FINAL SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

TRICONEX TOPICAL REPORT 7286-545-1, REVISION 4

INVENSYS OPERATIONS MANAGEMENT

PROJECT NO. 709

ENCLOSURE

List of Acronyms

AC	alternating current
AI	analog input
AO	analog output
ASAI	application-specific action item
ASIC	application-specific integrated circuit
BTP	branch technical position
CE	conducted emissions
CFR	*Code of Federal Regulations*
CGD	commercial grade dedication
COTS	commercial off-the-shelf
CRC	cyclical redundancy check
CS	conducted susceptibility
D3	diversity and defense-in-depth
DAC	digital-to-analog converter
DC	direct current
DI	digital input
DI&C	digital instrumentation and controls
DO	digital output
EDM	Engineering Department Manual
EFT	electrically fast transients
EIA	Electronics Industries Association
EMI	electromagnetic interference
EMP	electronic main processor
EPRI	Electric Power Research Institute
ESD	electrostatic discharge
ETSX	3008N operating system
FMEA	failure modes and effects analysis
FPGA	field-programmable gate array
GDC	General Design Criterion
GL	Generic Letter
HICRc	Highly-Integrated Control Rooms – Communications Issues
I&C	instrumentation and control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I/O	input and output
IOM	Invensys Operations Management (Tricon V10 vendor)
ISG	Interim Staff Guidance
LTR	Licensing Topical Report
MIL-STD	Military Standard
MVDU	maintenance video display unit
NRC	U.S. Nuclear Regulatory Commission
NSR	non-safety-related
OS	operating system
PC	personal computer
PCB	printed circuit board
PDS	pre-developed software
PLC	programmable logic controller
QA	quality assurance
QAM	Quality Assurance Manual
QPM	Quality Procedures Manual
RAI	Request for Additional Information

RAM	random-access memory
RE	radiated emissions
RFI	radio-frequency interference
RG	regulatory guide
RPS	Reactor Protection Systems
RRS	required response spectrum
RS	radiated susceptibility
RS	Recommended Standard
RTC	real-time clock
RTD	resistance temperature detector
RTM	requirements traceability matrix
RXM	remote extender module
SDPE	Special Dedication Parts Evaluation
SDS	software design specification
SE	safety evaluation
SMP	Software Management Plan
SOE	sequence of events
SOP	Software Operations Plan
SPDS	Safety Parameter Display System
SQAP	Software Quality Assurance Plan
SR	safety-related
SRP	Standard Review Plan
SRS	software requirements specification
SSE	safe shutdown earthquake
Std	Standard
STP	Software Test Plan
SVDU	safety video display unit
SVVP	Software Verification and Validation Plan
TCM	Tricon Communication Module
TR	Technical Report
TRS	test response spectrum
TS	technical specification
TSAP	test system application program
TXS	TELEPERM XS
V&V	verification and validation

Table of Contents

1.0 Introduction 1
2.0 Regulatory Evaluation 2
2.1 Scope of Triconex Platform Changes V9.5.3 to V10.5.1 2
2.2 Regulatory Criteria........ 5
2.3 Precedents 9
3.0 Technical Evaluation........ 9
3.1 Tricon V10 Platform Description 10
3.1.1 Tricon V10 System Overview........ 10
3.1.2 Tricon V10 System Hardware 11
3.1.3 Tricon V10 System Software 23
3.2 Development Process 28
3.2.1 Tricon V10 Software Design Review........ 29
3.2.2 Commercial Grade dedication of predeveloped software........ 32
3.3 Environmental qualification........ 35
3.3.1 Test system configuration 38
3.3.2 Pre-Qualification Testing........ 39
3.3.3 Radiation WITHSTAND Test 40
3.3.4 Temperature and Humidity Testing 41
3.3.5 Seismic Withstand Testing........ 43
3.3.6 EMI/RFI Withstand Testing 48
3.3.7 Surge Withstand Testing........ 53
3.3.8 Electrostatic Discharge Withstand Testing 55
3.3.9 Class 1E to Non-1E Isolation Testing........ 57
3.3.10 Performance Proof Testing 60
3.4 Platform Integrity Characteristics........ 63
3.4.1 Response time 63
3.4.2 Deterministic Performance 64
3.4.3 Diagnostics and Self-Test Capabilities........ 65
3.5 Failure Modes and Effects Analysis 67
3.6 Reliability and Availability Analysis........ 68
3.7 Communications Independence 68
3.7.1 Communications with Safety Channels/Divisions 70
3.7.2 Communications With Non-Safety Systems........ 71
3.7.3 Staff Guidance in DI&C-ISG-04 74
3.8 Secure Development and Operational Environment 97
3.8.1 Lifecycle Phases 97
3.9 Diversity and Defense-in-Depth........ 112
3.10 Conformance with IEEE STD 603-1991........ 112
3.10.1 IEEE 603-1991 Clause 4, “Safety System Designation” 113
3.10.2 IEEE STD 603-1991 Clause 5, “Safety System Criteria”........ 113
3.10.3 IEEE STD 603-1991 Clause 6, “Sense and Command Features – Functional and Design Requirements”........ 127
3.10.4 IEEE STD 603-1991 Clause 7, “Execute Features – Functional and Design Requirements”........ 128
3.10.5 IEEE STD 603-1991 Clause 8, “Power Source Requirements”........ 129
3.11 Conformance with IEEE STD 7-4.3.2-2003 130
3.11.1 IEEE STD 7-4.3.2-2003 Clause 5, “Safety System Criteria”........ 130
3.12 Summary of Regulatory Compliance 140
4.0 Limitations and Conditions........ 142
4.1 Generic Open Items 142

4.2 Plant-Specific Action Items 142
5.0 Conclusion 147
6.0 References 147

FINAL SAFETY EVALUATION BY THE

OFFICE OF NUCLEAR REACTOR REGULATION

TRICONEX TOPICAL REPORT 7286-545-1, REVISION 4

INVENSYS OPERATIONS MANAGEMENT

PROJECT NO. 709

1.0 INTRODUCTION

By letter dated September 9, 2009 (Reference 1), as supplemented by letters dated November 13, 2009 (Reference 2), and July 11, 2010 (Reference 3), Invensys Operations Management (IOM) requested U.S. Nuclear Regulatory Commission (NRC) approval for the “Triconex Topical Report,” IOM Document No. 7286-545-1, Revision 4 (Reference 4), hereafter referred to as the licensing topical report (LTR). The supplemental documents provided under the cover letter dated September 22, 2009, and the subsequent cover letters dated from October 30, 2009, through August 12, 2011, provided additional information that clarified and supported the technical claims documented in the LTR and did not expand or change the scope of the LTR.

The LTR was accepted for review by letter dated August 11, 2010 (Reference 67). The acceptance letter identified IOM commitments to supply supplemental documents. These documents provide additional information to support the review of the design details and qualification of the Tricon V10 platform and were submitted under the cover letter dated August 5, 2010, with an enclosure (Reference 59) providing summary responses to NRC inquiries for clarification within the acceptance letter.

The LTR revision describes the completion of all testing and documentation requirements of Electric Power Research Institute (EPRI) Technical Report (TR)-107330 for Version 10.5.1 (V10) of the Tricon Triple Modular Redundant (TMR) Programmable Logic Controller (PLC) platform, which is an evolutionary upgrade to the NRC approved Version 9.5.3 (V9), documented in Triconex Topical Report 7286-545-1-A, “Qualification Summary Report,” (Reference 34). The current LTR revision includes a summary of the equipment qualification for the Tricon V10 and a synopsis of the differences between the Tricon V9 System and the Tricon V10 System.

The NRC staff conducted an audit at the IOM facility in Irvine, California, on December 15 -17, 2010 (Reference 6). The purpose of the audit was to inspect IOM procedures and processes that are referenced in the LTR and audit documented products of commercial grade dedication activities. During the site visit, thread audits were performed, the hardware configuration of the Tricon qualification test specimen was observed, and performance characteristics and functional capabilities of the platform were observed. The results of the audit are documented in the March 14, 2011, Audit Report (Reference 6).

The NRC’s approval of the Tricon V9 platform is documented in its safety evaluation report (SER), “Review of Triconex Corporation Topical Reports 7286-545, “Qualification Summary Report” and 7286-546, “Amendment 1 to Qualification Summary Report, Revision 1” (TAC NO. MA8283)” (Reference 9), which formed the basis for the NRC staff’s safety evaluation (SE) of the Tricon V10 platform. The NRC staff focused its review efforts on the impact of V10 platform changes on the V9 platform safety conclusions documented in the SE. For those hardware and software items that are common to both the V9 and V10 platforms, the NRC's approval is documented in the V9 platform SE. However, changes to review guidance since 2001 required some aspects of the V9 platform to be reevaluated or evaluated in greater detail and the regulatory findings are documented herein.

2.0 REGULATORY EVALUATION

The purpose of this SE is to evaluate whether the Tricon V10.5.1 platform is suitable for use in safety-related (SR) applications in nuclear power plants (NPP). Thus, the review of the LTR and supporting technical documents is intended to determine whether sufficient evidence is presented to enable a determination with reasonable assurance that subsequent licensing applications referencing this platform can comply with the applicable regulations to ensure that the public health and safety will be protected. This evaluation and associated audit activities are not intended to completely assess all aspects of the design and implementation of any specific SR application (e.g., reactor protection system or engineered safeguards actuation system) and full compliance with relevant regulations will need to be evaluated on a plant-specific basis. However, the review scope is sufficient to allow the reviewer to reach the conclusion of reasonable assurance within the platform-level context.

2.1 SCOPE OF TRICONEX PLATFORM CHANGES V9.5.3 TO V10.5.1

The Tricon V10 PLC system is designed and built with the same basic architecture as the V9 PLC system. It is a fault-tolerant PLC that uses a triple modular redundant (TMR) architecture in which three parallel control paths are integrated into a single overall system. The system is designed to use two-out-of-three voting with the intent of providing uninterrupted process operation with no single point of random hardware failure.

However, many of the previously approved components within the V9 platform have been updated or replaced in the V10 platform. The most prominent changes to the Tricon V10 platform are the main processor (MP) module and the communications module. The Tricon V9.5.3 MP module, 3006N MP is replaced by the 3008N MP in the Tricon V10.5.1. Multiple communications modules available for V9.5.3 have been replaced with a single module configuration, the Tricon Communication Module (TCM). The complete list of hardware (HW) and software (SW) changes implemented within the Tricon V10 platform is provided in Tables 1 and 2 below (Reference 10). The Tricon V9 HW and SW components are also listed for comparison.

IOM included an Application Guide in Appendix B of the LTR that describes a generic safety system application using the V10 platform. The Application Guide was provided to facilitate a better understanding of the platform's potential safety system applications in NPPs. However, the NRC staff did not make any safety determination regarding the Application Guide and this appendix is not approved by this SE.

In addition to the V10 platform changes, IOM also submitted the Nuclear Safety Integration Program Manual (NSIPM) and an SE Maintenance Plan as part of the LTR. The NSIPM governs application specific development activities that occur at IOM's facility. The SE Maintenance Plan describes IOM's process to evaluate and document any future changes to the approved platform. The NRC staff reviewed these documents, but made no safety determinations on these programs and, therefore, they are not approved by this SE. It is an application-specific action item (ASAI) to review any application specific development activities governed by the NSIPM.

The NRC staff evaluated non-safety input and output (I/O) connections made to modules in a Remote Expansion Chassis IOM PN 8112N (as noted below in Table 1) that is part of a SR system as required by Clause 5.6 of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991.

TABLE 1 – Summary of Hardware Changes

Module	Tricon V9.5.3 System	Tricon V10.5.1 System
Main Processor	3006N	3008N
	Hardware floating point processor	Embedded floating point software
Communication Module	Three modules: • 4119AN (EICM) • 4329N (NCM) • 4609N (ACM)	One module: • 4352AN (TCM) Fiber Optic
I/O Modules Analog Input (AI)	3700AN (0-5 VDC)	3721N (0-5 or -5 to +5 VDC, Differential) Next Generation Module, SMT
	3701N (0-10 VDC) – Through Hole	3701N2 (0-10 VDC) - SMT
	3510N (Pulse Input)	3511N (Pulse Input) – Faster Input Scan
	3703EN (Isolated)	Same
	3708EN (ITC)	Same
	3704EN (0-5/0-10 VDC, High Density)	Removed
	3706AN (NITC)	Removed
I/O Modules Analog Output (AO)	3805EN (4-20 mA)	3805HN (4-20 mA) – Supports increased inductive loads
I/O Modules Digital Input (DI)	3501TN 115V AC/DC – Through Hole	3501TN2 115V AC/DC – SMT
	3502EN 48V AC/DC – Through Hole	3502EN2 48V AC/DC – SMT
	3503EN 24V AC/DC – Through Hole	3503EN2 24V AC/DC – SMT
	3504EN 24/48 VDC – Through Hole	Removed
	3505EN 24 VDC – Through Hole	Removed
I/O Modules Digital Output (DO)	3604EN 24 VDC 3624N 24 VDC, Supervised	3625N 24 VDC, Supervised/ Unsupervised Next Generation Module
	3601TN 115 VAC	Same
	3603TN 120 VDC	Same
	3607EN 48 VDC	Same
	3623TN 120 VDC, Supervised	Same
	3636TN (Relay Output)	Same
Remote Extender Modules: **Primary** **Remote**	4210N (Single Mode Fiber Optic cable) 4211N (Single Mode Fiber Optic cable)	4200N (Multi Mode Fiber Optic cable) 4201N (Multi Mode Fiber Optic cable)
I/O Module Term Panels	Version 8 Term Panels Version 9 Term Panels	Removed

Module	Tricon V9.5.3 System	Tricon V10.5.1 System
		9794-110N PI 9782-110N AI 9561-810N DI 9561-110N DI 9664-810N DO 9663-610N DO 9563-810N DI 9662-810N DO 9662-610N DO 9668-110N RO 9667-810N DO 9562-810N DI 9783-110N AI 9795-610N AI 9790-610N AI 9764-310N AI 9860-610N AO
Signal Conditioners	Signal Conditioner (-100 to 100 °C) Pt (7B34-01-1) Signal Conditioner (0 to 100 °C) Pt (7B34-02-1) Signal Conditioner (0 to 200 °C) Pt (7B34-03-1) Signal Conditioner (0 to 600 °C) Pt (7B34-04-1)	Same
	Not included	Four additional Signal Conditioners: 7B34-CUSTOM (0 to 200 °C) 7B34-CUSTOM (0 to 600 °C) 7B30-02-1 (0 to 100 mV) 7B14-C-02-1 (0 to 120 °C)
Power Supplies:	ASTEC Power Modules	Vicor Power Modules
120 V	8310N	8310N2
24 VDC	8311N	8311N2
230 VAC		8312N2
Chassis:		
Main	8110N	8110N2
Expansion	8111N	8111N
Remote Expansion*	8112N	8112N

*Remote Expansion Chassis PN 8112N may be configured as non-safety

TABLE 2 – Summary of Software Changes

Module	**Tricon V9.5.3 System Software Version**	**Tricon V10.5.1 System Software Version**
TriStation 1131 Developer's Workbench *(Application Development Software)*	v3.1	v4.7.0
Main Processor Software: **Application Processor** **I/O Processor COM Processor**	TSX 5211 IOC 5212 COM 5206	ETSX 6271 IOCCOM 6054
Communication Module Software: **TCM** **Common V9.5.3 COM** **EICM** **NCM** **ACM**	Not Applicable ICM 4930 IICX 5276 NCMX 5028 ACMX 5203	TCM 6276 Not Applicable Not Applicable Not Applicable Not Applicable
I/O Module Software: **AI 3721N**	Not Applicable	AI 6256
DO 3625N	Not Applicable	DO 6255
AI 3701N/N2	AI/NITC 4873	AI/NITC 5661
IAI 3703EN	EIAI/ITC 5491	EIAI/ITC 5916
ITC 3708EN	EIAI/ITC 5491	EIAI/ITC 5916
PI 3510N	PI 4559	Not Applicable
PI 3511N	Not Applicable	PI 5647
AO 3805EN/HN	EAO 5595	EAO 5897
DI 3501TN/TN2 DI 3502EN /EN2 DI 3503EN/EN2	EDI 5490	EDI 5909
DI 3505EN	EDI 5490	Not Applicable
DI 3504EN	HDI 5499	
AI 3704EN	HDI 5499	
DO 3601TN DO 3607EN	EDO 5488	EDO 5781
DO 3604EN	EDO 5488	Not Applicable
RO 3636TN	ERO 5497	ERO 5777
DO 3603TN	TSDO 5502	TSDO/HVDO 6273
DO 3623TN	TSDO 5502	TSDO2 5940
DO 3624N	TSDO 5502	Not Applicable
Remote Extender Modules	RXM 3310	Same

2.2 REGULATORY CRITERIA

The acceptance criteria used as the basis for this review are defined in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Revision 5, dated March 2007. NUREG-0800, which is referred to as the Standard Review Plan (SRP), sets forth a method for reviewing compliance with applicable sections of Title 10 Part 50 of the *Code of Federal Regulations* (10 CFR), "Domestic Licensing of Production and Utilization Facilities." Specifically, SRP Chapter 7, "Instrumentation and Controls," addresses the requirements for instrumentation and control (I&C) systems in nuclear power plants based on light-water reactor designs. The procedures for review of digital systems applied in this evaluation are principally contained within SRP Chapter 7 and are augmented and supplemented by Interim Staff Guidance (ISG).

The suitability of a digital platform for use in safety systems depends on the quality of its components; quality of the design process; and system implementation aspects such as real-time performance, independence, and online testing. Because this equipment is intended for use in safety systems and other SR applications, the submitted LTR was evaluated in accordance with the provisions of IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” based on the guidance contained in SRP Chapter 7, Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std 603,” and Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std 7-4.3.2,” which provide acceptance criteria for these two standards.

SRP Chapter 7, Table 7-1, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety,” identifies design criteria and regulations from 10 CFR Part 50 that are applicable to I&C systems and are relevant for general review of the suitability of a digital I&C (DI&C) platform for generic SR applications. Many of the review criteria of the SRP depend on the design of an assembled system for a particular application, whereas the LTR presents the elements of hardware and system software in the Tricon V10 platform that can be used in a variety of safety applications. Since no plant-specific application of the platform as a safety system is associated with the LTR, this SE is limited to the evaluation of compliance with the relevant regulations and guidance documents to the degree to which they can be satisfied at the platform level. In effect, fulfillment of system-level requirements can only be partially evaluated on a generic basis based on the capabilities and characteristics of the Tricon V10 platform.

Determination of full compliance with the applicable regulations remains subject to plant specific licensing review of a full system design based on the Tricon V10 platform. Thus, it is an ASAI to establish full compliance with the design criteria and regulations identified in SRP Chapter 7, Table 7-1, which are relevant to specific applications of DI&C systems at the time the application is submitted to NRC for approval. This and other ASAIs identified in the evaluation documented in Section 3 are compiled in Section 4.2 of this report.

The following regulations and design criteria in 10 CFR Part 50 are applicable in whole or in part for general review of the suitability of this I&C platform for generic SR applications at NPPs:

- 10 CFR 50.55a(a)(1), “Quality Standards for Systems Important to Safety,” requires that “structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed”
- 10 CFR 50.55a(h), “Protection and safety systems,” incorporates by reference the 1991 version of IEEE Std 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” including the correction sheet dated January 30, 1995
- 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants”
    - General Design Criterion (GDC) 1, “Quality Standards and Records”
    - GDC 2, “Design Basis for Protection Against Natural Phenomena”
    - GDC 4, “Environmental and Dynamic Effects Design Basis”
    - GDC 13, “Instrumentation and Control”

- GDC 20, “Protection System Functions”
- GDC 21, “Protection System Reliability and Testability”
- GDC 22, “Protective System Independence”
- GDC 23, “Protective System Failure Modes”
- GDC 24, “Separation of Protection and Control”
- GDC 25, “Protection System Requirements for Reactivity Control Malfunctions”
- GDC 29, “Anticipated Operational Occurrences”

SRP Chapter 7, Table 7-1, identifies regulatory guides (RGs), branch technical positions (BTPs), and industry standards that contain information, recommendations, and guidance and, in general, provide an acceptable basis to implement the above requirements for both hardware and software features of SR DI&C systems. Based on the scope of the Tricon V10 platform and the limitations of a platform-level review, the following guides and positions are determined to have relevance for consideration in this SE:

Note: Revision levels are identified here and not listed throughout the SE.

- RG 1.22, Revision -, “Periodic Testing of Protection System Actuation Functions”
- RG 1.47, Revision 1, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”
- RG 1.53, Revision 2, “Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems”
- RG 1.62, Revision -, “Manual Initiation of Protection Actions”
- RG 1.75, Revision 3, “Physical Independence of Electrical Systems”
- RG 1.89, Revision 1, “Qualification for Class 1E Equipment for Nuclear Power Plants”
- RG 1.97, Revision 4, “Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident”
- RG 1.100, Revision 3, “Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants,” which conditionally endorses IEEE Std 344-1987, “IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations”
- RG 1.152, Revision 3, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 7-4.3.2-2003, “Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations”
- RG 1.168, Revision 1, “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 1012-1986, “IEEE Standard for Software Verification and Validation Plans,” and IEEE Std 1028-1988, “IEEE Standard for Recommended Practices for Software Design Descriptions”
- RG 1.169, Revision -, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 828-1990, “Software Configuration Management Plans,” and IEEE Std 1042-1987, “IEEE Guide to Software Management”
- RG 1.170, Revision -, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 829-1983, “Software Test Documentation”
- RG 1.171, Revision -, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 1008-1987, “IEEE Standard for Software Unit Testing”

- RG 1.172, Revision -, "Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 830-1984, "Guide for Software Requirements Specification"
- RG 1.173, Revision -, "Developing Software Life Cycle Processes for Digital Computer Systems used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 1074-1995, "IEEE STD for Developing Software Life Cycle Processes"
- RG 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," which endorses IEEE Std 1050-1996, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations," and specified test methods from Military Standard (MIL-STD)-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment" and International Electrotechnical Commission (IEC) 61000, "International Electrotechnical Commission Series of EMI/RFI Test Methods"
- RG 1.209, Revision -, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," which endorses IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
- SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- SRP BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions"
- SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance"
- DI&C-ISG-04, "Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc)," September 28, 2007.

The Tricon V10 is an upgrade product based on previous designs. Some design elements of the Tricon V10 pre-date IOM's 10 CFR Part 50 Appendix B process and therefore certain industry guidelines that address dedication and qualification processes are applicable. The NRC staff has reviewed and accepted the following industry guidance documents based on conditions established in SE reports.

- EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," as accepted by the NRC SE dated April 30, 1996
- EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," as accepted by the NRC SE dated April 1997
- EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," as accepted by the NRC SE dated July 30, 1998

It should be noted that industry standards, documents, and reports use the word "requirements" to denote provisions that must be implemented to ensure compliance with the corresponding document. Additionally, these standards, documents, and reports provide guidance or recommendations that need not be adopted by the user to ensure compliance with the corresponding document, and the optional items are not designated as "requirements." The word "requirement" is used throughout the instrumentation and control discipline. However, licensee or vendor documentation of conformance to the "requirements" provided in industry standards, documents, and reports referenced in this SE constitutes conformance with NRC regulatory requirements only insofar as the standards, documents and reports are endorsed by the NRC. Other use of the word "requirements" in these documents does not indicate that the "requirements" are NRC regulatory requirements.

2.3 PRECEDENTS

Four topical reports for digital platforms have previously been approved by the NRC. These platforms are the HFC-6000, AREVA TELEPERM XS (TXS), the Westinghouse Common Q, and the Invensys Triconex, and they were generically qualified in accordance with the approved guidance of EPRI TR-107330. The corresponding SE reports (References 11, 12, 13, and 9 respectively) for these platforms document the findings of the reviews by NRC staff and constitute applicable precedents that are considered in the conduct of this review.

Specific precedents employed to support this review address environmental qualification, exceptions to key performance requirements specified by EPRI TR-107330, and Commercial Grade Dedication (CGD) of previously developed software (PDS). Each of the SEs for the generic platforms (i.e., TXS, Common Q, and Tricon V9) addresses deficiencies in the environmental qualification program for the respective platforms either through treatment as generic open items or identification of a commitment to retest on a plant-specific basis. The SE for the Tricon V9 platform (Reference 9) provides a precedent for the treatment of exceptions to the response time performance requirement from EPRI TR-107330. The SE for the Common Q platform (Reference 13) provides an evaluation of dedication activities by Combustion Engineering Nuclear Power (now owned by Westinghouse) for commercial grade items, including software, which is used in the platform. The commercial dedication of a Siemens-designed application-specific integrated circuit (ASIC) for use as the system support controller on platform printed circuit boards (PCBs) provides a precedent from the SE for the TXS platform (Reference 12) regarding the treatment of custom chips that provide processor support functionality for board management.

3.0 TECHNICAL EVALUATION

This SE follows the guidance contained in SRP Chapter 7. Chapter 7 of the NRC SRP provides guidance on reviewing complete NPP designs of I&C systems. Revision 5 to SRP Chapter 7 also includes review criteria for digital systems. The guidance is applicable to the review of TRs for evaluating the suitability of generic digital platforms for SR use through consideration of general system requirements. Based on examination of SRP Chapter 7, Table 7-1, Appendix 7.0-A, “Review Process for Digital Instrumentation and Control Systems,” and Appendix 7.1-A, “Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety,” the relevant regulatory requirements, BTPs, ISG, and acceptance criteria that can be addressed in part at the platform level are identified in Section 2.2 of this SE. The evaluation of the Tricon V10 platform against the identified acceptance criteria is documented in the following subsections.

IOM designed and built the Tricon PLC system as a commercial grade system, rather than specifically for use in SR systems in NPPs. As a result, the design process was not governed by 10 CFR Part 50 Appendix B and the related process documentation may not be fully consistent with BTP HICB-14. EPRI TR-106439 and TR-107330 recognize that commercial design practices differ from nuclear specific design practices and discuss how the essential technical characteristics of products meet the requirements, intent, and quality characteristics needed for SR systems in NPPs.

The evaluation described in this section is based on review of the information contained within the LTR. The Tricon V10 platform is described in Section 2.1 of the LTR. Sections 2.2 and 2.3 describe the product qualification. Section 5 of the LTR contains discussion of key safety system design topics, such as security, diversity, and communications. The material contained in these sections of the LTR was the principal focus of the SE and is the primary source of the descriptive information on the Tricon V10 platform presented in this section. Supplemental documentation docketed by IOM provides supporting and/or clarifying information that was considered in this evaluation. Specific reference to the source documentation is given where key information or supporting evidence from any of these additional documents proved to be essential to the conduct of the evaluation.

3.1 TRICON V10 PLATFORM DESCRIPTION

This section provides an overview of the Tricon V10 system. A detailed description of the system is provided in the following IOM documents; "Technical Product Guide, Tricon systems" (Reference 15), and the "Planning and Installation Guide" (Reference 16). The specific hardware and software that has been qualified is identified in the "Master Configuration List" (Reference 17). Table 3-1 in Section 3.3 of this document lists the Tricon V10 modules that have been qualified for nuclear SR applications.

3.1.1 TRICON V10 SYSTEM OVERVIEW

A typical Tricon V10 system (for example, one division of a reactor protection system) would consist of one or more 19-inch rack or panel mounted chassis. Each Tricon V10 system includes a main chassis, illustrated in Figure 2-1, and may also include additional expansion chassis.

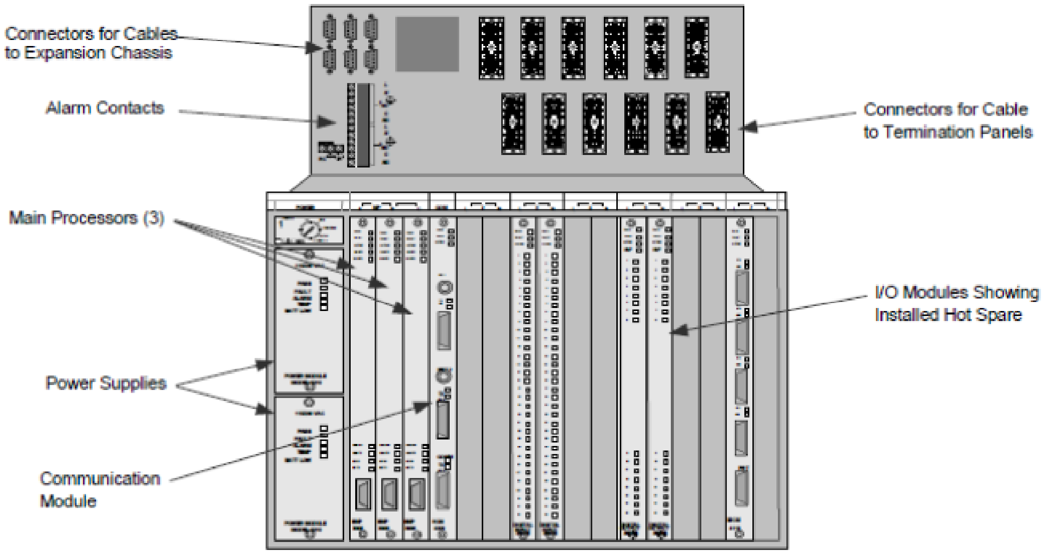

Connectors for Cables to Expansion Chassis
Alarm Contacts
Connectors for Cable to Termination Panels
Main Processors (3)
I/O Modules Showing Installed Hot Spare
Power Supplies
Communication Module

Figure 2-1 – Tricon V10 Main Chassis

Each chassis is powered by two independent, redundant power supplies, each capable of providing the full power requirements of the chassis. Thus, the system can withstand a power supply failure without interruption.

