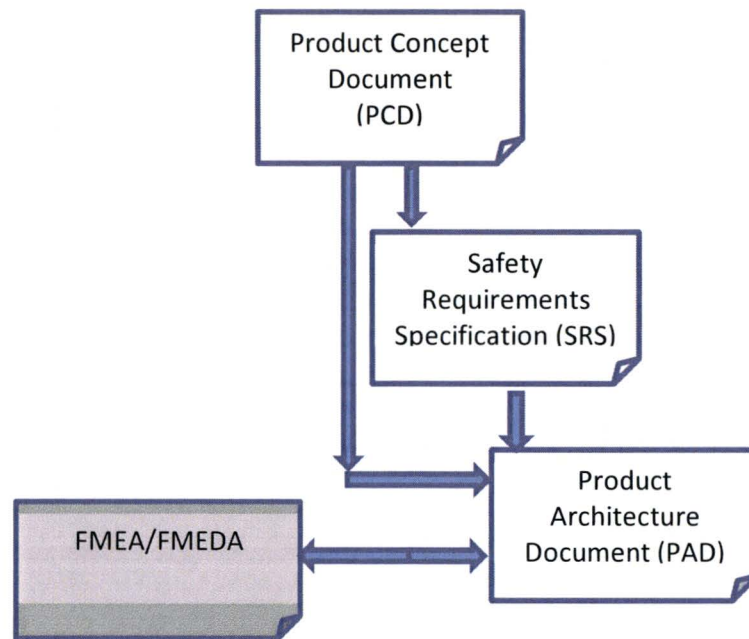


Figure 7-3: High-Level RadICS Platform Requirements Documents

7.3.3 RadICS Module Electronic Design and Implementation

RadICS develops I&C systems based on the pre-qualified RadICS Modules. The development cycle complies with requirements of IEC 62566:2011. IEC 62566 uses the term “HDL-Programmed Device (HPD)” for integrated circuit configured via HDLs.

The ED for the FPGAs on the standard RadICS Modules are developed using the “V cycle” model described in the IEC standards, as shown in Figure 7-2.

The electronic design development and V&V processes are two important processes in the lifecycle of FPGA-based I&C systems. The development process can be further divided into the design phase and the implementation phase. The final result of these two phases is FPGA electronic design integration. V&V supports the whole development process and is applied to the output of each development step with appropriate checks, comparisons, and analysis. The high-level documents are reviewed and approved before considering the subsystem or component levels.

The initial and the most critical step of the overall development process is the design process, which includes a preliminary (or architectural) design and detailed design. The preliminary design defines all

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 212 of 350
--------------	--------------------	-----------	---	-----------------



functional blocks (performing functions such as voting or simple mathematical operations), their interfaces and connections, and other information required in the next phase. At this step, such criteria as reliability, design traceability, and design verifiability are defined. The output of the preliminary design process is the textual or graphical description (diagrams) of design partitioning and other design requirements. Upon completion of this design activity, a design review is performed, which may result in creating a modified design partitioning or correction of the initial requirements.

[[

]]^{a,c,e}

These rules may support and assure different safety aspects of the design.

For the verification of detailed design outputs, [[
]]^{a,c,e}

The next important step is implementation, [[
]]^{a,c,e}. The appropriate procedures of V&V are connected with each activity of the implementation phase.

[[



II^{a,c,e}

Integration testing is intended to demonstrate that the electronic design implemented in the FPGA chip performs according to its specification and system architecture. This testing complements the integration testing accomplished by the ED Functional Testing (i.e., simulation). For the integration testing, the FPGA chip, which now has the integrated electronic design, is installed on the board for which it was developed. The inputs of the board are connected to a special test bench, which feeds them with input signals in accordance with testing stimuli. The outputs of the board are connected to a data acquisition system which collects the response of the board on input stimuli.

Output signals (response) are analyzed in accordance with pass/fail criteria.

The development tasks and output documents for the Platform EDs for the RadICS Modules are summarized in Table 7-2.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 214 of 350
--------------	--------------------	-----------	---	-----------------



Table 7-2: Generic RadICS ED Task Descriptions

HPD Lifecycle Stage	Task Description	Task Results	Standards Requirements
Life cycle and other general requirements for HPD projects	To develop planning document including: <ul style="list-style-type: none"> – FSMP – Configuration Management Plan – Overall V&V Plan – Document Plan Personnel Management Plan	FSMP and a set of supporting plans	IEC 62566 (2) IEC 61513 (5, 6.3) IEC 60880 (5) IEC 60987 (4)
[[
]] ^{a,c,e}			
HPD Requirements Specification	Based on system requirements a set of requirements for HPD Electronic Design is defined, including: <ul style="list-style-type: none"> – functions to be provided by the HPD, modes (such as POWERED-OFF, STARTUP, RUN (SAFE) mode, etc.) and transitions between these modes – I/Os, external interfaces requirements – parameters which can be modified during operation – performance requirements and restrictions – assumptions regarding the HPD environment – fault detection and diagnostics requirements 	Safety Requirements Specification Product Architecture Document	IEC 62566 (6.1 - 6.4) IEC 61513 (6.2.2, 6.2.3, 6.4.2, 6.4.3) IEC 60880 (6) IEC 60987 (5)
HPD Requirements Specification Review	Completeness and compliance of HPD requirements with system requirements are verified after HPD requirements specification phase.	SRS Review Report PAD Review Report	IEC 62566 (6.6) IEC 61513 (6.4.2.3, 6.4.3.3) IEC 60880 (software aspects)



HPD Lifecycle Stage	Task Description	Task Results	Standards Requirements
II			
HPD ED Design	Based on HPD Requirements Specification Document, required system functions (specific system behavior) are defined using pre-developed blocks (application related functional blocks) which are provided as a FBL. Integration of application related functional blocks is done in accordance with HPD Requirements Specification	FPGA / CPLD Electronic Design Detailed Description	II ^{a,c,e}
			IEC 62566 (8.3, 8.6)
			IEC 61513 (6.2.4, 6.4.3)
			IEC 60880 (7)
HPD ED Design Review	To examine ED DD implementation	ED DD Review Report	IEC 60987 (6.1-6.7, 6.9)
			IEC 62566 (8.7)
			IEC 61513 (6.4.4.4)
HPD Implementation	Logic synthesize the gate-level description (netlist) of the HPD, then place and route (floor plan) is performed and results in the physical description needed to produce the HPD, such as HPD programming file or bitstream file. Implementation of bitstream file in HPD.	ED DD build (bitstream *.pof) files with associated documentation HPD with implemented bitstream file	IEC 60880 (8.2.2)
			IEC 62566 (8.4)
			IEC 61513 (6.2.4)
			IEC 60880 (7)



HPD Lifecycle Stage	Task Description	Task Results	Standards Requirements
HPD Verification	To implement systematic V&V process for each of the stage of HPD life cycle	Overall V&V Plan VHDL Static Code Analysis / Code Review Reports VHDL Functional Test Plans and Specifications VHDL Functional Test Reports ED Logic Level Simulation and Timing Test Reports ED Static Timing Analysis Test Reports	IEC 62566 (9) IEC 61513 (6.3.2.2) IEC 60880 (8.1, 8.2.1, 8.2.3) IEC 60987 (7.1-7.7)
HPD System Integration	System integration involves all the activities necessary to ensure that the programmable and non-programmable components to work together as a system.	Integration Test Plan	IEC 62566 (10.1 – 10.3) IEC 61513 (6.2.5, 6.4.5) IEC 60880 (9.1, 9.2, 9.4) IEC 60987 (7.8)
HPD Integration Testing	Integration testing is performed to check internal and external system interfaces, as well as system functions.	Fault Insertion Test Plan, Specification and Report Integration Test Plan, Specification, and Report	IEC 62566 (10.4 - 10.6) IEC 61513 (6.4.5.3) IEC 60880 (9.3, 9.5)

NONPROPRIETARY



HPD Lifecycle Stage	Task Description	Task Results	Standards Requirements
System Validation	Validation is performed to check compliance of whole system with initial system requirements specification. This is mainly a black box type of test.	Validation Test Plan, Specification, and Report	IEC 62566 (11) IEC 61513 (6.2.6, 6.4.6) IEC 60880 (10) IEC 60987 (7.9)

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 218 of 350
--------------	--------------------	-----------	---	-----------------



7.3.4 RadICS System Integration and Validation

System integration involves all the activities necessary to ensure that the programmable and non-programmable components to work together as a system. Integration testing is performed to check internal and external system interfaces, as well as system functions. Validation is performed to check compliance of whole system with initial system requirements specification. Validation is mainly a black box type of test.

7.3.5 Project-Specific Application Process

Project-specific applications are developed using the RadICS Platform components and consists of configuring the RadICS Modules, Chassis, and Cabinets to perform the required system functions. The hardware design is reduced to choosing the required amount and type of cabinets, chassis, and modules in accordance with the system requirements specification.

A set of high-level design documents are produced to develop a project-specific I&C system using the standard RadICS Modules. Before starting FPGA electronic design development, the following documents are prepared and reviewed:

- Technical Requirement Specification describes the overall objectives of the system development as determined by the technical, functional, customer, and commercial goals and requirements.
- Safety Requirements Specification identifies all safety related requirements imposed of the final system, including requirements from appropriate nuclear standards and basic safety standards, such as IEC 61508, and from the specific safety requirements of the given application.
- System Architecture Description provides an overview of the intended system architecture and allocates specific requirements to the various subsystems, such as hardware, application logic, and diagnostic logic.

These can also be combined into a single document based on end user documentation requirements.

At this point, the same process described in Sections 7.3.3 and 7.3.4 is used to complete the project-specific system development. The RPCT can be used to configure EDs for various applications using the AFBL. The project-specific testing focuses on the functional requirements for the system design (i.e., system architecture connections and LM Application ED). The generic RadICS Platform testing of the RadICS Modules and associated Platform EDs is not repeated for a specific project.

The development process for project-specific applications developed using the RadICS Platform technology described in this topical report are intended to be implemented by RadICS.

The following constraints are applied to the development of Application ED:

- []

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 219 of 350
--------------	--------------------	-----------	---	-----------------

]]^{a,c,e}

The RadICS Platform Application Guide presented in Appendix A provides requirements for applying the RadICS Platform in NPP I&C systems classified as safety-related and is used in conjunction with other user documentation provided by RadICS for application of the RadICS Platform.

7.4 RadICS Platform Verification and Validation

Given the criticality of nuclear safety system applications using RadICS Platform technology, implementation of a rigorous approach to V&V in compliance with widely recognized standards is necessary to ensure that RadICS Platform systems developed for NPPs are high quality products that meet customer and regulatory requirements. The following V&V methods are used:

- Document review and comments
- Various types of analysis, including Static Code Analysis, FMEDA etc.;

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 220 of 350
--------------	--------------------	-----------	---	-----------------



- Modeling with the use of simulators
- Various types of testing, including functional testing, fault insertion testing, load and validation testing, with the use of automated facilities

Proven V&V tools are used whenever possible over manual methods to eliminate human error. The above tools are purchased only from well-established vendors with a good track record of configuration management, V&V, problem notification and resolution, and support and training materials.

The RPC Radiy QMS prescribes that all commercial software tools used for V&V should be tested and evaluated with the issuance of relevant evaluation reports. In addition to commercial software tools, RPC Radiy uses its custom software and hardware tools for V&V activities have been developed for use with the RadICS Platform. Examples of such tools are VHDL-based Test Benches for code verification.

RPC Radiy V&V capabilities are provided by a department that is technically, administratively, and financially independent from the Design departments. Personnel performing V&V activities have strong theoretical background and practical experience on design and testing of software and FPGA ED. The RPC Radiy practices are in line with those followed by other organizations involved in the design of FPGA-based safety and non-safety I&C solutions for NPPs, as described in EPRI document 1022983 (Reference 7-10). RPC Radiy methods are consistent U.S. and international standards. RadICS V&V personnel also participate in the RadICS Platform V&V activities.

7.4.1 Roles and Responsibilities

The Project Verification Manager coordinates the Verification Team that provides independent internal verification of the design team outputs. The Project Verification Manager is also responsible for preparation of the Overall V&V Plan and its subsidiary plans to ensure compliance of the safety planning measures, including all design and V&V activities, with the applicable national and international nuclear standards.

The Verification Team is independent from design teams because of compliance with the following principles:

- [[

]]^{a,c,e}

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 221 of 350
--------------	--------------------	-----------	---	-----------------



An independent organization (*exida* LLC) reviewed the Overall V&V Plan, the RadICS V&V process, RadICS Platform results, and corresponding documents. They also performed the FMEA and FMEDA for the RadICS Platform.

The V&V process is closely connected with project management, quality assurance, configuration management, and the change control processes. The overall project management process is supervised by the Project Manager. Safety management activities are supervised by Project and Functional Safety Coordinator. The Quality Assurance Team is responsible for quality of all RadICS Platform life cycle processes, including V&V.

All changes of RadICS Platform components arisen by defects discovered during V&V activities are performed under change control procedure in accordance with established procedures. The Change Control Board is responsible for approving changes to the RadICS Platform and managing the implementation of the approved changes, including V&V results and feedback implementation.

The responsibilities for V&V activities are defined in the Overall V&V Plan. The qualifications of the V&V Team and Qualification Testing Team members' competence are defined in the Project Personnel Plan, which includes competencies for knowledge of product domain, functional safety, analysis techniques, and safety concepts. Training records are kept up to date and maintained by the RPC Radiy Human Resource department.

7.4.2 Methods and Tools

At each stage of the RadICS Platform safety life cycle, the design outputs (e.g., a specification, description, or code) is verified. This verification may be done by review, inspection, analysis and/or testing (listed in increasing order of preference). These methods and the resulting output are described below:

- Review and comment (R&C) is a recorded check of a document's content and correctness that does not follow an analytic process or use a tool, except that it includes the use of a checklist. The resulting output is a completed checklist that becomes a necessary part of each of the documents or a main part of a Code Review Report.
- Document Inspection (DI) is a detailed formal process of verifying a document, according to a defined procedure. The resulting output is a Review Report (RR).
- Analysis involves a discipline analysis or use of a special tool. Examples of these analyses are FMEDA and Static Code Analysis. The resulting output document is a report (e.g., FMEDA report).
- Testing involves preparation of a test procedure and a test report, as defined by the corresponding plan and specification. The resulting output document is a test report. Different types of testing are performed for integrated RadICS Platform and for parts of the RadICS Platform, including ED/FBL Functional Testing (FT), ED Netlist File Logic Level Simulation and Timing Simulation, ED Floor Plan File Static Timing Analyses, Module Fault Insertion Testing (FIT), RadICS Platform Integration Testing, RadICS Platform Validation Testing, RadICS Platform EQ Testing.



At the final stages of RadICS Platform design, all outputs that resulted in RadICS hardware (i.e., different types of RadICS Modules with the associated ED and a completed chassis) are validated during Integration Testing and Validation Testing using corresponding testing procedures. The test results are thoroughly analyzed to ensure that all requirements have been met.

V&V activities are performed at every life cycle phase and for every activity. As shown in Section 7.3.1, the RadICS Platform safety life cycle is broken down into activities (A1 through A11). For each activity, the inputs, design outputs, and V&V outputs, as well as, the method of V&V for each document are defined in the Overall V&V Plan. The V&V tasks are shown graphically in Section 7.3.1. The major V&V documents (i.e., analysis reports and test reports) are each identified as specific document types, and as individual documents in the Project Document Plan.

Tools used for V&V are discussed in Section 8.3.

7.4.3 Implementation Activities

The RadICS Platform has a number of identifiable components, each requiring its own testing, integration testing, followed by overall RadICS Platform integration and validation testing. In addition to integrated overall V&V activities, V&V is performed for three types of RadICS Platform components:

- Hardware modules
- Module FPGA Electronic Designs (including PFBL and AFBL)
- RPCT (as a part of custom tools)

The V&V tasks discussed below correlate to the V&V tasks shown in Figure 7-4.

Integrated RadICS Platform V&V activities include:

[[



Hardware Module verification includes:

[[

]]^{a,c,e}

EDs (including FBL) verification includes:

[[

]]^{a,c,e}



RPCT and Application Logic/AFBL includes:
[[

]]^{a,c,e}
A summary of the RadICS Platform development lifecycle activities (including V&V) is shown in Figure 7-4.



II

II^{a,c,e}

Figure 7-4: RadICS Platform Development Activities (including V&V)

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 226 of 350
--------------	--------------------	-----------	---	-----------------



7.4.4 V&V Administrative Requirements

V&V processes are performed under control of Project FSMP and Overall V&V Plan requirements.

7.4.4.1 Anomaly Resolution and Reporting

All found anomalies are identified, reported, and analyzed by the responsible V&V Team in appropriate V&V reports.

A decision on resolution of anomalies is ultimately a responsibility of the Change Control Board in the cases when impact analysis, which is performed by the responsible V&V Team member, identifies that anomaly resolution could have an impact on the previous stage/stages of the design life cycle. Anomaly resolutions and decisions for changes for a product are completed by the responsible Development Team.

The responsible V&V Team members repeat the applicable part of V&V activity(s) to prove the anomaly resolution was effective. The appropriate records about anomaly findings, analysis, and resolution are included in the appropriate V&V reports.

7.4.4.2 Task Iteration Policy

The Validation Test Report for activity V17, Qualification Test Report for activity V18, as well as FMEDA Reports for activity V5, is approved by the Project Manager. All other V&V documents are approved by Project and Functional Safety Coordinator. The Project Manager and Project and Functional Safety Coordinator are decision makers for formal completion of appropriate V&V activities and for transition to the next product development stage. Such transition is allowed only after resolution of all identified anomalies.

7.4.4.3 Deviation policy

Any deviation from the Overall V&V Plan is documented as the next revision of the Overall V&V Plan. The information required for deviations includes task identification, rationale, and impact analysis. Project Manager is responsible for approving deviations from the Overall V&V Plan.

7.4.5 V&V Documentation Requirements

The Project Document Plan specifies the requirements for documents to be produced under the Project FSMP and the Overall V&V Plan. The standardized document requirements are intended to facilitate traceability, modification, and translation of documentation.

7.4.5.1 V&V Reporting

The following types of reports are produced as the result of V&V activities:

- Review Reports for activities V1-V4 , V5 (Hardware design review), V6, V7, and V10
- FMEDA Reports for activity V5

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 227 of 350
--------------	--------------------	-----------	---	-----------------



- Test Reports for activities V9, V12-V18, and V21
- Static Code Analysis / Code Review Reports for activities V8, V11, and V22

Detailed requirements for the reports for each of the V&V activities are specified in the Overall V&V Plan. All V&V activities findings are documented in the corresponding reports.

All V&V outputs are Configuration Items and all Configuration Management and Change Control activities are applied for V&V outputs in accordance with the Project Configuration Management Plan, as described in Section 7.5.

7.4.5.2 V&V Test Documentation

V&V activities V9, V12-V18, and V21 are based on testing methods including:
[[

]]^{a,c,e}

The Overall V&V Plan specifies the content of the specific Test Plan for which Test Specification/Test Procedure and Test Report are required. [[

]]^{a,c,e} The specific plans which the Overall V&V Plan covers

are:

- FIT Plan and Specifications:
 - [[

-]]^{a,c,e}
- Integration Test Plan:
 - The primary aim of the Integration Test Plan is to identify and plan integration tests or other verification methods (if testing is inappropriate) for the requirements from PAD to prove that RadICS Platform meets these requirements:



- [[

]]^{a,c,e}

- Validation Test Plan:
 - The primary aim of the Validation Test Plan is to identify and plan validation tests or other verification methods (if testing is inappropriate) for the requirements from SRS and Overall V&V Plan to prove that RadICS Platform meets these requirements:
 - [[

]]^{a,c,e}

- Qualification Test Plans (Qualification Testing Team responsibility):
 - Testing of the entire product:
 - [[

]]^{a,c,e}

- Functional Test Plan and Specification (which combines both component (i.e., unit) testing and integrated ED testing):
 - [[

]]^{a,c,e}

7.4.5.2.1 Test Plans

Test Plans are prepared based on the Overall V&V Plan and the part of the RadICS Platform architecture they cover. They address the same subjects as the Overall V&V Plan, but they focus on their specific scope of the RadICS product. Test Plans can serve as the first revision of the corresponding Test Specification and Test Procedure. Test Plans will document:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 229 of 350
--------------	--------------------	-----------	---	-----------------



- What RadICS equipment or components and what functions are to be tested
- The method of verification or validation (test (wherever possible) or analysis) for each requirement in the scope of the plan
- Detailed acceptance (pass/fail) criteria for each type of tests/analysis or for each of the verified/validated initial requirements
- The testing equipment needed and degree of automation of the tests
- Other resources needed for the tests (e.g., who should be present)
- The general approach to performing the tests

7.4.5.2.2 Test Specifications

Test Specifications are prepared from each Test Plan. A Test Specification is usually the first draft of a Test Procedure and includes test case descriptions. The developed test procedure may remain part of the Test Specification document, as specified in the Test Specification. It is produced before the procedure so as to provide a high-level perspective for the tests. The Test Specification usually provides the basis for tracing the testing of requirements for V&V. It shall:

- Define the test objectives:
 - Information to Record Before and After the Tests
 - Identification of Test Cases
 - Specifically identify what equipment/components and what functions are to be tested
- Define how the components and functions will be tested, expanding this to the level where it is clear that the tests cover the requirements completely and are in sufficient step by step detail that they are repeatable or automatable
- Define acceptance criteria for each component, requirement, or function test
- State any assumptions
- Define which test environment is to be used for what tests
- Ensure coverage of all operating modes and a full range of operating conditions in each mode for IT/VT only

If the Test Specification is in sufficient detail that it ensures repeatability, then it essentially includes the Procedure and a separate procedure document is not needed.

7.4.5.2.3 Test Procedures

A Test Procedure document can expand the Test Specification down to repeatable detailed procedural steps, including the detailed pass/fail acceptance criteria where needed to ensure that tests are repeatable, and where it is not practical to include a fine level of detail in the Test Specification. A separate Test Procedure document is not required if the Test Specification is sufficiently detailed.

Test Procedures are usually formatted to facilitate recording of step-by-step test results. They include:

- Expansion to detailed, repeatable steps of every test specified in the Test Specification
- Provision for recording the test results step by step and review check-off at key milestones

A separate Test Procedure document is used for complicated tests. Test Procedures are generally used only for EQ testing.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 230 of 350
--------------	--------------------	-----------	---	-----------------



7.4.5.2.4 Test Reports

The Test Report consists of a summary portion and a detailed portion. The summary portion summarizes:

- Precisely what was tested (hardware/firmware/software versions, etc.)
- The versions of the design documentation that correspond to the RadICS Platform Hardware, ED, and software under test
- What equipment was used for the test (the test environment and configuration, calibration sheets of test equipment)
- Who performed the test (signatures of testers)
- A summary and analysis of all test anomalies
- A summary of all changes to the Configuration Items under test
- A summary of any re-testing performed and the impact analysis to support the degree of regression testing (if any were required – else statement that none were required)
- A summary of the final results and open items (if any)

The detailed portion consists of the marked up detailed test procedure.

7.4.5.2.5 Test Coverage and Pass/Fail Criteria

Test Plans are traceable to design documents and also traceability to Test Specifications and Test Reports. Each Test Specification includes the basis for the selection and detailing of Test Cases to ensure full test coverage. Typical test case approaches are:

- Functional and black box testing to demonstrate requirements coverage
- White box testing to ensure full code structure coverage, using modified condition/decision coverage
- Interface testing using test cases deduced from boundary value analysis or equivalence classes
- Performance/stress testing (such as combinations of variables at extreme values, tests with a fully-loaded system)
- Error guessing
- Full coverage of all functions defined in the corresponding user manuals

Appropriate test cases developed from these principles are applied during:

- Unit testing of VHDL on test-benches
- Integration testing
- Validation testing

The planning of test coverage is dynamic and continues as the design proceeds. A chart of tests is generated and the assignment of tests to various test specification documents is maintained (i.e., allocation of various kinds of tests to Fault Insertion Tests, Integration Tests and Validation Tests) to ensure complete test coverage. It is not possible to test for all hardware or functional configurations in certain cases (e.g., all permutations of RadICS Modules in rack locations). In these cases, a basic set of configurations are tested that collectively provide test coverage of the full set of configurations.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 231 of 350
--------------	--------------------	-----------	---	-----------------



Each test step of the test specifications/procedure is written so that they form step-by-steps instructions and provide the tolerance criterion for pass or failure of the test step. The tolerance criterion may be stated for each step, sequence of steps or larger part of a test specification/procedure, and there may be difference tolerances for different kinds of readings. Tolerance criteria are established in the Overall V&V Plan, but if different criteria are required, then the specific Plan document for the tests in question (e.g., the Integration Test Plan for integration tests) specifies them. In general qualitative criteria are to be avoided if possible, but are unavoidable for the following examples:

- Display color: colors that clearly distinguishable are to be used, and the acceptance criterion is that the specified color is recognized by a tester whose color vision is accepted by the V&V Manager as accurate.
- Timing: time of response is normally treated as a quantitative measure (e.g., when testing how long the RadICS component takes to change an output state in response to a stimulus).