The Tricon V10 is triple redundant from input terminal to output terminal, as shown in Figure 2-2. The triple modular redundant (TMR) architecture is intended to allow continued system operation in the presence of any single point of failure within the system. The TMR architecture is also intended to allow the Tricon V10 to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. In the presence of a fault, the Tricon V10 will alarm the condition, remove the affected portion of the faulted module from operation, and continue to function normally in a dual redundant mode. The system returns to the fully triple redundant mode of operation when the affected module is replaced.

To facilitate module replacement, the Tricon V10 chassis includes provisions for a spare module, logically paired with a single input or output module. This design allows on-line, hot replacement of any module, under power while the system is running, with no impact on the operation of the application.

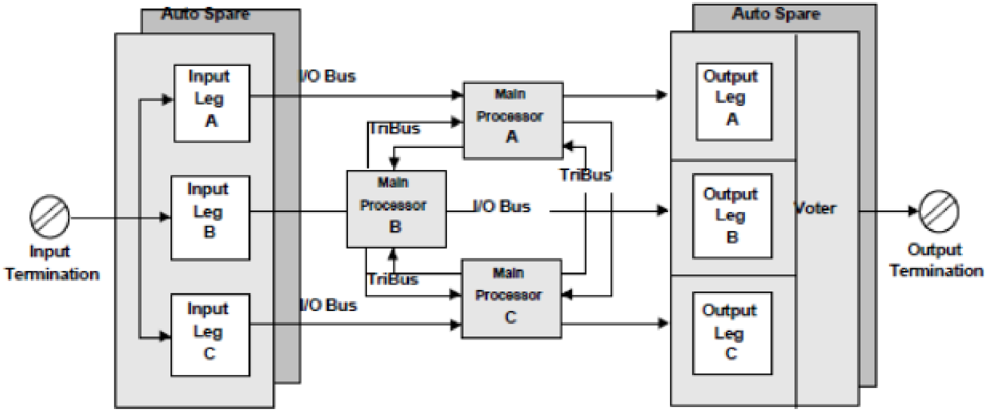


Figure 2-2 – Triple Modular Redundant Architecture

Figure 2-2 shows the arrangement of the input, MP, and output modules. As shown, each input and output module includes three separate and independent input or output circuits or legs. These legs communicate independently with the three main processor modules. Standard firmware is resident on the MP modules for all three microprocessors as well as on the input and output modules and communication modules (not shown in Figure 2-2).

3.1.2 TRICON V10 SYSTEM HARDWARE

The main components of a Tricon V10 system are the chassis, the termination panels, the power supply modules, the main processor, I/O modules, and communication modules. Functional requirements for this hardware are specified in Section 4.3 of EPRI TR-107330. Compliance of the Tricon V10 hardware with these requirements is summarized in the Requirements Traceability Matrix (RTM), Appendix A of the LTR. A description of this hardware is provided below.

3.1.2.1 8110N2 MAIN CHASSIS

A Tricon V10 system consists of one main chassis (shown in Figure 2-1) and up to fourteen additional expansion chassis. The Tricon V10 main chassis supports the following modules:

- Two redundant power supply modules
- Three main processors
- Communications modules
- I/O modules

The main chassis also has a key switch that sets the system operating mode:

- RUN – Normal operation with read-only capability by externally connected systems, including TriStation. Normally, the switch is set to this position and the key is removed and stored in a secure location.
- PROGRAM – Allows for control of the Tricon V10 system using an externally connected personal computer (PC) running the TriStation software, including application program downloads.
- STOP – Stops application program execution.
- REMOTE – Allows writes to application program variables by a TriStation PC or by MODBUS masters and external hosts.

As shown in Figure 2-3, the Tricon V10 backplane is designed with dual independent power rails. Both power rails feed each of the three legs on each I/O module and each main processor module residing within the chassis. Power to each of the three legs is independently provided through dual voltage regulators on each module. Each power rail is fed from one of the two power supply modules residing in the chassis. Under normal circumstances, each of the three legs on each I/O module and each main processor module draw power from both power supplies through the dual power rails and the dual power regulators. If one of the power supplies or its supporting power line fails, the other power supply will increase its power output to support the requirements of all modules in the chassis.

The Tricon V10 also has dual redundant batteries located on the main chassis backplane. If a total power failure occurs, these batteries maintain data and programs on the main processor modules for a period of six months. The system will generate an alarm when the battery power is too low to support the system.

The 8110N main chassis approved for the Tricon V9 is functionally equivalent to the 8110N2 qualified with the Tricon V10. However, they are not interchangeable.

3.1.2.2 8111N EXPANSION CHASSIS

The expansion chassis is the same as approved for V9 and is used locally to increase the number of I/O modules in the Tricon V10 PLC system. The expansion chassis are interconnected via three separate RS-485 data links, one for each leg of the three I/O legs. If communication modules are installed, three separate RS-485 data links are required for the three communications busses. The Tricon expansion chassis can support the following modules:

- Two redundant power supply modules
- Communications modules (in the first expansion chassis only)
- I/O modules

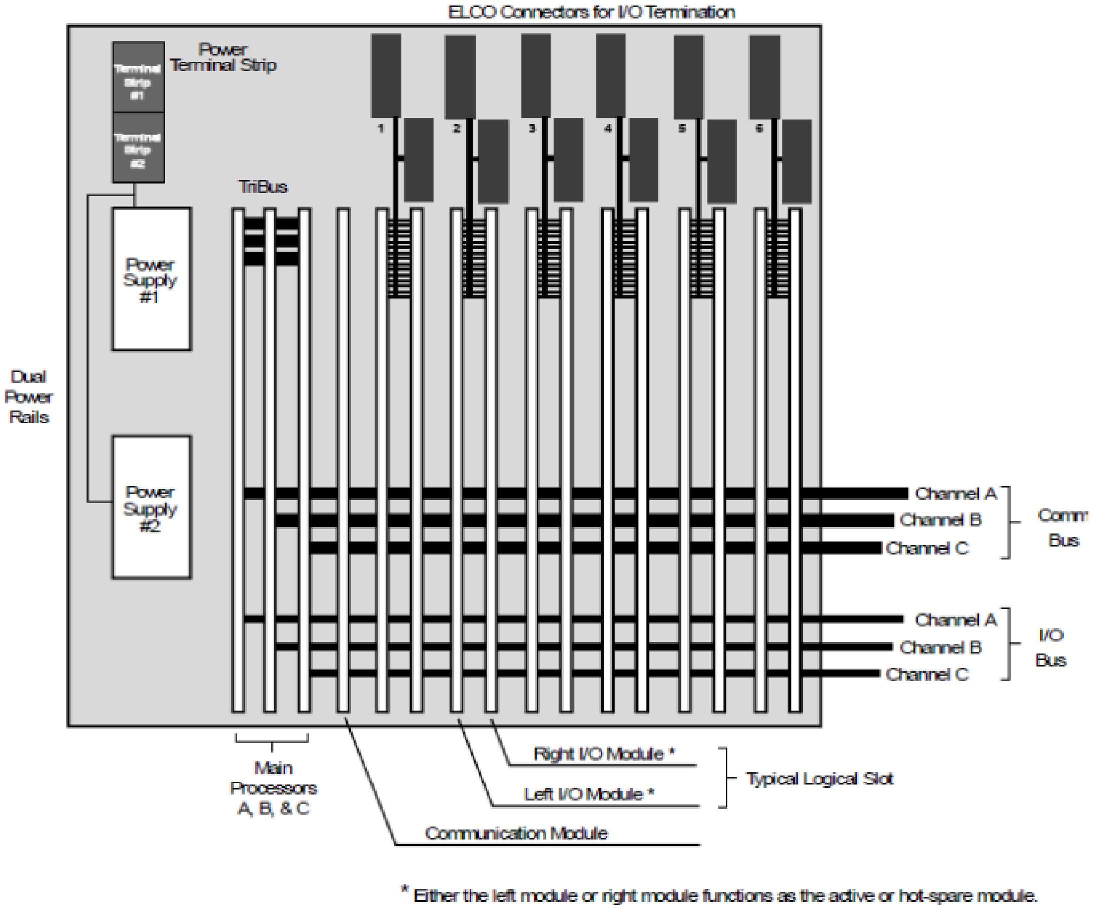


Figure 2-3 – Tricon V10 Chassis Backplane Configuration

3.1.2.3 8112N REMOTE EXPANSION CHASSIS

The remote expansion chassis are similar to the expansion chassis, but are used for remote locations, rather than locally. As such, each remote expansion chassis has remote extender modules (RXMs) that serve as repeaters or extenders of the Tricon V10 I/O bus to allow communications with the main chassis and expansion chassis within a channel or a division. A single remote RXM chassis or module would not be configured to communicate with more than one channel/division.

The Tricon V10 remote extender chassis uses the same type of power supplies as the main chassis, and has the same dual and redundant power bus arrangement. The 8112N remote expansion chassis was approved with the Tricon V9 and is unchanged as qualified with the Tricon V10.

3.1.2.4 4200N PRIMARY & 4201N REMOTE EXTENDER MODULES

RXMs are multi-mode fiber optic modules that allow expansion chassis to be located up to 1.2 miles away from the main chassis. An RXM connection consists of three identical modules, serving as repeaters/extenders of the Tricon I/O bus that also provide ground loop isolation.

Each RXM has single channel transmit and receive cabling ports. Each of the three 4200N Primary RXMs is connected to the 4201N remote RXMs housed in the remote chassis. Each pair of RXMs is connected with two fiber optic cables operating at a communication rate of 375 Kbaud. The interfacing cabling is unidirectional for each channel. One cable carries data transmitted from the primary RXM to the remote RXM. The second cable carries data received by the primary RXM from the remote RXM. The RXMs provide immunity against electrostatic and electromagnetic interference. The fiber optic cables provide Class 1E to Non-Class 1E isolation between a SR main chassis and a non-safety-related (NSR) expansion chassis.

The Tricon V9 was qualified with the 4210N and 4211N primary and remote RXM set which used single mode fiber optic cable. The V10 was qualified with the 4200N Primary and 4201N remote RXM set which uses multimode fiber optic cable. Both use the same software (see Table 2 above) and differ in the type of fiber optic cable that is supported. The V10 supported multimode fiber optic cable is capable of a 1.2 mile span while the V9 supported single mode version is capable of a 7.5 mile span. Though both RXM sets have been qualified, they are not interchangeable across the platforms because they were not qualified as interchangeable.

3.1.2.5 EXTERNAL TERMINATION ASSEMBLIES

The external termination assemblies (ETAs) are printed circuit board panels used for landing field wiring. The panels contain terminal blocks, resistors, fuses, and blown fuse indicators. The standard panels are configured for specific applications (e.g., digital input, AI, etc.). The thermocouple input termination panel provides cold-junction temperature sensors and upscale, downscale, or programmable burnout detection. The resistance temperature device (RTD) termination panels include signal conditioning modules. Each termination panel includes an interface cable that connects the termination panel to the Tricon V10 chassis backplane. The following ETAs were qualified with the Tricon V10 platform: 9794-110N PI, 9782-110N AI, 9561-810N DI, 9561-110N DI, 9664-810N DO, 9663-610N DO, 9563-810N DI, 9662-810N DO, 9662-610N DO, 9668-110N RO, 9667-810NDO, 9562-810N DI, 9795-610N AI, 9790-610N AI, 9860-610N AO, 9764-310N AI, and 9783-110N AI.

3.1.2.6 8310N2, 8311N2, AND 8312N2 POWER SUPPLY MODULES

All power supply modules are rated for 175 watts, which is sufficient to supply the power requirements of all configurations expected in SR applications. Two different power supply modules can be used in a single chassis. Three models are available to support different power sources: 120 VAC/DC (alternating or direct current), 230 VAC, and 24 VDC.

The power supply modules possess built in diagnostic circuitry to check for out-of-range voltages and/or over temperature conditions. Indicator light emitting diodes (LEDs) on the front face of each power module provide module status as follows:

Indicator	Color	Description
PASS	Green	Input Power is OK
FAULT	Red	Power Module is not OK
ALARM	Red	Chassis Alarm Condition
TEMP	Yellow	Over-temperature Condition
BATT LOW	Yellow	Battery Low Condition

The power supply modules also contain the system alarm contacts. The chassis backplane provides terminal strip interfaces for power and alarm connections. The alarm feature operates independently for each power module.

On the main chassis, the alarm contacts on both power supply modules actuate on the following states:

- System configuration does not match the control-program configuration
- A digital output module experiences a Load / Fuse error
- An AO module experiences a Load error
- A configured module is missing somewhere in the system
- A module is inserted in an unconfigured slot
- A fault is detected on a Main Processor or I/O module in the main chassis
- A fault is detected on an I/O module in an expansion chassis
- A main processor detects a system fault
- The inter-chassis I/O bus cables are incorrectly installed (i.e., cross connected)

The alarm contacts on at least one of the chassis power supplies will actuate when the following power conditions exist:

- A power module fails
- Primary power to a power module is lost
- A power module has a low battery or over temperature condition

The alarm contacts on both power modules of an expansion chassis actuate when a fault is detected on an I/O module.

3.1.2.7 3008N MAIN PROCESSOR MODULES

The Tricon V10 main processor subsystem utilizes three 3008N MP modules to control the three separate legs of the system. Each 3008N MP module operates independently with no shared clocks, power regulators, or circuitry. Each 3008N MP module controls one of the three signal processing legs in the system and each contains two 32-bit processors. One of the 32-bit processors is a dedicated, leg-specific I/O and communication (IOCCOM) microprocessor that processes all communication with the system I/O modules and communication modules.

The second 32-bit primary processor manages execution of the safety control program and all system diagnostics at the main processor module level. Between the two 32-bit primary processors is a dedicated dual port random access memory (RAM) allowing for direct memory access data exchanges.

The operating system (ETSX 6271), run-time library, and fault analysis for the main processor is fully contained in flash memory on each 3008N MP module. As shown in Figure 3-2, the Tricon V10 PLC system has four separate bus structures, the Tribus, the communications bus, the I/O bus, and the bus internal to each of the main processor modules. Each of these bus structures is triplicated. The main processors communicate with one another through a proprietary, high speed, voting, bi-directional serial channel called TriBUS. Each main processor has an I/O channel for communicating with one of the three legs of each I/O module. All external data coming into the main processor comes through the dual port RAM and does not require handshaking or use of interrupts. Each main processor has an independent clock circuit and selection mechanism that enables all three main processors to coordinate their operations each scan to allow voting of data and exchange of diagnostic information.

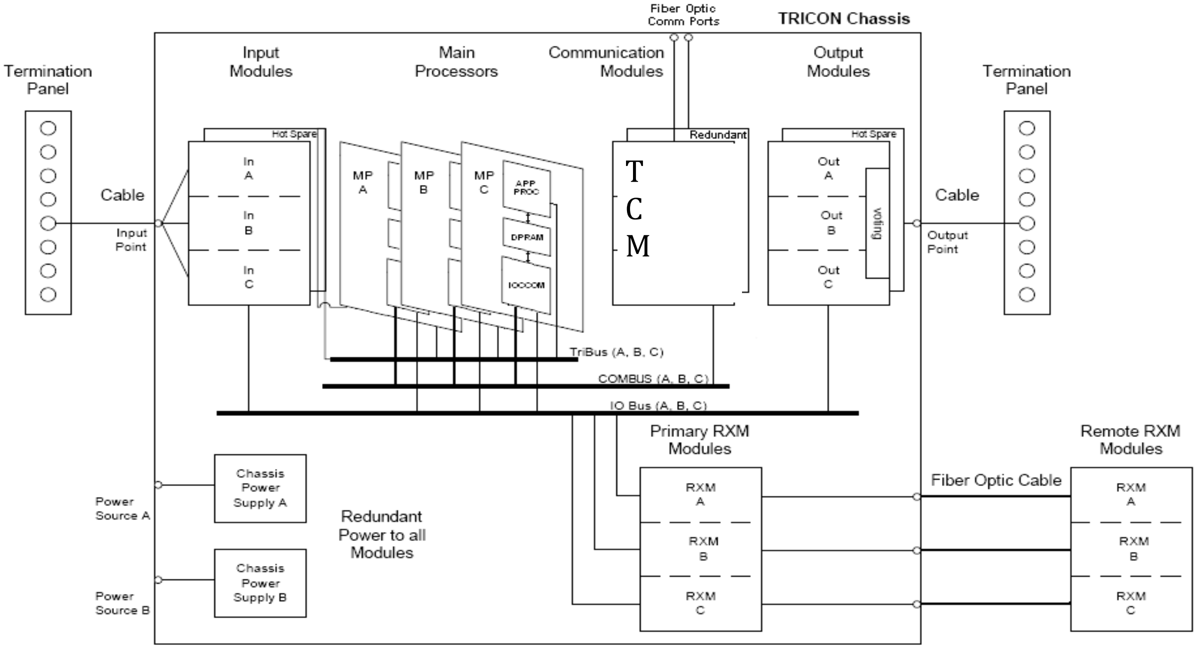


Figure 3-2 – Tricon Bus Diagram

The IOCCOM (IOCCOM 6054) processors constantly poll respective legs for all the I/O modules in the system. They continually update an input data table in dual port RAM on the main processor module with data downloaded from the leg-specific input data tables from each input module. Communication of data between the main processor modules and the I/O modules is accomplished over the triplicated I/O data bus using a master-slave communication protocol. The system uses cyclic redundancy checks (CRC) to ensure the correctness of data transmitted between modules. Should a main processor module lose communication with its respective leg on any of the input modules in the system, or the CRC reveals that the data has been corrupted, the system will retry the data transmission up to three times. If unsuccessful, input tables at the main processor module level are constructed with data in the de-energized state. Errors such as an open circuited data bus, short circuited data bus, or data corrupted while in transit will force the input table entries to the de-energized state.

At the beginning of each scan, each primary processor takes a snapshot of the input data table in dual port RAM, and transmits the snap shots to the other main processor modules over the TriBUS. This transfer is synchronized using the TriClock. Each module independently forms a voted input table based on respective input data points across the three snapshot data tables. If a main processor module receives corrupted data or loses communication with one of the other 3008N MP modules, the local table representing that respective leg data will default to the de-energized state. If a disagreement occurs, the value found in two out of three tables prevails and the third is corrected accordingly. One-time differences that result from sample timing variations are distinguished from a pattern of differing data. Each main processor maintains data about the necessary corrections in local memory. Any disparity is flagged and used at the end of the scan by the built-in fault analyzer routines of the Tricon V10 PLC system to determine whether a fault exists in a particular module. This feature is essential to maintaining deterministic behavior in the triple modular redundant architecture.

For digital inputs, the voted input table is formed by a two out of three majority vote on respective inputs across the three data tables. The voting scheme is designed for de-energize to trip applications, always defaulting to the de-energized state unless voted otherwise. Any single leg failure or corrupted signal feeding a main processor module is corrected or compensated for at the main processor module level when the voted data table is formed.

For AIs, a mid-value selection algorithm chooses an AI signal representation in the voted input table. The algorithm selects the median of the three signal values representing a particular input point for representation in the voted input tables. Any single leg failure or corrupted signal feeding a main processor module is compensated for at the main processor module level when the voted data table is formed. Errors are alarmed.

The primary processors then execute the application safety program in parallel on the voted input table data and produce an output table of values in dual port RAM. The voting schemes explained above for analog and digital input data ensure the process control programs are executed on the same input data value representations. The IOCCOM processors generate smaller output tables, each corresponding to an individual output module in the system. Each small table is transmitted to the appropriate leg of the corresponding output module over the I/O data bus.

The transmission of data between the main processor modules and the output modules is performed over the I/O data bus using a master-slave communication protocol. The system uses CRC to ensure the data transmitted between modules is not corrupted. If the CRC reveals that the data has been corrupted, the system will retry the data transmission up to three times. If unsuccessful, that respective leg data table at the output module level will default to the de-energized state. Watchdog timers on each output module leg ensure communication has been maintained with its respective main processor module. If communication has not been established or has been lost, the respective leg data table will default to the de-energized state to protect against open or short-circuited data bus connections between modules.

The main processor diagnostics monitor the proper operation of each main processor as well as each I/O module and communication channel. The main processor modules process diagnostic data recorded locally and data received from the input module level diagnostics in order to make decisions about the health of the input modules in the system. All discrepancies are flagged and used by the built in fault analyzer routine to diagnose faults. The main processor diagnostics perform the following:

- Verification of fixed-program memory.
- Verification of the static portion of RAM.
- Verification of the dual port RAM interface with each IOCCOM.
- Checking of each IOCCOM's ROM, dual port RAM access and loopback of RS-485 transceivers.
- Verification of the TriTime interface.
- Verification of the TriBUS interface.

When a fault is detected on a 3008N MP module, it is annunciated and voted out, and processing continues through the remaining two 3008N MP modules. When the faulty main processor module is replaced, it runs a self-diagnostic to verify its proper operation. When the self-diagnostic is successfully completed, the main processor module then begins the process of “re-education,” where the control program is transferred from each of the working units into the returning main processor module. All three 3008N MP modules then resynchronize data and voting, and the replacement processor module is allowed back in service.

3.1.2.8 INPUT/OUTPUT MODULES

As shown in Figure 2-2, all TMR input modules contain three separate, independent processing systems, referred to as legs, for signal processing (Input Legs A, B, and C). The legs receive signals from common field input termination points. The microprocessor in each leg continually polls the input points, and constantly updates a private input data table in each leg’s local memory. Signal conditioning, isolation, or processing required for each leg is also performed independently. The input modules possess sufficient leg-to-leg isolation and independence so that a component failure in one leg will not affect the signal processing in the other two legs.

Input data is sampled continuously, in some modules compared and/or voted, and sent to the 3008N MP modules. Each main processor module communicates via an individual I/O bus with one of the triplicated microprocessors on each I/O module. In each main processor module, the IOCCOM microprocessor reads the data and provides it to the application processor through a dual port RAM interface. For AIs, the three values of each point are compared, and the middle value is selected. The control algorithm is invoked only on known good data.

All input modules include self-diagnostic features designed to detect single failures within the module. Fault detection capabilities built into various types of input modules include the following:

- The input data from the three legs is compared at the main processor module, and persistent differences generate a diagnostic alarm.
- Digital input modules test for a stuck on condition by momentarily driving the input for one leg low in order to verify proper operation of the signal conditioning circuitry. A diagnostic alarm is generated if the input module does not respond appropriately.
- Analog input modules include high accuracy reference voltage sources which are used to continuously self-calibrate the analog-to-digital converters. If a converter is found to be out of tolerance, a diagnostic alarm is generated.
- Several input modules also include diagnostics to detect field device failures.

A detailed description of each type of input module, including fault detection and data validation processes, is provided in Section 5 of “System Safety Concept,” IOM Document No. 9100112-001 (Reference 33).

After the application processor in each 3008N MP module completes the control algorithm, data is sent out to the output modules. Outputs from the 3008N MP modules are provided to the IOCCOM microprocessors through dual port RAM. The IOCCOM microprocessors then transfer that data to the triplicated microprocessors on the output modules. The output modules then set the output hardware appropriately on each of the triplicated sections and vote on the appropriate state and/or verify correct operation. Discrete outputs use a unique, patented, power output voter circuit. This voter circuitry is based on parallel-series paths that pass power if the driver for legs A and B, or legs B and C, or legs A and C command them to close (i.e., 2-out-of-3 vote). AOs use a switching arrangement tying the three legs of digital to analog converters to a single point.

All output modules include self-diagnostic features designed to detect single failures within the module. The major fault detection capabilities built into output modules include the following:

- Digital output modules include output voter diagnostics that toggle the state of one leg at a time to verify that the output switches are not stuck on or off.
- Supervised digital output modules include a voltage and current loopback circuit that checks for open circuits (i.e., blown fuse) and short circuits in the field wiring.
- AO modules include a voltage and current loopback circuit. On these modules, one of the three legs drives the field load, and the other two legs monitor the loopback current to verify the module output current is correct.

A detailed description of the output modules, the voting processes, and fault detection processes is provided in the Planning and Installation Guide (Reference 16).

If one of the three legs within an I/O module fails to function, an alarm is raised by the 3008N MP modules on the main chassis power modules. If a standby module is installed in the paired slot with the faulty module, and that module is deemed healthy by the 3008N MP modules, the system automatically switches over to the standby unit and takes the faulty module off line. If no standby unit is in place, the faulty module continues to operate on two of the three legs and protection and control is unaffected. The user obtains a replacement unit and plugs it into the system into the logically paired slot associated with the failed module. When the 3008N MP modules detect the presence of a replacement module, they initiate local health state diagnostics and, if the module is healthy, automatically switch over to the new module. The faulty module may then be removed and returned to the factory for repair.

If a standby module is installed and both it and its pair are deemed healthy by the 3008N MP modules, each of the modules is exercised on a periodic basis. The 3008N MP modules will swap control between the two modules. By periodically using both modules, any faults are detected, alarmed, and the failed module replaced while a standby module is in place. This use of standby modules does not cause any interruption of protection or control functions.

The Tricon V9 safety evaluation stated that all Tricon I/O modules have a common core. However, two of the new modules for V10, 3721N Analog Input and 3625N Digital Output have a new common core called “Next Generation” (NG). The NG common core is based on the common core staff reviewed and approved with V9. The NG common core based modules may be used interchangeably with older design common core cards such that NG cards can be configured in any chassis configuration and co-located with V9 based cards without special exception or modification as qualified.

The NG common core has equivalent levels of fault detection as were approved for V9 I/O modules. Card level scan times for the NG core input modules are 10 milliseconds (msec) as opposed to the 50 msec times typical for cards approved on the V9 platform. Security is similar to V9 cores. Firmware (FW) for NG cores cannot be downloaded from the main processor and no access points are available when the card is installed in the chassis. The NG cards must be removed from the chassis, which the system will alarm, in order to change the FW. The NG modules installed in the wrong slot or with FW loads that do not match that programmed in the application processor will be ignored, which is the same as was previously approved.

3.1.2.8.1 ANALOG INPUT MODULES

The following types of AI modules are available for SR use in NPPs:

- Model 3721N (AI 6256) is a TriStation configurable 0-5 VDC or -5-+5 VDC analog input module with 32 differential DC-coupled inputs. The model has a +6 percent over-range. The 3721N uses the NG common core.
- Model 3701N2 (AI/NITC 5661) is a 0-10 VDC analog input module with 32 differential DC-coupled inputs. It is equivalent to the 3701N approved with the Tricon V9 platform, but has been implemented with surface mount components. The 3701N2 hardware and software were re-qualified for the Tricon V10 platform.
- Model 3511N (PI 5647) is an 8 channel, non-commoned pulse input module with 16 bit resolution and +/- 0.01 percent accuracy from 1-20 kilohertz (kHz). It is based on the 3510N approved with the Tricon V9 platform with the same specifications except update rate has been improved from 50 msec to 25 msec, worst case. This pulse input module is optimized for measuring speed of rotating machinery. It does not have totalization capability.
- Model 3703EN (EIAI/ITC 5916) is a 0-5 or 0-10 VDC isolated AI module with 16 differential isolated inputs. This module has a selectable voltage range and upscale or downscale open-input detection and a +6 percent over-range measurement capability. Model 3703EN was approved for use with the Tricon V9 platform and was qualified with the Tricon V10 platform.
- Model 3708EN (EIAI/ITC 5916) is an isolated thermocouple input module with 16 differential isolated inputs. This module can support thermocouple types J, K, T, and E, and can be programmed to provide upscale or downscale burnout detection. In addition to the Pass/Fault/Active indicator lights, this module has an indicator light that shows a failure of a cold-junction transducer. Model 3708 EN was approved for use with the Tricon V9 platform and was qualified with the Tricon V10 platform.

3.1.2.8.2 ANALOG OUPUT MODULES

The following types of AO modules are available for SR use in NPPs:

- Model 3805HN (EAO 5897) is the only AO module available for use in nuclear power plants with the Tricon V10 platform and is a 4-20 milliampere (mA) AO module. This model has eight DC-coupled outputs, all with a common return. This module provides for redundant loop power sources with individual indicators. If this option is used, the licensee must provide external loop power supplies for AOs. The 3805HN is based the 3805EN approved with the Tricon V9 platform, but has a minor enhancement to improve inductive load capability.

3.1.2.8.3 DIGITAL INPUT MODULES

The following types of digital input modules are available for SR use in NPPs:

- Model 3501TN2 (EDI 5909) is a 115 VAC/DC digital input module with 32 isolated input points. This model has standard diagnostics, but does not have the ability to verify the transition of a normally energized circuit to the off state. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 input points is on or off. The 3501TN2 is a surface mount version of the 3501TN approved for use on the Tricon V9 platform. The software has minor updates and was qualified with the Tricon V10 platform.

- Model 3502EN2 (EDI 5909) is a 48 VAC/DC digital input module with 32 inputs. Four groups of 8 inputs use a common reference point. Unlike the Model 3501TN2, this model can continuously verify the transition of a normally energized circuit to the off state. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 input points is on or off. The 3502EN2 is a surface mount version of the 3502EN approved for use on the Tricon V9 platform. The software has minor updates and was qualified with the Tricon V10 platform.
- Model 3503EN2 (EDI 5909) is a 24 VAC/DC digital input module with 32 inputs. Four groups of 8 inputs use a common reference point. Like the Model 3502EN2, this model can continuously verify the transition of a normally energized circuit to the off state. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 input points is on or off. The 3503EN2 is a surface mount version of 3503EN approved for use on the Tricon V9 platform. The software has minor updates and was qualified with the Tricon V10 platform.

3.1.2.8.4 DIGITAL OUPUT MODULES

The following types of digital output modules are available for SR use in NPPs:

- Model 3625N (DO 6255) is a 24 VDC digital output module with 32 output points that use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module also has indicator lights showing if each of the 32 output points is on or off. This module uses the NG common core.
- Model 3601TN (EDO 5781) is a 115 VAC digital output module with 16 outputs that do not use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off. Model 3601TN was approved for use with the Tricon V9 platform and requalified with functionally equivalent software with the Tricon V10 platform.
- Model 3603TN (TSDO/HVDO 6273) is a 120 VDC digital output module with 16 outputs that use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off. Model 3603TN was approved for use with the Tricon V9 platform and requalified with functionally equivalent software with the Tricon V10 platform.
- Model 3607EN (EDO 5781) is a 48 VDC digital output module with 16 outputs that do not use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off. Model 3607EN was approved for use with the Tricon V9 platform and requalified with functionally equivalent software with the Tricon V10 platform.
- Model 3623TN (TSDO2 5940) is a 120 VDC supervised digital output module with 16 outputs that use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off. Model 3623TN was approved for use with the Tricon V9 platform and requalified with functionally equivalent software with the Tricon V10 platform.
- Model 3636TN (ERO 5777) is the only relay output module available for SR use in nuclear power plants for the Tricon V10 platform. The 3636TN has 32 normally open non-common simplex outputs. The Model 3636TN relay output module receives output signals from the main processors on each of the three legs. The three sets of signals

are then voted, and the voted data is used to drive the 32 individual relays. Each output has a loopback circuit that verifies the operation of each relay switch, independent of the presence of a load. Ongoing diagnostics test the operational status of the relay output module. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 output points is on or off. Model 3636TN was approved for use with the Tricon V9 platform and requalified with functionally equivalent software with the Tricon V10 platform.

3.1.2.9 4352AN TRICON COMMUNICATION MODULE

Like the I/O modules, the TCM has three separate communication busses and three separate communication bus interfaces, one for each of the three 3008N MP modules. Unlike the I/O modules, however, the three communication bus interfaces are merged into a single microprocessor. That microprocessor votes on the communications messages from the three 3008N MP modules and transfers only one of them to an attached device or external system. If two-way communications are enabled, messages received from the attached device are triplicated and provided to the three 3008N MP modules.

The communication paths to external systems have CRCs, handshaking, and other protocol-based features. These features are supported in hardware and FW. FW provides core functionality common to all the communication modules with additional coding to support the specific communication protocol.

The three communications modules of the V9 system have been replaced by one communication module, the 4352AN TCM Fiber Optic module. The TCM allows the Tricon V10 to communicate with other Tricon platforms and with external hosts over fiber optic networks. The TCM provides two fiber optic port connectors which support peer-to-peer, time synchronization, and open networking to external systems. In addition, the TCM contains four serial ports allowing the Tricon V10 to communicate with Modbus master and slaves. Each serial port is uniquely addressed and supports the Modbus protocol.

The TCM provides functional isolation by handling all the communications with external devices. In addition, the TCM has been qualified for SR applications and contributes to the overall reliability of the communication link through the use of IP address discrimination and CRCs, and testing has demonstrated that it will protect the safety core from network storms and other communication failures as detailed in IOM Document NTX-SER-10-14, “Tricon V10 Conformance to RG 1.152,” Appendix A (Reference 35). This testing was performed by an independent third-party (Wurldtech) to validate the robustness of the Tricon V10 platform against communication failures. Wurldtech performed testing of a number of scenarios testing the communications link in the presence of a communications failure. This testing is further discussed in Section 3.8.1.2 of this SE. This report and the data it contains is proprietary; however, in summary, this testing verified the effectiveness of the TCM to cope with various communication failures, demonstrating proper handling of rogue and invalid protocol packets, and continued operation under network storm conditions without adverse impact on the TMR 3008N MP control algorithm. The test configuration included monitoring of digital output signals to confirm that the Tricon application program running on the TMR 3008N MPs was unperturbed. This testing validated that the TCM will discard rogue, invalid, and excessive Ethernet packets (such as during data storms), thereby ensuring the operation of the TMR 3008N MPs was unperturbed during communication failures. The results of the Wurldtech testing validated the added reliability the TCM provides to the communication link. The third party vendor, Wurldtech, and associated certification are not endorsed by NRC and are not approved in this SE. However, the NRC staff credits the testing as a limited demonstration of the TCM's ability to protect the safety function. Upon total loss of all TCMs, the safety function will continue to operate without interruption.

IOM developed a communication application safety layer for communication between an external processor and the Tricon V10 system. This is an additional layer of protection provided by the communication protocols at the application layer of the network stack. The Peer-to-Peer (P2P) and Safety Application Protocol (SAP) protocols ensure end-to-end integrity of safety-critical messages. System architectures requiring data transfer between SR Tricons over a network would use the P2P protocol over an isolated, point-to-point network. Architectures requiring safety-critical data exchange with video display units would utilize the SAP which is reviewed in Section 3.7.1 of this SE. Tricon V10 conformance to ISG 4 is evaluated in Section 3.7.3 of this SE.

3.1.3 TRICON V10 SYSTEM SOFTWARE

The Tricon V10 system software consists of the operating system that is resident on the various microprocessors within the system, the non-safety TriStation 1131 software used to develop application programs, and the application program itself. Functional requirements for this software are specified in Section 4.4 of EPRI TR-107330. Compliance of the Tricon V10 software with these requirements is summarized in the Requirements Traceability Compliance Matrix, Appendix A of the LTR (Reference 4). The following subsections describe each of these software types in greater detail.

3.1.3.1 TRICON V10 OPERATING SYSTEM: ETSX 6271

The Tricon V10 operating system software consists of the firmware that resides on the microprocessors in the 3008N MP, I/O, and communication modules. Two sets of dedicated function microprocessor firmware exist within the 3008N MP module. The application processor in the 3008N MP is the primary 32-bit microprocessor and has the operating environment firmware. The IOCCOM microprocessor (the I/O and communication interfaces) has its own FW to communicate with the I/O and communication modules. The primary microprocessor FW includes all the built-in self-diagnostics and triple modular redundancy functions; no additional diagnostic functions need to be developed by the user in the application program.

The operating system (ETSX version 6271) consists of three tasks: Scan Task, Communication Task, and Background Task. The prioritizations, subtasks, and relationship to the communications processor (IOCCOM) and its functions are described below and depicted in Figures 2-4 through 2-6.

Upon power up (when a 3008N MP Module is inserted in the appropriate slot of the main chassis), the 3008N MP goes through the power up initialization and diagnostics. The power up sequence includes a series of power up diagnostics – Microprocessor tests, RAM tests, Flash memory tests, Watchdog test, Clock Calendar test, etc. The power up sequence is also initiated by hardware and software reset of the 3008N MP. Upon successful completion of Power up sequence, the 3008N MP enters the Scan Task. Figure 2-4 shows the ETSX version 6271 tasks and priorities.

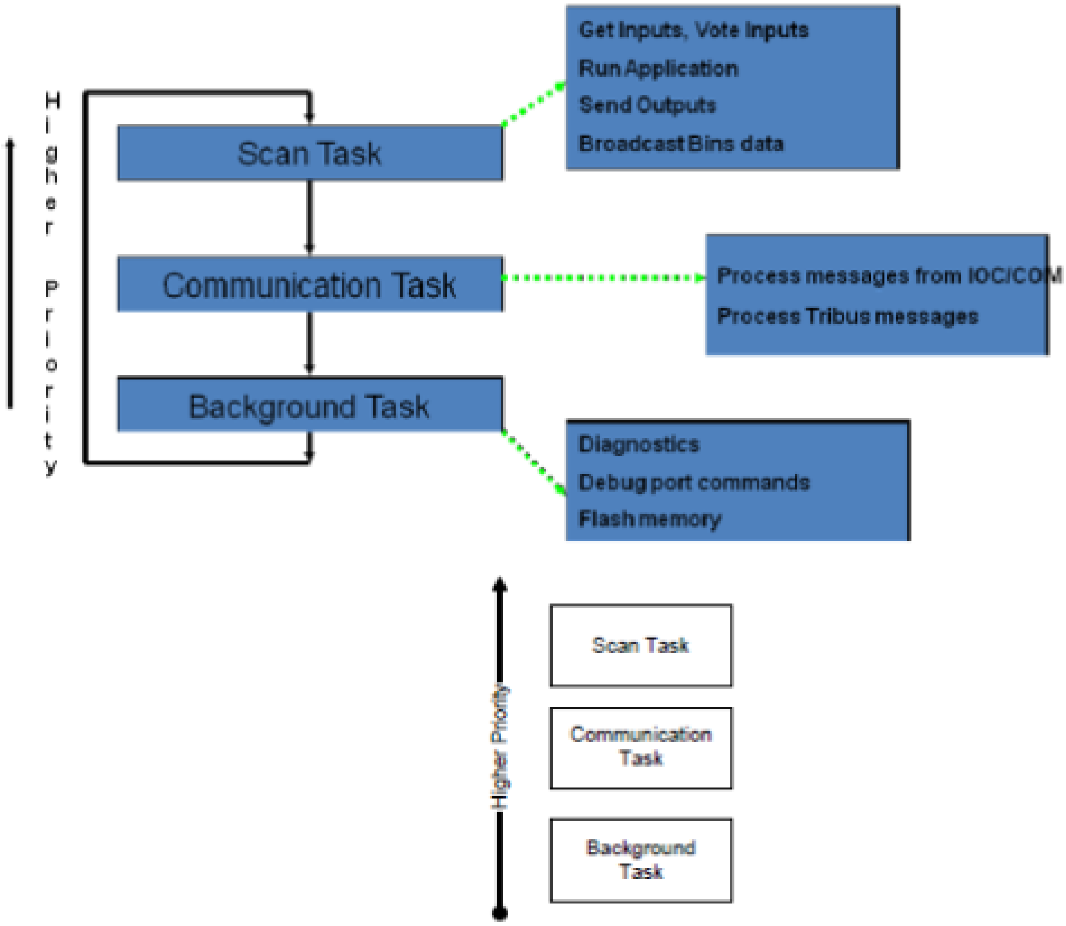


Figure 2-4 - ETSX tasks and priorities

The scan is divided between these tasks as illustrated in Figure 2-5.

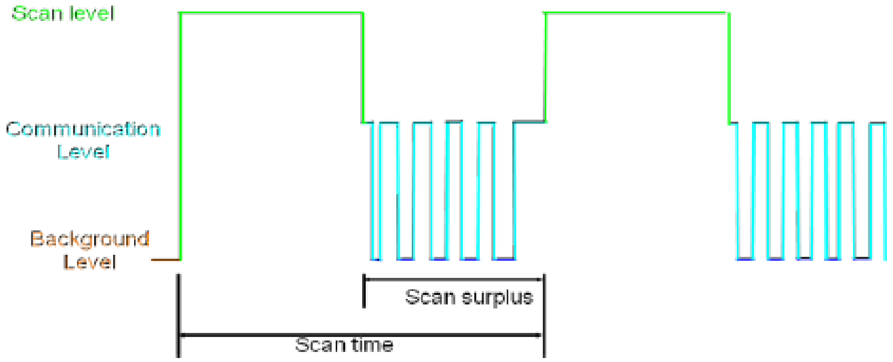


Figure 2-5 - ETSX task scheduling

The Scan Task performs the following steps:

1. Get Inputs from IOCCOM Memory
2. Perform TriBUS Transfer
3. Process any synchronization requests
4. Run Control Program
5. Send Outputs
6. Coordinate End of Scan

The Communication Task runs every 10 msec or when a communication port interrupt occurs. The Communication Task does the following:

1. Process Messages from IOCCOM
2. Process Messages from Communication Modules
3. Fill TriBUS Communication Buffers
4. Check Event Buffers
5. Send Diagnostic Messages across secondary channel
6. Perform Transport Task
7. Do any loader background work (TriStation messages for download)
8. Handle any TriBUS Messages from other MPs

The Background Task is responsible to run diagnostics, handle debug port commands, and write information to flash memory. ETSX Version 6271 is synchronized with the IOCCOM processor at the beginning of every scan. This is illustrated in Figure 2-6.

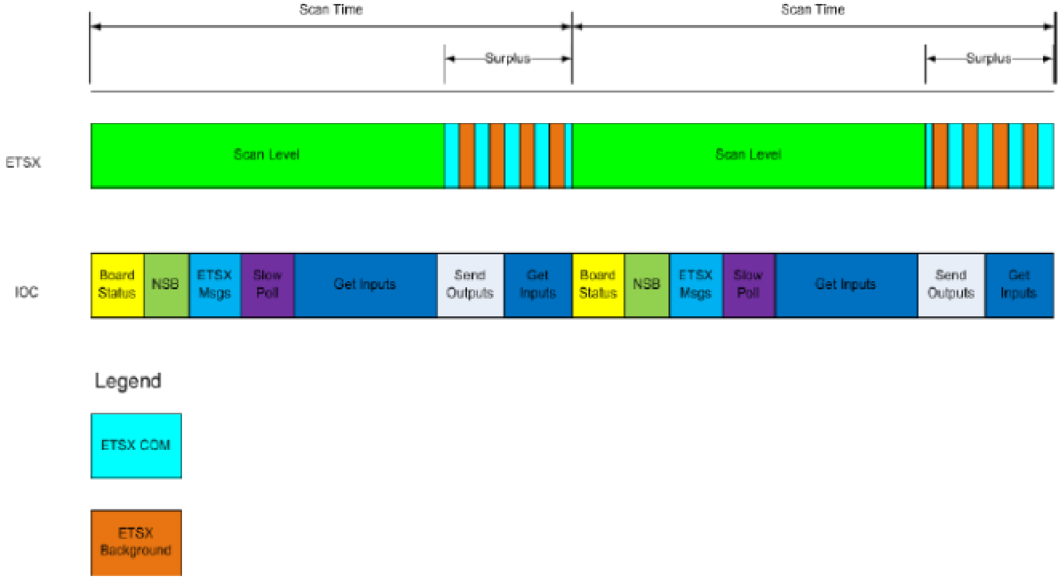


Figure 2-6 - ETSX and IOCCOM synchronization

The system FW resident on the I/O modules is designed around a common core which supports communication with the main processor modules and processing of the I/O data. Specific customization of the core software is applied to fit the needs of the specific type of module and the data to be acquired. This customization includes the integral fault detection capabilities. Each of the three microprocessors on a module (i.e., in each of the three independent legs) runs exactly the same FW. Each microprocessor interfaces to only one leg of the I/O bus, and thus to only one main processor module.

As described in the preceding sections, the design of the software includes features to detect and mitigate system faults. These features include hardware and software based diagnostics. The diagnostic capabilities of the system are validated when hardware or software changes are made in any module. The validation requires that the stuck at zero, stuck at one, and contact noise from the automated fault injection system produce the pre-defined, expected diagnostic result. Failure to produce the correct result is evaluated and corrected exactly like a failure to produce any diagnostic result.

The level of diagnostic self test capabilities of new modules in the Tricon V10, including the 3008N MP module, is similar to the capabilities reviewed on the Tricon V9. The diagnostics are integrated into the base Tricon V10 and require no special application programming. In addition, data is made available to the application program concerning program operation, results of arithmetic operations, and other internal faults. Thus, requirements imposed on the application program relating to error detection are limited to providing appropriate error recovery and annunciation of faults. The NRC staff observed fault detection verification testing at IOM's Irvine, California facility that demonstrated IOM's method for verifying fault detection capabilities. Faults were injected on a live card connected to an operational Tricon V10 chassis via extender cables. Faults were assessed through a maintenance terminal connected to a TCM module in the main chassis. A robotic system could optionally be employed to run extensive real time fault insertion testing.

3.1.3.2 TRISTATION 1131 V4.7.0 PROGRAMMING SOFTWARE

Application programming is generated using the TriStation 1131 Developer's Workbench, which runs on a standard PC. The current version is TriStation 1131 V4.7.0, an upgrade from TriStation 1131 V3.1 evaluated with the Tricon V9. TriStation 1131 V4.7.0 maintains the features described in the V9 SER (Reference 9) and adds support for 3008N MP, TCM and NGIO modules as well as Windows XP host environment compatibility. The TriStation 1131 does not perform SR functions. It is a software tool which allows end-users to develop application programs and download those applications to the target Tricon V10. The TriStation 1131 PC would not normally be connected while the Tricon V10 is performing safety critical functions. However, it is physically possible for the TriStation PC to be connected at other times and this must be prevented or controlled in a manner such that the Tristation tool cannot affect the safety related functions of the Tricon V10 processor through plant-specific procedures and administrative controls.

The TriStation 1131 software provides four programming languages, including Structured Text, Function Block Diagrams, Logic Diagrams, and an IOM-defined Cause and Effect Matrix language, called CEMPLE. The software implements a Graphical User Interface comprising language editors, compilers, linkers, emulation, communication, and diagnostic capabilities for the Tricon V10 PLC system.

The TriStation 1131 Developer's Workbench translates the various languages into native mode executable code. The Cause and Effect Matrix, Logic Diagrams, and Function Block Diagrams are translated into Structured Text. The Structured Text is translated into an emulated code. The emulated code is then translated into native mode assembly language. This code is then assembled and linked with native mode code libraries to generate an executable program. Up to this point, all application development may be performed off line, with no physical connection between the TriStation PC and the Tricon V10.

The TriStation 1131 Developer's Workbench also provides emulation capabilities for the Tricon V10. The tool provides a capability for running an emulation code version of the program on the PC. Capabilities exist for manual input of program variables and observation of program outputs on the PC screen, with the inputs and output values merged and displayed with the program blocks. The simulation function of the TriStation tool was not approved for use as a V&V tool within the context of Tool Requirements stated in IEEE Std 7-4.3.2 in the Tricon V9 safety evaluation. Any use of the TriStation simulation functions as a means of performing V&V activities would not be allowed unless the tool outputs are subject to complete V&V or if the tool itself is developed using the same or equivalent high quality lifecycle process as is required for the Tricon V10 SR software.

Compiled application programs are downloaded to the Tricon V10 through a communication module. Programs and translated code are protected by 32-bit CRC. During the download process, the individual communication blocks have CRC protection. Communication blocks with computed CRC that does not match the transmitted CRC are rejected. In addition, the program segments, which may span communication blocks, have an overall 32-bit CRC. The 32-bit CRC for each program is stored both in the TriStation and in the Tricon V10.

The user may request a comparison between the content of the Tricon V10 and the data stored in the TriStation to be confident that the application in the Tricon V10 and the application last downloaded through the TriStation are identical. Comparison failures would indicate that the application in the Tricon V10 and the content of the TriStation are no longer the same.

3.1.3.3 SAFETY-RELATED PLANT-SPECIFIC APPLICATION PROGRAM

The application program implements the desired safety system protection, monitoring, and control functions defined by the design basis documents for the facility-specific system. Therefore, the actual application programming is not included in the generic qualification of the Tricon V10.

The TriStation 1131 software offers various support functions for security, change detection, and documentation or comments integrated with the SR application programming. These features should provide a basis on which a utility could build a workable software control and configuration management process.

In addition to the support features offered by the TriStation 1131, the standardized language features will aid in the development of safety critical functions. The TriStation 1131 function subset does not allow such constructs as looping and GOTO that could inadvertently result in infinite program flow loops or at least in non-deterministic execution timing. This reduces the chance of bad programming constructs creating unexpected system hangs, further reducing the chance of system failures.

3.1.3.4 SOFTWARE DEVELOPMENT TOOLS

IOM does not credit any software tools in the development of the Tricon V10 platform other than the TriStation 1131. Although some testing requires the use of data loggers or standard computer applications to collect data, IOM manually verifies all results.

3.2 DEVELOPMENT PROCESS

The regulation at 10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed. SRP Chapter 7, Appendix 7.0-A, Section 3.H, "Review Process for Digital Instrumentation and Control Systems," states that "All software, including operating systems, that is resident on safety system computers at runtime must be qualified for the intended applications. Qualification may be established either by producing the PDS items under a 10 CFR 50, Appendix B quality assurance program or by dedicating the item for use in the safety system as defined in 10 CFR 21."

The regulatory bases used by the NRC staff for review are listed below. Also, NRC staff evaluated V10.5.1 against RG 1.152, Revision 3, which does not consider cyber security. Cyber security is covered under 10 CFR 73.54 and RG 5.71 and was not evaluated as part of this LTR review.

In the case of the Tricon V9 PLC system, the NRC staff determined that the required software documentation was contained within the following IOM documents:

- IOM quality and engineering procedures, which provide planning requirements for quality assurance, V&V, configuration management, and test activities.
- The original Tricon PLC system functional requirements specifications.
- A series of Tricon PLC system software design specifications that define the incremental changes to the system.
- Test procedures and test reports applicable to each system revision for both hardware and software.
- The Tricon PLC system software release definition documents that identify software changes made in each revision.
- The Tricon PLC system user documentation.

As part of its review and approval of the V9 Tricon platform, the NRC staff reviewed the Software Qualification Report and the associated documentation, and determined that the IOM QA and engineering procedures were of sufficient quality to provide reasonable assurance that the development process met the provisions for software planning documents as defined in BTP-14. In addition, the NRC staff found that the software development, V&V, and test documentation of the Tricon PLC software was in compliance with both IOM procedural requirements and the general requirements of current industry standards. The NRC staff further determined that the Tricon PLC system software documentation was acceptable for software intended for SR use in nuclear power plants.

In developing the Tricon V10 system, several additions were made to these development processes. IOM document NTX-SER-09-05, Revision 2 (Reference 10), Tables 1-5 provide descriptions of the changes. Changes to the three IOM documents that govern IOM internal development, the Quality Assurance Manual (QAM), Quality Procedure Manual (QPM), and the Engineering Department Manual (EDM) are described below:

Quality Assurance Manual (QAM) – Changes reflect integration of corporate structure with Invensys Process Systems and expansion of scope to include 10 CFR Part 50 Appendix B and American Society of Mechanical Engineers (ASME) NQA-1-1994 as well as improvements to training and customer product support. The NRC staff identified no reduction in previous commitments.

Quality Procedure Manual (QPM) – Changes reflect revision to corporate structure and improvements to commercial grade dedication, product discrepancy reporting and return material authorizations. The NRC staff identified no reduction in previous commitments. Four new procedures were added since 2001: Technical Support Documentation, Quality Records Retention, Quality Surveillances, and Certification of QA Personnel.

Engineering Department Manual (EDM) – Significant additions were made to EDM 12.00, “Product Development Process,” and EDM 12.30, “Design Reviews.” Changes reflect stronger conformance to IEEE Std 1012, IEC 61508, and ASME NQA-1. EDM 12.00 defines the design lifecycle phases which have not changed since reviewed for Tricon V9. The NRC staff identified no reduction in previous commitments.

3.2.1 TRICON V10 SOFTWARE DESIGN REVIEW

The bases used by the NRC staff for the review of the Tricon V10 PLC system software include SRP Chapter 7, BTPs 14 and 18, EPRI TR-107330, and TR-106439. IOM documented the compliance of the Tricon V10 PLC system with these standards in IOM Document No. 7286-545-1, Revision 4, "Triconex Topical Report" (Reference 4).

Software qualification activities involved evaluating the processes, procedures, and practices used to develop the software; reviewing the software architecture; and assessing the history of the software and its associated documentation and operating experience. The object of this software qualification was to give the NRC staff reasonable assurance that the quality of the Tricon V10 PLC system software is equivalent to the quality expected of a product developed under a nuclear QA program complying with Appendix B to 10 CFR Part 50.

The NRC staff used the following criteria to determine the acceptability of the software used in the Tricon V10 PLC system:

- SRP Section 7.1, "Instrumentation and Controls – Introduction."
- SRP Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems."
- BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."
- BTP HICB-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems."
- RG 1.152, Revision 3, which endorses IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations.”

IOM submitted its evaluation of the Tricon V10 PLC system and TriStation 1131 V4.7.0 software, including documentation, development practices, and operating history against these criteria. Details of the IOM evaluation are contained in the "Software Qualification Report," IOM Document No. 9600164-535, Revision 1 (Reference 41), and the independent third party review, “Critical Digital Review of the Triconex Tricon V10.2.1” (Reference 32), by MPR Associates. The NRC staff reviewed this evaluation, as well as original design documents and procedures, as discussed in the following subsections:

Process Documentation:
Development documentation is required by several IOM procedures. Engineering Procedure EDM 12.00, “Product Development Process,” requires the preparation of a requirements specifications, design specifications, detailed design documents, test plans, and test reports. The content of these documents is specified by other procedures such as EDM 30.10,

"Hardware Requirements Specification," and EDM 40.10, "Software Specification Content & Format." A requirements traceability matrix is required to be documented in the software design documents. However, the current practice is to define and control requirements in the Telelogic DOORS® requirements management tool. DOORS® provides the capability to maintain, check, and visually display requirements traceability between requirements, detailed design, and testing procedures, meets the intent of the requirement, and provides satisfactory control. Traceability into the code is currently not automated in DOORS®.

Peer Review:
IOM engineering procedures prescribe several levels of work product review. In addition, peer reviews of all controlled development documents are part of the design reviews that are conducted in accordance with procedure EDM 12.30, "Design Reviews." This procedure stipulates formal, comprehensive, and documented committee reviews of all work products. The results of these reviews, and resolution of the comments, are incorporated into development documents and controlled. In addition, procedure EDM 21.00, "Engineering Change Order Control," provides for a governing body called the Change Control Board (CCB) that is responsible for approving (along with the project manager) all engineering changes.

Validation and Testing:
Product validation is controlled by Engineering Procedure EDM 90.10, "Product Validation," Engineering Procedures EDM 30.30, "Hardware Test Specification," and EDM 40.10, "Software Specification Content & Format." EDM 90.10 stipulates that a test plan will be developed as part of the requirements phase of the product lifecycle. The EDMs further clarify the content of the test plans. EDM 90.10 also describes the handling of test discrepancies and the review and approval of test results.

Requirements Traceability:
EDM 40.10, "Software Specification Content & Format," requires that a requirements traceability matrix is documented in the software design documents. IOM currently uses an automated requirements control program, DOORS® to control and document their requirements, which meets the intent of the requirement and provides satisfactory control.

Safety Analysis:
Procedure EDM 12.00, "Product Development Process," requires the generation of a Failure Modes and Effects Analysis (FMEA) as part of the design phase. Engineering Procedure EDM 90.20, "Failure Modes and Effects Analysis," provides guidance for the preparation of the analysis. The software development procedures do not explicitly require a separate software safety hazards analysis. However, the existence of fault insertion testing is considered to partially compensate for the absence of such analysis.

Configuration Management:
Engineering Procedure EDM 20.00, "Configuration Management," and associated procedures describe a thorough configuration management system. This includes product identification and change control.

Issue Tracking and Resolution:
Issue tracking and resolution is controlled by the configuration management procedures EDM 21.10, "Engineering Change Request (ECR)," and EDM 21.30, "Change Impact Analysis." EDM 21.10 defines the content, generation, processing, review, and release of ECRs. EDM 21.30 provides guidance on formally determining the impact of a product change on

documentation, design, and relevant standards. These procedures describe a thorough, robust issue tracking and resolution process.

Continuing Engineering and Reporting Failures:
Continuing engineering is handled in accordance with change and issue control procedures. Quality Assurance Procedure QAM-13.3, "10 CFR Part 21 Reporting of Defects and Noncompliance," provides guidance consistent with 10 CFR Part 21 for reporting defects and deviations that could affect nuclear safety to the NRC.

IOM adopted a corporate level QAM and omitted the previously reviewed QAM. The expanded QA program adds an additional layer of QA management, led by a single Global Nuclear QA Director. Although the IOM V&V program is not in compliance with IEEE Std 1012, as endorsed by RG 1.168, Revision 1, this change improves its compliance to IEEE Std 1012 regarding organizational structure. Portions of the original QAM that were not redundant were mapped to the QPM and EDM. IOM also significantly expanded the design process in the EDM. EDM 12.00, "Product Development Process", defines the established process flow and product lifecycle phases. This procedure documents the IOM commitment to perform third party independent reviews as recommended in the Tricon V9 SE and further strengthens their overall commitment to IEEE Std 1012.

All Tricon configurations are independently reviewed and tested by TÜV Rheinland. As a part of the independent review, TÜV Rheinland assesses process changes and performs full V&V including source code reviews in accordance with IEC 61508. As NRC does not endorse IEC 61508, the independent design review portion of the TÜV review cannot be credited. Because TÜV performs the same tests on the Tricon as IOM performs, the independent testing can be credited provided the design and process are independently reviewed to NRC endorsed criteria.

It is important to note that the Tricon V10 platform includes changes that were incrementally tested in a number of configurations since 2001. Stated another way, the most recent TÜV testing only addresses changes made since the last commercial configuration release. The last nuclear qualified configuration was in 2001. Therefore, all TÜV testing since 2001 that includes changes that are part of the Tricon V10 must be credited. The NRC staff opted, based on previous review of TÜV testing in the Tricon V9 SE, to review one representative report for the configuration Tricon V10.2.1 because it was a significant release. The NRC staff reviewed TÜV report 968/EZ 105.06/06 (Reference 52). The NRC staff found that the report was of similar quality to the report accepted in the Tricon V9 SE and credit it on that basis.