For the Static Code Analysis Test, the VHDL-code Static Code Analysis/Code Review is successfully completed if all identified violations and/or defects have been resolved or adequate reasons for all unresolved violations have been documented with corresponding justifications. The decision on the admissibility of such justifications is taken jointly and agreed to by the Project Verification Manager and Electronic Design Development Team Leader.

The Static Timing Analysis is successfully completed if the ED Netlist files are free of timing violations against the predefined timing constraints defined by the ED Development Team in the Project Design Constraints Document. Logic Level Simulation and Timing Simulation testing is successfully completed if the test results take into account the maximum and minimum possible delays of the signal propagation in the selected FPGA chip model and they confirm the positive results obtained during the ED Functional Testing.

To simplify the Logic Level Simulation and Timing Simulation test efforts, the same ED Test Benches used in Functional Testing are utilized.

7.5 RadICS Configuration Management Process

The RadICS Platform configuration management process applies throughout the lifecycle of the RadICS Platform and project-specific applications. According to IEC 61513, a configuration management process must be established to document and control the functional and physical attributes of all components, to record and report all changes and to verify their compliance with requirements. Configuration management of the RadICS Platform and its applications is performed according to requirements as outlined in IEC 60880:2006 and IEC 62566.

According to RadICS practices and requirements under IEC 61508-2 and IEC 61508-3 (6.2.10, 7.16), all project activities shall be subject to a configuration management plan, which defines the tools, procedures to be used, activities to be performed, their sequence and timing within the product lifecycle and responsibilities for their execution.



7.5.1 Roles and Responsibilities

Configuration management process utilizes the following participants:

- Configuration Management Board (CMB)
- Change Control Board (CCB)

The CMB and CCB are formed at the planning stage for a RadICS project (either Platform or project-specific application). CMB and CCB memberships are determined by the RadICS Personnel Plan for the project.

The CMB implements the following activities:

- [[

]]^{a,c,e}

The CCB implements the following activities in compliance with established procedures:

- [[

]]^{a,c,e}

The primary structure of each change implementation board or development team involved in the configuration management process, as well as the personnel assignments to such boards (or teams), is given in RadICS Personnel Plan for the project.

7.5.2 Process Controls

The Configuration Management Plan implementing procedure identifies the generic Configuration Items for a RadICS project. It identifies the Configuration Items generated by RPC Radiy (e.g., hardware, documents, and software elements), as well as, the externally supplied Configuration Items such as development and V&V tools.

The list of the controlled RadICS Platform Configuration Items is a multilevel hierarchical structure. The top level specifies the following Configuration Items:

- Hardware
- FBL

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 233 of 350
--------------	--------------------	-----------	---	-----------------



- AFBL
- FPGA ED
- Tools
- Documents
- Work Instructions and Guides

The hierarchy of the controlled RadICS Platform Configuration Items is given in Figure 7-5.

[[

]]

Figure 7-5: Hierarchy of the Controlled RadICS Configuration Items

7.5.2.1 Configuration Items

Naming Configuration Items includes system of:

- Identifiers for RadICS Platform items and item versions, providing unique identifier for each of the items
- Marking of the items and their versions

Identifiers for all specific RadICS Platform Configuration Items are developed based on the RadICS Document Plan for the project.

The acquisition of Configuration Items is performed after the identification and naming of Configuration Items is completed. The acquisition process is implemented in this order to effectively control the RadICS Platform Configuration Items. After each Configuration Item is created and named, it is

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 234 of 350
--------------	--------------------	-----------	---	-----------------



transferred under the control of the configuration management tool in order to implement version control.

Only a single version of tools for a RadICS project is installed on the development computers used for the specific RadICS project. The version and status of each Configuration Item is checked using the configuration management tool, before a development activity is executed.

Configuration documents and work instructions (in the form of electronic copies) are stored in two separate locations under control of the configuration management tool. The stored copies can be on the same or different media.

Each optical disc is assigned a unique identifier along with a date and time stamp for the disc creation, as specified in the RadICS project Document Plan for the project. Data storage identifiers are recorded in the configuration management tool.

7.5.2.2 Configuration Baselines

A Baseline is a RadICS Platform configuration version, related to a specific life cycle stage, which is verified and approved. The Baseline is the basis for implementation of further life cycle stages.

Once a Baseline for a set of Configuration Items is established, implementation of changes into those Configuration Items is controlled by a formal change control process. The change implementation process for the items of any of established baseline is regulated by the change control procedures for RadICS Platform components and RadICS Platform-based applications.

Baselines in RadICS life cycle include specific RadICS Platform Configuration Items relevant to the appropriate RadICS life cycle process.

The RadICS Platform life cycle has the following baselines:

- [[

]]^{a,c,e}

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 235 of 350
--------------	--------------------	-----------	---	-----------------



The complete actual list of Configuration Items for each of the baselines is presented in the Document Plan for the specific project.

In addition to the Configuration Items specified within each of the baselines, there are the following baseline-independent Configuration Items, which are under control of the configuration management tool:

- Documents
- Tools
- Work Instructions and Guides

7.5.3 Implementation Activities

The main configuration management implementation activities are: change control, configuration status accounting, and configuration auditing. Each of these implementation activities is described below.

7.5.3.1 *Change Control*

For each of the identified Configuration Items, changes control is performed in accordance with established procedures for RadICS Platform components and RadICS Platform-based applications.

The change control activities consist of implementation of the approved changes, including preparation of change requests, performing an impact analysis, and obtaining approval/rejection. Approved changes are implemented with appropriate documentation, verification, validation, as well as required notifications. Reasons for the necessity to implement changes are regulated by the change control procedure for RadICS Platform components and RadICS Platform-based applications.

Configuration changes are managed to ensure that all needed changes are made and unnecessary (and possibly damaging) changes are not made. Needed changes may arise from field feedback from customers, from internal testing, or from approved product upgrades. An impact analysis is performed to support the approval decision and to help determine the extent of retesting that will be needed. Finally, every time a RadICS module is modified, it is entered into the configuration management system. All of these aspects of managing change are illustrated in Figure 7-6.



[[

]]^{a,c,e}**Figure 7-6: Change Control Work Flow**

The Product Safety Manual provides end users and system integrators with instructions on how to report problems with the RadICS Platform.

When a report concerning a possible problem with the RadICS Platform or a delivered system is received from an end user or system integrator that is or could possibly be associated with a possible hazardous event, a Change Request is always initiated. This Change Request is processed to completion with a high

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 237 of 350
--------------	--------------------	-----------	---	-----------------



priority. The Functional Safety Coordinator is responsible for ensuring that the change request is promptly processed to completion.

7.5.3.2 Configuration Status Accounting

Configuration status accounting is realized after the establishment of the Requirements Baseline and proceeds during the entire RadICS Platform life cycle. Configuration Item status accounting consists of monitoring, documenting, and notification regarding any changes in RadICS Platform configuration. Configuration Items status accounting is performed using configuration management tool(s).

The following information is used for configuration status accounting:

- List of items, which are traced and included into RadICS Platform configuration versions and/or baselines and into change control, represented in configuration audit reports
- Reports on RadICS Platform configuration status accounting (including versions of items, status of change requests, and data concerning approved changes) are generated after each lifecycle stage using a configuration management tool

The configuration audit reports are available to the project personnel. The configuration management tool can generate the following reports at any time:

- RadICS Configuration Items allocation report: reflects allocation of all items in the RadICS Platform (i.e., list of items, their description, and location)
- Report on established RadICS baseline: a list of all Configuration Items of the given RadICS project baseline with identification of appropriate attributes for each of the items

The Release Baseline configuration is verified with the actual configuration, approved in the corresponding documents prior to release the customer. V&V results are presented in the acceptance testing reports.

7.5.3.3 Configuration Auditing

After release of each of the established baselines, baseline configuration audit is performed. Interrelationship of these audits with the RadICS Platform life cycle is shown in Figure 7-7. Each Configuration Audit is directed towards check of correctness of the RadICS Configuration Items functional and physical features implementation for the specific project.



[[

]]^{a,c,e}

Figure 7-7: RadICS Baseline Configuration Audits

A Configuration audit is performed in order to confirm compliance of RadICS configuration hardware and software items implementation with their technical documents. Compliance identification process consists in review of design documents, source codes, as well as user documents, and is directed towards check of the fact that:

- Each established RadICS baseline includes correct versions of items
- All documents are issued, approved and correspond to RadICS configuration

The configuration audit results are documented in the configuration audit reports for each stage. A Configuration Audit shall be performed after establishing of each baseline within the RadICS project. There are [[]]^{a,c,e} configuration audits corresponding to appropriate baselines in RadICS project to be performed:

- [[



•

II^{a,c,e}

The output from each of the Configuration Audits is documented as each audit is performed. The audit reports include the appropriate checklists to ensure consistent reviews. After performance of the configuration audit, there may be findings. Such findings are resolved and re-audited following the same process in order to verify that the findings were completely resolved.

7.6 Requirements for the RadICS Platform and Applications

Platform Functional requirements are divided into the following groups:

- Safety requirements
- Performance requirements
- Qualification requirements

The high level safety, performance, and qualification requirements are illustrated in Figure 7-8.

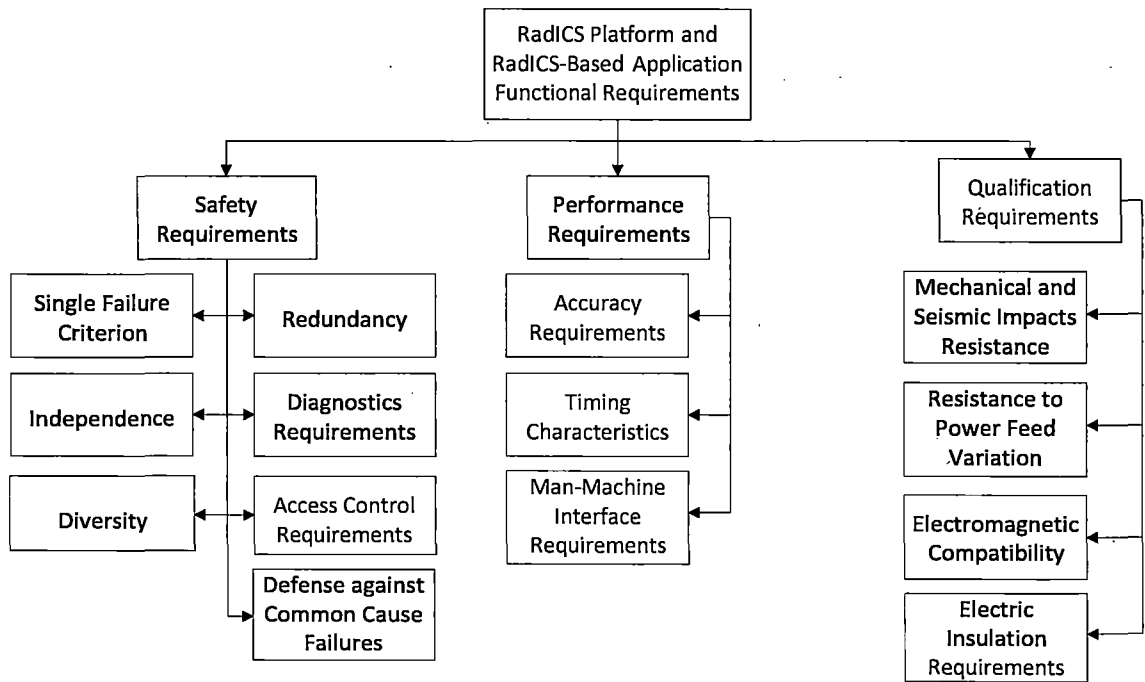


Figure 7-8: RadICS Platform and Applications Requirements



7.6.1 Allocation of Requirements

The allocation of RadICS Platform requirements has up to three dimensions:

- Modules to which they apply (MA = module allocation)
- Means of meeting the requirement (IA = implementation allocation)
- Means of V&V (by testing) (TA = test allocation)

Module Allocation is used for requirements that apply to or are implemented by one or more Module(s).

The module allocations used for the RadICS Platform are:

Symbol	Meaning	Description
ALL	All Modules	The requirement applies to all Modules.
I/O	All I/O Modules	The requirement applies to all I/O Modules (AIM, DIM, DOM, AOM, and OCM).
AIM, etc.	Named Modules only	The requirement applies to all named Modules (LM, AIM, DIM, DOM, AOM, and OCM), and no others.

Implementation Allocation is used for requirements that are implemented via conventional electronic hardware, via ED (i.e., VHDL), or a combination of both. The implementation allocations used for RadICS Platform are:

Symbol	Meaning	Description
ED	Electronic Design	The design child documents are the architecture design of the functionality of the VHDL design, followed by detailed design and coding.
HW	Hardware	Conventional components (e.g., timers, FETs, varistors, etc.) are required to meet some requirements. Because the design tools produce only graphic objects, the next level of design document verifiable from examination of anything textual is the hardware design review report.
PSM	Product Safety Manual	The requirement is for statements in the User Safety Manual, not for a something to be implemented in the product.

Testing Allocation starts with understanding the environment needed to execute and test a requirement. For this reason, the SRS and PAD provide preliminary allocations of what level of test will

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 241 of 350
--------------	--------------------	-----------	---	-----------------



be used for verifying requirement implementation. The allocation is designed to both identify every requirement to be tested and to identify tests to completely cover the requirement. These allocations need not be final, since the requirements tracing tool is updated throughout the development process and will record which test plan or specification covers the requirement. The test allocations used for RadICS Platform are:

Symbol	Meaning	Description
FIT	Fault Insertion Test	FIT tests are 'negative' tests, designed to test the integrity requirements. If separately determined on the basis of the FMEDA which credits the claimed fault detection functions described in the PAD, these do not have to be repeated
FT	Functional Test	These are the 'positive' tests of the intended functionality of the RadICS Platform, and may be conducted at any reasonable test level (e.g., module, integration, validation)
NT	No test needed	Justifiable when a requirement is just a collector and simply points to (requires) other requirements that are tested.
VT	Validation Test	Test that should be conducted as part of Validation testing.

7.6.2 Documentation of Design Requirements

The RadICS Platform SRS specifies the functionality and properties of the RadICS Platform as a black box (i.e., no content describing the internal modularization of the RadICS).

The RadICS Platform PAD describes the hardware components and the principles of operation, including required diagnostics.

The PAD also includes separate requirements for hardware and software, as required by IEC 61508. The PAD allocates the functional specification from the SRS to the specific Modules, operational modes of modules, and the use and operation of hardware units (from which modules are built). It describes their operation and specifies the design for inter-module communications.

7.6.3 Maintainability and User Friendliness Requirements

Design features which enhance maintainability and user friendliness of the RadICS Platform are described in Table 7-3. The checklist items below are taken from Part 7 of IEC 61508.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 242 of 350
--------------	--------------------	-----------	---	-----------------



Table 7-3: Maintainability and User Friendliness Requirements

Clause	Checklist Items from IEC 61508/7-B.4	How this Recommendation is Met
B.4.2	Items to consider where human operation is needed for some functions	
	the need for human intervention is restricted to an absolute minimum	[[]] ^{a,c,e}
	the necessary intervention is as simple as possible	[[]] ^{a,c,e}
	The potential for harm from operator error is minimized	[[]] ^{a,c,e}
	the intervention facilities and indication facilities are designed according to ergonomic requirements	[[]] ^{a,c,e}
	the operator facilities are simple, well labelled and intuitive to use	[[]] ^{a,c,e}

[illegible]



Clause	Checklist Items from IEC 61508/7-B.4	How this Recommendation is Met
B.4.4	Considerations for limiting operational possibilities	
	limiting the operation within special operating modes, for example by key switches	The use of keyswitches is explained in Section 6.9
	limiting the number of operating elements	[[]] ^{a,c,e}
	limiting the number of generally possible operating modes	[[]] ^{a,c,e}
B.4.5	Operation only by skilled operators	
	Training is commensurate with the SIL level and complexity of the maintenance activities	[[]] ^{a,c,e}
	Training includes understanding of the process hazards	[[]] ^{a,c,e}
B.4.6	Protection against operator mistakes	
	Wrong inputs (value, time, etc.) are detected via plausibility checks or monitoring of the EUC	[[]] ^{a,c,e}

7.6.4 Requirements Tracing Tool

The implementation status of the RadICS Platform safety requirements are documented in a Requirements Traceability Matrix. The requirements tracing tool has the following capabilities:

- Capable of capturing requirements, design and implementation statements (solutions), as well as analysis and test procedures and reports, and identify them by a unique ID
- Capable of linking the requirements, design solutions, analyses, and tests

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 245 of 350
--------------	--------------------	-----------	---	-----------------



As a minimum, the tracing information is given by means of a cross-reference list between requirement and allocation to component(s) and related design and verification documents and paragraph. The cross-reference allows for forward and backward tracing. Any additional safety requirement identified during the Architectural Design and Verification (derived requirement) are also entered in Requirements Traceability Matrix.

All design and test specifications are reviewed to verify that they implement the requirements allotted to them.

The requirements tracing tool may be adapted or modified for a RadICS project based on customer requirements.

7.7 Development Process Metrics

Quality metrics are used throughout the RadICS life cycle to assess the effectiveness of the software QA program. The metric approach discussed below is used to conform to the requirements in IEEE Std 7-4.3.2-2003 clause 5.3.1.1 (Reference 7-11), as endorsed by RG 1.152 (Reference 7-12).

7.7.1 Software Quality Metrics Based on Anomaly Reports

The FSMP and the Overall V&V Plan define the anomaly reporting and resolution process used during the RadICS development process. All software review and test reports include a discussion of the anomalies found and their resolution. These software and design anomalies are recorded as open issues in RadICS action tracking system during each phase of development.

7.7.2 Software Quality Metrics Based on V&V Open Issues

The FSMP and the Overall V&V Plan require the use of an action tracking process for all stages of software development and V&V. The open issues are assessed using the following indicators:

- Total number of V&V open issues in the open issues backlog as a function of calendar time
- Number of project open issues discovered by V&V team compared to the total number of open issues
- Severity statistics associated with anomalies and open issues discovered during V&V activities
- Number of anomalies discovered by V&V team during review and testing

7.7.3 Software Quality Metrics Based on Test Coverage

The software V&V plans defines quality metrics based on test coverage calculation. Requirements coverage is a required metric that is defined as the fraction of requirements specified in the top-down design documents that are traceable into test plan and specifications. A comprehensive 100% functional coverage is required. It is recognized that some requirements may not be testable; therefore, alternate analytical verification means are defined. The coverage is recalculated by crediting approved

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 246 of 350
--------------	--------------------	-----------	---	-----------------



means of alternative verification. Code structure coverage metrics are defined as the fractions of code components that are covered during testing. RadICS use the following coverage metrics to approve VHDL 100% code coverage with tests:

- 100% statement coverage
- 100% branch coverage
- 100% modified condition/decision coverage

The software V&V reports provide evidence that 100% requirements test coverage as well as 100% code structure test coverage is achieved.

7.8 Development Process Training

All persons assigned responsibilities for a RadICS project are be informed of their responsibilities, as specified in the Project FSMP. All persons assigned to the project are technically qualified in terms of formal education, specific product training, specific training on quality procedures (including the Project FSMP), and relevant professional experience.

The Project Personnel Plan lists the current incumbents for each role, the competence requirements for the roles, and the compliance of the incumbent for each role. Where each design team (software, electronic design, hardware, mechanical) consists of more than just the development manager (i.e., the team leader), the rest of the team should collectively have the same competency as the team development manager. Each member of the team is required to have the technical education and specific training required to execute the assigned responsibilities. Each team is assessed for its combined competencies and shown to cover all required competencies for the work performed by the team.

The Technical Director performs a training needs analysis based on the matrix of competencies for the various job functions and develops an annual training plan in accordance with the Project Training procedure. Training is conducted in accordance with the training plan by both in-house and external training resources. Training records include the training material, participant lists, feedback forms, and training results. Training records for each employee are maintained by the Human Resources organization. The training instructor is responsible for determining if the training objectives were met for each student.

All personnel playing a significant role on a RadICS project will received IEC 61508 training and will indicate that they understand their responsibilities.

If performance weaknesses are disclosed, they are addressed by documenting planned corrective action, such as training.

7.9 Chapter 7 References

- 1 Safety Guide IAEA NS-G-1.3, "Instrumentation and Control systems important to safety in nuclear power plants"
- 2 Safety Standards Series No. NS-R-1, "Safety of Nuclear Power Plants: Design"

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 247 of 350
--------------	--------------------	-----------	---	-----------------



- 3 Safety Guide IAEA NS-G-1.3, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants"
- 4 IEC 61508:2010, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems"
- 5 IEC 61513:2001, "Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems"
- 6 IEC 60880:2006, "Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions"
- 7 IEC 60987:2007, "Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems"
- 8 IEC 62566:2011, "Nuclear power plants – Instruments and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions"
- 9 RTCA/DO 254, "Design Assurance Guidance for Airborne Electronic Hardware"
- 10 Electric Power Research Institute, "Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems," 1022983, 2011
- 11 IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
- 12 Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"



8 Electronic Design Development

The RPC Radiy Electronic Design Development Team was responsible for the development of the ED for RadICS Modules and the RadICS FBL. ED is a set of FPGA configuration files that are installed (loaded) into the RadICS Modules. RPC Radiy used a defined and controlled process to develop the RadICS Platform ED that complies with the requirements of IEC 61508:2010 (Reference 8-1).

When developing RadICS Platform safety applications, RPC Radiy and RadICS use tools and components (i.e., FPGA chips) manufactured by Altera using the FPGA design flow defined in the Altera user manuals. The chipsets and related tools are part of the Altera Functional Safety Data Package, which was certified to IEC SIL 3 (reference TÜV Rheinland Certificate No. 968/EL 693.00/10). Tools are used for development and/or V&V efforts. These tools are described in Section 8.3.

8.1 *RadICS Electronic Design Process*

Development of the RadICS Module ED is a step-by-step process translating the RadICS requirements into ready-to-use electronic modules as bitstream files.

The RadICS Module ED development process is defined in procedures as is accomplished in eight phases:

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

A set of documents and files is generated during each ED phase, which is used as input to the subsequent phases of development ED or is part of the final outcome of ED development.

Figure 8-1 shows the relationship of the phases of the RadICS Platform ED development life-cycle and the documents produced.



[[

]]^{a,c,e}**Figure 8-1: RadICS ED Development Lifecycle and Documents**

Chapter 8 only describes the ED stages of development for the RadICS Modules and FBL with a summary of the V&V methods for each ED phase. The complete RadICS Platform V&V methods are described in Section 7.4.

The following sections contain a description of each of the ED development stages, including:

- Input data
- Implementation details
- Outputs
- Methods of Verification

The ED phases are implemented independently for each RadICS Module.

Inputs and outputs are the documents (RPC Radiy or vendor) and/or files and artifacts created for the project.

8.1.1 Development of Electronic Design Architecture Description

The inputs for the ED Architecture Description phase are:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 250 of 350
--------------	--------------------	-----------	---	-----------------



- RadICS Platform PAD
- [[ports]]^{a,c,e}

At this stage an ED AD is developed for each RadICS Module and documented in an ED DD.

[[

ts]]^{a,c,e}, the ED AD development may begin. The ED AD is developed for each of the RadICS Modules and all on-board components (e.g., ED AD for the PSWD CPLD). Any common components are developed once and used in all Modules across the platform.

The ED AD contains the following information:

- Top-level architecture requirements, including:
 - [[

]]^{a,c,e}

- ED diagnostic architecture

[[

]]^{a,c,e} This information is utilized in the

Synthesis and Place and Route stages.

The outputs of the ED Architecture Description phase are:

- ED DD for each RadICS Module and an [[]]^{a,c,e}

All output documents from this stage are reviewed and verified for completeness and implementation of all input requirements. [[

]]^{a,c,e}

8.1.2 Development of Function Block Library Detailed Description

The FBL development steps described here apply to both the PFBL and the AFBL development and V&V activities. The PFBL and AFBL are two separate entities. Some additional steps are taken and separate AFBL documents are produced both for design and V&V to ensure the AFBL is properly documented and structured for use in safety-related applications. The inputs, outputs, and additional development steps for the AFBL are described in Section 8.2.

The inputs for the FBL Detailed Description phase are:

- ED DD for each RadICS Module and an [[

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 251 of 350
--------------	--------------------	-----------	---	-----------------

]]^{a,c,e}

At this stage, the RadICS FBL Detailed Description document is developed, which contains the detailed requirements for PFBL). In the course of PFBL development, the following elements are detailed:

- Scope and Purpose
- [[
- Platform requirements for each of Units, including:
 - [[

]]^{a,c,e}]]^{a,c,e}

The output of the FBL Detail Description phase is:

- FBL Detailed Description

The outputs of this phase are verified by two methods:

- [[

]]^{a,c,e}

The RadICS FBL is uniquely developed by RPC Radiy for the RadICS Platform. [[

]]^{a,c,e}

8.1.3 Development of Function Block Library Code

The steps described here apply to both the PFBL and AFBL development and V&V activities. The PFBL and AFBL are designed together as one library; however, additional steps are taken and separate documents are produced both for design and V&V to ensure the AFBL is properly documented and structured for use in safety-related applications. The outputs and additional development steps for the AFBL are described in Section 8.2.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 252 of 350
--------------	--------------------	-----------	---	-----------------



The inputs for the FBL Code phase are:

- FBL Detailed Description
- [[]]^{a,c,e}

At this stage, the FBL VHDL Code document is developed by implementing the functions that are defined in the FBL Detail Description document. [[

]]^{a,c,e}

The outputs of the FBL Code phase are:

- FBL VHDL Code
- FBTB Test Report

The outputs of this phase are verified by [[]]^{a,c,e}:

- [[

]]^{a,c,e}

8.1.4 Development of Electronic Design Detailed Description

The inputs for the Electronic Design Detailed Description phase are:

- ED AD for each RadICS Module
- FBL Detailed Description

At this stage, the ED DD document is developed for each RadICS Module. These documents contain the detailed requirements for all FPGA components on each RadICS Module. The ED DD development includes the following elements:

- Scope and Purpose of the Document
- [[

]]^{a,c,e}



The output of the Electronic Design Detailed Description phase is:

- ED DD for each RadICS Module

The outputs of this phase are verified by two methods:

- [[

]]^{a,c,e}

8.1.5 Development of Electronic Design Code

The inputs for the Electronic Design Code phase are:

- FBL VHDL Code
- ED DD for each RadICS Module

At this stage, the functions defined for each ED are implemented using the VHDL language. This coding represents the formal representation of the hardware description language (VHDL Design Files). It uses a structural decomposition and top-down design.