The independent design review was again performed by MPR Associates. The review included an assessment of changes to the design process since the Tricon V9 review as well as an assessment of all the hardware and software changes. Further, MPR assessed the new communications module (TCM) against the guidance in ISG 4 and developed application notes for the use of the TCM in safety systems. The NRC staff thoroughly reviewed the report, IOM Document No. 9600164-539, "Critical Digital Review (CDR) of the Triconex Tricon V10.2.1" (Reference 32), and found it to be of similar quality to the V9 evaluation and accept it on that basis. The CDR is referenced throughout this evaluation.

The third independent review was performed by JLM Digitech Digital Licensing Services, "Independent Tricon V10 Equipment Qualification Assessment" (Reference 25). The report gives an independent assessment of the qualification testing against the requirements of EPRI TR-107330. The NRC staff determined that JLM Digitech Licensing Services independent assessment was similar in quality to the MPR and TÜV independent assessments and credit it on that basis.

During the December 2010 audit (Reference 6), the NRC staff verified line by line changes made to a number of IOM process manuals. The NRC staff found that the audited changes were consistent with the docketed descriptions of change (as described above) for the Tricon V10 software quality and development processes. The audit also confirmed requirements traceability in key areas of the Tricon V10 development, supporting IOM adherence to process. The NRC staff found that later design documents had improved traceability, consistent with ongoing process improvements. Requirements traceability had been identified as an area of concern in the Tricon V9 SE.

The NRC staff determined that the software development process and the new or revised software components developed for Tricon V10.5.1 meet the criteria of SRP Chapter 7, BTP 14, BTP 18, EPRI TR-107330, and EPRI TR-106439. Software elements in modules that were reused from Tricon V9.5.3 were accepted under the previous Tricon V9.5.3 SE, and are accepted for use in Tricon V10.5.1 under this SE.

3.2.2 COMMERCIAL GRADE DEDICATION OF PREDEVELOPED SOFTWARE

EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” provides detailed guidance for the evaluation of existing commercial computers and software to meet the provisions of IEEE Std 7-4.3.2-2003, which was endorsed in RG 1.152, Revision 2.

The CGD guidance provided in EPRI TR-106439 involves identifying the critical characteristics of the commercial grade digital equipment based on the safety-related technical and quality requirements, selecting appropriate methods to verify the critical characteristics to enable dedication of the digital equipment, and maintaining the dedication basis over the service life of the equipment. The guidance adapts the methods established in EPRI NP-5652, “Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications,” to digital equipment and is consistent with the guidance contained in Generic Letter (GL) 89-02, “Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products,” and GL 91-05, “Licensee Commercial-Grade Procurement and Dedication Programs.”

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

Verification of the critical characteristics is at the heart of the dedication process. EPRI TR-106439 adapts four acceptance methods defined in EPRI NP-5652 to establish an approach to verify the characteristics for digital equipment. The four methods are:

- Method 1 --- Special Tests and Inspections
- Method 2 --- Commercial Grade Survey of Supplier
- Method 3 --- Source Verification
- Method 4 --- Acceptable Supplier/Item Performance Record

EPRI TR-106439 states that verification of the critical characteristics for digital equipment will require the use of more than one of the methods since no one method will typically be sufficient by itself.

The IOM procedure for conducting commercial grade dedication is EDM 76.00, "Dedication of Products for Nuclear Service." (Reference 18) The NRC staff reviewed the procedure and concluded that IOM has properly followed their process as defined in Sections 4.3, "Dedicated Parts Evaluation" which calls for definition of critical characteristics and evaluation by a combination of methods 1-4 as outlined in EPRI NP-5652.

In IOM Document No. 9100055-501, "Special Dedicated Parts Evaluation, Wind River Software" (Reference 21), IOM describes the SR function of the PDS as: "Software facilitates transfer of communication messages in TCM as an element of TCM firmware. Operability of SW must be highly reliable. Since this software is common to TCMs in all channels, software must have a very low probability of common cause failure that results in inoperability."

It further describes the critical characteristics of the item as:

1. Identification of Item (vendor part/model/version)
2. Operability/Reliability of Software

In Appendix A of IOM Document No. 9100055-501, "Special Dedicated Parts Evaluation, Wind River Software" (Reference 21), IOM provides a detailed breakdown of the PDS components and describes the third party PDS functionality versus the IOM generated code in the transmission of SR data using the P2P protocol. The NRC staff used this information to better understand the role of the third party PDS and to focus review efforts on requirements and testing that are related to the third party PDS.

IOM states that they used a combination of EPRI NP-5652 methods 1, 3, and 4. The NRC staff reviewed the TCM System Requirements Specification (Reference 36), the TCM Traceability Matrix (Reference 37), IOM document, "Invensys QA Documentation Package of Wind River, Commercial Grade Survey" (Reference 20), and IOM Document No. 9100055-501, "Special Dedicated Parts Evaluation, Wind River Software" (Reference 21), as detailed in Sections 3.2.2.1, 3.2.2.2, and 3.2.2.3 below and determined the third party PDS, as specifically configured in the TCM, meets the criteria of EPRI TR-106439, IEEE Std 7-4.3.2-2003, and EPRI NP-5652.

3.2.2.1 SPECIAL TESTS AND INSPECTIONS

As part of the acceptance approach for CGD of digital equipment, EPRI TR-106439 identifies special tests and inspections as means to support verification of physical, performance, and dependability characteristics. In addition to referencing the CGD guidance in EPRI TR-106439, the EPRI TR-107330 guidance on generic qualification of PLCs for SR applications specifically identifies black box testing in Section 7.6.2 as one compensatory quality activity for legacy software to confirm conformance to its generic requirements. Code inspections, software object testing, software component testing, and functional testing are means of generating the compensatory evidence on critical design characteristics to confirm acceptable quality and performance in support of the CGD of PDS.

The purpose of functional testing is to test the functionality of hardware modules and associated software components. In this case, the integrated FW for the TCM, which includes both IOM developed code and the PDS, must demonstrate proper operation in an integrated environment.

IOM Document No. 9100055-501, “Special Dedicated Parts Evaluation, Wind River Software” (Reference 21), describes in detail the TCM functionality in relation to the PDS and IOM components to establish the critical characteristic. As described, the critical characteristic was verified by observing verified communications through the TCM. This makes much of the documented testing of the Tricon V10 configured with a TCM credible for showing proper operation of the PDS.

The NRC staff reviewed IOM Document No. 6500155-011, Revision 2.6, “TCM TSAA Software Test Description” (Reference 38), which describes a setup with a Tricon chassis with three 3008N MP modules and a TCM connected through a network hub to a PC running the TriStation 1131 software. Specific tests are described in this document that require reading and writing of “bins” data in the Main Processor module using the TSAA protocol. The NRC staff credits these tests because the data is written and read back through the TCM which verifies data in both directions. The NRC staff further reviewed test coverage through the TCM Traceability Matrix (Reference 37), identifying confirmation of testing of other protocols as well as diagnostics, fault detection, and event logging.

The NRC staff determined the TCM has been thoroughly tested to demonstrate all documented functionality sufficient to satisfy the EPRI TR-106439 criteria of functional test for CGD.

3.2.2.2 SOURCE VERIFICATION

As an element of the acceptance approach for CGD of digital equipment, EPRI TR-106439 identifies source verification as a means to support verification of dependability characteristics for a single item or shipment of items. Of the dependability characteristics, “built-in quality” addresses less quantifiable elements related to the development process and accompanying documentation. EPRI TR-106439 identifies review of vendor processes and documentation as a method of verification (associated with CGD Methods 2 or 3) for assessing the built-in quality. These processes and documentation include: (1) design, development, and verification processes, (2) quality assurance program and practices, and (3) V&V program and practices. Acceptance criteria include evidence that the vendor maintains a QA program that is generally in compliance with a recognized standard and that a process was used for legacy software which addresses essentially the same elements as the current QA process. The methods of verification include review of the evolution of vendor procedures and practices for software development, V&V, and testing as well as determination of the degree to which the QA program and software development process were applied. It is noted that preparation of supplemental documentation may be necessary.

IOM conducted a source verification of Wind River Systems Inc. located in Alameda, California. IOM Document No. 9100055-501, “Special Dedicated Parts Evaluation, Wind River Software” (Reference 21), includes the definition of the critical characteristic used for source verification activity with a supporting technical discussion that gives a detailed account of the PDS function during SR data transfer. IOM document, “Invensys QA Documentation Package of Wind River, Commercial Grade Survey” (Reference 20), includes the source verification plan and report with supporting documentation of the on-site review of quality assurance, configuration management and product verification related to the specific version of the PDS. The report concludes that the vendor procedures and practices for software development, V&V, and testing and the application of quality program and software development process applied to develop and maintain the PDS provides assurance of adequate built in quality for the software.

The NRC staff reviewed the documentation package and the IOM source verification report. The report gives background on the third party vendors’ quality process which was supported with documentation of past certifications. The report further described the current quality system, configuration management process, and V&V process. The NRC staff concluded that the docketed information is sufficient to assess the critical characteristic described in the Special Dedication Parts Evaluation of the PDS.

The NRC staff determined that the docketed evidence of the third party vendor's quality system, configuration management system, and product verification for the specific version of PDS, meets the criteria for the source verification in EPRI TR-106439.

3.2.2.3 PERFORMANCE RECORDS

EPRI TR-106439 identifies review of product operating history as a method to support verification of the dependability characteristics of reliability and built-in quality as part of the acceptance approach for CGD of digital equipment. As part of the guidance on generic qualification of PLCs for SR applications given in EPRI TR-107330, the CGD guidance in EPRI TR-106439 is referenced as a source of acceptable compensatory quality activities for legacy software. Section 7.6.2 of EPRI TR-107330 also specifically identifies particular compensatory quality activities that include evaluation and analysis of documented operating experience for product revisions involving legacy software elements in similar applications, provided the revisions are under continuing configuration control.

IOM docketed a listing of known issues from the PDS developer in IOM document, "Invensys QA Documentation package of Wind River, Commercial Grade Survey" (Reference 20), related to the TCM performance. The list clearly states whether issues had been corrected or just acknowledged. The NRC staff reviewed the list and found no outstanding issues that would impact TCM performance. Additionally, the TCM with integrated third party PDS was originally released with Tricon V10.0 in 2006 and was independently assessed by TÜV. The TCM has been in commercial use for 5 years and currently has no outstanding product alert notices (PAN) that indicate performance issues with the TCM related to the third party PDS. The NRC staff determined the operating history of the TCM meets the criteria of EPRI TR-106439 and supports CGD of the third party PDS.

3.3 ENVIRONMENTAL QUALIFICATION

SRP Chapter 7, Appendix 7.0-A (page 7.0-A-14), Section H, "Review of the Acceptance of Commercial-Grade Digital Equipment," contains guidance for the review of commercial equipment and references RG 1.152, Revision 2. RG 1.152, Revision 2, endorses IEEE Std 7-4.3.2003. IEEE Std 7-4.3.2-2003, Clause 5.4.2, defines the Qualification of Existing Commercial Computers for use in SR applications in nuclear power plants. SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," Section 5.4.2, "Qualification of Existing Commercial Computers," provides acceptance criteria for equipment qualifications (in accordance with IEEE Std 7-4.3.2, Clause 5.4.2). This section states that EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," and EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants," provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," which was accepted by an NRC SE dated July 30, 1998, presents a set of requirements to be applied to the generic qualification of PLCs for application to SR I&C systems in NPPs. It is intended to provide a qualification envelope for a plant-specific application. It is an ASAI for the applicant/licensee to verify that the as-tested envelope bounds the requirements of the specific application.

The Tricon V10 PLC hardware is qualified for a mild environment, such as a main control room and auxiliary electrical equipment rooms. IOM performed pre-qualification, environmental, seismic, electromagnetic interference/radio frequency interference (EMI/RFI), electrical fast transient, surge withstand, and Class 1E to Non-Class 1E isolation tests; these tests were performed in the listed order and in accordance with the requirements of EPRI TR-107330. A test system (as described below) was assembled and used for all tests; this system was reconfigured as necessary to support the protocol and worst-case loading scenario for each test. IOM performed qualification testing on the following Tricon V10.2.1 equipment (see Table 3-1), documented in the "Master Configuration List," IOM Document No. 9600164-540 (Reference 17), as configured in the "Tricon System Description," IOM Document No. 9600164-541(Reference 22), and tested as specified in the following guidance; EPRI TR-107330, EPRI TR-102323-R1, IEEE Std 323, IEEE Std 344, IEEE Std 381, IEEE Std 384, IEEE Std 7-4.3.2-2003, RG 1.100, RG 1.209, and RG 1.180, Revision 1.

Qualification of Tricon V10.5.1 is by analysis based on the Tricon V10.2.1 tests and documented in Section 4.0 of the LTR. There are no hardware differences between the Tricon V10.2.1 and Tricon V10.5.1. The changes to the SW and their impact on qualification are discussed in Section 3.2.1 of this SE.

IOM performed pre-qualification testing as described in EPRI TR-107330 with the exceptions described in detail below. The following tests were performed in accordance with EPRI TR-107330 as documented in the "Equipment Qualification Summary Report," IOM Document No. 9600164-545 (Reference 24); Radiation Exposure, Temperature and Humidity, Seismic, EMI, Electrical Fast Transient Response (EFT), Surge Withstand Test, Electrostatic Discharge (ESD), and Class 1E to Non-Class 1E Isolation Testing. Operability and prudency tests were conducted before, during, and after the qualification testing.

IOM documented non-compliances and test anomalies in the individual qualification reports and the qualification summary report as described below. The Tricon V10 did not fully comply with EMI and seismic requirements, but met the criteria for the remaining tests. RG 1.180, Revision 1, MIL-STD-461E, CE101, and CE102 requirements were not fully met. Also, IEC 61000-4-3, Radiated Susceptibility and IEC 61000-4-6, Conducted Susceptibility were not fully met. The specific limitations are detailed in Section 4.5 of the "Equipment Qualification Summary Report," IOM Document No. 9600164-545 (Reference 24) and described below.

TABLE 3-1 – List of Components Used in Qualification

Module No.	Description
8110	Main chassis
8111	Expansion Chassis
8112	Remote Expansion Chassis
8310	High Density Power Module 115 VAC
8311	High Density Power Module 24 VDC
8312	High Density Power Module 230 VAC
3008	Enhanced Main Processor
4352A	Communication Processors
3701	Analog Input-Differential, DC Coupled

Module No.	Description
3703E	Analog Input-Isolated, 16 Points
3721	NGAI, Analog Differential, 32 Points
3708E	Thermocouple Input, Differential, Isolated
3805E	Analog Output, Non-isolated, Common Return
3501T	Digital Input-Non-Commoned, Isolated, 32 pts
3502E	Digital Input-Commoned Groups of 8, 48 V
3503E	Digital Input-Commoned Groups of 8, 24 V
3511	Pulse Input-Non-Commoned, Balanced
3601T	Digital Output-Non-Commoned, Isolated, 115 VAC
3603T	Digital Output-Commoned, Isolated, 120 VDC
3623T	Digital Output-Supervised, Commoned, 120 VDC
3607E	Digital Output-Non-Commoned, Isolated, 48 VDC
3636T	Digital Output-Relay Output, NO, Simplex
3625	NGDO, Digital Output, 32 pts, 24 VDC
9794-110N PI	External Termination Panel
9782-110N AI	External Termination Panel
9561-810N DI	External Termination Panel
9561-110N DI	External Termination Panel
9664-810N DO	External Termination Panel
9663-610N DO	External Termination Panel
9563-810N DI	External Termination Panel
9662-810N DO	External Termination Panel
9662-610N DO	External Termination Panel
9668-110N RO	External Termination Panel
9667-810N DO	External Termination Panel
9562-810N DI	External Termination Panel
9783-110N AI	External Termination Panel
9795-610N AI	External Termination Panel
9790-610N AI	External Termination Panel
9764-310N AI	External Termination Panel
9860-610N AO	External Termination Panel
1600083-600, 7B34-CUSTOM	RTD Signal Converter, 0 to 600 C
1600083-200, 7B34-CUSTOM	RTD Signal Converter, 0 to 200 C
1600024-040, 7B34-04-1	RTD Signal Converter, 0 to –600 C
1600024-030, 7B34-03-1	RTD Signal Converter, 0 to –200 C
1600024-020, 7B34-02-1	RTD Signal Converter, 0 to –100 C
1600024-010, 7B34-01-1	RTD Signal Converter, -100 to 100 C
1600082-001, 7B30-02-1	RTD Signal Converter, 0 to 100 mV
1600081-001, 7B14-C-02-1	RTD Signal Converter, 0 to 120 C
4200	Primary RXM, Fiber Optic

Module No.	Description
4201	Remote RXM, Fiber Optic

Note: Module numbers correctly show the part number used for qualification without the “N” nuclear qualified designator (e.g., 8110N) and in no way implies that the commercial equivalents (e.g., 8110) are interchangeable with the nuclear qualified parts listed in Table 1 of this document.

3.3.1 TEST SYSTEM CONFIGURATION

The Tricon Under Test (TUT) consisted of four Tricon chassis populated with selected input, output, communication, and power supply modules as noted in the table above. The TUT also included external termination assemblies provided for connection of field wiring to the Tricon input and output modules. The System Description (Reference 22) shows the general arrangement and interconnection of the Tricon Test Specimen chassis and provides an overview and description of the test specimen and test system. Analog and digital inputs to the test specimen were generated using a two-chassis simulator Tricon system. This system was configured with a simulator application program that was used to create a variety of static and dynamic input signals. Other test equipment was used to provide additional AIs to the TUT. Analog and digital outputs from the TUT were monitored with indicator lights and a PC-based data acquisition system (DAS). The DAS also monitored analog and digital inputs to the TUT. Data was recorded and analyzed by the DAS during the various tests to verify proper operation of individual input and output points.

Two PCs running the TriStation software were used to communicate with and monitor the status of the TUT and the simulator Tricon system. The TriStation software used for this purpose was TriStation 1131, which is Windows based software. During each of the qualification tests, operation of the TUT was monitored and recorded by the DAS. The recorded data was evaluated in detail before, during, and after the test period. The data evaluation considered operation (per the Test Specimen Application Program (TSAP)) of at least one input or output point on each I/O module installed in the TUT, and operation of all peripheral communication interfaces including the Simulator Tricon Peer-to-Peer and MODBUS interfaces.

The TUT multi-channel test configuration and the overall test strategy are documented in the “Master Test Plan,” IOM Document No. 9600164-500, Revision 5 (Reference 23). The TSAP for the Tricon V10 was developed under IOM’s Appendix B program and was used in the performance of qualification testing including pre- and post-qualification operational and prudency tests. The NRC staff concluded that the TSAP met the requirements of EPRI TR-107330, Section 6.2.2, based on its review of the “Test Specimen Application Program Software Validation and Verification Plan,” IOM Document No. 9600164-513 (Reference 39), “Test Specimen Application Program Software Validation and Verification Report,” IOM Document No. 9600164-536 (Reference 40), “Independent Tricon V10 Equipment Qualification Assessment,” Section 2.0 (Reference 25), and Appendix 2 of the “Master Test Plan” (Reference 23).

The NRC staff notes that multi-mode fiber optic cables and any interconnecting hardware used to connect primary and remote RXMs are not included in the qualification program. Licensees using RXM configurations are required to supply this equipment and it is an ASAI to verify that these user supplied components meet IOM specifications and are qualified for the specific environmental conditions.

3.3.2 PRE-QUALIFICATION TESTING

IOM performed pre-qualification testing to (1) confirm that the Tricon PLC test system was properly configured and operational, (2) provide baseline performance data for comparison with data obtained during and after qualification testing, and (3) validate the test procedures. Pre-qualification testing included the following assessments:

- The system setup and checkout test documented proper configuration and operation of the Tricon PLC test system, including hardware, software, input and output simulators; test and measurement equipment; and interconnecting cabling.
- The operability test to establish baseline performance included tests for analog module accuracy, system response time, operation of discrete inputs and outputs, performance of timer functions, failover tests (associated with the failure of redundant components), loss of power, detection of failure to complete a scan, power interruption, and power quality tolerance.
- Prudency testing demonstrated the ability of the Tricon PLC system to operate within specifications under dynamic conditions. The prudency test included a burst of events test, a serial port receiver failure test, and a serial port noise test.

The pre-qualification testing was designed to follow the requirements of Section 5.2 of EPRI TR-107330 by establishing baseline conditions for the TUT that followed the published specifications and by verifying system configuration/setup and proper operation. This testing exposes the TUT to various normal and abnormal conditions of input/output operation and power source variations. This testing includes operability testing and prudency testing as specified in EPRI TR-107330, Sections 5.3, 5.4, 5.5, and 6.4.3. All testing prerequisites were met, although an engineering change order was required to address failures of two AO points (3805 AO Module). These points were subsequently successfully retested. The system setup and checkout test documented the proper configuration and operation of the TUT.

The establishment of the baseline performance was acceptable and the results of the prudency testing showed the TUT was able to operate within specifications under dynamic conditions. The pre-qualification testing and the ensuing results meet the guidance presented in EPRI TR-107330, Section 5.

IOM described several exceptions during the prequalification tests:

- PLC library Software Objects Testing – IOM did not perform software object testing as part of the pre-qualification test. IOM Document No. 9600164-535, “Software Qualification Report,” Sections 5.2 and 7.3 (Reference 41) described the credited testing by independent reviewer TÜV Rheinland which includes source code reviews based on documented requirements as well as validation testing. IOM independently verified each incremental revision of the product in this manner. The NRC staff concludes that the collective independent review and testing performed by TÜV Rheinland since the NRC staff evaluated Tricon V9.5.3 is appropriately credited.
- Burn-in Testing – IOM did not perform separate burn-in tests as prescribed in EPRI TR-107330 Section 5.2F. The LTR justifies this exception by taking credit for routine burn-in testing that is performed as part of the manufacturing process for the Tricon PLC system hardware. The NRC staff determined that IOM manufacturing burn-in process satisfied EPRI 107330 criteria in Section 4.1.3.1 of the V9 safety evaluation (Reference 9).

- Response Time - EPRI TR-107330 Section 4.2.1.A gives a response time requirement of 100 msec based on a given list of test set requirements. The IOM test configuration required to adequately meet other qualification testing requirements does not conform to the given response time test set criteria. The Tricon response time is dependent on specific system configuration and is calculated for each application. The acceptance criteria used for NRC staff's evaluation is based on the calculated maximum response times given in IOM Document No. 9600164-731 Section 4.0 (Reference 43). Tested maximum response times (which met the calculated response times) were given in IOM Document No. 9600164-566, Section 6.0 (Reference 44); DI to DO loop 83.0 msec, AI to DO loop 119.0 msec, AI to AO loop 126.5 msec. Similar exception was approved by the NRC staff in Section 4.3.5 of the V9 SE (Reference 9).

Further details of the testing can be found in the following IOM documents:

Document Title	IOM Document No.
Set-up & Checkout Test Procedure	9600164-502
Operability Test Procedure	9600164-503
Prudency Test Procedure	9600164-504
TSAP SW Requirements Spec	9600164-517
TSAP SW Design Description	9600164-518
TSAP V&V Plan	9600164-513
TSAP Final V&V Report	9600164-536
Pre-Qualification Operability Test Report	9600164-560
Pre-Qualification Prudency Test Report	9600164-570

The NRC staff concluded that the pre-qualification testing met the intent of EPRI TR-107330.

3.3.3 RADIATION WITHSTAND TEST

Radiation testing of the Tricon was performed in accordance with the requirements of EPRI TR-107330 Sections 4.3.6.1 and 4.3.6.2 and IEEE Std 381-1977 at the University of Massachusetts, Lowell. The Tricon met all applicable performance requirements after application of the radiation test conditions. The radiation test included the withstand capability of the Tricon to a rapid dose of radiation that would be normally provided as a long term, low level 1000 RAD gamma dose integrated over a 40 year period in a mild environment.

The radiation test acceptance criteria are as given below based on Appendix 4 of the Master Test Plan (Reference 23) and EPRI TR-107330, Section 4.3.6:

- The TUT shall not exhibit any exterior damage or degradation as a result of gamma radiation exposure based on visual examinations performed following Radiation Exposure Testing. Such conditions include, but are not limited to, blistered protective coatings, deformation, crazing or discoloration of plastic components, and deformed or visually embrittled cable insulation.
- The TUT shall pass the post radiation operability test following the completion of radiation exposure testing.
- The TUT shall pass the post radiation prudency test following the completion of radiation exposure testing.

Radiation exposure testing of the TUT was performed on December 13 and 14, 2006, at the University of Massachusetts, Lowell. The testing complied with the specific requirements of EPRI TR-107330, Section 4.3.6, and the general requirements of IEEE Std 381-1977. TUT components were exposed to Co60 gamma radiation doses of 1000 RAD plus margin in exposures just over 2 hours in duration. Due to limitations of the source and the size of the overall test set, components were exposed separately. Each component received the required dose plus margin.

Post testing inspection revealed no visible effects from the exposure. Operability and prudency test results shows that exposure to the radiation test conditions had no adverse effect on the TUT.

The NRC staff reviewed the “Radiation Test Report,” IOM Document No. 9600164-533 (Reference 45), and determined that the level of exposure is consistent with installation in a mild environment, as specified in Section 4.3.6 of EPRI TR-107330 and IEEE Std 381-1977. On the basis of these tests, the NRC staff concludes that the Tricon V10 PLC system hardware is qualified to the radiation exposure levels specified in the EPRI TR and the IEEE standard. However, before installing plant-specific Tricon PLC system equipment, licensees will need to verify that the expected radiation exposure for the equipment is enveloped by the radiation withstand capacity of the Tricon PLC system equipment. This is an ASIA.

3.3.4 TEMPERATURE AND HUMIDITY TESTING

Environmental qualification testing of the TUT was performed in accordance with EPRI TR-107330, Sections 4.3.6 and 6.3.3, and IEEE Std 381-1977 and includes the following:

- The test PLC shall meet its performance requirements during and following exposure to abnormal environmental conditions of 40 °F to 140 °F and 5 percent to 95 percent relative humidity (RH) (non-condensing) according to a time varying profile (see Figure 4-4 of the EPRI TR-107330).
- Environmental testing shall be performed with the power supply sources set to values that maximize heat dissipation in the test PLC.
- Power supplies shall be loaded such that nominal current draws at nominal power supply output voltages are equal to the power supply rating.
- The test PLC shall be powered with its TSAP operating during environmental testing, with 1/2 of the discrete and relay outputs ON and loaded to their rated current. In addition, all AOs shall be set to between 1/2 and 2/3 of full scale. Section 4.3.6.2 of EPRI TR-107330 requires that the generic PLC meet its performance requirements over abnormal environmental conditions of 40 °F to 120 °F and 10 percent to 95 percent RH (non-condensing). Section 4.3.6.3 of EPRI TR-107330 requires that the test PLC operate for the environmental (temperature and humidity) withstand profile given in Figure 4-4 of the TR. The profile includes a beginning ramp-up period (unspecified in duration) from ambient to 140 °F and 90 percent RH (non-condensing). These conditions are held for 48 hours minimum, after which the Operability and Prudency tests are run. Conditions are then ramped down over a four hour minimum period to 40 °F and 5 percent relative humidity. These conditions are held for 8 hours minimum, after which a second Operability test is run. Conditions are then ramped up over a four hour minimum period to ambient temperature and relative humidity. The equipment is stabilized at ambient conditions, after which a final Operability test is run. Section 6.3.3 of EPRI TR- 107330 requires that Environmental Testing be performed with margins of 5 F and 5 percent applied to the temperature and humidity values given above.

The environmental test acceptance criteria are as given below based on Appendix 5 of the Master Test Plan (Reference 23), and EPRI TR-107330, Section 4.3.6:

- The TUT shall operate as intended during and after exposure to the environmental test conditions. Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) collected during testing shall demonstrate operation as intended.
- The TUT shall pass the Operability Test following at least 48 hours of operation at high temperature and humidity, following at least 8 hours of operation at low temperature and humidity and upon completion of the test.
- The TUT shall pass the Prudency Test following at least 48 hours of operation at high temperature and humidity.

Environmental testing of the TUT was performed on December 13, 2006, through January 15, 2007, at National Technical Systems in Boxborough, Massachusetts. Results of the testing are described in "Environmental Test Report," IOM Document No. 9600164-525 (Reference 46). As described in the test report and depicted below in Figure 3.3.4-1, the actual sequence of testing was as follows:

- Installation in the National Technical Systems environmental test chamber, and stabilization at ambient temperature and relative humidity conditions.
- Ramp-up to 140 °F and 95 percent RH over a 4 hour period.
- Hold at 140 °F and 95 percent RH for a 1 hour period.
- Troubleshoot test system for a 1 hour period.
- Hold at 140 °F and 95 percent RH for a 47 hour period.
- High temperature Operability Test performed over an 8 hour period.
- High temperature Prudency Test performed over a 2.5 hour period.
- Attempt ramp-down to 35 °F and 5 percent RH over a 17 hour period.
- Return to ambient and perform repairs of test chamber over a 100 hour period.
- Ramp-down to 35 °F and 5 percent RH over a 6 hour period.
- Hold at 35 °F and 5 percent RH for an 8 hour period.
- Low temperature Operability Test performed over a 9 hour period
- Ramp-up to ambient temperature and RH over a 5 hour period.
- Hold at ambient temperature and RH for a 2 hour period.
- Ambient temperature Operability Test performed over a 13 hour period.

The environmental chamber experienced a mechanical failure during the transition from high temperature, high humidity conditions to low temperature conditions. The transition was originally planned to occur in no less than four hours as prescribed by requirements. As a result of the chamber failure, the TUT was returned to ambient conditions for approximately 100 hours. On repair of the chamber, the transition to low temperature was continued and required approximately six hours. The NRC staff reviewed the details of the test equipment failure as described in the "Environmental Test Report," IOM Document No. 9600164-525 (Reference 46) and concluded that the minimum four hour transition time is not a challenging temperature transition and because the equipment under test was not disturbed, the delay at ambient for test chamber repairs does not significantly impact the outcome of the test. The separate manufacturing burn-in performed on all production Tricon equipment, including the equipment used for this test, also provides support that the equipment performs as designed.

IOM recorded two internal diagnostic faults during the high temperature hold period. As described in the Environmental Test Report (Reference 46), the Model 3708E thermocouple input module reported a diagnostic fault message during the high temperature hold period. The fault cleared automatically during ramp-down from the high temperature hold period. The normal operating performance data recorded during Environmental Testing showed that the affected points of the module continued to operate correctly in the presence of the fault. The high temperature Operability Test analog I/O accuracy data shows that the points of the module continued to meet the accuracy specifications in the presence of the fault. Model 3623T 120 VDC digital output module also reported a diagnostic fault message during the high temperature hold period. The detected fault did not impact the proper operation of the TUT during testing.

IOM performed operability and prudency tests both during and after the environmental test. No adverse effect on the TUT performance were reported.

The NRC staff reviewed the “Environmental Test Report,” IOM Document No. 9600164-525 (Reference 46) and determined that the Tricon V10 met the requirements of EPRI TR-107330, Sections 4.3.6 and 6.3.3, and IEEE Std 381-1977.

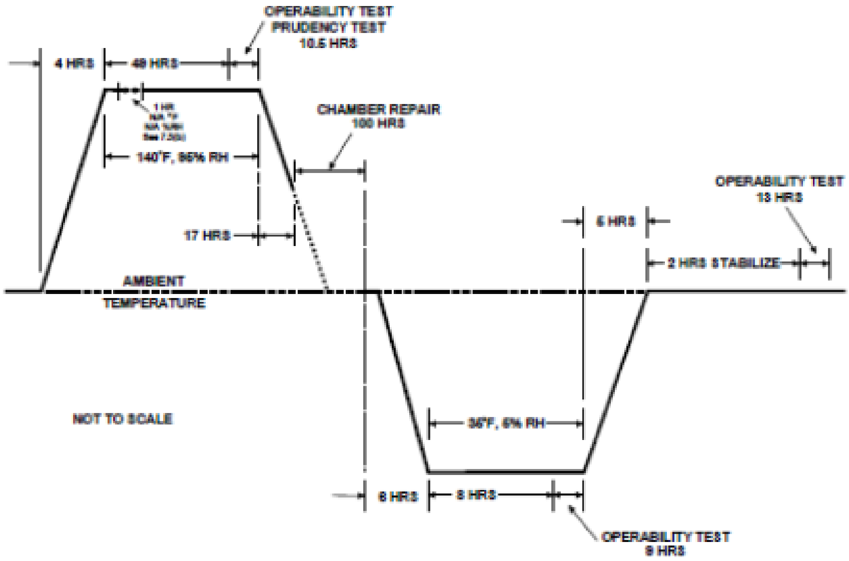


Figure 3.3.4-1 – Environmental Test Applied Temperature and Humidity Profile

3.3.5 SEISMIC WITHSTAND TESTING

To demonstrate that the Tricon V10 meets the requirements for Seismic Category 1 Safety System, IOM subjected the TUT to seismic simulation testing during Safe Shutdown Earthquake (SSE) and Operating Basis Earthquakes (OBEs). Seismic Testing conforms to the requirements of IEEE Std 344-1987 and Sections 4.3.9 and 6.3.4 of EPRI TR-107330. In addition to demonstrating the performance requirements under the specified conditions, a resonance search procedure was also conducted.

Attachment 6 of the Master Test Plan (Reference 23) describes the seismic test plan. The Seismic Test Procedure is IOM Document No. 9600164-507. For seismic testing, IOM performed a resonance search followed by five simulated OBEs and one simulated SSE at 9.75 g’s and 14 g’s respectively, based on 5 percent damping. The simulation vibrations are required to be applied tri-axially (in three orthogonal directions), with random frequency content.

Seismic testing was performed at NTS facilities in Acton, Massachusetts. NTS personnel provided testing services and established test conditions as specified in the TR-107330 specification, including documenting the mounting of the TUT to the seismic test apparatus.

The TSAP was loaded and operating during seismic testing, exercising all TUT components, and supporting automated test data collection. The resulting data documented TUT operation in accordance with the applications depicted in the project functional diagrams. Data also supports monitoring performance of the module 3636T electromechanical relay contacts during testing. Additionally, operability testing was conducted at the completion of the seismic tests. The seismic test acceptance criteria are as given below based on Appendix 6 of the Master Test Plan, Reference 23, and EPRI TR-107330, Section 4.3.9:

- The TUT shall operate as intended during and after application of the OBE and SSE vibrations. Evaluation of normal operating performance data (inputs, outputs, and diagnostic indicators) shall demonstrate operation as intended.
- During and after application of the OBE and SSE vibrations, all connections on the TUT shall remain intact, all modules installed in the TUT shall remain fully inserted, and no functional or non-functional parts of the TUT shall fall off.
- The operation of the chassis power supply normally open alarm relay contacts and the Model 3636T electromechanical relay module output contacts shall be monitored during application of the OBE and SSE vibrations. The relay contacts shall change state in accordance with the TSAP. Any spurious change of state of the relay contacts shall not exceed 2 msec in duration. Any spurious change of state of the power supply alarm relay contacts from open to closed shall not exceed 2 msec in duration.
- The TUT shall pass the Operability Test following completion of the seismic testing.

The TUT was populated with selected main processor, input, output, communication, chassis interface, and chassis power supply modules. The TUT power was supplied by variable AC and DC power sources configured as described in the “Seismic Test Procedure,” IOM Document No. 9600164-507. During seismic testing, both power supply modules in each chassis were energized. Chassis 1 and 2 each included a 120 VAC chassis power supply module and a 24 VDC chassis power supply module. Chassis 3 and 4 each included a 120 VAC chassis power supply module and a 230 VAC chassis power supply module. However, to accommodate seismic testing at minimum external power supply voltages, the test system power supply configuration was temporarily modified for testing of TUT Chassis 3 and 4 to allow the voltages to the 120 VAC and 230 VAC chassis power supply modules to be set independently. The power supplies to the 120 VAC and 230 VAC chassis power supply modules were set to the minimum allowable operating voltage as specified by the manufacturer.

The TUT chassis was mounted to the seismic test table in accordance with mounting details provided on IOM Drawing No. 9600164-102. The seismic test mounting simulated a typical 19-inch rack mount configuration using standard Tricon V10 front and rear chassis mounting brackets and fastener hardware, and standard Tricon V10 external termination assembly mounting plates. Details on the equipment arrangement for seismic testing are provided in the IOM Seismic Test Report (Reference 27).

The TSAP was loaded and operating during seismic testing, exercising all TUT components, and supporting automated test data collection. The TSAP revision used was “V10_TSAPREV_0.” During seismic testing, the relay output configuration did not meet the requirements of Section 6.3.4.2 of EPRI TR-107330. However, a large number of relay output points (32 total) were monitored, which IOM considered a significantly representative number of relay output points, and thus, met the intent of the TR-107330 requirement to have points in both the ON and OFF positions throughout testing.

The Tricon V10 did not fully comply with the seismic requirements. The seismic table achieved the EPRI TR-107330 OBE and SSE Required Response Spectrum test levels throughout most of the required frequency range. Test equipment limitations resulted in a reduced response spectrum during the performance of seismic testing. Specifically, in the low frequency region (below 6 Hz), limitations of the table velocity and displacement prevented achieving the full EPRI TR-107330 Required Response Spectrums.

The as-tested spectrum is depicted in the LTR and shown below. Results of the testing are described in the Seismic Test Report, Reference 27.

Resonance search testing demonstrated that the simulated mounting configuration was stiff enough so that there were no resonances below 100 Hz. Specifically, for seismic testing, the weight loadings of the four TUT chassis were varied from light (chassis 3) to moderate (chassis 2) to heavy (chassis 1 and 4) to demonstrate seismic vibration susceptibility for various chassis loadings.

Table 5-1 of EPRI TR-107330 requires that Operability and Prudency Testing be performed during SSE. Because the duration of each OBE/SSE test (approximately 30 seconds) did not support full Operability or Prudency Testing, IOM did not perform the Operability and Prudency Tests during the Seismic Tests. Data collected during and after each OBE and SSE test demonstrated that the TUT operated as intended throughout the testing.

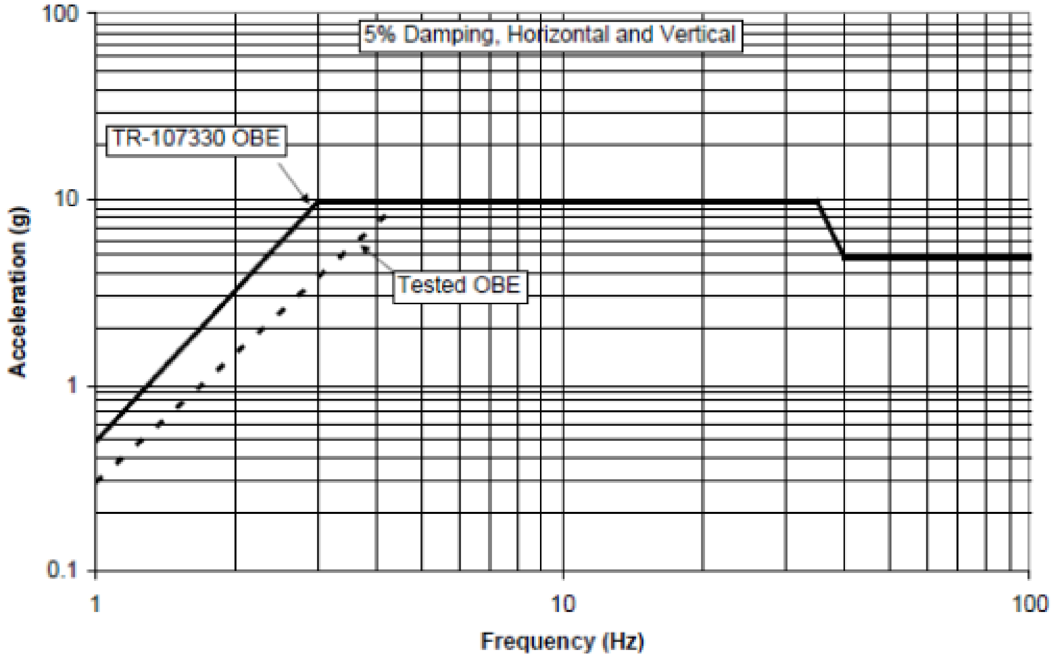
Table 5-1 and Section 6.3.4.3 of EPRI TR-107330 require post-seismic Operability Testing to assess the impact of exposure to the OBE and SSE vibrations on the operability of the test specimen. Test results provided in the Seismic Test Report showed that exposure to the OBE and SSE vibrations had no adverse effects on the TUT performance.

The TUT was visually inspected for damage or degradation following each OBE and SSE test. During inspection of Chassis 1 and 2, after OBE test No. 3, IOM had to address problems with the interface cable connection. A cable restraint at the tie-down point was modified, retesting was not required. To avoid this problem in a plant-specific installation, IOM’s field installation guidance will describe how to secure this cable. In addition, there were other cases of physical damage and degradation in TUT Chassis 1 and 2 during OBE tests, but these were corrected, and the equipment was successfully retested.

During setup/checkout testing, IOM determined that an interposing relay would be required to monitor the chassis alarm contacts as a result of the test setup. This configuration had a potential to mask contact chatter during the test. Therefore, the TUT chassis alarm relays were not seismically qualified as part of seismic testing.

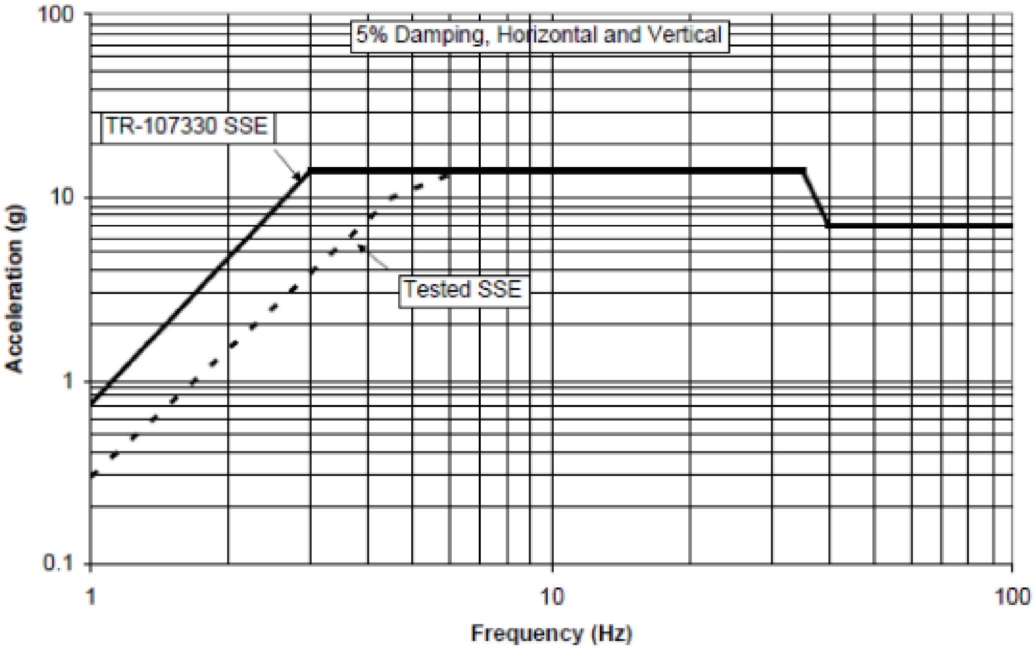
The NRC staff determined that the tested Tricon V10 system equipment is qualified to the tested triaxial seismic simulator table limits shown in Figures 3.3.5-1 through 3.3.5-3 below, with the exception of the low frequency region (below 6 Hz). For this reason the NRC staff finds that the Tricon V10 system did not fully meet the requirements of EPRI TR-107330 for seismic requirements, and before using Tricon V10 system equipment in SR systems in a NPP, licensees must determine that the plant-specific seismic requirements are enveloped by the capabilities of the Tricon V10 system. This determination and the suitability of the Tricon V10 system for a particular plant and application is the responsibility of the licensee.

Figure 3.3.5-1 – OBE Test Acceleration



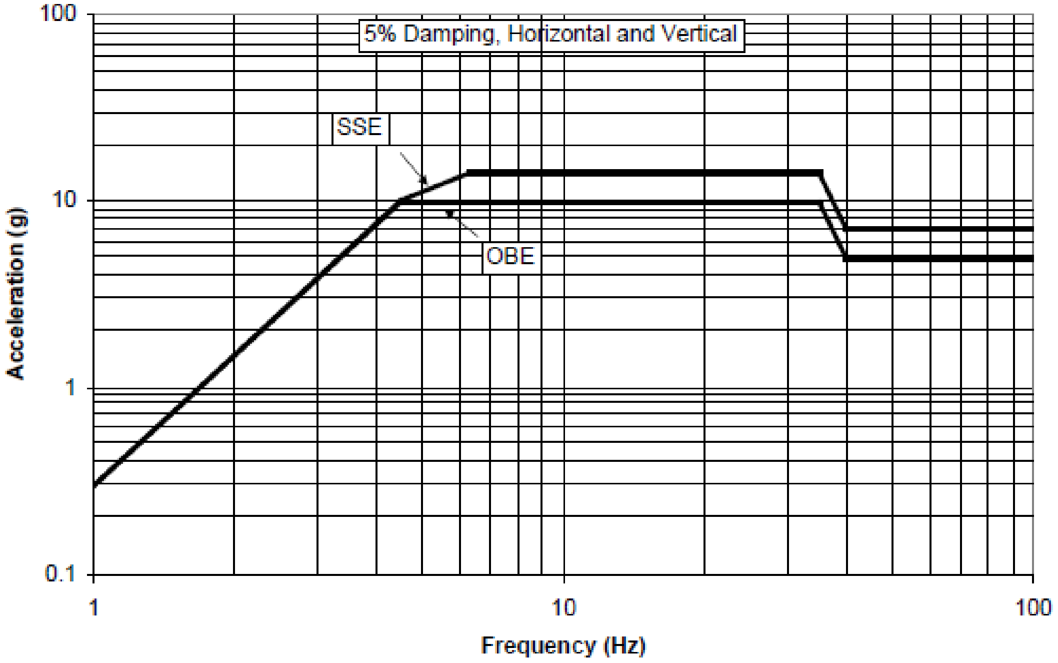
Frequency	Tested Level	TR-107330 Level
1.0 Hz	0.3 g	0.5 g
3.0 Hz	4.0 g	9.8 g
4.5 Hz	9.8 g	9.8 g
35 Hz	9.8 g	9.8 g
40 Hz	4.9 g	4.9 g
100 Hz	4.9 g	4.9 g

Figure 3.3.5-2 – SSE Test Acceleration



Frequency	Tested Level	TR-107330 Level
1.0 Hz	0.3 g	0.75 g
3.0 Hz	4.0 g	14 g
4.5 Hz	10 g	14 g
6.3 Hz	14 g	14 g
35 Hz	14 g	14 g
40 Hz	7.0 g	7.0 g
100 Hz	7.0 g	7.0 g

Figure 3.3.5-3 – Horizontal and Vertical Seismic Withstand Response Spectrum



Frequency	OBE	SSE
1.0 Hz	0.3 g	0.3 g
4.5 Hz	10 g	10 g
6.3 Hz	10 g	14 g
35 Hz	10 g	14 g
40 Hz	4.9 g	7.0 g
100 Hz	4.9 g	7.0 g

3.3.6 EMI/RFI WITHSTAND TESTING

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

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

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

EMI and RFI testing was performed in accordance with EPRI TR-102323, Revision 1, Section 6.3.2 of EPRI TR-107330, and RG 1.180, Revision 1, to demonstrate the suitability of the Tricon V10 platform for qualification as a SR device with respect to EMI/RFI emissions and susceptibility.

All of the TUT components were subjected to EMI/RFI testing as required. EMI/RFI testing of the TUT was performed inside open frame racks. The testing was performed in accordance with EPRI TR-107330 and RG 1.180 test method requirements.

The specific tests conducted include the following MIL-STD-461E and IEC test methods:
The following EMI/RFI emissions tests were performed:

- MIL-STD-461E, Test Method CE101, Conducted Emissions, 30 Hz to 10 kHz
- MIL-STD-461E, Test Method CE102, Conducted Emissions, 10 kHz to 2 MHz
- MIL-STD-461E, Test Method RE101, Radiated Emissions, 30 Hz to 100 kHz
- MIL-STD-461E, Test Method RE102, Radiated Emissions, 2 MHz to 1 GHz

The following EMI/RFI susceptibility tests were performed:

- IEC 61000-4-3, Radiated Susceptibility, 26 MHz to 1 GHz
- IEC 61000-4-6, Conducted Susceptibility, 150 kHz to 80 MHz
- IEC 61000-4-8, Radiated Susceptibility, Power Line Frequency Magnetic Field
- IEC 61000-4-9, Radiated Susceptibility, Pulsed Magnetic Field
- IEC 61000-4-10, Radiated Susceptibility, Damped Oscillatory Magnetic Field
- IEC 61000-4-13, Conducted Susceptibility, Harmonics and Interharmonics
- IEC 61000-4-16, Conducted Susceptibility, Common-Mode Disturbances

The EMI/RFI test acceptance criteria are as follows, based on Appendix 7 of the “Master Test Plan,” IOM Document No. 9600164-500 (Reference 23), and EPRI TR-107330, Section 4.3.7:

- The TUT shall meet allowable equipment emission limits as specified in RG 1.180, Revision 1, for conducted and radiated emissions.
- The TUT shall operate as intended during and after application of the EMI/RFI test levels specified in RG 1.180 for conducted and radiated susceptibility.

In addition, evaluation of normal operating performance data (inputs, outputs, and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance criteria from Section 4.3.7 of EPRI TR-107330:

- The main processors and coprocessors shall continue to function
- The transfer of I/O data shall not be interrupted
- The emissions shall not cause the discrete I/O to change state
- Analog I/O levels shall not vary more than 3 percent

EMI/RFI testing of the Tricon V10 was performed from February 17 through April 16, 2007, at National Technical Systems in Boxboro, Massachusetts. The TUT was installed in the EMI/RFI chamber in open-frame racks as required by the EPRI TR-107330. Wiring connections and grounding were in accordance with the manufacturer's recommendations. Additional EMI/RFI protective and mitigating devices such as power or I/O line filters, enclosed cabinets, and extra cable shielding were not used so that the specific emissions and susceptibilities of the equipment could be determined.

During EMI/RFI testing, the TUT was powered with TSAP operating. The AC and DC power sources to the TUT chassis power supplies were set at nominal source voltage and frequency conditions. In order to minimize transmission of outside EMI/RFI sources into the EMI/RFI test chamber, all power, signal, and communications cables entering the EMI/RFI test chamber were passed through filters located in the chamber walls. Because the number of pass-through filters was limited, only one circuit per I/O module was connected. The results of the EMI/RFI testing on the TUT, as documented in "EMI/RFI Test Report," IOM Document No. 9600164-527 (Reference 26), are as follows:

The TUT does not fully comply with the allowable equipment emissions levels defined in RG 1.180, Revision 1, for MIL-STD-461E, CE101, and CE102 testing.

MIL-STD-461E, Test Method CE101: Conducted Emissions, 30 Hz to 10 kHz

- 120 VAC Chassis Power Supply Line Lead. Conducted emission exceeded at:
  179.7 Hz by 11.2 dBμA 538.8 Hz by 8.9 dBμA
  299.8 Hz by 13.8 dBμA 659.7 Hz by 2.1 dBμA
  419.7 Hz by 13.0 dBμA 899.6 Hz by 1.5 dBμA

- 120 VAC Chassis Power Supply Neutral Lead. Conducted emission exceeded at:
  179.9 Hz by 11.0 dBμA 539.7 Hz by 9.6 dBμA
  299.8 Hz by 14.9 dBμA 659.9 Hz by 2.8 dBμA
  419.3 Hz by 13.1 dBμA

- 230 VAC Chassis Power Supply Line Lead. Conducted emission exceeded at:
  179.9 Hz by 4.0 dBμA 539.7 Hz by 7.6 dBμA
  299.8 Hz by 8.3 dBμA 659.7 Hz by 6.0 dBμA
  419.7 Hz by 8.7 dBμA 779.6 Hz by 1.7 dBμA

- 230 VAC Chassis Power Supply Neutral Lead. Conducted emission exceeded at:
  179.9 Hz by 3.8 dBμA 539.7 Hz by 7.5 dBμA
  299.8 Hz by 8.2 dBμA 659.7 Hz by 5.9 dBμA
  419.7 Hz by 8.6 dBμA 779.6 Hz by 1.6 dBμA

MIL-STD-461E, Test Method CE102: Conducted Emissions, 10 kHz to 2 MHz

- 120 VAC Chassis Power Supply Line Lead. Conducted emissions exceeded at:
  50.0 kHz by 1.5 dBμA

The TUT discrete and analog I/O hardware, which does not fully comply with the minimum susceptibility thresholds required by RG 1.180, Revision 1, for the EMI/RFI susceptibility tests as listed below:

IEC 61000-4-3 Testing: Radiated Susceptibility, 26 MHz to 1 GHz

- RTD Signal Conditioning Module 1600083-600
- RTD Signal Conditioning Module 1600083-200
- RTD Signal Conditioning Module 1600024-030
- RTD Signal Conditioning Module 1600024-020

IEC 61000-4-6 Testing: Conducted Susceptibility, 150 kHz to 80 MHz

- RTD Signal Conditioning Module 1600081-001
- Digital Output Module 3601T (115 VAC) with ETA 9663-610N

IEC 61000-4-10 Testing: Radiated Susceptibility, Damped Oscillatory Magnetic Field

- Due to test execution anomalies, the results of this testing were determined not to be valid. Therefore, compliance with IEC 61000-4-10 is indeterminate.

The NRC staff reviewed the “EMI/RFI Test Report,” IOM Document No. 9600164-527 (Reference 26), and determined that the tested Tricon V10 system met the EMI/RFI test acceptance criteria discussed above and is qualified up to the tested limits described above, with the exceptions as noted for the 8310 High Density Power Module (120VAC), 8312 High Density Power Module (230VAC), RTD Conditioning Modules 1600083-600, 1600083-200, 1600024-020, 1600024-030, 1600081-001, Digital Output Module 3601T (115VAC) with ETA 9663-610N, and the IEC 61000-4-10 testing.

Given the exceptions noted above, the NRC staff determined that the Tricon V10 PLC system did not fully meet the guidance of RG 1.180, Revision 1, for conducted or radiated emissions or susceptibility. Before using the Tricon V10 system equipment in SR systems in a nuclear power plant, licensees must determine that the plant-specific EMI requirements are enveloped by the capabilities of the Tricon V10 system as approved in this SE. This determination and the suitability of the Tricon V10 system for a particular plant and application is the responsibility of the licensee.

3.3.6.1 ELECTRICAL FAST TRANSIENT

RG 1.180, Revision 1, Section 5.3, requires that the PLC under qualification be tested for electrical fast transient (EFT) susceptibility in accordance with the requirements of IEC 61000-4-4. RG 1.180, Sections 5.3 and 4.2, include the requirements for EFT testing of the AC and DC power supplies and signal leads respectively.

EFT testing of the TUT is described in the “EFT Test Procedure,” IOM Document No. 9600164-514. The TUT was subjected to the following EFT tests:

- 120 VAC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
- 230 VAC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
- 24 VDC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
- Peripheral Communications Cables: ± 0.5 kV and ± 1.0 kV
- ETA Input Power Wires: ± 0.5 kV and ± 1.0 kV
- Analog Input/Output Wires: ± 0.5 kV and ± 1.0 kV

- RTD /T/C and Pulse Input Wires: ± 0.5 kV and ± 1.0 kV
- Discrete Input/Output Wires: ± 0.5 kV and ± 1.0 kV

The EFT test acceptance criteria were as follows, based on Appendix 8 of the Master Test Plan (Reference 23) and EPRI TR-107330, Section 4.3.7:

- Applying the EFT Test voltages to the specified TUT interfaces will not damage any other module or device in the TUT, or cause disruption of the operation of the backplane signals or any other data acquisition signals.
- The TUT shall operate as intended during and after application of the IEC 61000-4-4 EFT test levels specified in Sections 4.2 and 5.3 of RG 1.180, Revision 1, for low exposure applications. Specifically:
  - IEC 61000-4-4: Power Leads, Level 3 Test Voltage Level: 2 kV max.
  - IEC 61000-4-4: Signal Leads, Level 3 Test Voltage Level: 1 kV max.
- Evaluation of normal operating performance data (inputs, outputs, and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance from Section 4.3.7 of EPRI TR-107330:
  - The main processors shall continue to function.
  - The transfer of I/O data shall not be interrupted.
  - The applied EFT disturbances shall not cause the discrete I/O to change state.
  - Analog I/O levels shall not vary more than 3 percent (of full scale).

EFT testing of the TUT was performed from March 26 through 28, 2007, at National Technical Systems in Boxborough, Massachusetts. During EFT testing, the TUT was powered with the TSAP operating. The AC and DC power sources to the TUT chassis power supplies were set at nominal source voltage and frequency conditions. The arrangement and grounding of the system during EFT testing was as described for the EMI/RFI tests.

During EFT testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during, and after each test to verify normal operation of the system and all peripheral communication interfaces. Results of the EFT testing are documented in the EFT Test Report. Data collected during and after each voltage test demonstrate that the TUT operated as intended throughout the testing.

IOM concluded the following from the EFT testing:

- EFT Testing of the TUT was performed in accordance with the applicable requirements of RG 1.180, Revision 1, and IEC 41000-4-4. The following EFT tests were performed:
  - 120 VAC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
  - 230 VAC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
  - 24VDC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
  - Peripheral Communications Cables: ± 0.5 kV and ± 1.0 kV
  - ETA Input Power Wires: ± 0.5 kV and ± 1.0 kV
  - Analog Input/Output Wires: ± 0.5 kV and ± 1.0 kV
  - RTD, /T/C and Pulse Input Wires: ± 0.5 kV and ± 1.0 kV
  - Discrete Input/Output Wires: ± 0.5 kV and ± 1.0 kV
- The TUT met all applicable operational and performance requirements during and after each application of the EFT Tests voltages.
- The EFT Test results demonstrate that the Tricon V10 PLC will not experience operational failures or susceptibilities due to exposure to repetitive electrical fast transients on the power and signal input/output leads. The specific Tricon hardware

which was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List.

The NRC staff reviewed the “Electrical Fast Transient Test Report,” IOM Document No. 9600164-521, Revision 1 (Reference 53), and determined that the Tricon V10 exhibits acceptable performance against electrical fast transients as addressed in RG 1.180, Revision 1.

3.3.7 SURGE WITHSTAND TESTING

EPRI TR-107330, Section 4.6.2, requires that surge withstand testing of the PLC be conducted in accordance the requirements of EPRI TR-102323. RG 1.180, Revision 1, provides an NRC approved alternative to the Surge Withstand Testing specified in EPRI TR-102323. Surge Withstand Testing of the TUT AC power supplies was performed in accordance with IEC 61000-4-5 and IEC 61000-4-12 requirements.