[[

]]^{a,c,e}

When performing the VHDL language coding, developers are guided by the [[

]]^{a,c,e}

The outputs of the Electronic Design Code phase are:

- ED VHDL Code for each RadICS Module
- [[

]]^{a,c,e}

The outputs of this phase are verified by two methods:

- [[



]]^{a,c,e}

8.1.6 Synthesis

The inputs for the Synthesis phase are:

- ED VHDL Code for each RadICS Module
- [[]]^{a,c,e}

At this stage, the ED VHDL Code is automatically synthesized into logical view cells fitting the corresponding FPGA chip. [[

]]^{a,c,e}

The outputs of the Synthesis phase are:

- Generated synthesis reports consisting of builds for each RadICS Module
- [[]]^{a,c,e}
- RadICS Module ED Synthesis Results Review Reports

[[

]]^{a,c,e}

8.1.7 Place and Route

The inputs for the Place and Route phase are:

- Synthesis Database [[

]]^{a,c,e}

At this stage, a Netlist is automatically created and is presented in the Place and Route format with the specific location of each logical cell, the links between them, and other resources of the FPGA. [[

]]^{a,c,e}

The outputs of the Place and Route phase are:

- Generated performance Place and Route reports consisting of builds
- [[]]^{a,c,e}
- ED Place and Route Results Review Reports for each RadICS Module

[[

]]^{a,c,e}

8.1.8 Bitstream Generation

The inputs for the Bitstream phase are as follows:

- Place and Route Database [[]]^{a,c,e}

The purpose of this step is to create a programming file for implementation into the RadICS Module, (i.e., used for configuring logical cells on the FPGA chip by using the onboard programmer). [[

]]^{a,c,e}

The outputs of the Bitstream phase are:

- Programming files for each RadICS Module and generated reports on the implementation of the bitstream generation consisting of builds
- Modules ED Bitstream Generation Results Review Reports.

[[

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 256 of 350
--------------	--------------------	-----------	---	-----------------



]]^{a,c,e}

After completion of the ED, the Bitstream files are implemented in the RadICS Modules. Module tests are carried out in phases (i.e., Fault Insertion Testing, Integration Testing, and Validation Testing).

8.2 Application Function Block Library Electronic Design Development

The AFBL is designed to provide a fully validated and qualified function block language that is sufficiently rich in the capabilities of the blocks that RadICS Application ED can be designed entirely using only the AFBL blocks. Several activities, in addition to the steps described in Sections 8.1.2 and 8.1.3, are taken to further document and verify the AFBL.

8.2.1 AFBL Design Activities

The input for the RadICS AFPL and associated user documents is the RadICS PAD.

The outputs for the RadICS AFBL user documents are:

- RadICS AFBL Function Block Reference Manual
- RadICS Application Logic User Manual

The AFBL Function Block Reference Manual defines the Application Function Blocks that are available in the AFBL for the design engineer to create Application Logic for safety-related RadICS projects.

The Application Logic User Manual is provided inform the application designer about the AFBL structure and constraints; Function Block list; and a Function Block descriptions (e.g., purpose, parameters, functional requirements, and usage examples). This document also describes the process of Application ED creation (using the Quartus-based approach).

All RadICS AFBL blocks are designed for safety applications and the following rules are applied:

- All blocks test application logic inputs and tuning parameters, as well as intermediate results to ensure that no error condition can result in computational exceptions (e.g., due to divide-by-zero, underflow, overflow or any other error condition). The blocks also ensure that that there is no violation of the fundamental assumptions behind the calculation algorithm used within the block.
- Where overflows are possible, internal calculations are performed to higher precision than SINT16 (signed 16-bit integer format) and then truncated to SINT16.
- All blocks that could be subject to either of the foregoing conditions provide appropriate diagnostic output signals that are used in the Application ED for error management.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 257 of 350
--------------	--------------------	-----------	---	-----------------



In addition to checking that input data do not cause problems, the RadICS AFBL blocks protect their operational integrity by ensuring that the tuning parameters, singly and in concert, are consistent with the requirements of the computational algorithm used inside the block. Integrity defenses include:

- All AFBL blocks perform validation of the tuning values and their inputs to ensure that the values are consistent with the concept of the block. Each tunable block outputs a tunable parameter status signal set to TRUE if tuning parameter validation succeeds, and FALSE if it fails.
- If a tuning parameter of a block, alone or in concert with any other tuning parameters, fails the validation tests, the SOR will be set by the RadICS Platform. This action will drive all safety-function outputs on RadICS Modules to the safe state. Some RadICS Module outputs may be designed during configuration to be used for non-safety-critical functions (e.g., alarms) and will remain functional. The SOR will not be reset until the tuning validation succeeds and an operator then activates the SOR reset button.
- The DEFPAR block minimum and maximum parameters can provide partial protection against accidental violation of the validation criteria for tuning parameters that are set via the Application Tuning Station (ATS). If tuning parameters of a block are set dynamically by Application Logic, the Application ED should including appropriate logic in the design to prevent violation of the tuning parameter criteria.

The AFBL Function Block Reference Manual and the RadICS Application Logic User Manual are used together to produce Application ED for a RadICS project. This Reference Manual defines the AFBL blocks. The User Manual is used to familiarize the user with the AFBL structure and constraints, the functional blocks list, and their description (i.e., purpose, parameters, functional requirements, and usage examples). This document also describes the process of Application ED creation using Quartus-based approach.

8.2.2 AFBL Methods of Verification and Validation

The V&V activities for the AFBL are conducted in a similar manner as for the PFBL described in Section 8.1.2 and 8.1.3; however, a separate set of phase activities and documents are produced. The V&V engineers perform reviews of the AFBL design documents and produce review reports in addition to performing functional testing.

The outputs of AFBL development are verified by three methods:

- Verification of AFBL design documents and issuance of the Application Logic User Manual Review Report to verify the completeness of each document and ensure that they are aligned with the phase inputs
- Static analysis review of the VHDL code and issuance of the AFBL Static Code Analysis / Code Review Report
- Functional testing of the VHDL code based on the AFBL Functional Test Plan and Specification and issuance of the AFBL Functional Test Report

The AFBL development is not considered complete if the verification and validation effort reveals deficiencies. If deficiencies are detected, the AFBL is refined and verified until all deficiencies are resolved.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 258 of 350
--------------	--------------------	-----------	---	-----------------



8.3 FBL and Module Electronic Design and V&V Tools

The RadICS Platform development process uses several commercial tools to produce the FBL and the ED for the RadICS Modules. The tool types used for ED development are:

- VHDL Tool Suite for VHDL code development
- Static analysis tool
- VHDL simulation tool
- Test coverage analysis tool
- VHDL simulation tool
- Test automation tool
- Compiling tool
- Integrated development environment

Proven tools are preferred over manual methods. Software-based tools are purchased only from long-established vendors with a good track record of configuration management, V&V, problem notification and resolution, product support, and training material. A Project Tool Selection and Evaluation Report are prepared for all commercially available tools to be used that specifies each tool by function, name, manufacturer, and version number. RPC Radiy has a policy in place for tool upgrades, in which the revised tool is used to regenerate an existing application, which is then tested for errors.

Each tool used for RadICS ED and FBL development is classified according to its application. The tools are classified as defined in IEC 61508:2010. Software tools are divided into the following classes:

- T1 – generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system (e.g., a text editor or a requirements or design support tool with no automatic code generation capabilities; configuration control tools). These tools are not discussed in this Topical Report.
- T2 – supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software (e.g., a test harness generator; a test coverage measurement tool; a static analysis tool).
- T3 – generates outputs which can directly or indirectly contribute to the executable code of the safety related system (e.g., a tool to change set-points during system operation; an optimizing compiler where the relationship between the source code program and the generated object code is not obvious; a compiler that incorporates an executable run-time package into the executable code).

The tools are evaluated based on a standard set of criteria, as shown in Table 8-1.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 259 of 350
--------------	--------------------	-----------	---	-----------------



Table 8-1: RadICS Tool Evaluation Criteria

Evaluation Criterion	Tool Class		
	T1	T2	T3
[[
]] ^{a,c,e}

All tools used for a RadICS project are controlled within the scope of Configuration Management repository, as required by the Project Configuration Management Plan

Table 8-2 outlines the commercial tool profile used for ED development in RadICS projects.



Table 8-2: RadICS Commercial Development Tools

Tool Name	Tool Function	Tool Supplier	Tool Classification	Configuration Items Generated
Quartus II	[[]] ^{a,c,e}	Altera	[[]] ^{a,c,e}
HDL Designer	[[]] ^{a,c,e}	Mentor Graphics	[[]] ^{a,c,e}
Understand	[[]] ^{a,c,e}	Scientific Toolworks, Inc.	[[]] ^{a,c,e}
ModelSim	[[]] ^{a,c,e}	MentorGraphics	[[]] ^{a,c,e}
LabView	[[]] ^{a,c,e}	National Instruments Corp.	[[]] ^{a,c,e}
TestComplete	[[]] ^{a,c,e}	SmartBear	[[]] ^{a,c,e}
TopJTAG Probe	[[]] ^{a,c,e}	TopJTAG	[[]] ^{a,c,e}
Visual Studio	[[]] ^{a,c,e}	Microsoft	[[]] ^{a,c,e}
PostgreSQL	[[]] ^{a,c,e}	PostgreSQL Global Development Group	[[]] ^{a,c,e}



Tool Name	Tool Function	Tool Supplier	Tool Classification	Configuration Items Generated
Qt Creator	[[]] ^{a,c,e}	Qt Company	[[]] ^{a,c,e}
GNU Compiler Collection	[[]] ^{a,c,e}	The GNU Project	[[]] ^{a,c,e}

There are custom software and hardware tools for some V&V activities like Test Benches that are used as tools for RadICS Platform V&V (including ED and FBL verification and integration and validation testing). The details for the use of such Test Benches in V&V activities are defined in the RadICS FBL Functional Testing Plan and Specification, the RadICS Module FPGA ED Functional Testing Plans and Specifications, the RadICS Platform Integration Testing Plan, and the RadICS Platform Validation Testing Plan.

The work flow for RadICS ED development is shown in Figure 8-2.

[[

]]^{a,c,e}

Figure 8-2: Work Flow of Tools for FBL and ED Development

8.3.1 Quartus II

Quartus II is an integrated system-level design tool that is used to support RadICS Module ED and FBL VHDL design. It integrates design, synthesis, place and route, and verification into a single development environment. Quartus II has features that facilitate the design process:

- incremental compilation to reduce the design cycle time
- system-on-a-programmable-chip Builder for system-level design

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 262 of 350
--------------	--------------------	-----------	---	-----------------



- power analysis tools to meet stringent power requirements
- memory compiler function to easily use embedded memory

Altera has a closed loop quality and reliability system that conforms to the requirements of ISO 9001:2008 (Reference 8-2), MIL-I-45208 (Reference 8-3), and various Joint Electron Device Engineering Council standards. [[

]]^{a,c,e}

8.3.2 HDL Designer

HDL Designer is used for [[

]]^{a,c,e}. HDL Designer is an advanced design rule checking tool designed to detect problems early in the development cycle without behavioral simulation, including poor coding styles, improper clock and reset management, simulation and synthesis problems, poor testability, and source code issues. HDL Designer includes the DesignChecker feature, which enables RadICS development and V&V teams to view and manage the results of the linting session. Violation reports can be exported into a file for analysis.

[[

]]^{a,c,e}

HDL Designer is widely used in many industries with a wide global presence.

8.3.3 Understand

Understand is used for [[

]]^{a,c,e}. The Understand tool includes several useful features:

- Information Browser, which can display different kinds of information about entities (e.g., source files, classes, members, functions, types, methods, packages, interfaces, etc.). Information that is hierarchical in nature (such as a call relationship) can be expanded multiple levels.
- Architecture Browser, which shows a list of all the defined architectures in the database and provides a way to navigate individual architectures.
- Graphical Views, which presents information from internal database containing information about the entities and the relationships between entities in a convenient form. Two kinds of graphical views are available: hierarchy (shows relations between entities, from the starting entity through its children and successors) and structure (shows the structure of any entity that added to the structure of the code).



Understand is used in many industries in several countries. [[
]]^{a,c,e}

8.3.4 ModelSim

The ModelSim tool is used at the [[

]]^{a,c,e}

ModelSim supports Altera gate-level libraries and includes behavioral simulation, HDL test benches, and tool command language scripting. ModelSim implementation and quality assurance practices are guided by IEEE standards.

ModelSim is widely used in many industries and is favored by many military and aerospace sector companies. [[
]]^{a,c,e}

8.3.5 LabView

The LabView tool is used at the [[
]]^{a,c,e}. LabView is a system design software package that provides engineers with the tools they need to create any testing or measurement systems. It has highest bandwidth vector signal analyzers and digitizers. A key benefit of LabView over other development environments is the extensive capability for accessing instrumentation hardware. It had drivers and abstraction layers for many different types of instruments and buses that are represented as graphical nodes. The graphical nature makes it effective for test and measurement, automation, instrument control, data acquisition, and data analysis applications.

LabView is widely used in many industries.

8.3.6 TestComplete

TestComplete is used for [[

]]^{a,c,e}

Over 4 million software professionals and 25,000 organizations across 194 countries use SmartBear tools. Among them more than 5000 companies use TestComplete: Cisco, J.P. Morgan, McAfee, Intuit and Boeing are in this list.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 264 of 350
--------------	--------------------	-----------	---	-----------------



8.3.7 TopJTAG Probe

The TopJTAG Probe is [[

]]^{a,c,e}

8.3.8 Visual Studio

Visual Studio is an integrated development environment that includes code editor, debugger, compiler that supports the following programming languages: C, C++, C#. The Visual Studio Integrated development environment is used to perform compilation of the RPCT source code into Windows executable binary file. The RPCT is the multicomponent software platform that allows user to configure a complete RadICS system and associated MATS. Visual Studio is used to support design process of the RPCT Output Verification Tool. RPCT Output Verification Tool is software application which allows user to verify compliance between RPCT outputs and RadICS chassis application layer design specification. RPCT Output Verification Tool does not generate outputs which can directly or indirectly contribute to the executable code of the safety related system.

Visual Studio is one of the leading integrated development environments used worldwide for software development in C/C++/C# and is used by many different companies for development of desktop software in different fields by different companies. Visual Studio compiler was successfully assessed by *exida* for SIL 3 capable applications. [[

]]^{a,c,e}

8.3.9 PostgreSQL

PostgreSQL is an object-relational database management system used to implement the RPCT Application Project Database. RPCT Application Project Database is intended to store RPCT design data (i.e., RadICS hardware configuration, Application Logic design, and MATS configuration) and to allow for retrieval at the request of RPCT software components.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 265 of 350
--------------	--------------------	-----------	---	-----------------



PostgreSQL is cross-platform, free and open-source software and is used in different fields by different companies.

8.3.10 Qt Creator

Qt Creator is a cross-platform C++, JavaScript, and Qt Modeling Language integrated development environment. Qt Creator integrated development environment is used to support design process of the RPCT. RPCT is the multicomponent software platform which allows user to configure a complete RadICS system and associated MATS.

Qt Creator has been used in various systems requiring certification.

8.3.11 GNU Compiler Collection

The GNU Compiler Collection is used for compiling RPCT source code into Linux executable file. GCC performs full compilation sequence:

- preprocessing
- compilation
- assembly
- linking

The GNU Compiler Collection parses source code and creates an abstract syntax tree. It then transforms it to RTL, optimizes it, and translates it into assembler language.

The GNU Compiler Collection is the most popular C/C++ compilation tool for UNIX-based OS for the last 30 years. It has open-source status and a very wide community of users. Most of safety-critical UNIX-based projects are using the GNU Compiler Collection as the C/C++ compiler.

8.4 Application Electronic Design Tool

The AFBL described in Section 8.2 is utilized to create the Application ED which implements the required safety system logic. RPCT is the tool used for this design process and was developed for the RadICS Platform.

The RPCT is an integrated development environment, which enables a system designer to completely configure the:

- Overall architecture of the RadICS Platform-based I&C system that includes one or more RadICS chassis
- Detailed hardware configuration of each RadICS chassis,
- Application ED to operate in each RadICS chassis LM
- Tuning parameters in the Application ED for each LM
- Application Signals that will be monitored via MATS
- Architecture of the monitoring system that allows plant technicians and operators to perform their tasks

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 266 of 350
--------------	--------------------	-----------	---	-----------------



The Application ED is designed on logic schemas using the RPCT. The designer selects function blocks for each schema and links the blocks together to define the required signal flow. The blocks are selected from the AFBL via a simple dialog menu and inter-connected using icons and simple mouse operations. The inter-block signal values on a schema are internal to the schema and thus inaccessible outside the schema, except where connections are made via INPUT or OUTPUT blocks. The INPUT and OUTPUT blocks expand the signal connectivity to any number of logic schemas, to the hardware signal ports, and to external monitoring via the MATS. The RPCT User Manual explains the use of RPCT and is a resource manual for RadICS system designers.

The RPCT is used for the design process to configure the entire system. The RPCT is used to download the completed set of configuration files to the RadICS LMs. The LM to be configured are removed from the RadICS chassis and installed in the DLS for this operation. The RPCT is not used for any online activities.

8.5 Chapter 8 References

- 1 IEC 61508:2010, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems"
- 2 ISO 9001:2008, "Quality management systems – Requirements"
- 3 MIL-I-45208, "Inspection System"
- 4 TÜV Rheinland Certificate No. 968/EL 850.00/12



9 Equipment Qualification and Analysis

9.1 Equipment Qualification

Environmental qualification testing of the RadICS Platform Qualification Test Specimen (QTS) will be performed in accordance with the requirements of NRC RG 1.209 (Reference 9-1) and requirements of IEEE Std 323-2003 (Reference 9-2). The environmental qualification testing of the RadICS Platform QTS is also performed in accordance with the requirements for qualifying digital computers IEEE Std 7-4.3.2-2003 (Reference 9-3) and RG 1.152 (Reference 9-4).

Seismic qualification testing will be performed in accordance with RG 1.100 (Reference 9-5), IEEE Std 344-2004 (Reference 9-6), and the generic seismic spectra provided in EPRI TR-107330 (Reference 9-7).

Electromagnetic compatibility (EMC) qualification testing will be performed in accordance with the guidance provided in RG 1.180 (Reference 9-8).

EPRI TR-107330 also describes an approach for generically qualifying commercial Programmable Logic Controllers for safety-related applications. This approach was found acceptable by the NRC (Reference 9-9). The generic qualification approach for the RadICS Platform uses guidance from EPRI TR-107330, as applicable, to meet the requirements of IEEE Std 323-2003 and other NRC guidance.

9.1.1 Equipment to be Tested

The equipment to be tested is the RadICS Platform QTS. In accordance with EPRI TR-107330, a representative sampling of the RadICS Platform components are identified for evaluation and qualification testing. The assembled components of the RadICS Platform QTS include the following types of hardware modules and components:

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

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

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 268 of 350
--------------	--------------------	-----------	---	-----------------



A detailed description of the RadICS Platform QTS and the test system is provided in the QTS Specification (Reference 9-10). QTS and DAS system arrangement and wiring drawings will be prepared to provide additional hardware configuration information. A master configuration list will be prepared to provide detailed RadICS Platform QTS configuration information such as component serial numbers and software version numbers (Reference 9-11).

9.1.2 Equipment Qualification Testing

The RadICS Platform Equipment Qualification Plan (Reference 9-12) defines the scope of testing to be performed and provides a test plan for each of the individual qualification tests. The basic qualification test sequence is shown in Figure 9-1 and the individual tests are described briefly below.

9.1.2.1 Factory Acceptance Testing

Factory Acceptance Testing is performed at the end of the manufacturing and assembly phase to demonstrate compliance of the RadICS Platform QTS and Test System with the QTS Specification. During Factory Acceptance Testing, the RadICS Platform QTS will be powered with the input/output I/O modules operating under control of the TSAP and the connected test system simulation devices. The I/O field circuits will be configured with loads representative of the types intended for connection to the corresponding I/O module points, and other devices required for monitoring of the circuit operations. Burn-In Testing will be performed by RPC Radiy as part of the manufacturing process.

9.1.2.2 Pre-Qualification Acceptance Testing

The objective of Pre-Qualification Acceptance Testing is to demonstrate that the RadICS Platform QTS operate as intended prior to start of qualification testing, and to provide baseline acceptance data for qualification testing implementation of the Operability and Prudency Tests. Section 5.2 of EPRI TR 107330 provides guidance for implementation of pre-qualification acceptance testing. The RadICS Pre-Qualification Acceptance Testing includes System Setup and Checkout Testing, Operability Testing, and Prudency Testing. The RadICS Pre-Qualification Acceptance Testing can be performed with the RadICS Platform QTS in the environmental test chamber.

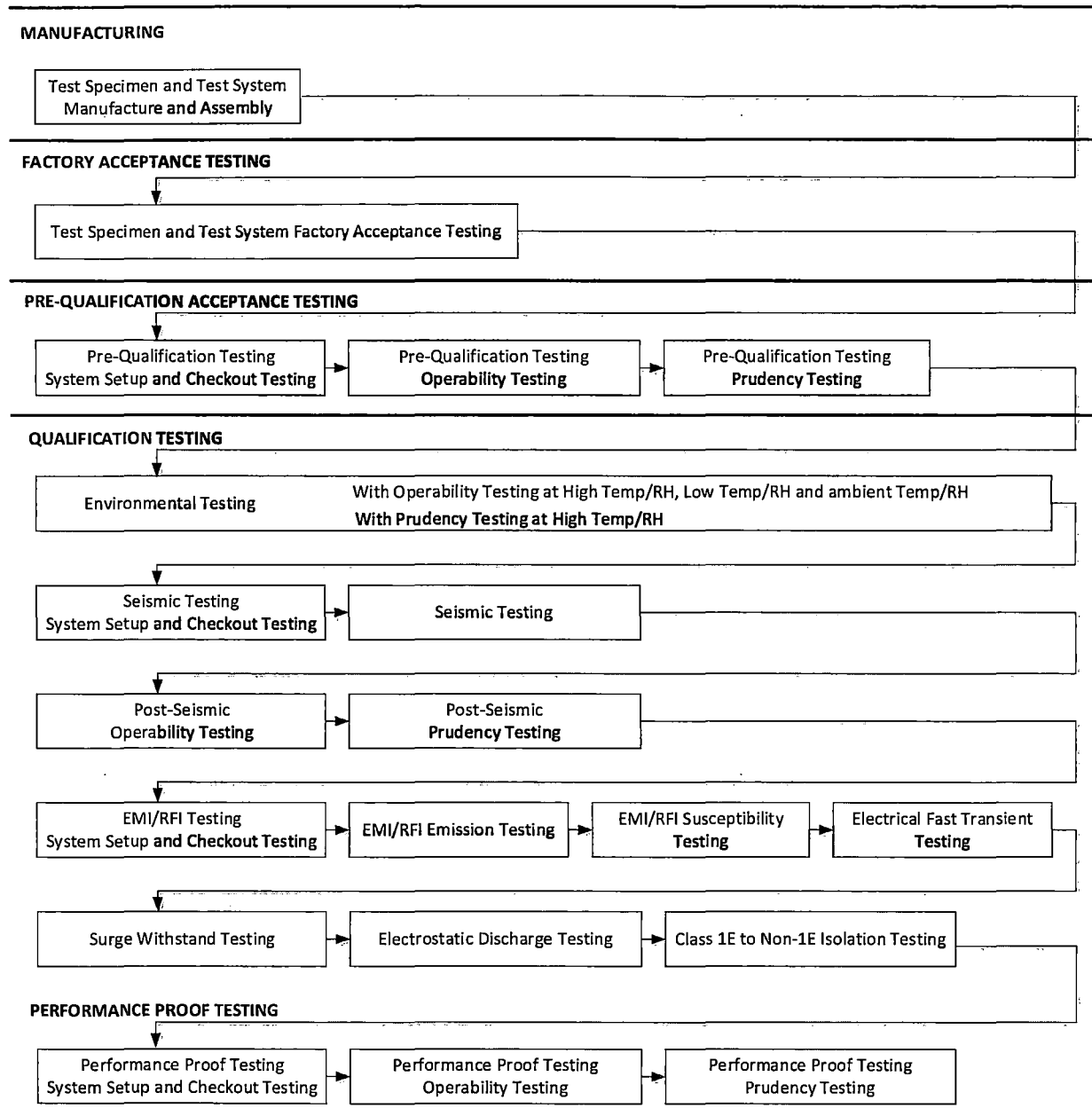


Figure 9-1: RadICS QTS Qualification Testing Sequence

9.1.2.3 Environmental Testing

The environmental testing demonstrates that the RadICS Platform QTS will not experience failures due to abnormal service conditions of temperature and humidity as required by RG 1.209 and IEEE Std 323-2003. Section 4.3.6 of EPRI TR 107330 defines the recommended normal and abnormal temperature

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 270 of 350
--------------	--------------------	-----------	---	-----------------



and humidity exposure levels the test specimen must withstand (i.e., the test specimen must continue to meet the manufacturer specified performance levels). The environmental testing sequence is:

- Assemble the RadICS Platform QTS in the environmental test chamber
- Perform the Pre-Qualification Acceptance Testing
- Expose the RadICS Platform QTS to varying temperature and humidity conditions according to the Environmental Testing procedures
- Perform Environmental Testing Operability and Prudency Testing at the times identified in the Environmental Testing procedures
- Remove the RadICS Platform QTS from the Environmental Test chamber

The Environmental Test acceptance criteria are based on Section 4.3.6 of EPRI TR-107330.