Surge withstand testing is described in the “Surge Withstand Test Procedure,” IOM Document No. 9600164-508. The TUT chassis power supplies and signal lines were subjected to the following surge tests:

- IEC 61000-4-5 Combination Wave: ± 2.0 kV (common mode and differential)
  - 120 VAC and 230 VAC Chassis Power Supplies
  - 24 VDC Chassis Power Supplies,
- IEC 61000-4-12 Ring Wave: ± 2.0 kV (common mode), ± 1.0 kV (differential)
  - 120 VAC and 230 VAC Chassis Power Supplies,
  - 24 VDC Chassis Power Supplies,
- IEC 61000-4-12 Ring Wave: ± 1.0 kV (common mode), ± 0.5 kV (differential)
  - AC and DC Rated Discrete Input Modules
  - AC and DC Rated Discrete Output Modules
  - Analog Input and Output Modules (RTD, T/C, Pulse, mV and mA)
  - TCM Modules, MODBUS Serial Ports
- IEC 61000-4-5 Combination Wave: ± 1.0 kV (common mode), ± 0.5 kV (differential)
  - AC and DC Rated Discrete Input Modules
  - AC and DC Rated Discrete Output Modules
  - Analog Input and Output Modules (RTD, T/C, Pulse, mV and mA)
  - TCM Modules, MODBUS Serial Ports

The surge withstand test acceptance criteria were as follows, based on Appendix 8 of the Master Test Plan (Reference 23) and EPRI TR-107330, Section 4.6.2:

- Applying the surge test voltages specified in Tables 15 and 22 of RG 1.180, Revision 1, to the specified TUT test points shall not damage any other module or device in the TUT, or cause disruption of the operation of the TUT backplane signals or any other data acquisition signals that could result in a loss of the ability to generate a trip.
- Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate satisfactory operation of the TUT during and after application of the surge test voltage. The data evaluations shall demonstrate that modules other than the one tested are not damaged and do not experience disruption of their operation.
- Per Section 6.3.5 of TR-107330, failures of one or more redundant devices are acceptable so long as the failures do not result in the inability of the TUT to operate as

intended. No faults or failures of redundant devices occurred during Surge Withstand Testing.

The surge withstand testing was performed from March 28 through April 13, 2007, at National Technical Systems in Boxborough, Massachusetts. Prior to the start of testing, all of the TUT modules (Main Processors (MPs), communication, and I/O) were removed and replaced with spare modules. This was done to protect the modules which had been through environmental, seismic, and EMI/RFI testing from damage that could occur during surge withstand testing, and preserve the condition of the original modules for final performance proof testing.

During surge withstand testing, the TUT was powered with the TSAP operating. The AC and DC power sources to the TUT chassis power supplies were set at nominal source voltage and frequency conditions. The arrangement and grounding of the system during surge withstand testing was as described for the EMI/RFI tests.

During surge withstand testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during, and after each test to verify normal operation of the system and all peripheral communication interfaces. Results of the surge withstand testing are documented in the Surge Withstand Test Report. Data collected during and after each voltage tests demonstrate that the TUT operated as intended throughout the testing.

IOM concluded the following based upon the testing:

1. Surge Withstand Testing of the TUT was performed in accordance with the applicable requirements of the IEC 61000-4-5 and IEC 61000-4-12 test methods. The following Surge Withstand tests were performed:

   - IEC 61000-4-5 Combination Wave: ± 2.0 kV
     - 120 VAC and 230 VAC Chassis Power Supplies,
       - Line to Neutral
       - Line to AC Ground
       - Neutral to AC Ground
       - Line and Neutral to AC Ground
     - 24 VDC Chassis Power Supplies,
       - High Side (+) to Low Side (-)
       - Low Side (-) to AC Ground
   - IEC 61000-4-12 Ring Wave: ± 2.0 kV
     - 120 VAC and 230 VAC Chassis Power Supplies,
       - Line to AC Ground
       - Neutral to AC Ground
       - Line and Neutral to AC Ground
     - 24 VDC Chassis Power Supplies,
       - Low Side (-) to AC Ground
   - IEC 61000-4-12 Ring Wave: ± 1.0 kV
     - 120 VAC and 230 VAC Chassis Power Supplies,
       - Line to Neutral
     - 24 VDC Chassis Power Supplies,
       - High Side (+) to Low Side (-)
   - IEC 61000-4-12 Ring Wave, IEC 61000-4-5 Combination Wave: ± 0.5 kV
     - AC Rated Discrete Input Modules
       - One Point per Module

        - Line to Neutral
        - Point ON and OFF
    - AC Rated Discrete Output Modules
        - One Point per Module
        - Line to Neutral
        - Point ON and OFF
- IEC 61000-4-12 Ring Wave, IEC 61000-4-5 Combination Wave: ± 1.0 kV
    - AC Rated Discrete Input and Output Modules
        - One Point per Module
        - Neutral to AC Ground
        - Point ON and OFF
    - DC Rated Discrete Input and Output Modules
        - One Point per Module
        - Low Side (-) to AC Ground
        - Point ON and OFF
    - Analog Input and Output Modules (RTD, T/C, Pulse, mV and mA)
        - One Point per Module
        - Shield to AC Ground
    - TRICON Communication Modules (TCMs), MODBUS Serial Ports
        - One Port
        - Connector Shield to AC Ground

2. The TUT met all applicable operational and performance requirements during and after each application of the Surge Withstand Test voltages.

3. The Surge Withstand Test results demonstrate that the Tricon V10 PLC will not experience operational failures or susceptibilities that could result in a loss of the ability to generate a trip due to exposure to Ring Wave and Combination Wave electrical surges to the components listed above. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List.

The NRC staff reviewed the "Surge Withstand Test Report," IOM Document No. 9600164-528 (Reference 54), and determined that the Tricon V10 meets the surge withstand performance criteria in EPRI TR-107330, EPRI TR-102323, Revision 1, and RG 1.180, Revision 1.

3.3.8 ELECTROSTATIC DISCHARGE WITHSTAND TESTING

EPRI TR-107330, Section 4.3.8, requires that the PLC under qualification be tested for immunity to the ESD test levels specified in EPRI TR-102323-R1. ESD Testing of the TUT was performed in accordance with IEC 61000-4-2, using the test levels defined in EPRI TR-102323-R1, Appendix B, Section 3.5. ESD testing is described in the "ESD Test Procedure," IOM Document No. 9600164-522.

The TUT was subjected to the following ESD tests:

ESD Direct Contact Discharges: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV

- Chassis 1 Battery Cover (4 points)
- Chassis 1 Control Keyswitch (1 point)
- All ETA Cable Chassis Connectors, Top Thumbscrews (25 points)
- All Chassis, Front Horizontal and Vertical Edges (32 points)

- Each Chassis Power Supply Module Type, Faceplate (3 points)
- Each Chassis Power Supply Module Type, Top Thumbscrew (3 points)
- Main Processor, TCM, RXM and I/O Modules, Top Thumbscrews (38 points)
- Model 4352A TCM Module Serial 1 Port, Metal Cable Connector (1 point)

ESD Direct Air Discharges: ± 2 kV, ± 4 kV, ± 8 kV and ± 15 kV

- Model 4352A TCM Module Net 1 Port, Plastic Cable Connector (1 point)
- Model 4352A TCM Module Net 2 Port, Plastic Cable Connector (1 point)

ESD Indirect Contact Discharges: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV

- Horizontal Coupling Plane, Parallel to Chassis Bottom Faces (4 points)
- Vertical Coupling Plane, Parallel to Chassis Front Faces (12 points)
- Vertical Coupling Plane, Parallel to ETAs (4 points)

The ESD test acceptance criteria are as follows, based on Appendix 8 of the Master Test Plan, (Reference 23), and EPRI TR-107330, Sections 4.3.7 and 4.3.8:

- Applying the ESD Test voltages to the specified TUT interfaces will not damage any other module or device in the TUT, or cause disruption of the operation of the backplane signals or any other data acquisition signals.
- The TUT shall operate as intended during and after application of the IEC 61000-4-2 Level 4 ESD test levels specified in Appendix B, Section 3.5 of EPRI TR-102323-R1 and Section 5 of IEC 61000-4-2. Specifically:
  IEC 61000-4-2: Air Discharges Test Voltage Level: ± 15 kV max.
  IEC 61000-4-2: Contact Discharges Test Voltage Level: ± 8 kV max.
- Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance from Section 4.3.7 of EPRI TR-107330:
  - The main processors shall continue to function.
  - The transfer of I/O data shall not be interrupted.
  - Applied ESD disturbances shall not cause the discretes to change state.
  - Analog I/O levels shall not vary more than 3 percent (of full scale).
- Per Section 4.3.8 of EPRI TR-107330, failures of one or more redundant devices due to application of ESD test voltages are acceptable so long as the failures do not result in the inability of the TUT to operate as intended.

ESD testing of the TUT was performed from April 4 through 6, 2007, at National Technical Systems in Boxboro, Massachusetts. During ESD testing; the TUT was powered with the TSAP operating. The AC and DC power sources to the TUT chassis power supplies were set at nominal source voltage and frequency conditions. The arrangement and grounding of the system during ESD testing was as described for the EMI/RFI tests.

During ESD testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during, and after each test to verify normal operation of the system and all peripheral communication interfaces. Results of the ESD testing are described in the ESD Test Report (Reference 55). Data collected during and after each voltage tests demonstrate that the TUT operated as intended throughout the testing.

Conclusions from this test are as follows:

1. ESD Testing of the TUT was performed in accordance with the applicable requirements of EPRI TR-102323-R1, Appendix B, Section 3.5 and IEC 41000-4-2. The following ESD tests were performed:

   ESD Direct Contact Discharges: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV
   - Chassis 1 Battery Cover (4 points)
   - Chassis 1 Control Keyswitch (1 point)
   - All ETA Cable Chassis Connectors, Top Thumbscrews (25 points)
   - All Chassis, Front Horizontal and Vertical Edges (32 points)
   - Each Chassis Power Supply Module Type, Faceplate (3 points)
   - Each Chassis Power Supply Module Type, Top Thumbscrew (3 points)
   - Main Processor, Communication, RXM and I/O Modules, Top Thumbscrews (38points)
   - Model 4352A TCM Module Serial 1 Port, Metal Cable Connector (1 point)

   ESD Direct Air Discharges: ± 2 kV, ± 4 kV, ± 8 kV and ± 15 kV
   - Model 4352A TCM Module Net 1 Port, Plastic Cable Connector (1 point)
   - Model 4352A TCM Module Net 2 Port, Plastic Cable Connector (1 point)

   ESD Indirect Contact Discharges: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV
   - Horizontal Coupling Plane, Parallel to Chassis Bottom Faces (4 points)
   - Vertical Coupling Plane, Parallel to Chassis Front Faces (12 points)
   - Vertical Coupling Plane, Parallel to ETAs (4 points)

2. The TUT met all applicable operational and performance requirements during and after each application of the ESD Tests voltages.

3. The ESD Test results demonstrate that the Tricon V10 PLC will not experience operational failures or susceptibilities due to exposure to electrostatic discharges to the components listed above. The main processors continued to function. The transfer of I/O was not interrupted. The TCM Peer-to-Peer and MODBUS communication links continued to operate correctly. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in Table 3-1.

The NRC staff reviewed the “Electrostatic Discharge Test Report,” IOM Document No. 9600164-522 (Reference 55), and determined that the Tricon V10 met the EPRI TR-107330, Section 4.3.8, and EPRI TR-102323, Revision 1, criteria for ESD performance.

3.3.9 CLASS 1E TO NON-1E ISOLATION TESTING

IOM performed isolation testing on the Tricon PLC test system in accordance with IEEE Std 384 and Section 6.3.6 of EPRI TR-107330. In particular, IEEE Std 384-1981 requires that: (a) the isolation device prevents shorts, grounds, and open circuits on the Non-Class 1E side from unacceptably degrading the operation of the circuits on the Class 1E side and (b) the isolation device prevents application of the maximum credible voltage on the Non-Class 1E side from degrading unacceptably the operation of the circuits on the Class 1E side. The details of the tests are described in the “Class 1E to Non-1E Isolation Test Procedure,” IOM Document No. 9600164-509.

The qualification of the Tricon V10 PLC is based on a system design which connects Non-Class 1E input/output circuits to modules installed in one or more separate chassis which are interfaced to the Class 1E portion of the PLC by fiber optic cables. This design provides electrical isolation of the Non-Class 1E input/output circuits because the fiber optic cables are incapable of transmitting electrical faults. Based on this system design, only the communication modules installed in the main chassis are required to provide Class 1E to Non-Class 1E electrical isolation capability (if these modules are used to interface to Non-Class 1E communication equipment). Accordingly, the TCM Module, RS-232 (MODBUS) was tested for Class 1E isolation capability. In addition, the 3636T Relay Output Module was tested for Class 1E electrical isolation capability. This allows interface to Non-Class 1E circuits (such as alarms or annunciators) without having to install a separate, fiber optically isolated chassis.

The objective of Class 1E to Non-Class 1E isolation testing is to demonstrate the suitability of the Tricon V10 PLC for qualification as a SR, Class 1E device with respect to providing electrical isolation at Non-Class 1E field connections. The "Class 1E to Non-1E Isolation Test Report" (Reference 57), IOM Document No. 9600164-529, summarizes the results of isolation testing.

Isolation requirements for the Tricon communication modules were performed as part of the Prudency Test. During prudency testing, the TUT response time was monitored and shown not to degrade for the TUT hardware configuration and TSAP. Further, IOM performed communication port fault testing. The testing involved subjecting the TUT communication ports to simulated faults of the receive line (the transmit line of the connected device) including open circuits, short circuits to ground, short circuits to the transmit line, and superimposed "white" noise. Test results show that the applied faults had no adverse effects on the TUT response time. These results are documented in the "Performance Proof Prudency Test Report," IOM Document No. 9600164-573 (Reference 56).

The TUT was installed in the NTS anechoic test chamber and mounted in open instrument cabinets. The electrical feeds to the TUT chassis power supplies were passed through filter capacitors and Line Impedance Stabilization Networks (LISNs) to minimize transmission of noise into and out of the test chamber and to standardize the effective impedance of the power supply circuits. The TUT input and output circuits were passed into the test chamber through EMI filters, also to minimize transmission of noise into and out of the test chamber. The AC and DC power sources to the TUT chassis power supplies were set at nominal source voltage and frequency conditions. The arrangement and grounding of the system during isolation testing was the same as for the EMI/RFI tests. At least one point on each I/O module was monitored for proper operation, and the communications modules were exercised through interfaces with external monitoring devices. The following TUT components were subjected to the isolation tests:

120 VAC/VDC Relay Output Module Model 3636T, Relay Output Point

- 600 VAC and 250 VDC for 30 sec, Line-to-Line, Output Point Open
- 600 VAC and 250 VDC for 30 sec, Line-to-Line, Output Point Closed
- 600 VAC and 250 VDC for 30 sec, Line-to-Ground, Output Point Open
- 600 VAC and 250 VDC for 30 sec, Line-to-Ground, Output Point Closed

Tricon Communication Module (TCM) Model 4352A, MODBUS Serial Port

- 250 VAC and 250 VDC for 30 seconds, Receive-to-Transmit Pins
- 250 VAC and 250 VDC for 30 seconds, All Pins to Ground

During isolation testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during, and after each isolation test to verify normal operation of the system and all peripheral communication interfaces. The test details are described in the Isolation Test Report (Reference 57).

Section 4.6.4 of EPRI TR-107330 requires that the PLC modules under qualification provide electrical isolation capability of at least 600 VAC and 250 VDC applied for 30 seconds. Per Section 7.2.2.1 of IEEE Std 384-1981, the highest voltage to which an isolation device Non-Class 1E side is exposed shall determine the minimum voltage level that the device shall withstand across the Non-Class 1E side terminals, and between the Non-Class 1E terminals and ground. The communication cables connected to the Tricon V10 TCM communication modules are expected to be routed separately from high voltage (greater than 120 VAC) cables. A line-to-line short to a three conductor 120 VAC cable could result in a maximum possible voltage exposure of 240 VAC. Therefore, the TCM MODBUS serial communication ports were tested for a maximum isolation capability of 250 VAC and 250 VDC (at 10 amps maximum) applied for 30 seconds. The Model 3636T Relay Output Module was tested to the full EPRI TR-107330 voltage levels of 600 VAC (at 25 amps maximum) and 250 VDC (at 10 amps maximum) as listed above.

The Class 1E to Non-Class 1E Isolation Test results demonstrates that the Model 3636T Relay Output Module and the Model 4352A Tricon Communication Module provide adequate electrical isolation per IEEE Std 384-1981 between the SR portions of the Tricon V10 PLC and connected NSR field circuits. The testing demonstrated electrical isolation capability of the relay output points to applied voltages of 600 VAC (at 25 amps maximum) and 250 VDC (at 10 amps maximum).

The Tricon V10 PLC Model 4201 Remote RXM fiber optic module was not tested because fiber optic cables are incapable of transmitting electrical faults from the remote Non-Class 1E RXM module to the primary RXM (which would be installed in the SR Tricon chassis). Thus, the Tricon V10 Model 4201 Remote RXM fiber optic module is considered an acceptable Class 1E to Non-Class 1E isolation device by design.

The TUT met all applicable performance requirements during and after application of the Class 1E to Non-Class 1E isolation test voltages. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List (Reference 17).

The isolation test results (together with the Prudency Test communication port fault tests) demonstrated that the Tricon Model 4352A TCM Module MODBUS serial communication ports provide adequate electrical isolation per IEEE Std 384-1981 between the SR portions of the Tricon V10 and connected NSR communication circuits. In addition, the testing demonstrated electrical isolation capability of the TCM MODBUS serial communication ports to applied voltages of 250 VAC and 250 VDC (at 10 amps maximum) for 30 seconds.

The NRC staff determined that the Tricon V10 system met the criteria of IEEE Std 384-1981 and Section 6.3.6 of EPRI TR-107330. It is the responsibility of the license to verify that the maximum test voltages cited above envelop the maximum credible voltages applied to Non-Class 1E interfaces.

3.3.10 PERFORMANCE PROOF TESTING

Performance proof testing was conducted at the completion of all qualification testing to demonstrate the continued acceptable performance of the TUT after being exposed to various qualification test conditions. Performance proof tests are merely a repeat of selected prequalification baseline tests to identify any changes in equipment performance. Performance proof testing includes operating the test system for 7 days with an elevated DC source, operability test, and prudency test. Appendix 9 of the Master Test Plan (Reference 23) describes the test plan for proof testing. Test procedures were developed for the operability test, IOM Document No. 9600164-566 and Prudency Test, IOM Document No. 9600164-573.

Performance proof testing was performed at the IOM facilities in Irvine, California. Test results are documented in the Performance Proof Operability Test Report (Reference 44) and Performance Proof Prudency Test Report (Reference 56). The results are contrasted to initial recorded benchmark performance data, as well as test data collected during environmental and seismic testing.

The Operability Test Procedure, Performance Proof Test successfully established performance data for the TUT in accordance with the IOM published specifications and/or EPRI TR-107330 specifications and all acceptance criteria stated in the procedure were met. In addition, the test results of the Operability Test Procedure, Pre-Qualification Test and Operability Test Procedure, Performance Proof Test were analyzed to determine any degradation in the performance of the TUT. The analyses established that the TUT performed in accordance with IOM published specifications and/or EPRI TR-107330 specifications before and after Qualification Tests and no degradation in the performance of the TUT were identified. Conclusions from this test are summarized below.

1. Analog Input/Output Module Accuracy – This test shall demonstrate that the overall accuracy of each AI and output module shall meet IOM published specifications.

   For all operability test runs, the accuracy of each analog I/O module of the TUT was demonstrated to meet the IOM published specifications. In addition, the test results show no degradation in module accuracy from pre-qualification testing throughout qualification and performance proof testing.

2. Response Time – This test shall demonstrate that the measured loop response times shall not vary more than ±10 percent from the baseline TUT loop response times. EPRI TR-107330, Section 4.2.1.A, requires an overall response time of 100 msec or less.

   For all operability test runs, the response times for digital input to digital output, AI to digital output and digital output and "round-robin" sequences of the TUT were measured. The test data demonstrates that the maximum response time equation provides a reliable upper bound on the maximum expected response times for a specific TUT hardware configuration and TSAP.

   Note that the TUT loop response times are a function of its actual hardware configuration and the scan time of the TSAP. The specified absolute response time is therefore not applicable to testing of the TUT and the TUT loop response times were measured during this test.

3. Discrete Input Operation – This test shall demonstrate that the OFF to ON and ON to OFF voltage switching levels of each tested digital input module point shall meet IOM published specifications.

   For all Operability Test runs, the OFF to ON and ON to OFF voltage switching levels of each digital input module of the TUT was demonstrated to meet the IOM published specifications. In addition, the test results show no degradation in discrete input module voltage switching levels from pre-qualification testing throughout qualification and performance proof testing.

4. Discrete Output Operation – This test shall demonstrate that the maximum current driven with maximum and minimum voltage of each tested digital output module point shall meet IOM published specifications.

   For all Operability Test runs, each discrete output module of the TUT was demonstrated to operate ON and OFF at the IOM published specifications for maximum operating current, and minimum and maximum operating voltage. In addition, the test results show no degradation in operation of the discrete output modules from pre-qualification testing throughout qualification and performance proof testing.

5. Timer Function Accuracy – This test shall demonstrate that the measured timer function time out periods shall not vary by more than ±1 percent or ±3 scan cycles from the baseline timer time out periods during this test.

   The application software timer function accuracy is a function of the scan time of the TSAP loaded in the TUT. The specified absolute baseline timer function accuracy criteria are not applicable to testing of the TUT. Therefore, this test was performed to determine the timer function for the TSAP loaded in the TUT.

   For all Operability Test runs, the time out periods of the application program timer functions were demonstrated to not vary from the measured pre-qualification baseline time-out periods by more than the greater of ±1 percent of the time out period or three application program scan cycles. In addition, the test results showed no degradation in timer function variation from pre-qualification testing throughout qualification and performance proof tests.

6. Failover Performance – This test shall demonstrate that the monitored discrete outputs shall not change state, the AOs shall not change by more than ±5 percent, and the main processor shall not reset during the simulated fault test period, and all simulated faults shall result in actuation of a chassis power supply alarm circuit.

   Tests were done to demonstrate automatic failover to redundant components on simulated failures of a main processor module, an RXM, a chassis expansion port cable, and chassis power supplies. All test results demonstrated acceptable failover operation of the TUT.

7. Loss of Power Performance / Failure to Complete a Scan Detection – This test shall demonstrate during the simulated loss of power, the TSAP shall cease operation, all monitored discrete output points shall open, all monitored AO points shall go to zero, and all communications with connected test system peripheral devices shall cease. On restoration of power, the TUT shall pass all start-up hardware diagnostics and shall automatically resume normal operation.

For all Operability Test runs, performance of the TUT was demonstrated on loss and restoration of power to the chassis power supplies. The test results demonstrated predictable and consistent response of the TUT to a loss of power. The test results also demonstrated predictable and consistent response of the TUT on recovery of power. In addition, successful restart of the TUT on restoration of power consistently indicated proper functioning of the watchdog timer mechanisms.

8. Power Interrupt Performance – This test shall demonstrate that the hold-up time for the chassis power supply modules shall be at least 40 msec on loss of the AC source power and the monitored discrete outputs shall not change state, the AOs shall not change by more than ±5 percent, and the main processor shall not reset during the power interrupt period.

   For all Operability Test runs, power hold-up time performance of the TUT chassis power supplies were demonstrated on an interruption of source power for approximately 40 msec. The test results demonstrated that the 120 VAC and 230 VAC chassis power supplies meet the EPRI TR-107330 acceptance criteria for hold-up time capability of at least 40 msec when installed as the only chassis power supply or when installed in combination with a second chassis power supply.

9. Power Quality Tolerance – This test shall demonstrate that the output voltage of the TUT chassis power supply modules shall show no appreciable change in voltage level or DC ripple content when subjected to the specified source power minimum and maximum voltage and frequency conditions.

   Tests were performed over IOM allowable ranges of voltage and frequency for each type of power supply included in the testing. All test results demonstrated acceptable performance of the TUT. In addition, power quality tolerance tests demonstrated acceptable performance of processor memory writes prior to Tricon reset on gradual loss of source power voltage.

   The Prudency Test Procedure, Performance Proof Test was performed following the successful completion of Operability Test Procedure, Performance Proof Test. Prudency testing involved exposing the TUT to various normal and abnormal conditions of input/output operation and source power at minimum source power supply voltage and frequency conditions. EPRI TR-107330, Section 5.4, describes the specific criteria to be met for prudency tests.

   The Prudency Test Procedure, Performance Proof Test demonstrated that performance data for the TUT were achieved at minimum source power supply voltage and frequency conditions under highly dynamic loading and adverse noise conditions in accordance with IOM published specifications and/or EPRI TR-107330 specifications and all acceptance criteria stated in the procedure were met with the exception of the failure of the AO module during burst of events test. This anomaly was evaluated, and IOM concluded that the test system loopback setup, which was designed for testing purposes, was the cause of the failure to meet the acceptance criteria. The test system loopback setup is not an installation arrangement that would be utilized by a customer. The AI module and the AO module will perform as intended, within the required accuracy, in a customer installation. The test results of the Prudency Test Procedure, Pre-Qualification Test and Prudency Test Procedure, Performance Proof Test were analyzed to determine any degradation in the performance of the TUT. The analyses established that the TUT performed in accordance with IOM published specifications and/or EPRI TR-107330 specifications before and, after

Qualification Tests and no degradation in the performance of the TUT were identified. Conclusions from this test are summarized below.

10. Burst of Events Performance – Burst of Events testing demonstrated the ability of the TUT to process rapidly changing input and output signals based on the control logic of the TSAP with the exception of the failure of the AO module during burst of events test, as described above.
11. Communication Port Failure Performance – Communication port failure testing demonstrated no effect on digital input to digital output, AI to digital output and AO, and "round-robin" response times during simulated failures of communication lines connected to communication ports on the TCM. Note that during this test the TUT loop response times failed to meet the acceptance criteria. IOM found that the failure was due to a DAS threshold issue. The TUT loop response times passed in the re-run.

3.4 PLATFORM INTEGRITY CHARACTERISTICS

SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," states that a special concern for digital computer-based systems is confirmation that system real time performance is adequate to ensure completion of protective actions within the critical time periods identified as required by Clause 4 of IEEE Std 603-1991. SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provides supplemental guidance on evaluating response time for digital computer-based systems, and discusses design constraints that allow greater confidence in analyses of results or prototype testing to determine real time performance. In summary, the integrity of a safety system is evidenced by a predictable response time, which in turn depends on deterministic behavior and fault management capabilities in addition to the timing characteristics of the hardware/software system.

3.4.1 RESPONSE TIME

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

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

The regulations that contain the basis for this requirement are in 10 CFR 50.55a(h). In addition, 10 CFR 50.36(c)(1)(ii)(A) requires inclusion of the limiting safety systems settings for nuclear reactors in the plant technical specifications (TSs), with those settings "so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded."

Section 4.2.1, Item A, of EPRI TR-107330 states "The overall response time from an input to the PLC exceeding its trip condition to the resulting outputs being set shall be 100 milliseconds or less," and cites conditions related to that time requirement. IOM took exception to the requirement of Section 4.2.1, Item A of EPRI TR-107330. The NRC staff evaluation of the IOM exception to the response time requirement can be found in Section 3.3.2 of this SE. On the basis of the response time values, the Tricon V10 PLC system is not in compliance with Section 4.2.1-A of EPRI TR-107330. The actual response time for any particular system will depend upon the actual system configuration and may vary significantly from simple to complex systems. The determination of the suitability of the Tricon PLC system response time characteristics for a particular plant application is a plant specific requirement and therefore is the responsibility of licensees.

The response time performance of a SR system based on the Tricon V10 platform is an ASAI and subject to plant-specific review to ensure that it satisfies its plant- and application-specific requirements for system response time presented in the accident analysis in Chapter 15 of the safety analysis report for the applicant's plant.

3.4.2 DETERMINISTIC PERFORMANCE

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

EPRI TR-107330 includes requirements intended to achieve deterministic execution cycle behavior such that an application and its constituent tasks will be completely executed within a specific time frame. In particular, Section 4.4.1.3, "Program Flow Requirements," specifies that, for those PLCs where scanning of the inputs and application program execution are performed in parallel, the PLC executive must provide methods for assuring that both the input scan and application program execution are completed each cycle. In effect, the EPRI guide specifies continuous, essentially non-interruptible, software architecture as the preferred software environment for safety functions.

The Tricon V10 software architecture has three main elements; ETSX version 6271, the executive for the application processor, IOCCOM, the executive for the communication processor and the executive on the various I/O modules. IOM provided a description of the ETSX version 6271 operating system, documented in Section 2.1.3 of the LTR, which outlines how the three elements execute and interact. Further details on interrupts, use of watchdog timers and self-diagnostics used to protect the safety function are outlined in request for additional information (RAI) 6 response, (Reference 8).

The Tricon PLC system uses a triple redundant architecture to provide fault tolerance and uninterrupted control in the presence of either hard failures of components or transient faults from internal or external sources. Sensor signals are received on termination assemblies, which are constructed as electrically passive circuit boards to which field wiring is attached. The termination module passes input signals from the field to an input module. Each input module consists of three identical and independent circuits, all contained on a single printed circuit assembly. Each of the three input legs asynchronously measures the input signals from the input termination module and places the values into input tables. Each input table is regularly interrogated over the I/O bus by the I/O communication processor which is located on the corresponding main processor module.