9.1.2.4 *Seismic Testing*

Seismic testing demonstrates the suitability of the RadICS Platform for qualification as a Category 1 seismic device based on seismic withstand testing performed on the RadICS Platform QTS in accordance with RG 1.100 and IEEE Std.344-2004. Section 4.3.9 of EPRI TR 107330 (corrected version) defines the seismic test levels to which the test specimen will be exposed, while the test specimen continues to meet the manufacturer specified performance levels. The seismic test acceptance criteria are based on Section 4.3.9 of EPRI TR-107330. The seismic testing can be performed in any order after completion of the environmental testing. The seismic testing sequence is:

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

9.1.2.5 *Electromagnetic Interference/Radio Frequency Interference Testing*

The objective of EMI/RFI testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility levels. EMI/RFI testing of the RadICS Platform QTS will be performed in accordance with RG 1.180, Revision 1, using additional guidance from EPRI TR-107330, as applicable. Grounding and shielding of the RadICS Platform is in accordance with IEEE Std 1050-1996 (Reference 9-13). Since the RadICS QTS does not include the 120 V level power supplies, certain AC power-related tests are not applicable. The specific EMI/RFI tests to be performed include:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 271 of 350
--------------	--------------------	-----------	---	-----------------



- EMI/RFI Emissions Tests

MIL-461E, CE101 (Reference 9-14)	Conducted Emissions, Low Frequency, AC and DC Power Leads
MIL-461E, CE102 (Reference 9-14)	Conducted Emissions, High Frequency, AC and DC Power Leads
MIL-461E, RE101 (Reference 9-14)	Radiated Emissions, Magnetic Field, QTS Surfaces and Leads
MIL-461E, RE102 (Reference 9-14)	Radiated Emissions, Electric Field, Antenna Measurement

- EMI/RFI Susceptibility Tests

IEC 61000-4-6 (Reference 9-15)	Conducted Susceptibility, Induced RF Fields, Power/Signal Leads
IEC 61000-4-16 (Reference 9-16)	Conducted Susceptibility, Common Mode Disturbance, Power/Signal Leads
IEC 61000-4-8 (Reference 9-17)	Radiated Susceptibility, Magnetic Field, Helmholtz Coil Exposure
IEC 61000-4-9 (Reference 9-18)	Radiated Susceptibility, Magnetic Field, Pulsed
IEC 61000-4-10 (Reference 9-19)	Radiated Susceptibility, Magnetic Field, Damped Oscillatory
IEC 61000-4-3 (Reference 9-20)	Radiated Susceptibility, High Frequency, Antenna Exposure
MIL-461 E, RS103 (Reference 9-14)	Radiated Susceptibility, High Frequency, Antenna Exposure [[^{a,c,f}]]

The testing specified in IEC 61000-4-13 (Reference 9-21) is not applicable to the RadICS QTS scope.

The EMI/RFI test acceptance criteria are based on Section 4.3.7 of EPRI TR-107330 and RG 1.180. The EMI/RFI testing can be performed in any order after completion of the environmental testing. The EMI/RFI testing sequence is:

- Setup the RadICS Platform QTS in the EMI/RFI test chamber
- Perform the Pre-EMI/RFI Testing System Setup and Checkout Test
- Perform EMI/RFI Emissions Testing
- Perform EMI/RFI Susceptibility Testing

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 272 of 350
--------------	--------------------	-----------	---	-----------------



- Perform EMI/RFI Testing Operability and Prudency Testing

The electrical-related tests in described in Sections 9.1.2.6 through 9.1.2.9 are typically performed as a set. The EMI/RFI Testing Operability and Prudency Tests can be performed once at the end of the electrical-related tests as the Performance Proof Testing described in Section 9.1.2.10.

9.1.2.6 Electrical Fast Transient Testing

The objective of electrical fast transient (EFT) testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to EFT susceptibility levels. EFT testing of the RadICS Platform QTS will be performed in accordance with RG 1.180 using additional guidance from EPRI TR-107330, as applicable. The specific EFT test to be performed is IEC 61000-4-4, (Reference 9-22). The EFT testing can be performed in any order after completion of the environmental testing. The EFT acceptance criteria are based on Sections 4.6.2 and 4.3.7 of EPRI TR-107330 and RG 1.180. The EFT addresses the review guidance in BTP 7-11 (Reference 9-23).

9.1.2.7 Surge Withstand Testing

The objective of surge withstand testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to surge withstand levels. Surge withstand testing of the RadICS Platform QTS will be performed in accordance with RG 1.180, using additional guidance from EPRI TR-107330 as applicable. The specific surge withstand tests to be performed include:

IEC 61000-4-5 (Reference 9-24)	Surge Immunity Test
IEC 61000-4-12 (Reference 9-25)	Oscillatory Waves Immunity Test

The surge withstand testing can be performed in any order after completion of the environmental testing. The surge withstand test acceptance criteria are based on Section 4.6.2 of EPRI TR-107330 and RG 1.180. The surge withstand testing addresses the review guidance in BTP 7-11.

9.1.2.8 Electrostatic Discharge Testing

The objective of electrostatic discharge (ESD) testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to ESD withstand levels. EPRI TR-107330, Section 4.3.8, requires that the test specimen under qualification be tested for ESD withstand capability in accordance with the requirements of EPRI TR-102323 (Reference 9-26). In accordance with EPRI TR-102323, the specific ESD Test to be performed is the Electrostatic Discharge Immunity Test in Part 4-2 of IEC 61000-4-2 (Reference 9-27). RG 1.180 provides no guidance for ESD Testing. The ESD Testing can be performed in any order after completion of the environmental testing. The ESD acceptance criteria are based on Sections 4.3.8 of EPRI TR-107330.



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

The objective of Class 1E to non-Class 1E isolation testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to providing electrical isolation at non-Class 1E field connections, as required by IEEE Std 384-1992 (Reference 9-28). EPRI TR-107330, Section 6.3.6, requires that the test specimen under qualification be tested for Class 1E to non-Class 1E isolation capability in accordance with the requirements of EPRI TR-107330, Section 4.6.4.

The non-1E isolation testing can be performed in any order after completion of the environmental testing. The EQ Plan, the Class 1E to non-Class 1E isolation testing acceptance criteria are based on Sections 4.6.4 of EPRI TR-107330. The Class 1E to non-Class 1E isolation testing addresses the review guidance in BTP 7-11.

9.1.2.10 Performance Proof Testing

The objective of Performance Proof Testing is to demonstrate the continuing acceptable operation and performance of the RadICS Platform QTS following completion of all hardware qualification testing. EPRI TR-107330, Section 5.5 requires a final performance of the Operability Test procedure on completion of qualification testing. As an alternative to this requirement, Performance Proof Testing will include a final performance of the System Setup and Checkout, Operability, and Prudency test procedures following completion of all hardware qualification testing, and comparison of the test results to the results for all previous performances of the Operability and Prudency test procedures. Acceptance criteria for performance monitoring of the RadICS Platform QTS during Performance Proof Testing will be as specified separately in the System Setup and Checkout, Operability, and Prudency Test procedures. In addition, comparison of the Performance Proof Operability and Prudency Test data to all other Operability and Prudency test data shall not indicate an unacceptable change in performance of the RadICS Platform QTS hardware.

9.1.2.11 Operability Testing

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

Operability testing is performed at the following times during hardware qualification testing:

- With Pre-Qualification Acceptance Testing
- At the completion of the high temperature, high humidity phase of Environmental Testing
- At the completion of the low temperature, low humidity phase of Environmental Testing (Note: If the specified relative humidity cannot be achieved for the specified temperature, then separate tests can be performed after the lowest relative humidity has been achieved at the specified temperature followed by running the test at the lowest temperature that can be achieved the specified relative humidity.)

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 274 of 350
--------------	--------------------	-----------	---	-----------------



- At the completion of Environmental Testing
- At the completion of the Seismic Testing
- With Performance Proof Testing

The operability tests satisfy the computer system testing requirements in IEEE Std 7-4.3.2-2003 Section 5.4.1.

9.1.2.12 Prudency Testing

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

Prudency Testing is performed at the following times during hardware qualification testing.

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

The prudency tests satisfy the computer system testing requirements in IEEE Std 7-4.3.2-2003 Section 5.4.1.

9.1.3 Generic Qualification Envelope

Successful execution of the RadICS EQ Plan will qualified the generic RadICS digital safety I&C platform for the qualification envelope summarized in Table 9-1.



Table 9-1: Generic Qualification Envelope for the RadICS Digital Safety I&C Platform

Equipment Qualification Category	Regulatory Requirements	Source of Qualification Test Specification	Qualification Envelope and Test Levels	Qualification Test Acceptance Criteria
Radiation Exposure	RG 1.209 and IEEE Std 323-2003	Section 4.3.6 of EPRI TR-107330	Qual. envelope: 1000 Rad Test level: 1000 Rad (by analysis)	Section 4.3.6 of EPRI TR-107330
Environmental (Temperature & Humidity)	RG 1.209 and IEEE Std 323-2003	Section 4.3.6 of EPRI TR-107330	Qualification envelope: 40 °F (4.4 °C) to 122 °F (50 °C) and 10 percent to 90 percent Relative Humidity (non-condensing) Test levels: 35 °F (1.7 °C) to 140 °F (60 °C) and 5 percent to 95 percent Relative Humidity (non-condensing)	Section 4.3.6 of EPRI TR-107330 and durations shown in accompanying figure.
Seismic	RG 1.100 and IEEE Std 344-2004	Section 4.3.9 of EPRI TR-107330 (corrected version). The OBE and SSE tests shall follow the Required Response Spectrum (RRS) curve given as Figure 4-5 in EPRI TR-107330 within the limits of the seismic test table, with the proviso that the minimum Zero Period Acceleration (ZPA) requirements are met.	Resonance search as described in Section 7.1.4 of IEEE Std 344-2004	Section 4.3.9 of EPRI TR-107330
			Five triaxial OBEs tests with a minimum ZPA of 4.9 g	
			One triaxial SSE test with a minimum ZPA of 7 g	
EMI/RFI	RG 1.180	EMI/RFI Emissions Tests		Section 4.3.7 of EPRI TR-107330 and RG 1.180 Emission limit: RG 1.180: Figure 3-1
		MIL-461E, CE101 Conducted Emissions, Low Frequency, AC and DC Power Leads	30 Hz to 10 kHz [[]] ^{a,c,t}	



Equipment Qualification Category	Regulatory Requirements	Source of Qualification Test Specification	Qualification Envelope and Test Levels	Qualification Test Acceptance Criteria
		MIL-461E, CE102: Conducted Emissions, High Frequency, AC and DC Power Leads	10 kHz to 2 MHz [[]] ^{a,c,r}	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Emission limit: RG 1.180 Figure 3-2
		MIL-461E, RE101: Radiated Emissions, Magnetic Field, QTS Surfaces and Leads	30 Hz to 100 kHz	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Emission limit: RG 1.180 Figure 3-3
		MIL-461E, RE102: Radiated Emissions, Electric Field, Antenna Measurement	2 MHz to 1 GHz	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Emission limit: RG 1.180 Figure 3-4
		EMI/RFI Susceptibility Tests		
		IEC 61000-4-6: Conducted Susceptibility, Induced RF Fields, Power/Signal Leads	150 kHz to 80 MHz Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level for power leads [[]]	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level - signal and 24 VDC power leads: 126 dBμV
		IEC 61000-4-16: Conducted Susceptibility, Common Mode Disturbance, Power/Signal Leads	15 Hz to 150 kHz and DC portion on Digital Inputs	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level - power leads: RG 1.180 Table 11 Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level - signal leads: RG 1.180 Table 15



Equipment Qualification Category	Regulatory Requirements	Source of Qualification Test Specification	Qualification Envelope and Test Levels	Qualification Test Acceptance Criteria
		IEC 61000-4-8: Radiated Susceptibility, Magnetic Field, Helmholtz Coil Exposure	60 Hz	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level - continuous: 30 A/m
				Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level - short duration: 300 A/m
		IEC 61000-4-9: Radiated Susceptibility, Magnetic Field, Pulsed	60 Hz to 50 kHz	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level: 300 A/m
		IEC 61000-4-10: Radiated Susceptibility, Magnetic Field, Damped Oscillatory	100 kHz and 1 MHz	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level: 30 A/m
		IEC 61000-4-3: Radiated Susceptibility, High Frequency, Antenna Exposure	26 MHz to 1 GHz	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level: 10 V/m
		MIL-STD-461 E – RS103: Radiated Susceptibility, High Frequency, Antenna Exposure	[[]] ^{a,c,f}	Section 4.3.7 of EPRI TR-107330 and RG 1.180 Susceptibility test level: [[]] ^{a,c,f}
Electrical Fast Transient	RG 1.180	IEC 61000-4-4	Power Leads (24 VDC), Test Voltage Level: [[]] ^{a,c,f} Signal Leads, Test Voltage Level: [[]] ^{a,c,f}	Sections 4.6.2 and 4.3.7 of EPRI TR-107330 and RG 1.180



Equipment Qualification Category	Regulatory Requirements	Source of Qualification Test Specification	Qualification Envelope and Test Levels	Qualification Test Acceptance Criteria
Surge Withstand	RG 1.180	Table 22 of RG 1.180 defines the IEC 61000-4-12 Ring Wave and IEC 61000 4-5 Combination Wave surge withstand levels for power supplies installed in [[



Equipment Qualification Category	Regulatory Requirements	Source of Qualification Test Specification	Qualification Envelope and Test Levels	Qualification Test Acceptance Criteria
Electrostatic Discharge	EPRI TR 107330, Section 4.3.8, requires that the test specimen under qualification be tested for ESD withstand capability in accordance with the requirements of EPRI TR-102323. RG 1.180 provides no guidance or requirements for ESD Testing.	IEC 61000-4-2	Maximum test levels of [[]] ^{a,c,f} for air discharges and [[]] ^{a,c,f} for contact discharges, corresponding to IEC 61000-4-2 [[]] ^{a,c,f} . Testing to contact discharges will include the lower levels of [[]] ^{a,c,f} . Testing to air discharges will include the lower levels of [[]] ^{a,c,f} .	Sections 4.3.8 of EPRI TR-107330
Class 1E to Non-Class 1E Isolation	IEEE Std 384-1992. EPRI TR 107330, Section 6.3.6, requires that the test specimen under qualification be tested for Class 1E to non-Class 1E isolation capability in accordance with the requirements of EPRI TR-107330, Section 4.6.4.	Sections 4.6.4 of EPRI TR-107330	Class 1E to Non-1E isolation points are tested for a maximum isolation capability of [[]] ^{a,c,f} VAC and [[250]] ^{a,c,f} VDC at a maximum [[]] ^{a,c,f} amps applied for [[]] ^{a,c,T} seconds.	Sections 4.6.4 of EPRI TR-107330



9.1.4 Maintenance of Generic Qualification

Hardware type tests were performed on a specific version of the RadICS Platform. However, the specific version of the RadICS Platform supplied for nuclear plant applications may be a later version. If later versions are supplied for nuclear safety-related applications, the qualification basis described in the RadICS Platform Equipment Qualification Report will be augmented with technical evaluations or additional testing, based on the requirements established in Section 6.4 of IEEE Std 323-2003.

9.2 Equipment Analysis

This section describes the following generic analyses that have been performed to establish the foundations for future system-level analyses for project-specific RadICS systems:

- Board/device-level predictive reliability and safety analyses, which includes an FMEDA
- Setpoint analysis support
- Limited life parts analysis
- Radiation susceptibility

9.2.1 Failure Modes, Effects, and Diagnostic Analysis

9.2.1.1 Objective

The objectives of the board/device-level predictive reliability and safety analyses are to provide generic FMEDA and reliability data for the RadICS hardware boards/devices identified in Section 6.2. These generic results are intended to be used as input data to support a system-level FMEA and reliability analysis for an NPP-specific RadICS Platform system.

9.2.1.2 Approach for the FMEDA

An FMEA is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A (Reference 9-30). The FMEDAs are consistent the FMEA guidance of IEEE Std 352-1987, Sections 4.1, 4.4, and 4.5 (Reference 9-31).

The failure rate data used for the FMEDAs are from the Electrical and Mechanical Component Reliability Handbook (Reference 9-32), which was derived using over ten billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates. For hardware assessment according to IEC 61508, only random equipment failures are of interest.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 281 of 350
--------------	--------------------	-----------	---	-----------------



It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis. The methods used to estimate the reliability of RadICS Modules that are installed in a rack are based on the Electrical and Mechanical Component Reliability Handbook instead of MIL HDBK 217F, which is recommended in IEEE Std 352-1987. The Electrical and Mechanical Component Reliability Handbook provides more current data for modern electronic hardware than MIL HDBK 217F.

The FMEDA for each RadICS Module considered the different groups of components that affected module functionality. The following groupings were evaluated:

Common	The portion of the RadICS Module that is always used.
Input	The portion of the RadICS Module used by one on-board input channel (designated DI and AI, respectively, for discrete and analog channels).
Output	The portion of the RadICS Module used by one on-board output channel (designated DO and AO, respectively, for discrete and analog channels).
LVDS	The portion of the LM providing communication to one I/O Module.

The following definitions for the failure of the device were considered in order to judge the failure behavior of the RadICS Modules.

Fail-Safe State	State where all discrete outputs are de-energized.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process. (abbreviation: S)
Fail Safe Detected	Failure that is detected by automatic self-diagnostics, which causes the output signal to go to the predefined fail-safe state (i.e., AOMs and/or DOMs dennergized). (abbreviation: SD)
Fail Safe Undetected	Failure that is safe and that is not diagnosed by automatic self-diagnostics. (abbreviation: SU)
Fail Dangerous	Failure that does not respond to a demand from the process (i.e., being unable to go to the defined fail-safe state).
Analog Input	Failure that deviates the measured input value by more than 2% of span and leaves the value within active scale.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics. (abbreviation: DD)
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics. (abbreviation: DU)



Annunciation Detected	Failure that does not directly impact safety but does impact the ability to detect a future fault (e.g., a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm. This condition leads to maintenance, and if the safety channel is not shut down (put into the safe state) during this maintenance, the time must be accounted for in any system level reliability calculation.(abbreviation: AD)
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (e.g., a fault in a diagnostic circuit) and that is not detected by internal diagnostics. AU failures are treated as No Effect failures for Safe Failure Fraction calculation. (abbreviation: AU)
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function. (abbreviation: NE) It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508:2010.
Fail Dangerous Undetected after Surveillance Test	Failure that is dangerous and that is not being diagnosed by either automatic diagnostics or the periodic surveillance test. (abbreviation: DUaPT)

The failure categories listed above expand on the categories listed in IEC 61508:2010, which are only safe and dangerous, both detected and undetected. Under IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. It is assumed that the probability model will correctly account for the Annunciation failures; otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

9.2.1.3 Results of the Board/Device-Level Reliability Analyses

A summary of the predicted reliability for each board/device is presented in Table 9-2. All results are reported in Failure in Time (1×10^{-9} failures per hour) at sea level.

Table 9-2: Summary of the Predicted Reliability of RadICS Modules

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{AD}	λ_{AU}	λ_{NE}	λ_{DUaPT}
II								

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 283 of 350
--------------	--------------------	-----------	---	-----------------



Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{AD}	λ_{AU}	λ_{NE}	λ_{DUaPT}
								$\lambda^{a,c,f}$

* included in the I/O module 'common' failure rates.

The RadICS Platform FMEDA satisfies the reliability requirements of IEEE Std 603-1991 Section 5.15 and IEEE Std 7-4.3.2-2003 Section 5.15.

9.2.2 Setpoint Analysis Support

9.2.2.1 Objective

EPRI TR-107330, Section 4.2.4 (recommends that the qualifier provide information about the qualified hardware to support a project-specific setpoint analysis. RG 1.105 (Reference 9-33) endorses ISA-S67.04-1994 (Reference 9-34), with qualifications, as the basis for performing a project-specific setpoint analysis.

The recommended setpoint analysis support information includes the following:

- A. Calibrated accuracy, including hysteresis and non-linearity, of the analog inputs and outputs
- B. Repeatability of the analog inputs and outputs
- C. Temperature sensitivity of the analog inputs and outputs
- D. Drift with time of the analog inputs and outputs
- E. Power supply variation effects on the analog inputs and outputs
- F. Error contribution of any arithmetic operations needed to implement a setpoint. The accuracy is based on using two additions and one multiplication on an input value plus a comparison. The error contributions is provided for both integer and floating point calculations.
- G. In addition, EPRI recommends that the qualification process identify those components, if any, on analog I/O modules that are sensitive to the following:
 - o Components where vibration could affect accuracy (e.g., potentiometers)
 - o Components where radiation exposure could affect accuracy
 - o Components where relative humidity could affect accuracy

The objective of the RadICS Setpoint Analysis Support Document (Reference 9-35) is to provide a single, concise listing of the accuracy, drift, and other relevant specifications of the RadICS digital safety I&C platform. These specifications are intended to enable a licensee to calculate instrument measurement uncertainties and establish critical control setpoints for a project-specific RadICS system based on ISA-S67.04-1994.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 284 of 350
--------------	--------------------	-----------	---	-----------------



9.2.2.2 Approach

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

- Analog Input Modules
- Discrete Input Modules
- Analog Output Modules
- Discrete Output Modules

The accuracy specifications have been compiled from manufacturer's documentation and the results of qualification testing of the RadICS Platform QTS.

9.2.3 Limited Life Parts Analysis

EPRI TR-107330, Section 4.7.8.2 requires the qualifier to perform a component aging analysis on the qualified hardware based on the normal and abnormal environmental conditions to which it is exposed. The purpose of this analysis is to provide a "qualified life" for components associated with the digital I&C platform under qualification. The component aging analysis described in EPRI TR-107330, Section 4.7.8.2 is not required for the standard RadICS Platform hardware, which will be installed in a mild environment, where repair is possible after an accident. Aging analysis is required only where equipment is installed in a harsh environment, where repair is not possible after an accident. RadICS will not comply with the incorrect guidance in EPRI TR-107330, Section 4.7.8.2.

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

The types of electronic components that typically have life limits are batteries and electrolytic capacitors. The RadICS equipment described in Section 6.2 does not use any batteries or electrolytic capacitors that require regular replacement.

Project-specific RadICS systems will be examined during the design phase to confirm if any life limited components are introduced in the hardware for a specific application. If any such components are identified, appropriate measures will be identified in the Product Safety Manual to manage the life-limited component.

9.2.4 Radiation Susceptibility Analysis

The radiation exposure susceptibility analysis demonstrates that the RadICS Platform Modules will not experience failures or unacceptable degradation due to expected radiation exposure from normal and abnormal service conditions as required by RG 1.209 and EPRI TR-107330. Section 4.3.6 of EPRI TR

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 285 of 350
--------------	--------------------	-----------	---	-----------------



107330 defines the normal and abnormal radiation exposure levels the equipment must withstand and continue to meet the specified performance levels.