As each input module is polled, the appropriate leg of the I/O bus transmits new input data to the application processor, where it is assembled into a table that is stored in memory for use in the hardware voting process. The input table in each application processor is transferred to its neighboring application processors over the Tribus. Hardware voting takes place during this transfer. The Tribus uses direct memory access to synchronize, transmit, vote, and compare data among the three application processors. If a disagreement occurs, the signal value found in two out of three tables prevails, and the third table is corrected accordingly. One time differences that result from sample timing variations are distinguished from a pattern of differing data. Each application processor maintains data about necessary corrections in local memory. Any disparity is flagged and used at the end of the scan by the built in fault analyzer routines of the Tricon PLC system to determine whether a fault exists on a particular module.

The application processors enter corrected data into the control program, which the application processor executes in parallel with the neighboring application processors. The control program generates trip or control signals on the basis of licensee specific application programs. The I/O communication processor on each 3008N MP module sends the output data to output modules via the I/O bus. In the event of a trip signal, the output modules use termination assemblies to transfer the trip signal to the actuation devices.

If an I/O module channel fails to function, an alarm is raised to the MPs. If a redundant module is installed in the paired slot with the faulty module, and that module is deemed healthy by the MPs, the system automatically switches over to the standby unit and takes the faulty module off line. If no standby unit is in place, the faulty module continues to operate on two of the three legs, and control is unaffected. The user obtains a replacement unit and plugs it into the system in the paired slot associated with the failed module. (This position is logically paired with the failed module’s location.) When the MPs detect the presence of a replacement module, they initiate local health state diagnostics and, if the module is healthy, automatically switch over to the new module. The user then removes the faulty module for repair or replacement.

If redundant modules are installed and both are deemed healthy by the MPs, the MPs will swap control between the redundant modules so that each is used on a periodic basis. By periodically using each module, any faults will be detected and alarmed, and the failed module will be replaced while a redundant module is in place. This use of redundant modules does not cause process upsets, and is undetectable outside of the Tricon PLC system.

The NRC staff reviewed specific details pertaining to determinism including the description of the software in Section 2.1.3 of the LTR, the full description of the three main executive programs that define a complete scan cycle including interrupts and watchdog timers from the RAI 6 response (Reference 8), IOM Document No. 9600164-731, “Maximum Response Time Calculations” (Reference 43), and changes outlined in the IOM Document No. NTX-SER-09-05 (Reference 10) that show there is no change that impacts determinism in the overall architecture or operation between the V9 and V10 configurations.

The NRC staff determined that the Tricon V10 platform meets the criteria regarding deterministic performance of SRP Chapter 7, Appendix 7.1-C, Section 6.1, SRP BTP 7-21, and EPRI TR-107330, Section 4.4.1.3 when appropriately implemented.

3.4.3 DIAGNOSTICS AND SELF-TEST CAPABILITIES

IEEE Std 603-1991 Clause 5.7 states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability be provided during power operation, and shall duplicate, as closely as practicable, performance of the safety function. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station; however, appropriate justification must be provided; acceptable reliability of equipment operation must be demonstrated; and the capability shall be provided while the generating station is shut down. SRP, Chapter 7, Appendix 7.1-C, Section 5.7, "Capability for Test and Calibration," provides acceptance criteria for IEEE Std 603-1991, Clause 5.7. Capability should be provided to permit testing during power operation and that when this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Section 5.7 further states that test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation. Section 5.7 further states that for digital computer based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup.

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

EPRI TR-107330 specifies that the PLC platform must provide sufficient diagnostics and test capability so that a combination of self-diagnostics and surveillance testing will detect all failures that could prevent the PLC from performing its intended safety function. The range of conditions for which diagnostics or test capabilities must be provided includes processor stall, executive program error, application program error, variable memory error, module communications error, module loss of configuration, excess scan time detection, application not executing, and field device (e.g., sensor, actuator) degradation or fault. The means of detection include watchdog timer, checksum for firmware and program integrity, read/write memory tests, communications monitoring, configuration validation, heartbeat, and self-diagnostics or surveillance test support features. Both online and power-up diagnostics are specified.

The IOM Planning and Installation Guide, a commercial manual with IOM part number of 9700077-012 (Reference 16), provides detailed descriptions of each diagnostic test and flag.

The Tricon V10 PLC system provides continuous self-testing, including monitoring memory and memory reference integrity, using watchdog timers, monitoring communication channels, monitoring central processing unit status, and checking data integrity. The Tricon V10 PLC system performs self-tests and I/O validation on each module. The Tricon V10 PLC system TMR architecture provides continuous self-testing to detect, tolerate, and alarm on single internal failures. The internal self-test functions are transparent to the application program and are an integral part of the base platform operating software. These diagnostics check each main processor, as well as each I/O module and communication channel. Transient faults are recorded and masked by the hardware majority-voting circuit. Persistent faults are diagnosed, and the faulted module can be replaced or operated in a fault-tolerant manner until replacement is completed.

System diagnostics monitor the health of each main processor module as well as each I/O module and communication channel. The main processor modules process diagnostic data recorded locally and data received from the input module level diagnostics in order to make decisions about the health of the input modules in the system. All discrepancies are flagged and used by the built in fault analyzer routine to diagnose faults. The main processor diagnostics perform the following:

- Verification of fixed-program memory
- Verification of the static portion of RAM
- Verification of the dual port RAM interface with each IOCCOM
- Checking of each IOCCOM's ROM, dual port RAM access and RS-485 loopback
- Verification of the TriTime interface
- Verification of the TriBUS interface

All input modules include self-diagnostic features designed to detect single failures within the module. Fault detection capabilities built into various types of input modules include the following:

- The input data from the three legs is compared at the main processor, and persistent differences generate a diagnostic alarm.
- Digital input modules test for a stuck on condition by momentarily driving the input for one leg low in order to verify proper operation of the signal conditioning circuitry. A diagnostic alarm is generated if the input module does not respond appropriately.
- Analog input modules include high accuracy reference voltage sources which are used to continuously self-calibrate the analog-to-digital converters. If a converter is found to be out of tolerance, a diagnostic alarm is generated.
- Several input modules also include diagnostics to detect field device failures.

All output modules include self-diagnostic features designed to detect single failures within the module. The major fault detection capabilities built into output modules include the following:

- Digital output modules include output voter diagnostics that toggle the state of one leg at a time to verify that the output switches are not stuck on or off.
- Supervised digital output modules include a voltage and current loopback circuit that checks for open circuits (e.g., blown fuse) and short circuits in the field wiring.
- AO modules include a voltage and current loopback circuit. On these modules, one of the three legs drives the field load, and the other two legs monitor the loopback current to verify the module output current is correct.

The NRC staff determined that the Tricon V10 meets the criteria of RG 1.22, RG 1.118, and IEEE Std 338-1987.

3.5 FAILURE MODES AND EFFECTS ANALYSIS

IOM performed a failure modes and effects analysis (FMEA) on the Tricon V10 platform, and documented that analysis in IOM Document No. 9600164-531 (Reference 28). Specifically, IOM performed the analysis on the system as configured for qualification testing discussed in Section 3.3 of this report. The FMEA was done in accordance with the guidelines of Section 6.4.1 of EPRI TR-107330 and IEEE Std 352, Sections 4.1, 4.4, and 4.5.

The FMEA was conducted in a similar manner to the Tricon V9 FMEA, (reference Tricon V9 SE Section 4.3.1) in that because failure mechanisms that affect a single leg of the triple modular redundant system generally have no effect on system operation, the FMEA also considered (1) failure mechanisms that are recognized as being highly unlikely but could affect multiple components, and (2) the coincident occurrence of otherwise single failures (i.e., multiple failures).

The NRC staff confirmed through the FMEA that the Tricon V10 is designed to fail to the safe state. The Tricon V10 is designed for de-energize to trip systems. Input related failures are designed to set input tables to the de-energized state. Output module voters are designed to fail to the de-energized state.

The NRC staff confirmed that the Tricon V10 FMEA was performed in accordance with the guidelines of Section 6.4.1 EPRI TR-107330 and IEEE Std 352, Sections 4.1, 4.4, and 4.5. The NRC staff determined that the FMEA is sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures. The NRC staff also determined that the Tricon V10 is designed to fail to the safe state. The analysis and results in the Tricon V10 FMEA are suitable for reference by licensees and for incorporation into plant-specific FMEA analyses.

3.6 RELIABILITY AND AVAILABILITY ANALYSIS

IOM performed a reliability and availability analysis of the Tricon V10 platform as specified in Section 4.2.3 of EPRI TR-107330 and documented the results in IOM Document No. 9600164-532, “Reliability / Availability Study for the Tricon V10” (Reference 47). Calculations were done for periodic test intervals ranging from 6 to 30 months. In all cases, the calculated reliability and availability were greater than 99.9 percent, which exceeds the recommended goal of 99.0 percent from the EPRI TR. For a periodic test interval of 18 months (corresponding to the typical nuclear power plant refueling outage cycle), the reliability is 99.9987 percent and the availability is 99.9990 percent.

The NRC staff reviewed this report and determined that the results of the Tricon V10 reliability and availability analysis (Reference 47) meet the criteria of EPRI TR-107330, Section 4.2.3.

3.7 COMMUNICATIONS INDEPENDENCE

IEEE Std 603-1991 Clause 5.6, “Independence,” requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. SRP Chapter 7, Appendix 7.1-C, Section 5.6, “Independence,” provides acceptance criteria for this requirement, and among other guidance, provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system.

IEEE Std 7-4.3.2-2003, endorsed by RG 1.152, Revision 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Clause 5.6, “Independence,” provides guidance on how IEEE Std 603 requirements can be met by digital systems. This clause of IEEE Std 7-4.3.2

states that, in addition to the requirements of IEEE Std 603-1991, data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence," provides acceptance criteria for computer equipment qualification. The regulation at 10 CFR Part 50, Appendix A, GDC 24, "Separation of protection and control systems," states that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired. Additional guidance on interdivisional communications is contained in "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4, Highly-Integrated Control Rooms Communications Issues (HICRc)." DI&C-ISG-04 compliance is discussed further in Section 3.7.3.

The NRC staff reviewed the overall design of a Tricon V10 SR system. As part of this review, the NRC staff evaluated applicability and compliance with SRP Section 7.9, "Data Communication Systems," SRP Chapter 7, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and SRP BTP 7-11, "Guidance on Application and Qualification of Isolation Devices." SRP BTP 7-11 provides guidance for the application and qualification of isolation devices, and applies to the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and non-safety systems.

The Tricon V10 supports bi-directional SR and NSR communications. SR communications are through the TCM using one of two proprietary protocols intended to enhance data integrity. The P2P protocol, used on the V9 Tricon, is used for SR communications between safety divisions. The SAP protocol is a new Tricon protocol intended for SR communications within a safety division. No specific SR communications function was described in the LTR, however, this capability is included within the scope of the Tricon V10 LTR and therefore, is discussed in Section 3.7.1 below.

Bidirectional communications used for communications between the SR Tricon V10 platform and other NSR systems is supported through two separate paths; the TCM and NSR I/O connected to modules in a remote RXM chassis. NSR to SR Tricon V10 communications are discussed in Section 3.7.2.

The main element of protection for all Tricon V10 communications is the 3008N Main Processor Module architecture. The main application processor that runs the control program is data isolated using a128K shared memory (dual port RAM (DPRAM)). All data used by the control program is pulled from pre-allocated addresses in the shared memory. Input data is written to the shared memory by a separate communications processor which controls both the I/O bus and the communications bus. The overall architecture is the same as the Tricon V9 as described in Section 2.1.2 of the Tricon V9 SE (Reference 9).

Communications for the Tricon V10 upgrade were evaluated against criteria in the guidance noted above. The three previously accepted communication modules used in Tricon V9.5.3, which was not evaluated against DI&C-ISG-04, were replaced by the 4352AN TCM. The NRC staff chose to first assess the impact of changes to the TCM to understand its capabilities and limitations. This allowed the NRC staff to apply those findings while evaluating how the system meets the guidance in DI&C-ISG-04.

3.7.1 COMMUNICATIONS WITH SAFETY CHANNELS/DIVISIONS

Communications between independent safety channels containing Tricon V10 processors is implemented via the TCM modules. The TCM is a communications device that serves to pass data between the three redundant communication busses and up to six external channels, two ethernet, and four RS-485. The TCM was designed under IOM's Appendix B process and qualified with the Tricon V10 as a SR device under IOM's nuclear qualification program (Reference 59). The TCM software is based on the software used in devices approved with the Tricon V9.5.3 and adds a new Safety Application Protocol (SAP). The device also uses a commercial operating system which IOM dedicated using EPRI NP-5652 methods 1, 3 and 4 which is reviewed in Section 3.2.2 of this SE.

Although the TCM uses updated versions of the processor, gatekeeper and transceiver chips, the architecture is similar to that of the previously approved 4329N Network Communications Module. A comparison of specifications and system designs showed that the TCM adds support for the SAP protocol and combines features found in previously approved communications modules. The NRC staff performed a thread audit on TCM V&V testing during the December 2010 audit at IOM's Irvine facility. Based on the review of the LTR (Reference 4), IOM Document No.NTX-SER-09-05, Sections 4.1 and 4.2 (Reference 10), and the audit results (Reference 6), the NRC staff concludes that the TCM is functionally equivalent to the previously approved communication modules.

IOM developed a Communication Application Safety Layer for SR communication between an external SR processor and the Tricon V10 system. This is an additional layer of protection provided by the P2P and SAP communication protocols at the application layer of the network stack. The P2P and SAP protocols are intended to ensure end-to-end integrity of safety-critical messages between SR processors. These protocols use software at the sending and receiving processors to provide additional fault mitigations such as message sequencing that are not accounted for through Ethernet or other parts of the Tricon V10 communication path. System architectures requiring data transfer between SR Tricons would use the P2P protocol over an electrically isolated, point-to-point network. Architectures requiring safety-critical data exchange with SR video display units would utilize the SAP. IOM Document No.NTX-SER-09-10 (Reference 29) describes the Tricon V10 conformance to ISG-04. The NRC staff's evaluation of the Tricon V10 conformance to ISG-04 is described in Section 3.7.3 of this SE.

All of the protocols except SAP were carried forward unchanged from the Tricon V9. The NRC staff reviewed the new SAP protocol including the following documents; "Safety Application Protocol Library Software Requirements Specification," IOM Document No. 6200260-001 (Reference 60), "Communication Application Safety Layer Interface Requirements Specification," IOM Document No. 6200154-099 (Reference 61), "TS1131 Libraries Software Verification and Validation Plan," IOM Document No. 9600355-001 (Reference 62), and "SAP Library Verification and Validation Test Report" (Reference 63). The protocol is implemented at the application layer which means that it is part of the TriStation 1131 library for Tricon V10. The documentation confirms testing of the TriStation 1131 library with the SAP protocol. However, the protocol will also be implemented at the application layer of the connected SR equipment, presumably a safety video display unit (SVDU). The protocol has not been tested with any specific external SR devices. Therefore, it is an ASAI to verify that the SAP library is tested in any proposed application specific SR devices connected to the TCM.

In Document No.NTX-SER-09-05, Section 4.2, IOM states that the TCM software was ported directly from the V9.5.3 modules. However, the real time operating system was replaced by a third party real time OS. As reviewed in Section 3.2.2 of this SE, IOM dedicated the third party pre-developed software (PDS) using EPRI-NP 5652 methods 1, 3, and 4. CGD of the PDS will only apply for use of the specific product noted in Section 3.2.2. IOM will have to separately dedicate other versions or products from this vendor. As stated in Section 3.7, the main element of protection of the safety function with regard to communications is the dual port/shared memory and the use of a separate communications processor. The P2P and SAP protocols provide additional data integrity mitigations for all SR communications. The TCM also provides CRC checks on all incoming data in addition to the protocol mitigations. Finally, the TCM has an access control capability to control Ethernet communications through IP address. Read and /or write permission for specific IP addresses can be programmed into an access control list through the TS 1131 programming software. The NRC staff did not review this feature with regard to potential cyber security benefits, but does credit it as an additional layer of secure development and operational environment (SDOE) protection to protect against inadvertent access in meeting RG 1.152, Revision 3, requirements in Section 3.8 of this SE.

The NRC staff determined that SR communications through the TCM is acceptable for use in safety systems in nuclear power plants subject to the guidance in DI&C-ISG-04. It is an ASAI to review any SR communications connections through the TCM with regard to DI&C-ISG-04 as detailed in Section 3.7.3 of this SE.

3.7.2 COMMUNICATIONS WITH NON-SAFETY SYSTEMS

Communications between SR Tricon V10 systems and NSR equipment are primarily through the TCM, similar to the SR communications described in Section 3.7.1. However, NSR I/O connected to a remote RXM chassis must also be considered communication with a non-safety system because the SR I/O bus crosses the SR/NSR boundary and adequate protection of the safety function must be demonstrated. Each type of NSR communication is discussed in Sections 3.7.2.1 and 3.7.2.2 below.

3.7.2.1 NSR COMMUNICATIONS VIA THE TCM MODULES

Section 3.2 of IOM document NTX-SER-09-10, “Compliance with NRC Interim Guidance ISG2 & ISG4,” Revision 2, (Reference 29) describes safety to non-safety communications using the TCM. There, IOM describes the use of a one way link (OWL) device as a data isolation device to provide additional protection for NSR communications to a SR Tricon V10 via the TCM. Specifically, IOM identified NetOptics Aggregator Tap model number PA-CU and cited precedent based on NRC Safety Evaluation, “Oconee Nuclear Station, Units 1, 2, and 3, Issuance of Amendments Regarding Acceptance of the Reactor Protective System and Engineered Safeguard Protective System (RPS/ESPS) Digital Upgrade” (Reference 64).

The NetOptics Port aggregator Tap, Model 96443, No. PA-CU, or PAD-CU, is a device intended to allow monitoring of a 10/100 BaseT Ethernet communication link by copying the communications and sending that copied information to a separate one-way communications link. Port A of the Port Tap is connected to the TCM, and Port B is connected to the Maintenance Terminal (maintenance video display unit (MVDU)). This allows for two way 10/100 BaseT Ethernet communication between the TCM and the MVDU. Port C of the Port Tap is attached to an external computer, and this port supports only one-way outbound communications. In this manner, the TCM can send messages to both the MVDU and an external computer. As with any Ethernet system, the Maintenance Terminal and the external computer will read the message headers to determine the intended recipient, and will ignore messages not addressed to that device.

In order for the NRC staff to verify that the port aggregator tap is capable of ensuring one-way communication from the TCM to the external computer, and ensuring that a failure of the port aggregator tap would not permit bi-directional connectivity, information regarding the internal operation of the port aggregator tap (Reference 66) was reviewed. An installation guide and product declaration, containing the schematic for part No. PA-CU and part No. PAD-CU, was also provided in a supplemental response for RAI 5, (Reference 65) from Duke Energy Corporation. According to the port aggregator tap schematics; all communication to the "one-way output" of the port aggregator tap is channeled through a set of internal operational amplifiers (op-amps). The physical design of op amps is such that proper biasing of the transistors is required in order to transmit the electrical signals to the external computer. These op amps prohibit the flow of data from the external computer to the TCM. The details of this review and the information provided are proprietary, and, therefore, will not be further discussed in this SE.

The NRC staff has determined that the data isolation function provided by the Port Tap device provides reasonable assurance that a fault or failure within the external computer system will not adversely affect the ability of a Tricon Safety System to accomplish its safety functions provided that the following ASAI's are performed.

1. Verify that the Port Tap device model number is either PA-CU, or PAD-CU. Use of any other device to accomplish this function will require additional analysis. Since the original review of part No. PAD-CU Port Tap required NRC staff examination of actual schematic drawings of the circuitry to determine that there was no inbound communications path associated with Port C, a similar schematic review for any replacement or updated model of the Port Tap must be performed to determine if the manner in which it is being used and configured are acceptable.

2. Ensure that the Port Tap device is configured in the manner illustrated in Figure 3.7.2.1-1 below.

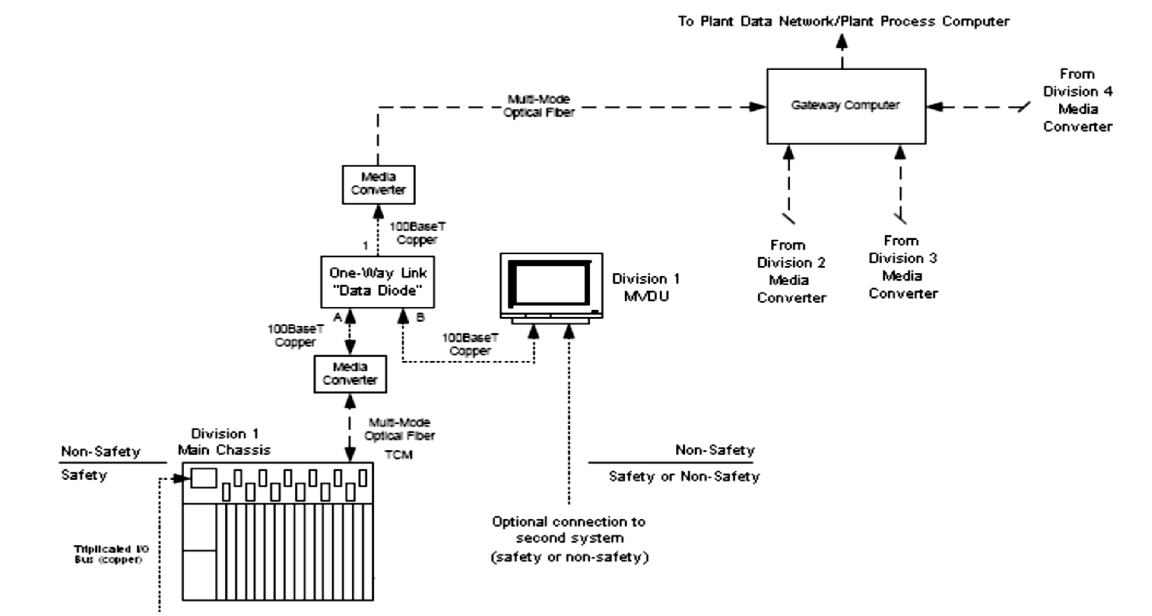

To Plant Data Network/Plant Process Computer
Multi-Mode Optical Fiber
Gateway Computer
From Division 4 Media Converter
Media Converter
100BaseT Copper
1
From Division 2 Media Converter
From Division 3 Media Converter
One-Way Link "Data Diode"
Division 1 MVDU
A
B
100BaseT Copper
100BaseT Copper
Media Converter
Multi-Mode Optical Fiber
TCM
Division 1 Main Chassis
Non-Safety
Safety
Non-Safety
Safety or Non-Safety
Triplicated I/O Bus (copper)
Optional connection to second system (safety or non-safety)

Figure 3.7.2.1-1 – Safety to Non-Safety w/ MVDU via One Way Link

In addition to the port tap device described above, the same layers of protection that apply to SR communications would also apply to communications with NSR equipment except that application layer protocols would not be used. Specifically, listed in order from the TCM back to the application processor, the mitigations are; TCM IP address discrimination, TCM data integrity check, IOCCOM single threaded bus master control scheme, IOCCOM data integrity check, IOCCOM com bus/ I/O bus separation, dual port RAM, fixed addressing in dual port RAM, read/write specific tag names for memory locations.

The NRC staff determined that NSR equipment (e.g., plant computer) may be connected to the TCM through a port tap device as described above. This approval is subject to application specific review items noted above to verify the port tap device meets the precedent criteria (i.e., verify model number) and to verify port tap configuration in the system. An MVDU may be connected through the port tap as shown in Figure 3.7.2.1-1. However, approval of the MVDU will require review of plant specific procedures and review of the plant specific configuration.

It is an ASAI to review all NSR communications connections through the TCM with regard to DI&C-ISG-04 as detailed in Section 3.7.3 of this SE.

3.7.2.2 NSR COMMUNICATIONS VIA THE REMOTE RXMS

IOM's Tricon V10 LTR asserted that the safety function is adequately protected when non-safety I/O is connected to the modules in a remote NSR RXM chassis. A remote NSR RXM chassis supports expansion of the safety I/O bus from the SR Primary RXMs via fiber optic cables. Such a connection represents two-way communication (RS-485 on the I/O bus) across the safety to non-safety barrier and adequate protection of the safety function must be demonstrated. Specifically, the upstream (closer to the application processor) SR portion of the I/O bus must be adequately protected from potential faults in the non-safety portion of the I/O bus. The NRC staff performed a detailed design review of the RXM connectivity within the Tricon V10 system, which included information in IOM letter dated August 3, 2010, "Supplementary Information –Selected Topics" (Reference 59, Items 1 and 4), responses to RAI questions 1 and 2 (Reference 8), and information obtained during the December 2010 audit at IOM (Reference 6).

As stated in Section 3.1.2.3 of this SE, the RXMs are connected by fiber optic cables and not electrical cables, and therefore, provide ground loop isolation and immunity against electrostatic and EMI, and they can be used as Class 1E-to-Non-Class 1E isolators between a SR main chassis and a NSR expansion chassis. Therefore, the NRC staff finds that the fiber optic cable between the primary and remote RXMs do provide adequate electrical isolation as required by the above regulations.

The NRC staff also identified several factors that support adequate data isolation protection of the safety function including I/O bus access, I/O bus control scheme and the protection of the safety function of the I/O bus by the interposing processor in the safety side RXM. As previously stated above, the dual port RAM and independent communications processor (IOCCOM) provide the primary protection for the safety processor. The IOCCOM verifies data integrity for all received messages. The I/O bus uses a single threaded master-slave configuration with IOCCOM as the bus master. The SR I/O bus access for NSR I/O data is controlled by an interposing processor in the RXM on the SR side such that no unrequested messages will be allowed onto the SR I/O bus. Further, the redundant Tricon V10 architecture will mitigate any single failures when the data is voted on the Tribus.

The NRC staff determined that the combination of these elements provided adequate protection to the safety side I/O bus and the overall safety function. All data received from a non-safety remote RXM must not be relied upon to perform the required safety function. Further NRC staff review and approval of this bidirectional NSR to SR data communication is provided below in Section 3.7.3. It is an ASAI to verify that adequate isolation is maintained in the application specific design and that no data received from the non-safety I/O is used by the control program to make a safety determination.

3.7.3 STAFF GUIDANCE IN DI&C-ISG-04

The NRC Task Working Group 4, "Highly Integrated Control Rooms-Communications Issues," developed interim NRC Staff Guidance on the review of communications issues applicable to digital safety systems. DI&C-ISG-04 (Reference 29) contains NRC staff positions on three areas of interest: (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations. Evaluation of a safety system against this guidance is an application-specific activity that requires an assessment of a full system design. Since the LTR does not address a specific application or establish a definitive safety system design, the evaluation against this guidance is limited to consideration of the means provided within the platform to specifically address issues related to interactions among safety divisions and between SR equipment and equipment that is not SR. A full safety system design, which is based on the Tricon V10 system, will require further evaluation against this guidance as an ASAI.

In IOM Document No. NTX-SER-09-10, Revision 2, "Compliance With NRC Interim Guidance ISG-2 & ISG-4" (Reference 29), IOM provided a position paper to explain how the Tricon V10 system (platform) design complies with the NRC staff guidance provided in DI&C-ISG-04, Revision 1 - Task Working Group No. 4 “Highly-integrated Control Rooms-Communications Issues.”

3.7.3.1 DI&C-ISG-04, STAFF POSITION 1 - INTERDIVISIONAL COMMUNICATIONS

Staff Position 1 of DI&C-ISG-04 provides guidance on the review of communications, which includes transmission of data and information among components in different electrical safety divisions (or channels) and communications between a safety division and equipment that is not SR. This ISG does not apply to communications within a single division or channel. This NRC staff position states that bidirectional communications among safety divisions and between safety and non-safety equipment may be acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. It goes on to say that systems which include communications among safety divisions and/or bidirectional communications between a safety division and non-safety equipment should adhere to the 20 points described below. The methods by which the Tricon V10 platform either meets these points or provides an acceptable alternative method of complying with NRC regulations are discussed below.

3.7.3.1.1 STAFF POSITION 1, POINT 1

Staff Position 1, Point 1, states that 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. It is recognized that division voting logic must receive inputs from multiple safety divisions.

As described in Section 3.1 of this SE, the Tricon V10 system safety channel is triple redundant from input terminal to output terminal, as shown in Figure 2-2. The triple modular redundant (TMR) architecture (i.e., three separate microprocessors) is intended to allow continued system operation in the presence of any single point of failure within the system. The TMR architecture is also intended to allow the Tricon V10 main processor (MP) to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. In the presence of a fault, the Tricon V10 channel will alarm the condition, remove the affected portion of the faulted module from operation, and continue to function normally in a dual redundant mode. The system returns to the fully triple redundant mode of operation when the affected module is replaced. Each Tricon TMR-channel monitors dedicated sensors allowing bi-stable logic within the Tricon V10 to operate completely independent of other Tricon channels/divisions. As shown in Figure 2-2, the termination panels pass input signals from the field to an input module or pass signals generated by an output module directly to field wiring. The Tricon V10 LTR does not propose any interchannel/interdivisional communications or input from any external systems to perform the Tricon V10 safety function and therefore, each channel is not dependent upon any information or resource originating from outside its own safety division.