9.3 Chapter 9 References

- 1 Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," March 2007
- 2 IEEE Std 323-2003, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
- 3 IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
- 4 Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
- 5 Regulatory Guide 1.100, Revision 3, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants," September 2009
- 6 IEEE Std 344-2004, "Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
- 7 EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996
- 8 Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control System," October 2003
- 9 NRC Letter dated July 30, 1998 to Mr. J. Naser (EPRI), "Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute Topical Report, TR-107330, Final Report, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants"
- 10 NRC RadICS Test Specimen (RTS-001) System Requirements Specification, Document No. 2015-RTS001-SRS-001
- 11 RadICS Platform Master Configuration List, Document No. 2016-RTS002-MCL-018
- 12 RadICS Equipment Qualification Test Plan, Document No. 016-RTS002-EQTP-004
- 13 IEEE Std 1050-1996, Guide for Instrumentation and Control Equipment Grounding in Generating Stations
- 14 Military Standard 461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," August 20, 1999
- 15 IEC 61000-4-6, "Testing and Measurement Techniques, Immunity to Conducted Disturbances Induced by Radio-Frequency Fields," May 2006
- 16 IEC 61000-4-16, "Testing and Measurement Techniques, Tests for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz," July 2002
- 17 IEC 61000-4-8, "Testing and Measurement Techniques, Power Frequency Magnetic Field Immunity Test," March 2001
- 18 IEC 61000-4-9, "Testing and Measurement Techniques, Pulse Magnetic Field Immunity Test," March 2001
- 19 IEC 61000-4-10, "Testing and Measurement Techniques, Damped Oscillatory Magnetic Field Immunity Test," March 2001

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 286 of 350
--------------	--------------------	-----------	---	-----------------



- 20 IEC 61000-4-3, "Testing and Measurement Techniques, Radiated, Radio-Frequency, Electromagnetic Field Immunity Test," February 2006
- 21 IEC 61000-4-13, "Testing and Measurement Techniques, Harmonics and Interharmonics Including Mains Signaling at AC Power Ports, Low Frequency Immunity Tests," March 2002
- 22 IEC 61000-4-4, "Testing and Measurement Techniques, Section 4: Electrical Fast Transient/Burst Immunity Test," July 2004
- 23 BTP 7-11, Revision 5, Guidance on Application and Qualification of Isolation Devices
- 24 IEC 61000-4-5, "Testing and Measurement Techniques, Section 5: Surge Immunity Test," November 2005
- 25 IEC 61000-4-12, "Testing and Measurement Techniques, Section 12: Oscillatory Waves Immunity Tests," September 2006
- 26 EPRI TR-102323, Revision 1, "Guidelines for Electromagnetic Interference Testing in Power Plants," January 1997
- 27 IEC 61000-4-2, "Testing and Measurement Techniques, Section 2: Electrostatic Discharge Immunity Test," April 2001
- 28 IEEE Std 384-1994, "Standard Criteria for Independence of Class 1E Equipment and Circuits"
- 29 NUREG/CR-5609, "Electromagnetic Compatibility Testing for Conducted Susceptibility Along Interconnecting Signal Lines," August 2003
- 30 MIL STD 1629A, Military Standard: Procedures for Performing a Failure Mode, Effects, and Criticality Analysis, 1980
- 31 IEEE Std 352-1987, "Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems"
- 32 **exida** LLC, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
- 33 Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation", December 1999
- 34 ISA-S67.04-1994, "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation", Instrument Society of America
- 35 RadICS Setpoint Analysis Support, Document No. 2016-RTS002-SAS-003



10 Diversity and Defense-In-Depth

10.1 Overview

Digital I&C systems can be vulnerable to CCFs caused by software, firmware, or programmed logic errors, which could defeat the redundancy achieved by hardware architecture. CCFs are of particular interest for a digital I&C system designed to perform in nuclear safety-related projects like a Protection System (PS).

10.2 Digital Common Cause Failures

NRC considers CCFs in digital systems to be a beyond design basis event and specifies the special methods for providing the necessary protection for digital PS projects. These methods use a D3 assessment as the primary design tool. Defense-in-depth is a principle that ensures multiple layers of I&C systems exist to provide protection against a wide spectrum of anticipated operational occurrences and postulated accidents, both design basis and beyond design basis. Diversity is a principle that ensures digital I&C systems are protected against postulated CCFs, specifically in portions of a digital I&C system that are not fully testable (e.g., the software, firmware, or programmable logic).

Protection against CCF is primarily provided at the overall I&C architecture level by implementing different lines of defense and diversity. Regulatory guidance on performing D3 analyses is provided in two main documents: BTP 7-19 (Reference 10-1) and NUREG/CR-6303 (Reference 10-2). These guidance documents are tailored to a D3 assessment performed for a project-specific safety-related I&C system, so much of the guidance is not applicable to a generic platform qualification process.

10.3 Defense Against Common Cause Failures

Individual safety I&C systems are generally designed with identical equipment (same hardware and software) in redundant divisions, therefore raising a CCF issue at the system level. As stated in IEC 60880-2006 (Reference 10-3), Section 13.2, "Design of software against Common Cause Failure":

"The basic and most important defense against common cause failure due to software is to produce software of the highest quality (i.e., as error-free as possible)."

The following are measures taken by RadICS as a line of defense against software CCFs (as described in Chapter 6):

- Program code volume reduction due to application of FPGA as programmable components
- Application of distributed software and separation of safety-related functions (IEC 61266 category A functions) from those of lesser categories (i.e., IEC 61266 (Reference 10-4) Categories B and C functions) and non-safety functions
- Application of development methods and tools aimed to prevent introduction of faults into software
- Self-diagnostic testing and fault tolerant design features
- Defensive programming
- Fail-safe design features

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 288 of 350
--------------	--------------------	-----------	---	-----------------



The RadICS Module Electronic Designs are based on life cycle processes that guarantee achievement of a high level of quality (see Chapters 7 and 8). It aims at avoiding errors by means of:

- Adherence to a strict and phased development process
- Re-use of proven components
- Use of simple and proven design principles based on clearly defined rules
- Avoidance of unnecessary complexity
- Use of proven tools for automated code generation as much as possible to reduce risk of human errors
- Eliminating errors as soon as possible
- Documents produced during a phase are formally verified and reviewed before starting the next phase
- V&V tasks are performed by an independent team
- Static verification is performed on all manual source code and parameters
- Unit tests, integration tests, validation tests, factory acceptance tests, site tests are planned and performed

The steps of defense against hardware CCFs realized for both the RadICS Platform and RadICS Platform-based projects include adherence to independence principle. Generally, adherence to independence principle means that the I&C system should preserve its capacity to execute prescribed functions necessary to ensure nuclear power plant safety under failure or deliberate inactivation of one redundant channel. Radiy best practices to implement this principle are the following:

- Screening and galvanic separation of input, output circuits and power circuits in each channel using electro-optical components
- Radial ("point-to-point") structure of connections between channels to preserve the possibility and accuracy of data exchange among the rest of channels in case one of them fails
- Physical separation of redundant I&C system channels that are housed in separate cabinets and powered from different sources
- Application of technical solutions and components proven in nuclear power plant operation experience

10.3.1 Diversity

The implementation of diversity in I&C echelons of defense is based on a project-specific application. For example, a nuclear power plant could use the RadICS Platform for the RTS and a completely separate platform for the ESFAS. Alternatively, a single RadICS Platform could be used for the PS at a nuclear power plant, implementing both the RTS and ESFAS safety functions with a separate DAS. The project-specific realization of different I&C echelons of defense using the RadICS Platform is beyond the scope of this Topical Report.

The RadICS Platform can be used employ signal diversity strategies. Signal diversity is defined as the use of different sensed parameters to initiate a protective action. Signal diversity is a project-specific design decision that can be effectively implemented with the range of input module capabilities in the RadICS Platform. Signal diversity can be used to significantly improve overall PS diversity.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 289 of 350
--------------	--------------------	-----------	---	-----------------



The RadICS Platform can also be used employ functional diversity strategies. Two signal channels are functionally diverse if they perform different physical functions or employ different algorithms. Functional diversity is a project-specific design decision that can be readily implemented by allocating functionally diverse channels to separate LMs in a RadICS Platform system. As with signal diversity, functional diversity can significantly improve overall PS diversity.

The RadICS Platform supports system architectures that employ signal diversity to defend against CCFs. The RadICS Platform also can be deployed as a diverse system as part of a project-level D3 strategy. These options do not affect the generic RadICS Platform features (i.e., the hardware, electronic design, or communications features described in Chapter 6). Instead, these options only affect certain project-specific system analysis.

10.3.2 Defense-in-Depth

The design principle of defense-in-depth is applied to safety-related I&C systems through the concept of echelons of defense. NUREG/CR-6303 defines four I&C echelons of defense: control system, RTS, ESFAS, and monitoring and indicator system. These four echelons are typically thought of as providing concentric barriers of protection.

The four echelons of defense described above are only conceptual and, with the exception of the monitoring and indication echelon of defense (see Section B.1.4 in BTP 7-19), NRC regulations do not require nor does this guidance imply that RTS and ESFAS echelons of defense must be independent or diverse from each other with respect to a CCF. NRC accepts that the RTS and ESFAS echelons may be combined into a single digital I&C PS platform. However, plant responses to postulated CCF that could impair a safety function must be shown to meet the acceptance criteria defined in BTP 7-19 regardless of the echelons of defense that may be affected. The project-specific D3 analysis should consider the nuclear power plant's suite of safety and nonsafety I&C systems.

With limited exceptions, meeting the current regulatory guidance on D3 in safety-related I&C systems and replacing existing analog systems with modern digital systems requires installation of a DAS that is separate from the I&C platform (or platforms) used by the PS.

10.4 Chapter 10 References

- 1 Branch Technical Position 7-19, Revision 6, "Guidance for Evaluation of Diversity and Defense- in-Depth in Digital Computer-based Instrumentation and Control Systems"
- 2 NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"
- 3 IEC 60880:2006, "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions"
- 4 IEC 61226:2009, "Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions"



11 Secure Development and Operational Environment

This chapter discusses the RadICS Platform secure development environment, the RadICS Platform vulnerability assessment, and implementation of the secure development and operational environment controls.

11.1 RadICS Secure Development Environment

RPC Radiy and RadICS have implemented a comprehensive set of security measures that are designed to eliminate credible vulnerabilities associated with company security management and the digital equipment development process. These security measures include:

- II

II^{a,c}

The RadICS Platform secure development environment is designed to meet the guidance in RG 1.152 (Reference 11-1) 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 (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations.

11.2 Development Environment Vulnerability Assessment

RPC Radiy and RadICS conducted vulnerability assessments for the RadICS Platform development environment to identify security vulnerabilities and identify potential security measures to mitigate identified vulnerabilities. RadICS used RG 1.152 as basis for this assessment. RadICS also used RG 5.71 (Reference 11-2) to understand potential U.S. customer requirements.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 291 of 350
--------------	--------------------	-----------	---	-----------------



The RadICS Platform development environment vulnerability assessment included:

- Analysis of potential hardware vulnerabilities for the development environment
- Analysis of potential software vulnerabilities for the development environment
- Analysis of potential configuration vulnerabilities for the development environment
- Analysis of potential network vulnerabilities for the development environment

The hardware vulnerability analysis of the development environment assessed the following potential vulnerabilities:

- [[

]]^{a,c}

The software hardware vulnerability analysis of the development environment assessed the following potential vulnerabilities:

- [[

]]^{a,c}

The configuration vulnerability analysis of the development environment assessed the following potential vulnerabilities:

- [[

]]^{a,c}

The network vulnerability analysis of the development environment assessed the following potential vulnerabilities:



- [[

]]^{a,c}

A list of possible threats to the development environment was developed. Each potential development environment vulnerability was assessed against the possible threats. Appropriate security measures for each vulnerability and effective means to implement them were identified.

The results of the RadICS Platform development environment vulnerability assessment were documented in a vulnerability assessment report (Reference 11-3).

11.3 Operating Environment Vulnerability Assessment

RPC Radiy and RadICS conducted vulnerability assessments for the RadICS Platform operating environment to identify potential security vulnerabilities and identify security measures to mitigate identified vulnerabilities. RadICS used RG 1.152 as basis for this assessment. RadICS also used RG 5.71 to understand potential U.S. customer requirements.

The RadICS Platform vulnerability analysis assessed the following potential vulnerabilities:

- [[

]]^{a,c}

Each potential operating environment vulnerability for the RadICS Platform was assessed and appropriate security measures for each vulnerability were identified.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 293 of 350
--------------	--------------------	-----------	---	-----------------



The results of the RadICS Platform operating environment vulnerability assessment were document in a vulnerability assessment report.

11.4 Secure Development and Operational Environment Controls

RPC Radiy has implemented a secure development procedure that specifies the security controls for the RadICS Platform development and operational environment. The procedure provides guidance for designing digital systems (both hardware and software) to ensure that they are free from vulnerabilities that could affect the reliability of the system.

The RadICS Secure Development and Operational Environment Procedure specifies the security controls for the RadICS Platform development and operational environment (Reference 11-4). It describes the methodology for complying with regulatory requirements for promoting high functional reliability, design quality, and a secure development and operational environment for the use of safety-related digital systems used in nuclear power plants. The procedure specifies the (1) measures and controls taken to establish a secure environment for development of the digital system against undocumented, unneeded, and unwanted modifications and (2) protective actions taken against a predictable set of undesirable acts, for digital assets, that could challenge the integrity, reliability, or functionality of a digital system during operations. The RadICS Platform secure development procedure plan was developed in accordance with the guidance contained in RG 1.152, RG 1.173 (Reference 11-5), and IEEE Std 1074-2006 (Reference 11-6).

The RadICS Platform secure development environment is supported by corporate Information Security Management System policies and procedures.

RPC Radiy and RadICS have instructions that define the process for identification of information that is a commercial secret or confidential information and define controls for circulation, processing, storage, and disposal.

RPC Radiy and RadICS have instructions that define the control of physical access to development areas.

RPC Radiy and RadICS have formal security training and awareness program that was developed to keep staff up to date on prescribed organizational security policies and procedures.

RPC Radiy and RadICS have procedures and instructions for the RadICS Platform development process that implement security controls identified in the development environment vulnerability analysis.

RPC Radiy and RadICS conduct periodic audits of security-related activities to verify that controls are effectively implemented.

The RadICS Platform design features identified in the development environment vulnerability analysis are described in Sections 6.3 on communications, 6.4 on platform diagnostics, and 6.9 on access control features.

11.5 Project-Specific Vulnerability Assessments

The RadICS Secure Development and Operational Environment Procedure specifies that a project-specific vulnerability assessment be prepared that contain results of vulnerabilities assessment and

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 294 of 350
--------------	--------------------	-----------	---	-----------------



appropriate phase-specific protective actions and controls. This document is intended for implementation at development environment to cover all the revealed vulnerabilities for the development stages, including:

- [[

]]^{a,c}

The security of electronic records is assured by two main methods:

- [[

]]^{a,c}

The RadICS project-specific lifecycle security activities and documentation are shown in Figure 11-1.



[[

]]^{a,c}

Figure 11-1: RadICS Project-Specific Lifecycle Security Activities

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 296 of 350
--------------	--------------------	-----------	---	-----------------



11.6 Chapter 11 References

- 1 RG 1.152, Revision 3, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," July 2011
- 2 RG 5.71, "Cyber Security Programs for Nuclear Facilities," January 2010
- 3 RPC Radiy Document D2.8, "RadICS Security Analysis Report"
- 4 RadICS Procedure QP 03-9, "Secure Development and Operational Environment Procedure"
- 5 RG 1.173, Revision 1, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," July 2013
- 6 IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes"



12 Compliance Summary for Key Regulations, Codes, and Standards

A summary of the key NRC regulatory requirements and acceptance criteria for I&C systems important to safety identified in Chapter 5 is provided for the RadICS Platform and associated development processes. The discussion is organized into four sections: Quality Assurance, Technical Requirements, Software Development Processes, and Secure Development and Operating Environment.

12.1 Quality Assurance

The quality assurance requirements applicable to the RadICS Platform Topical Report review are found in NRC RG 1.28 (Reference 12-1) and RG 1.152 (Reference 12-2).

12.1.1 Regulatory Guide 1.28

RG 1.28, Revision 4, endorses Part I and Part II requirements included in NQA-1-2008 and the NQA-1a-2009 Addenda (Reference 12-3) as providing an adequate basis for complying with the requirements of 10 CFR Part 50 Appendix B (Reference 12-4). Compliance with 10 CFR Part 50 Appendix B is an accepted method of satisfying 10 CFR Part 50 Appendix A (Reference 12-5) GDC 1.

Chapter 3 described the RadICS QAP. The RadICS organization was described and the key organizational responsibilities for quality were identified.

The RadICS QAP is the top level QA document. It was developed to meet the requirements of NQA-1-2008/ NQA-1a-2009 Addenda. The RadICS QAP is based on NEI 11-04A (Reference 12-6). The RadICS QAP establishes the quality system document structure, which includes the following:

- RadICS QAP is the upper tier quality requirements document
- RadICS Quality Procedures implement the QAP requirements for programs and processes
- RadICS Quality Work Instructions provide standardized methods to accomplish quality-related work
- RadICS Forms and Records are used to create the implementation evident for quality-related work

All RadICS activities for the processes described in the RadICS Topical Report are performed in accordance with the RadICS QAP.

A complete set of procedures was developed to implement quality controls for all 18 criteria from 10 CFR Part 50 Appendix B. A comprehensive training program was prepared for RadICS personnel on the key elements of the QAP document and implementing procedures. A qualification and training program was implemented for QA lead auditors and inspectors. The RadICS staff has been certified on the following topics:

- Internal/External Auditing topics and techniques
- Organization Safety Culture, Root Cause determination and Problem Solving techniques

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 298 of 350
--------------	--------------------	-----------	---	-----------------



- Means to identify and deal with Counterfeit, Fraudulent, and Suspect Items
- Commercial Grade Item Dedication

GQA completed a third party evaluation in August 2016 (Reference 12-7). Evaluation QAP_EVAL-2016 was performed to assess the adequacy of the RadICS Quality Assurance Program documents for meeting 10 CFR Part 50 Appendix B, 10 CFR Part 21, ASME NQA-1-1994, NQA-1-2008, and NQA-1a-2009. The evaluation was performed as a document audit of current policies and quality procedures to assess the RadICS QAP for addressing applicable requirements for control over quality activities for supplying nuclear safety-related digital instrumentation and control equipment. The scope of the evaluation included the latest approved revisions of the RadICS QAP, 42 Quality Procedures, and 3 significant Work Instructions.

The evaluation found that the RadICS QAP was a comprehensive network of policies, procedures, instructions, and forms that address the nuclear quality assurance requirements in detail. The RadICS QAP also reflect recent regulatory developments, provisions and guidance of impact to nuclear licensees and their suppliers. GQA concluded that the RadICS QAP is comprehensively documented and compliant with stated requirements. Three evaluation comments were submitted for corrective action in accordance with the RadICS QAP.

The RadICS QAP satisfies the quality assurance requirements of IEEE Std 603-1991 (Reference 12-8) Section 5.3.

12.1.2 Regulatory Guide 1.152

NRC RG 1.152, Revision 3, endorses IEEE Std 7-4.3.2-2003 (Reference 12-9) as an acceptable method for satisfying NRC regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants.

IEEE Std 7-4.3.2-2003 Section 5.3 identifies additional requirements that are necessary to satisfy the requirements of IEEE Std 603 for digital systems for the following topics:

- Software development (Section 5.3.1)
- Use of software tools (Section 5.3.2)
- Verification and validation (Sections 5.3.3 and 5.3.4)
- Configuration management (Section 5.3.5)
- Risk Management (Section 5.3.6)
- Qualification of existing commercial computers (Section 5.4.2)

The software development process described in Chapters 7 and 8 satisfy the requirements of IEEE Std 7-4.3.2-2003 Section 5.3.1.

The use of software tools described in Chapter 8 satisfies the requirements of IEEE Std 7-4.3.2-2003 Section 5.3.2.

The V&V activities described in Chapters 7 and 8 satisfy the requirements of IEEE Std 7-4.3.2-2003 Section 5.3.3. Compliance with IEEE Std 1012-2004 (Reference 12-10) is discussed in Section 12.3.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 299 of 350
--------------	--------------------	-----------	---	-----------------



The organizational independence of the organizations performing V&V activities for the RadICS Platform described in Chapter 3 satisfy the requirements of IEEE Std 7-4.3.2-2003 Section 5.3.4.

The software configuration management process described in Chapter 7 satisfies the requirements of IEEE Std 7-4.3.2-2003 Section 5.3.5. Compliance with IEEE Std 828-2005 is discussed in Section 12.3.

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.

The commercial grade dedication process described in Chapter 4 satisfies the commercial grade dedication process requirements of IEEE Std 7-4.3.2-2003 Section 5.4.2. The RadICS Platform commercial grade dedication process described in Chapter 4 also addresses the review guidance in BTP 7-18 (Reference 12-11).

12.2 Technical Requirements

The technical requirements applicable to the RadICS Platform Topical Report review are found in RG 1.153 (Reference 12-12), RG 1.152, Revision 3, DI&C-ISG-04 (Reference 12-13), and NUREG/CR 6082 (Reference 12-14).

12.2.1 Regulatory Guide 1.153

RG 1.153, Revision 1, endorses IEEE Std 603-1991 as an acceptable method for satisfying NRC regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants. 10 CFR 50.55a(h)(2) incorporates IEEE Std 603-1991 in the regulation by reference.

IEEE Std 603-1991 has a number of technical requirements that are addressed by the RadICS Platform design:

- Equipment Qualification (Section 5.4)
- System Integrity (Section 5.5)
- Independence (Section 5.6)
- Capability for Test and Calibration (Section 5.7)
- Control of Access (Section 5.9)
- Repair (Section 5.10)
- Identification (Section 5.11)
- Reliability (Section 5.15)

The RadICS Platform EQ program described in Chapter 9 satisfies the EQ requirements of IEEE Std 603-1991 Section 5.4. The RadICS Equipment Qualification Plan conforms to IEEE Std 323-2003 (Reference 12-15), as endorsed by RG 1.209 (Reference 12-16). The seismic qualification testing is performed in accordance with the IEEE Std 344-2004 (Reference 12-17), as endorsed by RG 1.100 (Reference 12-18), using the generic seismic spectra documented in EPRI TR-107330 (corrected version) (Reference 12-19). The electromagnetic compatibility testing is performed in accordance with testing standards endorsed by RG 1.180 (Reference 12-20). The licensee for a project-specific application of the RadICS Platform will

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 300 of 350
--------------	--------------------	-----------	---	-----------------



address the correspondence of the generic qualification envelope for the RadICS Platform with the site-specific qualification bounding envelopes.

The RadICS Platform predictability and repeatability design features described in Sections 6.3, 6.4, 6.8, and 6.10 satisfy the system integrity requirements of IEEE Std 603-1991 Section 5.5.

The RadICS Platform independence features described in Section 6.6 satisfy the independence requirements of IEEE Std 603-1991 Section 5.6 for the RadICS Platform equipment. The RadICS Platform isolation features also satisfy IEEE Std 384-1992(Reference 12-21), as endorsed by RG 1.75(Reference 12-22). The electrical fast transient testing, surge withstand testing, and Class 1E to non-Class 1E isolation testing in the RadICS EQ program described in Chapter 9 address the review guidance in BTP 7-11 (Reference 12-23).

The RadICS Platform design features described in Sections 6.7, 6.11, and 6.12 provide the capability for test and calibration, which satisfy the test and calibration requirements of IEEE Std 603-1991 Section 5.7. The specific means for complying with the system level test and calibration requirements must be assessed on a project-specific basis.

The RadICS Platform control of access features described in Section 6.9 satisfy the control of access requirements of IEEE Std 603-1991 Section 5.9. Additional means for complying with the system level control of access requirements must be assessed on a project-specific basis.

The RadICS Platform design features described in Sections 6.1.3, 6.4 and 6.7 along with the design considerations summarized in Section 7.6.3 facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment, which satisfy the repair requirements of IEEE Std 603-1991 Section 5.10.

The RadICS Platform Human-Machine Interface features described in Section 6.2.1.6 satisfy the identification requirements of IEEE Std 603-1991 Section 5.11. Additional means for complying with the system level identification requirements must be assessed on a project-specific basis.

The RadICS Platform FMEDA described in Section 9.2.1 satisfy the reliability requirements of IEEE Std 603-1991 Section 5.15.

12.2.2 Regulatory Guide 1.152

NRC RG 1.152, Revision 3, endorses IEEE Std 7-4.3.2-2003 as an acceptable method for satisfying NRC regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants.

IEEE Std 7-4.3.2-2003 has a number of technical requirements that are addressed by the RadICS Platform design:

- Computer system testing (Section 5.4.1)
- System integrity (Sections 5.5.1, 5.5.2, and 5.5.3)
- Independence (Section 5.6)
- Identification (Section 5.11)

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 301 of 350
--------------	--------------------	-----------	---	-----------------



- Reliability (Section 5.15)

The RadICS Platform EQ program described in Chapter 9 specifies the performance of operability and prudence tests, as defined in EPRI TR-107330. In RG 1.209, NRC noted that it has accepted EPRI TR-107330 as an acceptable method for addressing mild-environment qualification of digital platforms. The RadICS Platform EQ program satisfies the computer system testing requirements in IEEE Std 7-4.3.2-2003 Section 5.4.1.

The RadICS Platform predictability and repeatability design features described in Sections 6.3, 6.4, 6.8, and 6.10 satisfy the design for computer integrity requirements in IEEE Std 7-4.3.2-2003 Section 5.5.1. The RadICS Platform diagnostic features described in Section 6.4 were developed in accordance with the ED development process described in Chapters 7 and 8. The RadICS Module EDs were subject to the V&V process described in Section 7.4 and the configuration management process described in Section 7.5. The controls for the development of the RadICS Platform diagnostic features satisfy the design for test and calibration requirements in IEEE Std 7-4.3.2-2003 Section 5.5.2. The RadICS Platform diagnostic features described in Section 6.4 satisfy the fault detection and self-diagnostics requirements in IEEE Std 7-4.3.2-2003 Section 5.5.3. The RadICS Platform diagnostic features described in Chapter 6.4 address the review guidance in BTP 7-17. The use of these automatic test features as credit for performing Technical Specification surveillance test functions must be assessed on a project-specific basis. The RadICS Platform timing diagrams and Working Cycles described in Section 6.10 addresses the BTP 7-21 (Reference 12-24) review guidance regarding allocation of system timing requirements to the digital computer portion of the system. The system level aspects of system timing must be assessed on a project-specific basis.

The RadICS Platform communication features described in Sections 6.3, 6.4, and 6.6 satisfy the system independence requirements of IEEE Std 7-4.3.2-2003 Section 5.6.

The RadICS Module version authentication features of the RadICS Platform described in Section 6.1.3 satisfy the identification requirements of IEEE Std 7-4.3.2-2003 Section 5.11.

The RadICS Platform FMEDA described in Section 9.2.1 satisfies the reliability requirements of IEEE Std 7-4.3.2-2003 Section 5.15.

12.2.3 DI&C-ISG-04

The generic RadICS Platform communication independence features comply with the DI&C-ISG-04 guidance regarding inter-divisional communication. The generic RadICS Platform does not include priority logic for command prioritization. The generic RadICS Platform design supports multi-divisional communication only in divisional voting logic and divisional display processors as described in Chapter 6. The details of the alignment of the RadICS Platform capabilities with the criteria in DI&C-ISG-04 are presented in Appendix B.



12.2.4 NUREG/CR 6082

Section 2 of NUREG/CR-6082, Data Communications, has 15 questions intended to help focus reviews of data communication systems. Table 12-1 provides an evaluation the RadICS platform for those questions.

Table 12-1: Responses to NUREG/CR-6082 Communications System Questions

NUREG/CR-6082 Question	RadICS Platform
2.1.1. Is it an event-based or state based system?	The RadICS Platform is a state-based system that operates in a deterministic way, as described in Sections 6.3, 6.4, and 6.10. The communication between the RadICS Platform Chassis is asynchronous.
2.1.2. Is there an accurate picture of the layout?	The detailed architectures of the RadICS Modules and the connection of each Unit are known, as described in Section 6.2.4.
2.1.3. Are the data rates known between all nodes of the architecture? Are they known for upset and error conditions?	The data rates between all nodes of the architecture are based on the Work Cycle time. This Work Cycle time is constant, as described in Section 6.10. The Work Cycle time is fixed and based on the definition of the data sent on the network during the design phase. The consistency of data transmission is verified, as described in Sections 6.4 and 6.8.
2.1.4. Is the message mix known? Is it known for upset and error conditions?	The messages mix is well-characterized and the data are carried in defined protocols, as described in Section 6.3.3.
2.1.5. Are the timing and delay requirements known?	Timing and delay requirements are expressed in detailed system requirements. The response time of the RadICS Platform system is defined by a theoretical model (as described in Section 6.10) and verified on the equipment during factory tests.
2.1.6. Is the system "deterministic" and the effects of error recovery accounted for?	The protocol is deterministic. Even in case of errors, the Work Cycle time is constant, as described in Section 6.10. If there is any error, they are detected by the communication error detection features described in Section 6.4. Section 6.3 describes the response of the RadICS Platform to communication errors.



NUREG/CR-6082 Question	RadICS Platform
2.1.7. Is the actual link capacity including interface, operating system, and protocol performance effects being quoted, or is the vendor basing calculations on raw media bandwidth?	The Work Cycle time includes the timing of reception and transmission processing (described in Section 6.10) and is used to determine the actual link capacity.
2.1.8. What are the media requirements?	The media (cable and fiber optic) are defined in Section 6.3.1. The use of these media is tested for electromagnetic compatibility, as described in Section 9.1.2.5.
2.1.9. Does the design meet independence requirements?	The RadICS Platform independence features are described in Section 6.6.
2.1.10. What are the communications error performance requirements?	The RadICS Platform communication error detection features are described in Section 6.4.
2.1.11. What are the protocol requirements? What services should the protocol provide?	The media are off-the-shelf product. The RadICS Platform communication protocols are proprietary and developed by RPC Radiy, as described in Section 6.3.3.
2.1.12. Is there theoretical support for performance and reliability?	For performance, the cycle time of each Chassis is fixed and monitored, as described in Section 6.10. For reliability, the FMEDA described in Section 9.2.1 included an evaluation of the communication protocols.
2.1.13. Is there experimental support for performance and reliability?	Detection of failed components is supported by system self-tests. Then repair is limited to replacement of RadICS Modules and the cabling is facilitated by use of connectors. Restoration of RadICS Platform operation after identification of any failure of an electronic component is simple and not time consuming.
2.1.14. Is there an installed base? If proprietary, how many suppliers support the medium and the protocol software?	The RadICS Platform is already installed in many NPPs, as discussed in Chapter 2. The communication protocols are provided by RadICS Platform proprietary EDs.
2.1.15. Is there a good match between nodes processors, networks controllers, and operating system and protocol stack?	The RadICS Platform is already installed in safety systems of NPPs. This long-term installation and operation allows us to claim that there is a good match between all elements of the RadICS Platform.

12.3 Software Development Processes

The software development requirements applicable to the RadICS Platform Topical Report review are found in RGs 1.173 (Reference 12-25), 1.172 (Reference 12-26), 1.171 (Reference 12-27), 1.170

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 304 of 350
--------------	--------------------	-----------	---	-----------------



(Reference 12-28), 1.169 (Reference 12-29), and 1.168 (Reference 12-30). Additional review guidance is found in BTP 7-14 (Reference 12-31).

12.3.1 Regulatory Guide 1.173

RG 1.173, Revision 1, endorses IEEE Std 1074-2006 (Reference 12-32). IEEE Std 1074-2006 provides a structured approach for developing a software life cycle program consistent with this regulatory guidance. The life cycle processes for the RadICS Platform and Application ED were established according to the guidance provided in IEC 60880:2006 (Reference 12-33) and IEC 60508:2010 (Reference 12-34) and was documented in dedicated development plans, which are described in Chapters 7 and 8. The RadICS Module ED life cycle process described in Chapter 8 was established according to the guidance provided in IEC 62566:2011 (Reference 12-35). The RadICS Platform and Application ED lifecycles conform to IEEE Std 1074-2006, as endorsed by RG 1.173, Revision 1.

12.3.2 Regulatory Guide 1.172

RG 1.172, Revision 1, endorses IEEE Std 830-1998 (Reference 12-36). IEEE Std 830-1998 is a recommended practice for writing software requirements specifications; however, as a recommend practice, it does not identify and specific requirements. The RadICS Platform requirements documents described in Section 7.3.2 follow the recommendations in IEEE Std 830-1998, as endorsed by RG 1.172, Revision 1, with two exceptions. The RadICS Platform and Application ED requirements documents follow the format requirements of the respective quality assurance programs rather than the recommendation provided in IEEE Std 830-1998 Section 5. The RadICS requirements are not ranked for importance, as recommended by IEEE Std 830-1998 Section 4.3.5. RG 1.172, Revision 1, does not support the ranking approach recommended by IEEE Std 830-1998.

12.3.3 Regulatory Guide 1.171

This RG endorses IEEE Std 1008-1987 (Reference 12-37). IEEE Std 1008-1987 describes a structured approach for performing software unit testing. The Function Block Library testing described in Chapters 7 and 8 represent unit level testing for the RadICS Platform. The Function Block Library testing conforms to IEEE Std 1008-1987, as endorsed by RG 1.171, Revision 1.

12.3.4 Regulatory Guide 1.170

This RG endorses IEEE Std 829-2008 (Reference 12-38). IEEE Std 829-2008 provides a structured approach to software test documentation. Section 7.4.5.2 describes the RadICS approach to Platform and Application ED V&V test documentation. The test documents have been structured to reflect the use of RadICS Platform and Application ED development lifecycle, the use of FPGA technology, and conformance to respective quality assurance programs for document format. These adaptations are consistent with the provision identified in IEEE Std 829-2008 Section 6 and RG 1.170 Regulatory Position C.1. RadICS believes that the RadICS Platform test documentation conforms to the technical requirements of IEEE Std 829-2008 but not necessarily all of the administrative requirements.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 305 of 350
--------------	--------------------	-----------	---	-----------------



12.3.5 Regulatory Guide 1.169

This RG endorses IEEE Std 828-2005 (Reference 12-39). IEEE Std 828-2005 describes a structured approach to software configuration management. The RadICS approach to software configuration management is described in Section 7.5. The RadICS Platform and Application ED configuration management programs conform to the requirements in IEEE Std 828-2005, as endorsed by RG 1.169, Revision 1, with one exception. The RadICS Platform and Application ED lifecycles do not include interfaces with external organizations that design software for a project. As such, the interface controls specified in IEEE Std 828-2005 Section 3.3.5 are not implemented. The design interfaces internal to RadICS are controlled within the design control process.

12.3.6 Regulatory Guide 1.168

This RG endorses IEEE Std 1012-2004. IEEE Std 1012-2004 describes a structured approach to software V&V. The RPC Radiy and RadICS approach to software V&V is described in Chapters 7 and 8. The RadICS Platform and Application ED V&V programs activities and tasks have been adapted to reflect the use of RadICS Platform development lifecycle and the use of FPGA technology, as allowed by IEEE Std 1012-2004 Section 1.7. The RadICS Platform and Application V&V programs conform to the requirements in IEEE Std 1012-2004, as endorsed by RG 1.169, Revision 1, with five exceptions. The specific administrative requirements for administrative and formatting requirements specified in IEEE Std 1012-2004 Sections 7 and 8 are not followed. Instead, the V&V documents conform to established design practices and quality assurance program requirements. The criticality analysis is not performed, since all RadICS Module EDs are classified at the highest level for use in safety-related systems. The FMEDA describe in Section 9.2.1 and the IEC Safety Integrity Level certification described in Section 4.1.2.3 replace the hazards analyses specified in IEEE Std 1012-2004 Section 5 and Tables 1 and 2. The security vulnerability assessments described in Sections 11.2 and 11.3 replace the security analyses specified in IEEE Std 1012-2004 Section 5 and Tables 1 and 2. The RPC Radiy and RadICS approach to V&V test documentation described in Section 12.3.4 is used as an alternative to the test documentation requirements specified in IEEE Std 1012-2004 Section 6.3.1.

RG 1.168 also endorses IEEE Std 1028-2008 (Reference 12-40). IEEE Std 1028-2008 describes methods to perform to software reviews and audits. The RPC Radiy and RadICS approach to software reviews is described in Section 7.4.3. The RPC Radiy and RadICS approach to software audits is described in Sections 7.3.1, 7.5.3.3, and 11.4. RPC Radiy and RadICS perform the audits and documents the results in accordance with established practices and quality assurance program requirements instead of the methods specified in IEEE Std 1028-2008.

12.3.7 Branch Technical Position 7-14

BTP 7-14, Revision 5, provide a structured approach for developing software using a series of planning documents. The RadICS Platform EDs were developed according to the guidance provided in IEC 60880:2006 and IEC 61508:2010. The IEC SIL certification process requires that products developed under a FSMP. The FSMP is the main planning document and takes all IEC 61508:2010 requirements into consideration and mandates how they are applied throughout the product life cycle. The FSMP covers the same scope as five BTP 7-14 plans: Software Management Plan, Software Development Plan,

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 306 of 350
--------------	--------------------	-----------	---	-----------------



Software Quality Assurance Plan, Software Integration Plan, and Software Safety Plan. The comparable RadICS Platform documents are mapped to the BTP 7-14 planning scheme in Figure 12-1. The RadICS Platform Document D11.1, *Product Safety Manual*, is closely related to the Application Guide Documentation discussed in EPRI TR-107330.

The figure also shows the mapping of the RadICS Application ED development documents to the BTP 7-14 topics. The RadICS Software Quality Assurance Plan is the main planning document and covers the same scope as seven BTP 7-14 plans: Software Management Plan, Software Development Plan, Software Quality Assurance Plan, Software Integration Plan, Software V&V Plan, Software Configuration Management Plan, and Software Safety Plan. The RadICS Product Safety Manual covers the same scope as three BTP 7-14 plans: Software Installation Plan, Software Maintenance Plan, and Software Operations Plan.

12.4 Secure Development and Operating Environment

The secure development and operating environment guidance applicable to the RadICS Platform Topical Report review are found in RG 1.152, Revision 3.

12.4.1 Regulatory Guide 1.152

The RadICS Platform secure development and operating environment assessment provided in Chapter 11 satisfies the requirements of RG 1.152, Revision 3, Regulatory Position C.2.



[[

]]^{a,c}

Figure 12-1: Mapping RadICS Documents to BTP 7-14

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 308 of 350
--------------	--------------------	-----------	---	-----------------



12.5 Chapter 12 References

- 1 Regulatory Guide 1.28, Revision 4, "Quality Assurance Program Criteria (Design and Construction)"
- 2 Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
- 3 ASME NQA-1-2008, "Quality Assurance Program Requirements for Nuclear Facilities"
- 4 10 CFR Part 50 Appendix B, "Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants"
- 5 10 CFR Part 50 Appendix A, "General Design Criteria (GDCs)"
- 6 Nuclear Energy Institute Letter to NRC dated June 6, 2013, "Issuance of NEI 11-04A, Revision 0, Nuclear Generation Quality Assurance Program Description"
- 7 Global Quality Assurance letter to RadICS dated August 26, 2016, "Evaluation of the RadICS Quality Assurance Program Description"
- 8 IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations"
- 9 IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
- 10 IEEE Std 1012-2004, "IEEE Standard for Software Verification and Validation Plans"
- 11 BTP 7-18, Revision 5, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems"
- 12 Regulatory Guide 1.153, Revision 1, "Criteria for Safety Systems"
- 13 DI&C-ISG-04, Revision 1, "Highly Integrated Control Rooms - Digital Communication Systems"
- 14 NUREG/CR 6082, "Data Communications," August 1993
- 15 IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
- 16 Regulatory Guide 1.209, March 2007, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants"
- 17 IEEE Std 344-2004, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
- 18 Regulatory Guide 1.100, Revision 3, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants"
- 19 EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996
- 20 Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems"
- 21 IEEE Std 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits"
- 22 Regulatory Guide 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems"
- 23 BTP 7-11, Revision 5, "Guidance on Application and Qualification of Isolation Devices"
- 24 BTP 7-21, Revision 5, "Guidance on Digital Computer Real-Time Performance"
- 25 Regulatory Guide 1.173, Revision 1, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"



- 26 Regulatory Guide 1.172, Revision 1, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- 27 Regulatory Guide 1.171, Revision 1, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- 28 Regulatory Guide 1.170, Revision 1, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- 29 Regulatory Guide 1.169, Revision 1, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- 30 Regulatory Guide 1.168, Revision 2, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- 31 BTP 7-14, Revision 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- 32 IEEE Std 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes"
- 33 IEC 60880:2006, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions"
- 34 IEC 61508:2010, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems"
- 35 IEC 62566:2011, "Nuclear Power Plants – Instruments and Control Important to Safety – Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions"
- 36 IEEE Std 830-1998, "IEEE Recommended Practice for Software Requirements Specifications"
- 37 IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing"
- 38 IEEE Std 829-2008, "IEEE Standard for Software Test Documentation"
- 39 IEEE Std 828-2005, "IEEE Standard for Software Configuration Management Plans"
- 40 IEEE Std 1028-2008, "IEEE Standard for Software Reviews and Audits"



Appendix A: RadICS Platform Application Guide

The RadICS Platform Application Guide provides a summary of the guidance for applying the RadICS Platform in NPP I&C systems classified as safety-related. The application guidance is documented in the RadICS Product Safety Manual (Reference A-1), which meets the intent of the application guide documentation described in EPRI TR-107330 (Reference A-2). The qualified RadICS Platform equipment is documented in the Master Configuration List (Reference A-3).

A.1 RadICS Platform Capabilities

A.1.1 RadICS Platform Modes of Operation

The RadICS Platform has seven modes of operation. Five modes are associated with routine operation of the RadICS Platform. Two other modes are infrequent activities associated with changing parameters used by the Application Logic, calibrating the analog I/O channels, or changing a RadICS Module Electronic Design configuration.

A.1.1.1 Routine Modes of Operation

Figure A-1 provides an illustration of the evolution over time of the RadICS Platform, from initial startup through infrequent failures and maintenance and return to full operation. It is representative of the modes of operation that will be seen during routine system operation.

[[

]]^{a,c,e}

Figure A-1: Illustrative Timeline of RadICS Platform Operating Modes

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 311 of 350
--------------	--------------------	-----------	---	-----------------



- POWERED-OFF mode

The RadICS Platform is in the POWERED OFF mode when both 24 VDC supplies are removed. In the POWERED-OFF mode, all RadICS Platform outputs are in their safe state. The RadICS Platform will restart only if all power is removed and then the RadICS Platform is powered up by either one or both 24 VDC power sources. [[]]^{a,c,e}

- Power-up → STARTUP mode

When the RadICS Platform is powered up, there is a [[]]^{a,c,e} second period of operation in STARTUP mode during which all outputs are held in the safe state¹⁰ and the RadICS Platform performs all standard self-diagnostic tests plus some extra tests. At the end of STARTUP mode, all Application Logic is initialized, and ready to implement the Application ED.

- STARTUP mode → RUN (SAFE) mode with SOR Set

At the end of a successful STARTUP mode period (i.e., no safety-critical failures were detected), the RadICS Platform will allow the SOR to be reset. Until the SOR is reset, the RadICS Platform operates in RUN (SAFE) mode.

In RUN (SAFE) mode, the Application ED executes normally, setting the internal values of the outputs; however, all outputs are subjected to the SOR, which sets the final outputs to the safe state. (Note: Input Modules skip the RUN (SAFE) mode because they are not equipped with the SOR. They transition directly from STARTUP to RUN mode.)

- RUN (SAFE) → RUN mode with SOR Reset

Transition out of RUN (SAFE) mode into RUN mode occurs when the Reset-SOR input is closed and all conditions that set the SOR have cleared. There are two options to implement this feature:

- 1) Manual reset by the operator [[]]^{a,c,e}
- 2) Installed wiring that holds the reset circuit closed, thus providing an automatic transition from STARTUP mode, momentarily to RUN (SAFE) mode, and then within [[]]^{a,c,e} milliseconds to RUN mode.

Once the SOR is reset by the operator [[]]^{a,c,e}, the RadICS Platform transitions to RUN mode and all outputs are under control of the Application Logic.

¹⁰ [[]]

]]^{a,c,e}



- **FAULTED mode**

Each RadICS Module transitions to FAULTED mode from any other mode if the RadICS Platform detects any failure that could possibly render FPGA logic unable to correctly implement the intended safety function (e.g., [[

]]^{a,c,e} In FAULTED mode, all outputs of the Module are set to the safe state. [[

]]^{a,c,e} display and the FAULTED mode LED will be switched on. Operator intervention is required to restore normal operation by replacing the failed Module and resetting SOR.

The LM may also be forced into FAULTED mode by the Application Logic. In this case the LM will command all output Modules to go to the safe state. If the Application Logic forced the LM into FAULTED mode, [[

]]^{a,c,e}

A.1.1.2 Infrequent Modes of Operation

The TUNING mode is used to change parameters used by the Application Logic. The CONFIGURATION Mode is used for calibrating the analog I/O channels or changing a RadICS Module ED configuration.

- **TUNING Mode**

In this mode, parameters defined during the development of the Application Logic design can be adjusted by connecting a MATS Tuning PC with special software to the RadICS Platform. [[

]]^{a,c,e}

- **CONFIGURATION mode**

CONFIGURATION mode is used in a DLS, which is a separate RadICS Chassis that is not connected to the field, for the following maintenance operations:

1) [[

]]^{a,c,e}



A.1.2 Response to Platform Failures

At some random point in time, a failure of a RadICS Module may occur.

- I/O Failures

A failure of a complete I/O input Module (AIM or DIM) or an I/O channel on an input Module may occur. If this happens, it is reported to the Application Logic, which makes the decision on managing this failure.

A failure of an I/O channel on an output Module (i.e., DOM or AOM) may occur. When such a failure is detected by the DOM or AOM, it is reported to the Application ED. The Application Logic should be designed to command the opening of the specific digital or analog output.

When the digital or analog output channel failure is reported to the Application ED, the Application Logic may then force the complete DOM or AOM (or all DOMs and AOMs) into RUN (SAFE) mode (which opens all digital or analog output channels by two mechanisms) or FAULTED mode.

- LM Failures

A failure of a LM may occur. The LM is driven to FAULTED mode and drives all other output Modules to the Safe State via two mechanisms (every digital output channel is driven open, every analog output channel is driven to the safe conditions, and the SOR is set).

When the failed LM Module is replaced, and the LM starts up and when it is allowed to enter RUN mode, it re-activates the output Modules allowing them to return to RUN mode, and normal RadICS Platform operation resumes.

- FAULTED mode

Each RadICS module transitions to FAULTED mode from any other mode if:

- 1) The Platform ED detects any failure which could possibly render FPGA logic unable to correctly implement the intended safety function (e.g., power supply out of tolerance, clock failure, CRC check error) or
- 2) The Application Logic requests it (using the TRIP function block).

In FAULTED mode, all outputs of the module are set to the safe state. A failed module will indicate an error code on the 4-character display and the FAULTED mode LED will be switched on (except for a total power failure). Operator intervention is required to restore normal operation by replacing the failed module and resetting SOR.

The LM may also be forced into FAULTED mode by the Application Logic. In this case, the LM will display the corresponding code on the LM digital display and command all output modules to go to the safe state (which they do by commanding all individual outputs to the safe state and by setting the SOR). If the Application ED forced the LM into FAULTED mode, then it is possible that the LM itself has not failed

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 314 of 350
--------------	--------------------	-----------	---	-----------------



and will not need to be replaced. The RadICS system can be restored to normal operation by extracting and re-inserting the LM. This action causes the LM to go through its complete startup process.

A.1.3 User Designed Response to Platform Failures

The RadICS Platform will not go into a fail-safe mode automatically upon detection of the following failures and, therefore, the Application Logic must implement the desired action for these events:

- 1) Any failure of a field input signal,
- 2) Any failure of an individual I/O channel on a module,
- 3) Any complete failure of a module,
- 4) Any failure in a remote RadICS chassis which has switched to the RUN (SAFE) mode and that communicates with the local chassis under consideration (the resulting stale data from such a remote chassis must be detected by Application Logic in the local chassis), and
- 5) EEPROM failure after STARTUP (Note: These EEPROMs are used only at power-up, so a detected failure occurring during operation is an early warning that the next power-up will not succeed).

The Application Logic can be designed to detect these failures by:

- 1) Setting the safe state (for de-energize to trip applications) by forcing the LM into FAULTED mode via the TRIP function block,
- 2) Setting the safe state by setting the SOR via the SETSOR function block,
- 3) Driving appropriate DOs or AOs to the safe state, or
- 4) Simply setting a DO or AO to signal an alarm.

A.1.4 Local Indications of RadICS Platform Modes and Status

Each RadICS Module of has two LEDs on the front (RUN and FAULT) as well as a 4-character digital display. The LEDs are the major status indicators, as shown below:

FAULT LED	Off	No failure (or power failure)
	Flashing	(Occurs normally during startup) Non-critical failure when the RadICS Platform is not in startup sequence
	On	Critical failure
RUN LED	On	Normal Operation
	Flashing	While Module is in CONFIGURATION mode
	Off	(Occurs normally during startup) Critical failure (or power failure)

In the absence of failures, the 4-character display indicates the operating mode as follows:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 315 of 350
--------------	--------------------	-----------	---	-----------------



STARTUP	RUN (SAFE)	RUN	CONFIGURATION
STUP	RUNS	RUN	CFG

If a failure occurs the 4-character display shows an error code, and maintenance will generally be required. If the Application Logic has put the RadICS Platform into the safe state, then the 4-character display on the LM will display #1DB (if SOR set from Application Logic) or #1DC (if Application Logic puts system in Faulted Mode). The RadICS Product Safety Manual contains a listing of all the faults codes.

A.2 System Design Guidance

A.2.1 RadICS Chassis Configuration

The qualified RadICS Chassis configuration consists of one LM, located in slot F1 (left end from front side). Slot F2 (right end from front side) is not used. The 14 central module slots may be empty or used for any combination of I/O Modules. The backplane provides completely separate and dedicated communications lines between slot F1 and every optional module slot (i.e., 14 separate dedicated communications lines).

The qualified RadICS Chassis supports the use of EMI/RFI protection filters. They are mounted within the chassis at the rear directly behind their respective I/O Modules. The protection filters are specific to the type of I/O Module they protect. This means that changing the use of a slot from one type of module to another requires relocating the filters.

A.2.2 Power Supplies

The entire RadICS Chassis is supplied with one or two +24 VDC power supplies which are mounted externally to the RadICS Chassis. The two power sources are independently supplied to every module slot, and every module has its own galvanically isolated power supply sub-module which uses both supply lines.

The power supply requirements are two separate feeds, each meeting the following requirements:

Nominal:	24 VDC
Operating Limits:	[[]] ^{a,c,e} VDC to [[]] ^{a,c,e} VDC
Capacity:	Calculated based on rack configuration

The nominal maximum load for the RadICS Chassis depends on the numbers of modules of each type, and should be calculated by the end user. The end user should then allow a suitable margin in power supply capacity. The nominal maximum loads for each Module type are:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 316 of 350
--------------	--------------------	-----------	---	-----------------



Module	Consumption (Ampere)
LM	[[]] ^{a,c,e}
AIM	[[]] ^{a,c,e}
DOM	[[]] ^{a,c,e}
DIM	[[]] ^{a,c,e}
AOM	[[]] ^{a,c,e}
OCM	[[]] ^{a,c,e}

A.2.3 Environmental Conditions

The RadICS Platform should be stored and shipped, and operated within the environmental conditions indicated below:

Operating Temperature	0 – 50 °C (cabinet temperature)
Operating Temperature	
LM	0 – 70 °C [[]] ^{a,c,e}
AIM	0 – 85 °C [[]] ^{a,c,e}
DIM	0 – 85 °C [[]] ^{a,c,e}
DOM	0 – 85 °C [[]] ^{a,c,e}
AOM	0 – 85 °C [[]] ^{a,c,e}
OCM	0 – 70 °C [[]] ^{a,c,e}
Storage Temperature	-40 – +65 °C
Operating Humidity	Up to 95% (50 °C), Relative Humidity (non-condensing)
Storage Humidity	Up to 95% (50 °C), Relative Humidity (non-condensing)
[[]] ^{a,c,e}

Operating temperature of the RadICS Modules must be monitored because the failure rates do vary as a function of temperature. Temperature monitoring is used to ensure the RadICS Platform is operating within the qualified envelope. The Application Logic must be configured for monitoring of the surface temperature of the RadICS Modules to alarm or go to the safe state, as specified by the end user requirements.

A.2.4 Inputs and Outputs

The RadICS Modules have the following I/O capacities:

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 317 of 350
--------------	--------------------	-----------	---	-----------------



LM	Discrete inputs: 3 Channels (Channel 1 is reserved) Discrete outputs: 6 Channels
AIM	32 channels
DIM	32 channels
DOM	32 channels
AOM	32 channels
OCM	5 fiber optic channels and 5 RS-232/485 channels

Single chassis I/O capacity can be extended using OCMs to connect three chassis in series. The limit of three is RadICS recommendation, not a hard functional limitation. The end user can build a configuration with four or five chassis in series, provided that the time response and reliability are adequate for the application.

A.2.4.1 Discrete Inputs

The discrete inputs are dry contacts (24 VDC supplied by each discrete input channel). The contact properties are:

- sensed open: Impedance > 20 k Ω (provides < 2 mA (milliamp))
- sensed closed (low level): Impedance < 10.8 k Ω (provides \geq 2 mA)
- sensed closed (high level): Impedance < 2.7 k Ω (provides \geq 5 mA);

Maximum current: 10 mA per channel

[[

]]^{a,c,e}

Circuit Current	Interpreted Short-Circuit	Interpreted Field State
[[
]] ^{a,c,e}

A.2.4.2 Discrete Outputs

The discrete outputs are field effect transistor driven (Form A) with a voltage and current rating of 48 VAC/VDC and 500 mA.



A.2.4.3 Analog Inputs

The analog inputs have the following characteristics:

- Hardware range: 0 – 5.1 VDC
- Signal range: 0 – 5.0 VDC (0 – 20 mA using a precision 250 Ω resistor)
- Common mode rejection: 86 dB
- Input impedance (when powered on or off): 1 M Ω
- Diagnostic Discrepancy Threshold: 2% of full scale. [[

]]^{a,c,e}

A.2.4.4 Analog Outputs

Each of the analog output channels can operate in one of ranges listed below:

Option 1	Hardware range: 0 – 5.0 VDC Signal range: 0 – 5.0 VDC (using > 1 k Ω load) Diagnostic Discrepancy Threshold: 2% of full scale
Option 2	Hardware range: 4– 20.0 mA Signal range: 4 – 20.0 mA (using a 50 – 1000 Ω load) Diagnostic Discrepancy Threshold: 2% of full scale
Option 3	Hardware range: -10.0 – +10.0 VDC Signal range: -10.0 – +10.0 VDC (using > 1 k Ω load) Diagnostic Discrepancy Threshold: 2% of full scale
Option 4	Hardware range: 0– 20.0 mA Signal range: 0– 5.0 mA (using a 50 – 1000 Ω load) Diagnostic Discrepancy Threshold: 2% of full scale

An analog output channel will be declared failed if the discrepancy between the DAC and ADC Units exceeds the diagnostic discrepancy threshold.

A.2.5 Operational Features

Specific operational features that apply to the use of the RadICS Platform include the SOR and access controls for periodic maintenance.



A.2.5.1 *Safety Override Operation*

The SOR is a supplementary safety function of the RadICS Platform that permits a temporary override to safe-state values of the safety-critical outputs of the system when the SOR is set and allows a return to normal operation when the SOR is reset. The SOR may be used under administrative control to manually set RadICS Modules to a safe state while a maintenance work is performed in the rack.

The SOR can be set under any of several conditions (i.e., manual switch actuation or automatically by the Application Logic, if configured to do so). The SOR can only be reset by operator (or hardwired) action when all setting conditions are clear.

The SOR is always configured to be set globally by configuring the Set-SOR and Reset-SOR switches as inputs to the LM. The SOR can also be configured to be set locally (i.e., to affect only a specific output module) by configuring additional Set-SOR and Reset-SOR switches as inputs to one or more DOM or AOM.

A Keyswitch is recommended for the Set-SOR contacts for better assurance that the maintenance work has been authorized. A ganged continuous-contact pushbutton or switch can be used if there is a requirement to be able to quickly force the system into the safe state. A momentary-contact keyswitch is recommended for the Reset-SOR contact for better assurance that releasing the safe state has been authorized.

The SOR can also be configured to automatically transition through RUN (SAFE) mode to RUN mode by jumpering the set-SOR and Reset-SOR pinouts (analogous to continuously closed switches) at the SOR connectors on the RadICS Chassis.

A.2.5.2 *Access Control Features*

The RadICS Platform has access control features to support TUNING mode operation.

The TUNING Keyswitch is typically mounted on the RadICS Chassis and is connected directly to a dedicated contact input on the LM. The ARMED Keyswitch operates a dry contact supplied by end user is used by RadICS Platform. It may be driven by any secure means (e.g., keyswitch). The dry contact is used to indicate that the end user downstream safety logic is secured in safe state. The ARMED key contact is connected to a designated input on LM. The keyswitches can be mounted anywhere that is convenient to the end user and consistent with their functions.

The TUNING keyswitch is typically controlled by the control room staff. This keyswitch must be present and turned to the “tune” position for the RadICS Module to provide power internally to the designated tuning port used to connect the MATS Tuning PC. The tuning activity is signaled to the MATS and the control room, as specified by the end user requirements.

The ARMED keyswitch is used to permit complete testing of single or multiple safety functions within the RadICS Platform system. The keyswitch is used to force all safety field outputs of the RadICS Platform to the safe state regardless of the state of the RadICS Platform outputs. A contact from this logic is provided to the RadICS Platform to indicate the safety load is in the safe state. The end user uses the ARMED keyswitch to place the RadICS Platform field outputs in the safe state whenever tuning the

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 320 of 350
--------------	--------------------	-----------	---	-----------------



RadICS Platform Application ED and to test the effects of the tuning changes before putting the RadICS channel back online. The ARMED keyswitch circuit allows for complete testing by varying the input parameters through their complete range from non-trip conditions into trip conditions while the plant equipment is in the safe state at all times.

A.2.6 Setpoint Accuracy Calculations

The Setpoint Analysis Support document (Reference A-4) provides the data recommended in EPRI TR-107330 for the following RadICS Platform components:

- Analog Input Modules
- Discrete Input Modules
- Analog Output Modules
- Discrete Output Modules

The accuracy specifications have been compiled from manufacturer's documentation and will be updated based on the results of qualification testing of the RadICS Platform QTS.

A.2.7 Reliability Calculations

The RadICS Platform FMEA/FMEDA information can be used to develop reliability assessments, as specified by the end user requirements.

A.2.8 Equipment Qualification Envelope

The RadICS Platform will be qualified to the boundary conditions listed below. The parameters of the qualification envelope will be updated once the qualification testing is complete.

A.2.8.1 *Radiation Exposure Withstand Testing*

The radiation exposure withstand testing demonstrates that the RadICS Platform QTS will not experience failures or unacceptable degradation due to expected radiation exposure from normal and abnormal service conditions as required by RG 1.209 and EPRI TR-107330. Section 4.3.6 of EPRI TR 107330 defines the normal and abnormal radiation exposure levels the test specimen must withstand and continue to meet the specified performance levels.

A.2.8.2 *Environmental Testing*

The environmental testing demonstrates that the RadICS Platform QTS will not experience failures due to abnormal service conditions of temperature and humidity as required by RG 1.209 and IEEE Std 323-2003. Section 4.3.6 of EPRI TR 107330 defines the recommended normal and abnormal temperature and humidity exposure levels the test specimen must withstand (i.e., the test specimen must continue to meet the manufacturer specified performance levels).

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 321 of 350
--------------	--------------------	-----------	---	-----------------



A.2.8.3 *Seismic Testing*

Seismic testing demonstrates the suitability of the RadICS Platform for qualification as a Category 1 seismic device based on seismic withstand testing performed on the RadICS Platform QTS in accordance with RG 1.100 and IEEE Std 344-2004. Section 4.3.9 of EPRI TR 107330 defines the seismic test levels to which the test specimen will be exposed, while the test specimen continues to meet the manufacturer specified performance levels.

A.2.8.4 *Electromagnetic Interference /Radio Frequency Interference Testing*

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

A.2.8.5 *Electrical Fast Transient Testing*

The objective of EFT testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to EFT susceptibility levels. EFT testing of the RadICS Platform QTS will be performed in accordance with RG 1.180 using additional guidance from EPRI TR-107330, as applicable.

A.2.8.6 *Surge Withstand Testing*

The objective of surge withstand testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to surge withstand levels. Surge withstand testing of the RadICS Platform QTS will be performed in accordance with RG 1.180, using additional guidance from EPRI TR-107330 as applicable.

A.2.8.7 *Electrostatic Discharge Testing*

The objective of ESD testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to ESD withstand levels. EPRI TR-107330, Section 4.3.8, requires that the test specimen under qualification be tested for ESD withstand capability in accordance with the requirements of EPRI TR-102323.

A.2.8.8 *Class 1E to Non-Class 1E Isolation Testing*

The objective of Class 1E to non-Class 1E isolation testing is to demonstrate the suitability of the RadICS Platform for qualification as a safety-related device with respect to providing electrical isolation at non-Class 1E field connections, as required by IEEE Std 384-1992. EPRI TR-107330, Section 6.3.6, requires that the test specimen under qualification be tested for Class 1E to non-Class 1E isolation capability in accordance with the requirements of EPRI TR-107330, Section 4.6.4.



A.2.9 Application Logic Development

The Application Logic designer is responsible for designing into the logic the appropriate response to the Type III diagnostic signals specified in the system functional requirements specification. For example, the three diagnostic signals for a safety critical input (failure of the input signal, failure of the input channel hardware, and failure of the input module) should be carefully considered as possible reasons to drive the outputs to the safe state.

The RadICS Platform will not go into a fail-safe mode automatically upon detection of the following failures unless the Application Logic implements the desired action for these events:

- Any failure of a field input signal
- Any failure of an individual I/O channel on a Module
- Any complete failure of a Module
- Loss of communications between the LM and a DOM or AOM, which will only cause the affected DOM or AOM to go immediately to the safe state
- EEPROM failure after STARTUP, since these EEPROMs are used only at power-up. A failure detected during operation is an early warning that the next power-up will not succeed.

The end user should consult the RadICS Product Safety Manual for information on the Application Logic decisions that need to be made.

A.2.9.1 Verification of Chassis Configuration

The Application Logic design should include logic to verify the following:

- The correct type of module is present in the appropriate slots
- The modules present in these slots are certified for use with the RadICS Platform
- The modules are not in CONFIGURATION mode

A.2.9.2 Verification of I/O Module Status

The Application Logic design should include logic to verify the following:

- No module critical to the system operation for safety has been removed from the chassis
- No module critical to the SIS operation for safety has suffered a complete failure (i.e., FAULTED mode)

A.2.9.3 Detection of Safety-Critical I/O Failures

The Application Logic design should include logic to respond to I/O channel failures as specified in the system functional requirements specification.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 323 of 350
--------------	--------------------	-----------	---	-----------------



A.2.9.4 *Analog Input Signal Tolerance*

The Application Logic design should consider the tolerance involved in the self-diagnostic tests for an analog input channel hardware failure and the conversion accuracy in determining trip setpoints or any similar logic threshold. The Application Logic should incorporate specific considerations including:

- An AI channel is considered failed if the difference in reading of its two independent ADCs is > 2% of full-scale
- The discretization error due to 16-bit analog/digital conversion
- Reasonableness checks on analog inputs and calculated values.

A.2.9.5 *Setting the Safety Override or Tripping to Reach a Safe State*

The Application Logic can be designed to request the LM to set the SOR. In this state, all safety critical outputs are set to the safe state by the SOR, although in other respects the Application Logic runs normally. The SOR safe state is recoverable.

The Application Logic can be designed to request a SOR-RESET (by no longer requesting a SOR-Set, but the actual reset must be performed by an operator or technician unless the RadICS Platform has been wired for automatic transition into RUN mode.

The Application Logic can be designed to request the LM to go to FAULTED mode, which permanently drives all safety critical outputs to the safe state. This safe state is not recoverable: the RadICS Platform must be powered down and restarted or LM must be extracted and re-inserted.

The Application Logic can be designed to set the SOR on individual output modules only so they are put in the safe state.

It is usually advisable to set all safety critical outputs to the safe state when any one single output channel goes to the safe state, whether due to individual failure or the result of Application Logic action.

This action is advisable because to do otherwise would put some parts of a plant into a safe state but not others, thus possibly putting the plant into an unanalyzed state, which could pose unpredictable hazards. However, the decision to set all safety critical outputs to the safe state must be carefully evaluated based on system design requirements and potential operational impacts.

A.2.9.6 *Latching Trip Decisions*

The Application Logic should include logic to latch trip decisions, as specified in the system functional requirements specification.

It is strongly recommended that trip decisions be latched, where the Application Logic designer intends that the trip action be retained until maintenance activity is complete. This is particularly important for safety functions that trip on a process variable going high and the shutdown of the plant process could cause this parameter value to drop below the setpoint.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 324 of 350
--------------	--------------------	-----------	---	-----------------



A.2.9.7 Monitoring Module Temperature

The Application Logic should monitor the operating temperature of the RadICS Modules and specify whether the condition is alarmed or the Module is put into the safe state, as specified in the system functional requirements specification.

A.3 Installation

A.3.1 Physical Security

RadICS recommends that the RadICS Platform and other associated safety-related I&C equipment be installed in a secure location to which access is controlled.

A.3.2 Mounting

The minimum space required around the chassis is as follows:

- Vertical space above the fan assembly portion of the chassis: ≥ 3 cm
- Vertical space below the chassis: ≥ 3 cm
- Horizontal depth behind the chassis (to accommodate the I/O cables): ≥ 15 cm

The RadICS chassis is supported by its front panel and should be installed with required number of bolts and the supplied locking brackets. The bolts should be torqued to the specified values.

RadICS Modules must be fully inserted and the hold-down latches secured by screws. The screws should be torqued to the specified values.

The RadICS EMI/Surge Protection Modules must be fully inserted and the hold-down latches secured by screws. The screws should be torqued to the specified values.

Cables connected to the RadICS Chassis must be fully inserted and the locking bars is in the locked position. Unused connectors should be covered with a dust cap.

A.4 Routine Maintenance Activities

This section provides the recommended periodic inspection and testing procedures for the RadICS Platform. These requirements are intended to identify important considerations for maintaining the environmental qualification of the RadICS Platform.

A.4.1 Periodic Inspection

A visual inspection and then a physical inspection should be conducted periodically to confirm that the equipment is physically in the environment and condition that are expected. It is recommended to inspect the RadICS Platform whenever scheduled preventative maintenance is performed on equipment in the same cabinet.

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 325 of 350
--------------	--------------------	-----------	---	-----------------



Visually inspect the terminal blocks of all Modules and confirm:

- There is no evidence of corrosion (e.g., discoloration on conductors or terminals)
- There is no evidence of frayed wires

Physically inspect the RadICS Platform and its connections to confirm:

- The RadICS Chassis itself is firmly mounted
- All RadICS Modules are firmly in place and the latches are in the locked position
- All connector locking brackets are in place.

Inspect the RadICS Chassis vents for dust and confirm there is air flow at the vents at the front of the RadICS Chassis fan assembly.

A.4.2 Periodic Testing

The RadICS Platform has extensive self-testing features. These tests are supplemented by the following periodic tests that are typically performed during a refueling outage:

- [[

]]^{a,c,e}

- Test injection signals should be used to drive the input variables to the end of the instrumentation range at the safe end of the instrumentation range (i.e., apply conditions that do not trip the safety setpoint). The injection signal should be gradually increased (or decreased) until the setpoint trips to verify it meets requirements. The injection signal should be reduced (or increased) to below (or above) the trip setpoint to verify that the [[
]]^{a,c,e}. The injection signal should be driven to the high (or low) end of the instrumentation range to check the calibration of the signal.

A.4.3 Periodic Calibration

Periodic calibration of the analog inputs and outputs RadICS Platform is typically performed during a refueling outage. AIM or AOM calibration requires removing the module from the in-service chassis and installing it in the DLS. Calibration is performed in accordance with plant procedures.

A.4.4 Adjustable Parameter Tuning

Operational parameters may need to be adjusted during a reactor operating cycle or between cycles. The RadICS Platform provides the ability to tune these parameters via the Fiber Optic Tuning Interface. Tuning is normally locked out, and is enabled only by a keyswitch. In this mode, tuning parameters that

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 326 of 350
--------------	--------------------	-----------	---	-----------------



are specified in the Application ED can be adjusted by connecting a MATS Tuning PC with special software to the RadICS Platform system. The MATS Tuning PC requires a password.

The end user performs functional tests to confirm the tuning values before restoring the system to normal operation. The RadICS Platform system also checks tuning values for 'reasonableness' and basic validity. The Application Logic can also be engineered to perform other specified checks.

The LM will transition to the RUN (SAFE) mode if the TUNING keyswitch is present while ARMING keyswitch is not. The LM will transition to the TUNING mode if the TUNING and ARMING keyswitches are present. The LM will transition to the RUN mode if TUNING key or ARMING key is removed. The Tuning Parameters will be set to the previously stored values from the Tuning EEPROM if the keys are removed before a Tuning update is completed. The LM will transition into FAULTED mode if Type I faults are detected during self-diagnostics tests.

A.4.5 Product Life

The product lifetime of the RadICS Platform is 30 years from date of manufacture. There are no consumables related to RadICS Platform operation and periodic maintenance (e.g., batteries or electrolytic capacitors) that require periodic replacement.

A.5 Appendix A References

- 1 RadICS Document D11.1, "Product Safety Manual"
- 2 EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996
- 3 RadICS Platform Master Configuration List, Document No. 2016-RTS002-MCL-018)
- 4 RadICS Setpoint Analysis Support, Document No. 2016-RTS002-SAS-003



Appendix B: DI&C-ISG-04 Compliance Matrix

Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
1	INTERDIVISIONAL COMMUNICATIONS	
	<p>1 A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE Std 603.¹ It is recognized that division voting logic must receive inputs from multiple safety divisions.</p>	<ul style="list-style-type: none"> Physical and functional Independence of communication divisions is achieved by selecting appropriate system architectures and data communication protocols. The RadICS Platform features described in Sections 6.3 and 6.6 do not depend upon information coming from outside its safety division, except for trip requests coming from the other divisions and input to the voting logic. The RadICS LM in a safety division provides functions of input data acquisition, data processing, application logic execution, diagnostics, and output data conditioning that do not depend on the other safety divisions.
	<p>2 The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.</p>	<ul style="list-style-type: none"> RadICS Platform equipment and communications design prevents propagation of failures between redundant equipment in separate divisions. In addition, communication paths to non-safety I&C systems are electrically isolated with one-way communications from the RadICS Platform to the non-safety I&C system. These features prevent faults in a non-safety I&C system from adversely affecting the RadICS Platform. The implementation of radial (point-to-point) architecture in RadICS Platform inter-division communication links provide the RadICS Platform with the capability to maintain failure-free data exchange between I&C components even when one of the divisions has failed. Additional measures designed to achieve the desired physical and functional independence are the application of fiber-optic communication lines for data exchange between I&C components and the separation of safety and control functions from information and diagnostic functions. The RadICS LMs exchange voting logic data with other safety divisions by fiber optic interface that meets the SIL 3 safety requirement. Communication among safety divisions is point-to-point and asynchronous. The transmitting safety division sends only once during a Work Cycle. The Communication Units (i.e., OPTO, LVDS, LAN, and
Document ID:		2016-RPC003-TR-001
Revision:		0
		Page 328 of 350



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
		<p>RS-232/485) [[]]^{a,c,e}</p> <p>The receiving safety divisions do not need to wait or synchronize with these messages to issue their own safety actuations.</p> <ul style="list-style-type: none"> • IF SD of communications is crucial for providing safety integrity and functional safety. IF SD is performed by each safety division's RadICS Module ED SD, since communication interfaces cannot perform any actions except data transmission. • Generalized measures intended to provide IF SD are: <ul style="list-style-type: none"> - [[]] <p style="text-align: right;">]]^{a,c,e}</p>
3	<p>A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such</p>	<ul style="list-style-type: none"> • The only input coming from outside a safety division is the input needed for the system coincidence voting logic (i.e., request for actuation coming from the other independent divisions). Up to 4 divisions (i.e., LMs) can be used in system coincidence voting (e.g., 1-out-of-2, 2-out-of-3, 2-out-of-4 are possible). The LM will detect that it is connected with the correct LM in other chassis for system coincidence voting). • The safety system is kept as simple as possible and does not include functions not related to the safety functions.



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
	a complex design, therefore, should be avoided within the safety system.	
4	The communication process itself should be carried out by a communications processor ⁱⁱ 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.	<ul style="list-style-type: none"> The safety function is executed on the LM FPGA board and the actual data exchange communications between safety divisions is [[]]^{a,c,e} and transmitted to other safety division through the corresponding Optical Transceiver Unit (OPTO) using the Radiy Proprietary Protocol (RPP). Faster and more deterministic performance due to capability of executing logic functions and control algorithms in a parallel mode; due to advantage of native hardware parallelism. This provided the ability to [[]]^{a,c,e}
	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.	<ul style="list-style-type: none"> FPGA technology [[]]^{a,c,e} All communication links of the OPTO Unit are executed according point-to-point principle between two different Modules of the same type (e.g., LM to LM). [[]]^{a,c,e}. Each communication link uses a separate OPTO Unit. The OPTO Unit is safety related.
	The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 CFR Part 50, Appendix A and B.	<ul style="list-style-type: none"> RadICS Hardware, as well as, the FBL software are safety related items, and have been designed, qualified and fabricated, as described in Section 6 and Section 8.



Section #	DI&C-ISG-04 Requirements		Compliance of the RadICS Generic Platform
		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.	<ul style="list-style-type: none"> The RadICS Modules utilize [[]] ^{a,c,e} is entirely controlled by the FPGA with no chance of interference from external interfaces. This feature ensures that the safety function LM can always have access without delay to the communication data for transmission or reception of data.
		For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.	See above.
	5	The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the	<ul style="list-style-type: none"> The FPGA design of the RadICS Platform does [[]] ^{a,c,e} for different processes. Each FPGA has [[]] ^{a,c,e} and, as described above, the transfer of data is handled by the RadICS LMs that operate in a deterministic timeframe. The Work Cycle duration of each RadICS LM functioning in all modes (except POWERED-OFF and FAULTED modes) is [[]] ^{a,c,e} milliseconds (see Section 6.10).



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
	communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.	
6	The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	<ul style="list-style-type: none"> • Safety function logics with the RadICS Modules [[d]]^{a,c,e}. • Communications with LMs between safety divisions (system coincidence voting) is handled in communication processing Units that are [[]]^{a,c,e} which does not affect the Application ED and other RadICS Module Units [[]]^{a,c,e}
7	Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor.	<ul style="list-style-type: none"> • All communication links are pre-defined and established during implementation. All communications are implemented on a point-to-point basis that [[]]^{a,c,e} • All communications are transmitted in a [[]] to ensure correctness and integrity of each data message.
	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.	<ul style="list-style-type: none"> • DTP SD, due to specific structure, allow implementation of reliable IF SD. Each transmitted data packet includes the following data: <ul style="list-style-type: none"> – [[]]



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
]] ^{a,c,e}
	Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.	<ul style="list-style-type: none"> All data is transmitted during each Work Cycle. Each message is [[]]^{a,c,e}
8	Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.	<ul style="list-style-type: none"> FPGA technology allows for [[]]^{a,c,e} Communication between safety divisions and non-Class 1E equipment is not allowed while in safety operation except the following: <ul style="list-style-type: none"> Tuning Interface (see Section 6.9) MATS (see Sections 6.3 and 6.6) Communications ports are monitored [[]]^{a,c,e} except when specifically required (e.g., tuning interface). The safety division is placed in a safe state while the tuning interface is active. The interface to the MATS is one-way broadcast (i.e., non-interfering), rated at SIL 2. [[]]^{a,c,e} Thus the MATS is also non-interfering. In the sending safety division, failure to send to the non-Class 1E equipment due to communication does not impair the safety function of the division



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
	<p>9 Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.</p>	<ul style="list-style-type: none"> • The RadICS Module FPGA utilizes [[]] is entirely controlled by the RadICS Module FPGA with no chance of interference from external interfaces. This feature ensures that the LM can always have access without delay to the communication data for transmission or reception of data. • The areas of [[]]^{a,c,e}
	<p>10 Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g., engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware</p>	<ul style="list-style-type: none"> • [[]]^{a,c,e} • In TUNING mode, parameters which are provided for in the Application Electronic Design can be adjusted by connecting a laptop computer with special software to the RadICS LM. TUNING mode requires the use of a TUNING key and a contact that comes from the end user's downstream safety logic that indicates that this downstream logic is locked into the safe state (controlled by what is called the ARMING key). This permits the end user to fully test his tuning changes under safe conditions. Placing the Module in a safe state during tuning ensures only one safety division can undergo tuning at a time.
Document ID:	2016-RPC003-TR-001	Revision: 0 Page 334 of 350



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
	switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.	
11	Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division.	<ul style="list-style-type: none"> • [[]]^{a,c,e}
	For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.	See above.
12	Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 CFR Part 50, Appendix A.	<ul style="list-style-type: none"> • Communication transmission between safety divisions is implemented [[]]^{a,c,e}. Communications faults are detected using diagnostics performed by the receiving division LM. • Communication between safety divisions and non-Class 1E equipment is not allowed while in safety operation except the following: <ul style="list-style-type: none"> – Tuning Interface (see Section 6.9) – MATS (see Sections 6.3 and 6.6) • Communications ports are monitored [[]]^{a,c,e} except when specifically required (e.g., tuning interface). The safety division is placed in a safe state while the tuning interface is active. • The interface to the MATS is one-way broadcast (i.e.,

Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
		non-interfering), rated at SIL 2. Receiving ports not used on the ED level. Thus the MATS is also non-interfering.
	<p>Examples of credible communication faults include, but are not limited to, the following:</p> <ol style="list-style-type: none"> 1. Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise. 2. Messages may be repeated at an incorrect point in time. 3. Messages may be sent in the incorrect sequence. 4. Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message. 5. Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages. 6. Messages may be inserted into the communication medium from unexpected or unknown sources. 7. Messages may be sent to the wrong destination, which could treat the message as a valid message. 8. Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption. 9. Messages may contain data that is outside the expected range. 10. Messages may appear valid, but data may be placed in incorrect 	<p>Communication failures are detected and appropriate safety actions are taken (see Section 6.4).</p> <ol style="list-style-type: none"> 1. [[<p style="text-align: right;">]]^{a,c,e}</p> 4. Loss of messages is detected. [[<p style="text-align: right;">]] Failure to transmit or receive a message cannot interfere with the safety function.</p> 5. [[<p style="text-align: right;">]]^{a,c,e} If the is not received [[during the appropriate time window (message not received or monotony control indicator not updated)]]^{a,c,e}, this situation is detected.</p> 6. [[

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 336 of 350
--------------	--------------------	-----------	---	-----------------



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
	<p>locations within the message.</p> <p>11. Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).</p> <p>12. Message headers or addresses may be corrupted.</p>	<p>]]</p> <p>11. Broadcast storm will not have an effect on the receiving Module. [[</p> <p>]]^{a,c,e}. The Communication Units (i.e., OPTO, LVDS, LAN, and RS-232/485) are [[</p> <p>]]^{a,c,e}.</p> <p>The receiving safety divisions do not need to wait or synchronize with these messages to issue their own safety actuations.</p> <p>12. The receiving processing LM tests the [[</p> <p>]]^{a,c,e}</p> <p>corruption is detected.</p>
	<p>13 Vitalⁱⁱⁱ 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.</p>	<ul style="list-style-type: none"> • Communication failures are detected and appropriate safety actions are taken. • No error correction methods are used.
	<p>14 Vitalⁱⁱⁱ 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</p>	<ul style="list-style-type: none"> • [[]]^{a,c,e} Communications are always passed directly from sending node to receiving node with no chance for outside interference.
Document ID:	2016-RPC003-TR-001	Revision: 0 Page 337 of 350



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
	the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.	
15	Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.	<ul style="list-style-type: none"> • [[]], regardless of whether the data has changed or not.
16	Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 CFR Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)	<ul style="list-style-type: none"> • [[]] • Communication between safety divisions and non-Class 1E equipment is not allowed while in safety operation except the following: <ul style="list-style-type: none"> – Tuning Interface (see Section 6.9) – MATS (see Sections 6.3 and 6.6) • Communications ports are monitored [[]]^{a,c,e} except when specifically required (e.g., tuning interface). The safety division is placed in a safe state while the tuning interface is active. • The interface to the MATS is one-way broadcast (i.e., non-interfering), rated at SIL 2. [[]]^{a,c,e} Thus the MATS is also non-interfering. • In the sending safety division, failure to send to the non-Class 1E equipment due to communication does not impair the safety function of the division.
17	Pursuant to 10 CFR 50.49, the medium used in a vital ⁱⁱⁱ communications channel should be qualified for the anticipated normal and post-accident environments.	<ul style="list-style-type: none"> • The RadICS Platform includes selected medium and equipment used for communications (including optical fibers, twisted-shielded pair cables, etc.) that are qualified for mild environment usage (see Chapter 9).



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
	For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.	See above.
18	Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	<ul style="list-style-type: none"> Each transmitted message contains the data necessary to accomplish the needed safety functions and elements needed for diagnostic to allow the Modules to detect communication failure. [[]]
19	If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.	<ul style="list-style-type: none"> [[]]
20	The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.	<ul style="list-style-type: none"> The RadICS Platform has a deterministic behavior. The Work Cycle for each Module is fixed and the maximum response time for system architecture is established using the maximum response time of each LM and communication links. This deterministic behavior guarantees that safety outputs will always be delivered within the computed maximum response time limit. Errors in communications do not impact or increase the system maximum response time. See Section 6.10 for further details on Work Cycles and response times.



Section #	DI&C-ISG-04 Requirements	Compliance of the RadICS Generic Platform
2	COMMAND PRIORITIZATION	
		<ul style="list-style-type: none"> The generic RadICS Platform does not include a priority logic Module. Therefore, this section of DI&C-ISG-04 does not apply.
3	MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS	
3.1	<p>Independence and Isolation</p> <p>The following provisions are applicable to multidivisional control and display stations. These guidance provisions do not apply to conventional hardwired control and indicating devices (hand switches, indicating lamps, analog indicators, etc.).</p>	<ul style="list-style-type: none"> The generic RadICS Platform does not include multidivisional control and display stations. Therefore, the requirements for multi-division controls in this section of DI&C-ISG-04 do not apply.
	<p>1</p> <p>Nonsafety stations receiving information from one or more safety divisions:</p> <p>All communications with safety-related equipment should conform to the guidelines for interdivisional communications.</p>	<ul style="list-style-type: none"> Communication between Safety divisions and non-Class 1E equipment is not allowed while in safety operation except the following: <ul style="list-style-type: none"> Tuning Interface (see Section 6.9) MATS (see Sections 6.3 and 6.6) Communications ports are monitored [[]]^{a,c,e} except when specifically required (e.g., tuning interface). The safety division is placed in a safe state while the tuning interface is active. The interface to the MATS is one-way broadcast (i.e., non-interfering), rated at SIL 2. [[]]^{a,c,e} Thus the MATS is also non-interfering. In the sending safety division, failure to send to the non-Class 1E equipment due to communication does not impair the safety function of the division



Section #	DI&C-ISG-04 Requirements		Compliance of the RadICS Generic Platform
	2	<p>Safety-related stations receiving information from other divisions (safety or nonsafety):</p> <p>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.</p>	<p>RadICS systems require interdivisional communications to support voting logics. In addition, one-way (broadcast only) communications from safety divisions to non-safety display systems that can aggregate data and perform functions/display of data/interdivisional comparisons. The interface to the MATS is one-way broadcast (i.e., non-interfering), rated at SIL 2. [[]]^{a,c,e} Thus the MATS is also non-interfering.</p>
	3	Nonsafety stations controlling the operation of safety-related equipment	The generic RadICS Platform does not provide this control capability.
	4	Safety-related stations controlling the operation of equipment in other safety-related divisions	The generic RadICS Platform does not provide this control capability.
	5	<p>Malfunctions and Spurious Actuations.</p> <p>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.</p>	The generic RadICS Platform does not provide this control capability, therefore these requirements do not apply.
3.2		Human Factors Considerations	This will be determined on a project-specific basis.
3.3		Diversity and Defense-in-Depth (D3) Considerations	This will be determined on a project-specific basis.

DI&C-ISG-04 Notes

- i IEEE Std 603-1991 (cited in 10 CFR 50.55a(h)) provides the following definitions:

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

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 341 of 350
--------------	--------------------	-----------	---	-----------------



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

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

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

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

- ii "Processor" may be a CPU or other processing technology such as simple discrete logic, logic within an FPGA, an ASIC, etc.
- iii "Vital" communications as used herein are communications that are needed to support a safety function. Failure of vital communications could inhibit the performance of the safety function. The most common implementation of vital communications is the distribution of channel trip information to other divisions for the purpose of voting.



Appendix C: RadICS Electronic Design Documents

DI&C-ISG-06 (Reference C-1) contains a list of documents in Enclosure B that are identified for submittal with a license amendment request. The same list has been applied to digital I&C platform topical report reviews with mixed success. NRC has also been conducting a pilot license amendment request review using DI&C-ISG-06. In public meetings NRC has communicated lessons learned regarding the use of DI&C-ISG-06 for license amendment requests and topical report reviews.

An important lesson learned was with the usefulness of the documents submitted based on the DI&C-ISG-06 guidance. In particular, the list is not well suited for digital platform topical report reviews. NRC has indicated that it has found it more useful to get a smaller set of documents with the application and have access to other documents) via an electronic reading room) to conduct audits of the detailed design information that supports the information in the topical report.

The following document item numbers in Enclosure B of DI&C-ISG-06 are addressed directly in the RadICS Topical Report:

- 1.1, Hardware Architecture Descriptions
- 1.2, Quality Assurance Plan for Digital Hardware
- 1.16, Design Analysis Reports
- 1.20, Theory of Operation Description
- 2.1, Safety Analysis

The RadICS design documents are cross referenced to the relevant document item numbers in Enclosure B of DI&C-ISG-06 in Table C-1.

The following document item numbers from Enclosure B of DI&C-ISG-06 are not applicable to the generic platform RadICS Topical Report:

- 1.15, D3 Analysis
- 1.17, System Description
- 1.19, System Response Time Analysis Report
- 1.21, Setpoint Methodology
- 1.22, Vendor Software Plan
- 2.3, As-Manufactured, System Configuration Documentation
- 2.6, Summary of Test Results (Including FAT)
- 2.8, FMEA
- 2.9, System Build Documents
- 2.13, As-Manufactured Logic Diagrams
- 2.14, System Response Time Confirmation Report
- 2.16, Setpoint Calculations
- 3.1, Software Integration Report
- 3.2, Individual V&V Problem Reports up to FAT
- 3.4, Test Procedure Specification

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 343 of 350
--------------	--------------------	-----------	---	-----------------



- 3.5, Completed Test Procedures and Reports
- 3.6, Test Incident Reports
- 3.8, Software Project Risk Management Report
- 3.9, Circuit Schematics
- 3.10, Detailed System and Hardware Drawings
- 4.3, Software Training Plan
- 4.5, Site Test Documentation
- 4.7, Software Maintenance Manuals
- 4.8, Software Training Manuals
- 4.9, Installation Configuration Tables

C.1 RadICS Electronic Design Related Documents

Table C-1 contains a listing of the RadICS Platform design documents associated with the Electronic Designs for the RadICS Modules. An initial set of documents planned for submittal with the RadICS Topical Report (i.e., Phase 1 Submittals) is identified. Another set of documents to be submitted after completion of the RadICS EQ test program (i.e., Phase 2 Submittals) are identified. The remaining documents are available for audit, as requested by NRC. Additional documents (or extracts of key information) will be submitted, as requested by NRC during the topical report review.

Table C-1: RadICS Electronic Design Related Documents

RadICS Electronic Design Related Documents		DI&C-ISG-06 Category and Cross Reference
Number	Title	
D1.0	RadICS Product Concept Document	Available for Audit
D2.1	RadICS Functional Safety Management Plan	Phase 1 Submittal Items 1.4, 1.5, 1.6, 1.7, 1.8, and 1.24
D2.2	RadICS Configuration Management Plan	Phase 1 Submittal Item 1.10
D2.2.0	Baseline Independent Items Configuration Audit Report	Available for Audit Item 3.3
D2.2.1	Requirements Baseline Configuration Audit Report	Available for Audit Item 3.3
D2.2.2	Architecture Design Baseline Configuration Audit Report	Available for Audit Item 3.3
D2.2.3	Detailed Design and Coding Baseline Configuration Audit Report	Available for Audit Item 3.3

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 344 of 350
--------------	--------------------	-----------	---	-----------------



RadICS Electronic Design Related Documents				DI&C-ISG-06 Category and Cross Reference		
Number		Title				
D2.2.4		Integration Baseline Configuration Audit Report		Available for Audit Item 3.3		
D2.2.5		Release Baseline Configuration Audit Report		Available for Audit Item 3.3		
D2.3		RadICS Tool Selection and Evaluation Report		Available for Audit Items 1.23 and 2.17		
D2.4		RadICS Overall Verification and Validation Plan		Phase 1 Submittal Item 1.9		
D2.4.1		RadICS Verification and Validation Testing Checklists		Available for Audit		
D2.6		RadICS Document Plan		Available for Audit		
D2.6.1		Project Implementation Plan		Available for Audit		
D2.6.2		Project Repository Structure		Available for Audit		
D2.7		RadICS Personnel Plan		Available for Audit		
D2.7.1		Training Records		Available for Audit		
D2.8		RadICS Security Analysis Report		Phase 1 Submittal Items 1.26 and 1.27		
D2.9		RadICS Report about Compliance of FSMP to IEC 61508		Available for Audit		
D2.10		RadICS Functional Safety Management Plan Phase 3 Extension		Phase 1 Submittal Items 1.4, 1.5, 1.6, 1.7, 1.8, and 1.24		
D2.12		RadICS Project Change Log		Available for Audit		
D3.1		RadICS Safety Requirements Specification		Phase 1 Submittal Item 1.12		
D3.2		RadICS SRS Review Report		Available for Audit Item 2.2		
D3.7		RadICS Equipment Qualification Safety Requirements Specification		Available for Audit		
D3.8		RadICS Equipment Qualification Safety Requirements Specification Review Report		Available for Audi Item 2.2		
D3.9		RadICS Requirements Traceability Matrix		Available for Audit Item 2.7		
D3.9.1		RadICS Requirements Tracing Matrix book		Available for Audit Item 2.7		
Document ID:		2016-RPC003-TR-001		Revision:	0	Page 345 of 350



RadICS Electronic Design Related Documents		DI&C-ISG-06 Category and Cross Reference
Number	Title	
D3.9.2	RadICS Module Static Code Analysis / Code Review Report Tracing Report	Available for Audit Item 2.2
D4.0	RadICS Safety Validation Test Plan	Phase 1 Submittal Item 1.11
D4.1	RadICS Safety Validation Test Specification	Available for Audit Item 2.4
D4.2	RadICS Safety Validation Test Report	Available for Audit Item 2.5
D5.1	RadICS Product Architecture Document	Phase 1 Submittal Items 1.3 and 1.12
D5.2	RadICS PAD Review Report	Available for Audit Item 2.2
D5.4	RadICS AFBL/Application Logic Detailed Requirements Specification	Available for Audit
D5.5	RadICS AFBL/Application Logic Detailed Requirements Specification Review Report	Available for Audit
D7.23	RadICS Guideline on Design and Coding with VHDL	Available for Audit
D7.24	RadICS FMEDA Report	Available for Audit Items 1.18 and 2.15
D7.26.1 – D7.26-6	RadICS Modules Fault Insertion Test Specifications	Available for Audit Item 2.4
D8.11	RadICS FBL Detailed Description	Available for Audit Item 1.13
D8.12	RadICS FBL VHDL Code	Available for Audit Item 3.7
D8.13	RadICS FBL VHDL Static Code Analysis / Code Review Report	Available for Audit Item 2.2
D8.15	RadICS FBL Detailed Description Review Report	Available for Audit Item 2.2
D9.11	RadICS FBL Functional Test Plan and Specification	Available for Audit Item 2.4
D9.12	RadICS FBL Functional Test Report	Available for Audit Item 2.5



RadICS Electronic Design Related Documents			DI&C-ISG-06 Category and Cross Reference	
Number	Title			
D8.21.1 - D8.21.6	RadICS Modules ED Detailed Descriptions		Available for Audit Item 1.13	
D8.21.8	RadICS PSWD ED Detailed Description		Available for Audit Item 1.13	
D8.25.1 - D8.25.6	RadICS Modules ED Detailed Description Review Reports		Available for Audit Item 2.2	
D8.25.8	RadICS PSWD ED Detailed Description Review Report		Available for Audit Item 2.2	
D8.21.10	RadICS ED DD Data Protocols and Packages		Available for Audit	
D8.22.1 - D8.22.6	RadICS Modules ED VHDL Codes		Available for Audit Item 3.7	
D8.22.8	RadICS PSWD ED VHDL Code		Available for Audit Item 3.7	
D8.23.1 - D8.23.6	RadICS Modules ED VHDL Static Code Analysis / Code Review Reports		Available for Audit Item 2.2	
D8.23.8	RadICS PSWD ED VHDL Static Code Analysis / Code Review Report		Available for Audit Item 2.2	
D8.31	RadICS AFBL VHDL Detailed Description		Available for Audit	
D8.32	RadICS AFBL VHDL code		Available for Audit	
D8.33	RadICS AFBL VHDL Static Code Analysis/Code Review Report		Available for Audit Item 2.2	
D8.35	RadICS AFBL VHDL Detailed Description Review Report		Available for Audit Item 2.2	
D9.21.1 - D9.21.6	RadICS Modules ED VHDL Functional Test Plan and Specifications		Available for Audit Item 2.4	
D9.21.8	RadICS PSWD ED VHDL Functional Test Plan and Specification		Available for Audit Item 2.4	
D9.22.1 - D9.22.6	RadICS Modules ED VHDL Functional Test Reports		Available for Audit Item 2.5	
D9.22.8	RadICS PSWD ED VHDL Functional Test Report		Available for Audit Item 2.5	
D9.23.1 - D9.23.6	RadICS Modules ED Logic Level Simulation and Timing Test Reports		Available for Audit Item 2.5	
Document ID:	2016-RPC003-TR-001	Revision:	0	Page 347 of 350



RadICS Electronic Design Related Documents		DI&C-ISG-06 Category and Cross Reference
Number	Title	
D9.23.8	RadICS PSWD ED Logic Level Simulation and Timing Test Report	Available for Audit Item 2.5
D9.23.9.1 – D9.23.9.6	RadICS Modules ED Synthesis Results Review Reports	Available for Audit Item 2.2
D9.23.9.8	RadICS PSWD ED Synthesis Results Review Report	Available for Audit Item 2.2
D9.24.1 - D9.24.6	RadICS Modules ED Static Timing Analysis Test Reports	Available for Audit Item 2.5
D9.24.8	RadICS PSWD ED Static Timing Analysis Test Report	Available for Audit Item 2.5
D9.24.9.1 – D9.24.9.6	RadICS Modules ED Place and Route Results Review Reports	Available for Audit Item 2.2
D9.24.9.8	RadICS PSWD ED Place and Route Results Review Report	Available for Audit Item 2.2
D9.25.1 - D9.25.6	RadICS Modules ED Bitstream Generation Results Review Reports	Available for Audit Item 2.2
D9.25.8	RadICS PSWD ED Bitstream Generation Results Review Report	Available for Audit Item 2.2
D9.31	RadICS AFBL Test Plan and Specification	Available for Audit
D9.32	RadICS AFBL Functional Test Report	Available for Audit
D10.1	RadICS Integration Test Plan	Phase 1 Submittal Item 1.11
D10.2	RadICS Integration Test Specification	Available for Audit Item 2.4
D10.3	RadICS Integration Test Report	Available for Audit Item 2.5
D10.4	RadICS Hardware Fault Insertion Test Report	Available for Audit Item 2.5
D11.1	RadICS Product Safety Manual	Available for Audit Items 4.1, 4.2, 4.4, and 4.6



RadICS Electronic Design Related Documents		DI&C-ISG-06 Category and Cross Reference
Number	Title	
D11.4	RadICS Product Safety Manual Review Report	Available for Audit Item 2.2
D11.5	RadICS Application Function Block Library User Reference Manual	Available for Audit
D11.6	RadICS Platform Configuration Tool User Manual	Available for Audit
D11.10	AFBL User Reference Manual Review Report	Available for Audit
D11.11	RPCT User Manual Review Report	Available for Audit
D12.1	RadICS Functional Safety Management Audit Plan	Available for Audit
D12.2.1	RadICS Functional Safety Management Audit Report	Available for Audit
D12.2.2	RadICS Functional Safety Management Audit Report	Available for Audit
D12.2.3	RadICS Functional Safety Management Audit Report	Available for Audit
D12.3	RadICS Safety Case – FSMP Requirements Compliance	Available for Audit
D13.1	RadICS Functional Safety Assessment Plan	Available for Audit
D13.2	RadICS Functional Safety Assessment Report	Available for Audit
D13.3	RadICS IEC 61508 Assessment Recommendations	Available for Audit
2015-RTS001-SRS-001	NRC RadICS Test Specimen (RTS-001) System Requirements Specification	Available for Audit
2015-RTS001-SWRS-011	NRC RadICS Test Specimen (RTS-001) Software Requirements Specification	Available for Audit
2016-RTS002-PQP-001	Quality Assurance Project Plan	Available for Audit
2016-RTS002-MCL-018	Master Configuration List	Available for Audit
2016-RTS002-EQTP-004	Equipment Qualification Test Plan	Phase 1 Submittal Items 1.14 and 2.11
2016-RTS002-EQTP-018	Equipment Qualification Test Report	Phase 2 Submittal Item 2.12
2016-RTS002-FATP-005	Factory Acceptance Test Procedure	Available for Audit
2016-RTS002-SSCTP-006	System Setup and Checkout Test Procedure	Available for Audit
2016-RTS002-OTP-007	Operability Test Procedure	Available for Audit
2016-RTS002-PTP-008	Prudency Test Procedure	Available for Audit
2016-RTS002-PTP-009	Radiation Exposure Test Procedure	Available for Audit
2016-RTS002-ETP-010	Environmental Test Procedure	Available for Audit

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 349 of 350
--------------	--------------------	-----------	---	-----------------



RadICS Electronic Design Related Documents		DI&C-ISG-06 Category and Cross Reference
Number	Title	
2016-RTS002-STP-011	Seismic Test Procedure	Available for Audit
2016-RTS002-EMITP-012	EMI/RFI Test Procedure	Available for Audit
2016-RTS002-EFTTP-013	Electrical Fast Transient Test Procedure	Available for Audit
2016-RTS002-EFTTP-014	Surge Withstand Test Procedure	Available for Audit
2016-RTS002-ESDTP-015	Electrostatic Discharge Test Procedure	Available for Audit
2016-RTS002-1ETP-016	Class 1E to Non-1E Isolation Test Procedure	Available for Audit
2016-RTS002-SAS-003	RadICS Setpoint Analysis Support	Available for Audit
2015-RTS001-CGDP-LM-101	Commercial Grade Dedication Plan for LM	Phase 1 Submittal Item 1.25
2015-RTS001-CGDP-DIM-003	Commercial Grade Dedication Plan for DIM	Phase 1 Submittal Item 1.25
2015-RTS001-CGDP-DOM-102	Commercial Grade Dedication Plan for DOM	Phase 1 Submittal Item 1.25
2015-RTS001-CGDP-AIM-103	Commercial Grade Dedication Plan for AIM	Phase 1 Submittal Item 1.25
2015-RTS001-CGDP-AOM-104	Commercial Grade Dedication Plan for AOM	Phase 1 Submittal Item 1.25
2015-RTS001-CGDP-OCM-106	Commercial Grade Dedication Plan for OCM	Phase 1 Submittal Item 1.25
2015-RTS001-CGDP-CH-107	Commercial Grade Dedication Plan for Chassis	Phase 1 Submittal Item 1.25
2015-RTS001-CGDP-IOPM-131	Commercial Grade Dedication Plan for I/O Connections Protection Module	Phase 1 Submittal Item 1.25
2015-RTS001-CGDP-VM-132	Commercial Grade Dedication Plan for Ventilation Module	Phase 1 Submittal Item 1.25
2015-RTS001-CGDR-108	RadICS Commercial Grade Dedication Report	Phase 2 Submittal Item 2.18

C.2 Appendix C References

- 1 DI&C-ISG-06, Revision 1, "Licensing Process"

Document ID:	2016-RPC003-TR-001	Revision:	0	Page 350 of 350
--------------	--------------------	-----------	---	-----------------