As described in Section 3.1.2.1 of the SE, the Tricon V10 main chassis has a key switch that sets the system operating modes between RUN, PROGRAM, STOP, and REMOTE. When the Tricon V10 platform recognizes that the Tricon main processor is in an operational mode other than RUN, data can be provided to a safety channel from sources outside the respective channel (e.g., the TriStation 1131 PC). As described in Section 3.1.3.2 of this SE, plant procedures and administrative controls will restrict using the System Operating Mode keyswitch to change from the standard operational mode without placing the affected channel into bypass or trip.

For configurations involving SR Primary RXM Chassis and non-safety Remote RXM Chassis, the independence requirements of IEEE Std 603 are satisfied through design characteristics as well as administrative controls. As stated in Sections 3.1.2.3 and 3.1.2.4 of this SE, non-safety RXMs can only be configured to communicate with its assigned division/channel. Therefore, NSR remote RXM chassis and modules are typically considered within a division/channel. Nonetheless, since a NSR remote RXM module is physically located outside a SR division/channel Class 1 boundary, its independence from its respective SR RXM is evaluated below.

As stated in Section 3.7.2.2 of this SE, physical independence is maintained as follows:

> The SR Primary RXM Chassis is physically separate from the non-safety Remote RXM Chassis. Multi-mode fiber optic cables connect the SR 4200 Primary RXM modules to the non-safety 4201 Remote RXMs. The combination of physically separate chassis as well as distance between chassis satisfies this criterion.

Electrical independence: The RXM Chassis utilizes dual-redundant power modules, with the capability to utilize both AC and DC site electrical power sources to the chassis. Each RXM Chassis is configured with its own pair of redundant power modules, with SR RXM Chassis powered from site vital electrical power sources, and the non-safety RXM Chassis powered from non-vital sources. The SR Primary RXM Chassis would have redundant, qualified power modules. Furthermore, the multi-mode fiber optic cable interconnection between the SR Primary RXM Chassis and non-safety Remote RXM Chassis provide ground loop isolation and immunity against electrostatic and EMI. This combination of redundant, separate chassis power modules, site electrical sources, and RXM Chassis interconnection with fiber-optic cables meets the requirements for electrical independence.

Data communications independence: The SR Primary RXM 4200 modules provide a gatekeeper function to ensure communication failures on the non-safety Remote RXM do not propagate to the SR portion of the I/O bus. The master-slave CPUs on SR Primary RXMs monitor data messages and enable data transfer to and from the non-safety RXMs only for valid command messages to the downstream non-safety I/O modules. Another layer of protection is provided to ensure data communication independence by the embedded IOCCOM processor on the SR 3008N MP. During a command-response sequence between the IOCCOM and a non-safety I/O module the IOCCOM checks for erroneous (including invalid and unexpected) and corrupted messages, and will time-out the sequence when a packet is delayed and/or missing. The combination of the IOCCOM and the gatekeeper function in the SR Primary RXMs meet the requirements for communications isolation.

As a result of this review and the operational conditions noted above, the NRC staff determined that the Tricon V10 platform system complies with the guidance provided by Staff Position 1, Point 1. However, if a plant application of the Tricon V10 system invokes interchannel communications, then the specific interconnections defined for the plant-specific safety application must be determined and evaluated in a plant-specific review.

3.7.3.1.2 STAFF POSITION 1, POINT 2

Staff Position 1, Point 2, states that 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.

Communications pathways to a safety channel (or division) have the highest potential to produce adverse influences to a safety channel from a safety division (or channel), which is outside the division. As shown in Figure 3.7.3.1.2-1 below, multiple layers of defense are designed into the Tricon V10 system, including the hardware, the software, and the IOM communication protocols themselves.

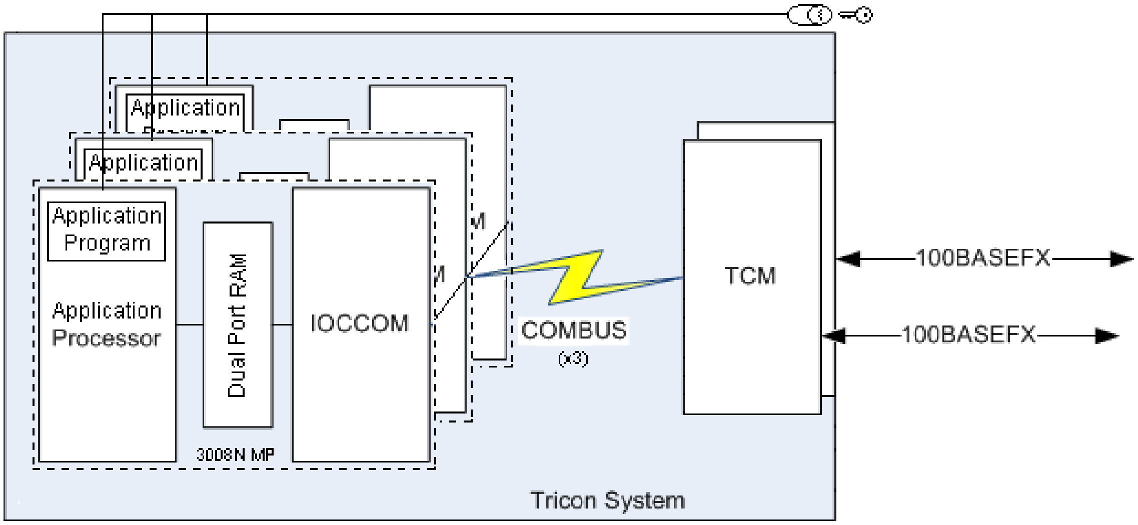


Figure 3.7.3.1.2-1 – Tricon V10 Communication Pathways

The communication path into a Tricon V10 safety channel includes the multi-mode fiber optic cable, the TCM, the triplicated Communication Bus (COMBUS), and the TMR 3008N MPs, which themselves contain the IOCCOM processor, dual-port RAM (DPRAM), and the embedded application processor that executes the control program. The TCM provides functional isolation by handling all the communications with external devices, and it has been qualified under the IOM Appendix B program for nuclear applications. The fiber optic cable prevents propagation of electrical faults into the safety processors. In addition, the TCM has been designed for high-reliability and contributes to the overall reliability of the communication link through the use of CRCs, and testing has demonstrated that it will protect the safety core from network storms and other communication failures. Upon total loss of all TCMs, the safety core will continue to function and execute the application program. Furthermore, the Tricon V10 system has been tested by Wurldtech and it has been shown to be resilient against the communication faults.

The COMBUS is a triplicated, internal communications bus utilizing a master-slave protocol with the TCM configured as the slave. The IOCCOM uses a CRC for integrity checks of COMBUS data. Each MP module contains an IOCCOM processor to handle the data exchange between the embedded application processor and either the I/O modules or the TCM. The IOCCOM processor is scan based, and does not use interrupts. IOCCOM maintains separation for I/O bus and COM message processing, applying checks on both the link-level formatting and CRCs. To ensure adequate execution time for SR I/O, the IOCCOM executes COM messages only while waiting for I/O responses. The application processor and IOCCOM exchange data through the DPRAM buffering system. The application safety processor has higher priority, but the design guarantees that the interface is shared – neither processor can starve the other processor accessing the DPRAM. The application processor assigns highest priority to executing the safety function, and messaging is rate-limited. In addition, the three safety 3008N MPs first vote on the message before acting on any message from the TCM.

Another layer of protection to the safety function (processor) is provided by the communication protocols at the Application Layer of the OSI protocol stack. For all communication links between SR equipment, the P2P and SAP protocols ensure end-to-end integrity of safety-critical messages, and thus do not rely upon the TCM(s) or IOCCOM for message integrity. System architectures requiring data transfer between SR Tricon V10 platforms over a network would use the P2P protocol over an isolated, point-to-point network. Architectures requiring safety-critical data exchanges with other SR devices (e.g., SR VDUs) would utilize the SAP protocol. Both protocols have been developed in accordance with the IOM Quality Assurance program and approved for use in nuclear SR applications (see Section 3.7.1 of this SE). Certain data integrity features are built into the protocols, such as message acknowledgement and negative acknowledgement (ACK/NAK).

The non-safety TriStation 1131 computer will be used to reprogram the application program installed on the Tricon controller(s). During these activities the Tricon is taken out of service with site administrative procedures and by taking the Tricon keyswitch out of the RUN mode. The Tricon keyswitch is a physical interlock that controls the mode of the MPs. It prevents the TCM from accepting “write” messages when placed in the RUN position. The position of the keyswitch is continuously monitored by the TMR MPs, with the MPs voting on the detected position of the keyswitch. The Tricon is designed so that an application program output can be provided to activate an annunciator window in the control room when the keyswitch is not in the RUN position. Furthermore, as described in Section 3.1.3.2 of this SE, plant procedures, and administrative controls will restrict using the System Operating Mode keyswitch to change from the standard operational mode without placing the affected channel into bypass or trip. The TriStation 1131 cannot modify firmware in the Tricon controllers. A separate tool is used to perform firmware upgrades with the Tricon module (e.g., 3008N MP, TCM, I/O module) removed from the chassis. The Tricon controller would have to be taken out of service (keyswitch to STOP) and the module removed from the chassis. These activities would be under site-specific administrative controls and performed in accordance with site-specific procedures.

For configurations involving SR Primary RXM Chassis and non-safety Remote RXM Chassis, Point 2 is satisfied through design characteristics of the Tricon V10 system. As stated in Sections 3.1.2.3 and 3.1.2.4 of this SE, non-safety RXMs can only be configured to communicate with its assigned division/channel. Therefore, NSR remote RXM chassis and modules are typically considered within a division/channel. Nonetheless, since a NSR remote RXM is physically located outside a SR division/channel Class 1 boundary, then the safety function of each safety channel should be protected from adverse influence from NSR RXMs associated with a division/channel.

As described in Point 1 above, physical and electrical separation is inherent in the design of the RXM Chassis. As described in Section 3.1.2.4 of this SE, the purpose of the remote RXM Chassis is to extend the Tricon V10 system I/O bus to locations at distances farther than the standard 9000-series copper cables can handle. Therefore, a non-safety Remote RXM Chassis would be physically separated from the SR Main and Primary RXM Chassis.

As described in the Tricon V10 LTR, the design of the Tricon V10 system RXM's does not allow data exchange between RXM Chassis in different safety divisions or channels. Hence, the Tricon V10 system is not dependent upon data from other safety divisions/channels. Deviations from this design would be a plant-specific configuration that would warrant further NRC review to verify compliance with this Point.

The Primary RXM gatekeeper function (the master CPU) protects the SR segment of the I/O Bus from invalid or erroneous data from the NSR RXMs. The master-slave CPUs on SR Primary RXMs monitor data messages and enable data transfer to and from the non-safety RXMs only for valid command messages to the downstream non-safety I/O modules.

Another layer of protection is provided by the embedded IOCCOM processor on the SR 3008N MP module during a valid command-response sequence between the IOCCOM and a non-safety I/O module. The IOCCOM checks for erroneous (including invalid and unexpected) and corrupted messages, and will time-out the sequence when a packet is delayed and/or missing. The combination of the IOCCOM in the safety main processor (3008N) and the gatekeeper function in the SR Primary RXMs meet the requirements for protection of the safety processor despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

As a result of this review and the design and operational conditions noted above, the NRC staff determined that the Tricon V10 safety system provides protection of the safety function and complies with the guidance provided by Staff Position 1, Point 2.

3.7.3.1.3 STAFF POSITION 1, POINT 3

Staff Position 1, Point 3, states that a safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of “significantly” used in the demonstration.

The design features of the Tricon V10 system as described in the LTR do not include any communications from outside a single channel (i.e., platform) that does not support the safety function. Each Tricon TMR-channel monitors dedicated sensors allowing bistable logic within the Tricon V10 to operate completely independent of other Tricon-channels/divisions. The termination panels pass input signals from the field to an input module or pass signals generated by an output module directly to field wiring. Consequently, the Tricon V10 platform is not overly complex and not subject to failures induced by complexity. The Tricon V10 system does include diagnostic and self-testing features which are built into the platform. However, these features are not dependent upon external inputs, and contribute to the Tricon V10 reliability and availability.

As a result of this review and the Tricon V10 platform design features noted above, the NRC staff determined that the Tricon V10 safety system complies with the guidance provided by Staff

Position 1, Point 3. However, the Tricon V10 system does provide allowances for potential connections between SR Tricon controllers using the P2P protocol, between a SR Tricon controller(s) and a SVDU(s) using the Safety Application Protocol (SAP), or between SR Tricon controllers and non-safety devices (MVDUs, non-safety Tricon controllers, etc.) using a One Way Link (OWL) device as discussed in Sections 3.7.1 and 3.7.2.1 of this SE. Although the P2P and SAP communication protocols have been approved (see Section 3.7.1) for SR application, interdivisional communications between SR Tricon V10 controllers using the P2P, SAP, or communications between SR Tricon V10 controllers and non-safety systems using other protocols would require plant specific analysis to verify compliance with this staff position.

3.7.3.1.4 STAFF POSITION 1, POINT 4

Staff Position 1, Point 4, states that the communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be SR, and must be designed, qualified, fabricated, etc., in accordance with 10 CFR Part 50, Appendices A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

As described in the Triconex Topical Report (Reference 4), all Tricon communication with external devices is conducted and supervised by one or more separate TCMs, which are contained within the Tricon V10 Main Chassis (channel). The TCMs operate asynchronously, sharing information only at end of the application processor scan. When the external device requests data, the communication processor forwards the data from the application processor received at the previous end of scan. When an external device transmits data to the Tricon V10 safety application processor, the communication processor passes the data to the application processor at next end of scan exchange. A simplified view of the Tricon communications system is shown in the Figure 3.7.3.1.4-1 below.

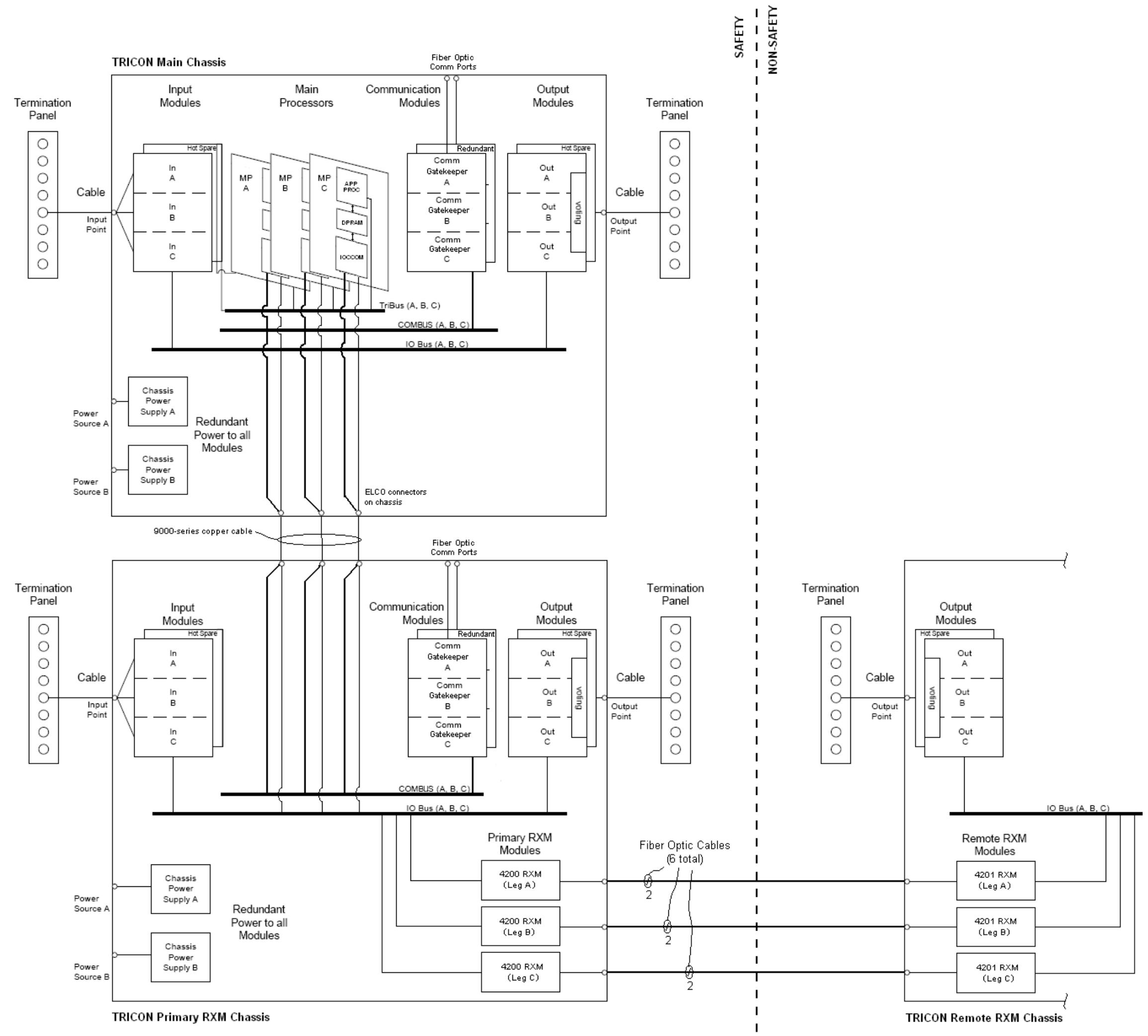


Figure 3.7.3.1.4-1 – Tricon V10 Communications

The TCM provides functional isolation by handling all the communications with external devices that may be connected to other divisions, and it has been qualified under the IOM Appendix B program for nuclear applications. A fiber optic cable is used between the TCM and external devices to prevent propagation of electrical faults into the safety processors. In addition, the TCM has been designed for high reliability and contributes to the overall reliability of the communication link through the use of Cyclic Redundancy Checks (CRCs). Testing has demonstrated that the TCM will protect the safety core from network storms and other communication failures (see Staff Position 1, Point 12). Upon total loss of all TCMs, the safety core will continue to function.

The internal communication path for external devices to and from the Tricon V10 platform is via the TCM, to the triplicated Communication Bus (COMBUS), and the TMR 3008N MPs (all are safety related and contained within the SR Main Chassis). The MPs contain the IOCCOM processor, dual-port RAM (DPRAM), and the embedded application processors that execute the safety control program. Valid messages received by the TCM are triplicated for transmission on the COMBUS and then to the IOCCOM, which is running at its own scan rate without the use of interrupts. The IOCCOM processor retrieves data from the DPRAM to send to either the I/O modules or the TCM, or deposits I/O data or communications (COM) messages into the

DPRAM for use by the application processor. Separate queues are provided in the IOCCOM for I/O Bus and COM messages. To ensure adequate execution time for SR I/O, the IOCCOM executes COM messages from the TCM only while waiting for I/O responses. The IOCCOM checks the link-level format and the CRC of all messages from the TCM. If the IOCCOM determines that the message is valid and correct, the data is placed into DPRAM.

Both the application processor and IOCCOM exchange data through the DPRAM. The application processor has higher priority, but the design is such that the interface is equally shared (i.e., neither processor can starve the other processor accessing the DPRAM). As with the IOCCOM, the DPRAM provides separate memory areas and queues for communication messages and I/O data. These “bins” are separated according to input, output, read-only, read-write, and data type (i.e., Boolean, Reals, Integers). The DPRAM includes extensive memory protection via parity checks, CRCs, checksum, and other mechanisms.

As stated previously, the application processor assigns highest priority to executing the safety function, and messaging is rate-limited. The three 3008N MPs vote on the message before acting on any message from the TCM. Conversely, the TCM votes on the messages from the three 3008N MPs and sends a single copy to an external device if two out of three messages agree.

The embedded application processor, IOCCOM, and TCM each runs its own scan loop (see Figure 2-6 in Section 3.1.3.1 of this SE). The embedded application processor and IOCCOM are synchronized to facilitate exchange of data through the DPRAM. The main scan loop (“ETSX”) of the embedded application processor consists of three tasks:

1) Scan Task,
2) Communication Task, and
3) Background Task.

The Scan Task sequence is essentially:

Input data from DPRAM and vote → Process control program → Send outputs to DPRAM.

The Communication Task is run after the Scan Task during the “Scan Surplus” period. The embedded application processor and the IOCCOM scan loops are synchronized such that during the Communication Task the IOCCOM deposits I/O and communications messages into the DPRAM for use by the embedded application processor at the beginning of the next Scan Task. The IOCCOM scan loop (“IOC loop”) gives priority to I/O data exchanges. During the IOC loop when the IOCCOM is waiting for responses from the I/O modules, scan time is allotted for COM messaging via the COMBUS.

As described in Sections 3.1.2.4 and 3.7.1.2 of this SE, another means of communications within a channel or division is via the remote RXMs. Communications data via the remote RXMs can be either SR or NSR data. NTX-SER-09-10, Section 2, “V10 Tricon Chassis Configurations,” and Section 3.2, “V10 Tricon Communications – Safety-to-Non-safety Communications,” propose safety-to-non-safety Tricon V10 architectures utilizing non-safety Remote Extender Chassis. Communications via the RXMs is accomplished as follows: The primary RXMs are qualified as Class 1E equipment. The remote RXMs are also qualified as Class 1E equipment, but may be used to transmit non-safety data to the primary RXMs and therefore must be evaluated as NSR equipment. Although the remote RXMs are qualified equipment, the connection of non-safety related I/O or use of non-1E power forces a NSR designation for the entire remote chassis. The following paragraphs describe how the Tricon V10 works to provide adequate protection between a SR primary RXM and a remote RXM in a NSR chassis.

The SR primary RXM contains two on-board microprocessors (CPUs) in a master-slave configuration. The master CPU monitors all messages coming from, and is directly polled by, the SR 3008N MP. The master CPU is responsible for the on-board diagnostics. It monitors the I/O bus for messages intended for the remote RXM in the NSR chassis, and provides the required responses. The slave CPU monitors all messages coming from the I/O modules (i.e., response messages from the remote RXMs). The slave CPU provides updated information to the master CPU regarding active I/O modules in its downstream path (e.g., in the non-safety RXM Chassis). Any errors the slave CPU detects are also passed to the master CPU. Together the master and slave CPUs enable/disable the communication multiplexer on the RXMs.

In normal mode, whenever the master CPU detects that the chassis number embedded in a valid command from the SR 3008N MP is addressed to an I/O module in its downstream leg, it will enable the communication multiplexer. Otherwise, it will be disabled. Therefore, noise and erroneous messages received by the SR Primary RXM while the communication multiplexer is disabled will not be passed to the SR IOCCOM on the SR 3008N MP. Consequently, the normal operation of the SR 3008N MP is protected from faults and/or noise from the non-safety Remote RXM and non-safety I/O modules. The I/O Bus is composed of separate command and response buses, which are fiber optic cables that are used between the SR primary RXM and NSR Remote RXMs to prevent propagation of electrical faults into the safety processors. Commands from the SR IOCCOM on the SR 3008N MP are sent over a separate path than the responses from the I/O modules. This separation of commands and responses at the hardware level ensures that I/O modules (I/O Bus slaves) respond only to valid commands from the IOCCOM via the SR Primary RXM.

The internal communication path for the primary RXM to and from the Tricon V10 safety function processor is via the triplicated I/O bus, then to the IOCCOM processor, and then to the DPRAM. As described for the TCM processors, communications between the safety function processor and the IOCOOM is via the DPRAM.

The NRC staff has reviewed the design and functionality of the communications process and the hardware and software used to implement this process, and has determined that the Tricon V10 system complies with Staff Position 1, Point 4.

3.7.3.1.5 <u>STAFF POSITION 1, POINT 5</u>

Staff Position 1, Point 5, states that the cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.

Staff Position 1, Point 4, and Section 3.1.3.1 of this SE describe the scan loop for the Tricon V10 controller. To summarize, the TMR 3008N MPs and TCM exchange messages asynchronously over the triplicated COMBUS. On board each 3008N MP, the embedded application processor and IOCCOM processor exchange data via a DPRAM. The application processor has higher priority for accessing the DPRAM. Data is deposited into DPRAM at the end of the embedded application processor Scan Task, which the IOCCOM processor retrieves during its own scan loop (synchronized with the embedded application processor scan loop). During surplus scan time, the Communication Task is run and the embedded application processor retrieves messages from the DPRAM in preparation for the next Scan Task. Priority is given to the application program and I/O data exchanges, with communication message exchanges with the TCM via the COMBUS occurring between scans.

As described in the IOM ISG-04 Position Paper (Reference 29) all data is exchanged at each End-of-Scan, therefore, communication message exchanges may require multiple scans to satisfy a host device (such as a Tricon, SVDU, or other device on the DCS) read or write communication function. Additional time (at least two scan loops) is required for a sending Tricon controller to get an acknowledgment from the receiving Tricon controller that the message has been received and processed. In fact, most messages from an external system require voting by the TMR 3008N MPs. Thus, typical message response times require three or more scans to complete – one scan to send and two scans for the response.

The IOM protocols used for safety-critical communications, P2P and SAP, are discussed in Staff Position 1, Points 1 and 2 above. The SAP and P2P protocols are responsible for the end-to-end integrity of safety-critical communications, and thus will be implemented during plant-specific application software development. Because of the additional functions these protocols specify at the Application Layer to protect communications, P2P and SAP will place a burden on the application processor and therefore extend the Tricon controller cycle time.

The Tricon V10 platform continuously monitors system functionality and performance, activating an alarm should scan time exceed the predicted performance. IOM Document No. 9600164-731 (Reference 43), “Maximum Response Time Calculation,” provides formulas to estimate the maximum response time for the various I/O module types. Application specific safety systems using the Tricon V10 platform will utilize the formulas and built-in features in the development of the SR application program. Also, thorough program operational testing will need to be conducted to determine the longest scan-time duration. The cycle times resulting from all these data processing activities will need to be calculated and compared to a plant's safety analysis to ensure safety-critical timing requirements are met. The Tricon V10 LTR did not provide a specific cycle time for the platform itself. In light of this evaluation, Staff Position 1, Point 5, cannot be assessed for the Tricon V10 platform and must be evaluated as an application specific review for a plant specific application.

3.7.3.1.6 STAFF POSITION 1, POINT 6

Staff Position 1, Point 6, states that the safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

For the Tricon V10 controller, the 3008N MP acts as the safety function processor in a Triple-Modular-Redundant configuration. Staff Position 1, Point 1, explains that Tricon V10 controllers are qualified TMR systems and are not dependent upon interdivisional communications or external systems to perform the safety function. This includes interrupts from external systems. The TMR 3008N MP application processors are isolated from data communications by the TCM. One or more TCM(s) act as the communication processor(s) to handle all communication protocol requirements (i.e., handshaking, start, stop bits). Also, the

TMR 3008N MP application processors are isolated from non-safety I/O data communications by the combination of the DPRAM, the IOCCOM, and the SR Primary RXM. There is no handshaking on the I/O bus.

The NRC staff review of the communications protocols associated with the communications used by the Tricon V10 platform does use communications handshaking, but this handshaking is done by the TCM communications modules. However, the safety function processor contained within the TRM 3008N MP communicates externally using only the dual-ported memory, and this process does not use handshaking or interrupts as described in Sections 3.1.2.7 and 3.7.1 of this SE. The NRC staff has reviewed the use of communications handshaking, and has determined that since all handshaking during system operations is done by the communications processor, and not by the safety function processor, the Tricon V10 platform complies with Staff Position 1, Point 6.

3.7.3.1.7 STAFF POSITION 1, POINT 7

Staff Position 1, Point 7, states that only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, and data bits, in the same locations in every message. Every datum should be included in every transmit cycle, regardless of whether it has changed since the previous transmission, to ensure deterministic system behavior.

All communications with external devices including remote RXMs are limited to Tricon-compatible protocols, as described in Section 3.0, of the Tricon V10 Compliance with ISG-02 & 04 document. Each protocol is well-defined and ordered, i.e. number of start and stop bits, timing, data frame format, number of data fields and check sum or Cyclic Redundancy Check (CRC) field. Should an error occur, the communication processor rejects the message. The message length may vary, however, as an external device may request a different number of data points within each request.

Extensive testing was performed by an independent third-party (Wurldtech) to validate the robustness of the Tricon V10 against communication failures. The Tricon V10 passed tests to verify the robustness of the TCM to various communication failures, such as proper handling of rogue and invalid protocol packets, and continued operation under network storm conditions without adverse impact on the TMR 3008N MP control algorithm. Ethernet, ARP, IP, ICMP, TCP, and UDP protocols were tested. The test configuration included monitoring of digital output signals to confirm that the Tricon application program running on the TMR 3008N MPs was unperturbed. Testing validated that the TCM will discard rogue, invalid, and excessive Ethernet packets (such as during data storms), thereby ensuring the operation of the TMR 3008N MPs was unperturbed during communication failures.

Communication between the 3008N MP and the remote RXMs via an I/O module uses a serial, asynchronous, RS485 master-slave protocol at 375 Kbps. The format of I/O message commands is fixed. The master and slave CPU's on the RXM ensure the messages are properly formatted and are valid command messages (e.g., chassis number, leg number, and slot number, correct CRC) so that there is an expected corresponding response message for every command message. Also, the IOCCOM processor performs a validity check before processing the response message (i.e., forwarding the I/O response data to the DPRAM on the 3008N MP for the embedded application processor to retrieve). Corrupted and improperly addressed messages will be ignored by the IOCCOM and I/O modules.

Based on this information, the NRC staff has determined that the Tricon V10 platform complies with Staff Position 1, Point 7.

3.7.3.1.8 STAFF POSITION 1, POINT 8

Staff Position 1, Point 8, states that data exchanged between redundant safety divisions or between safety and non-safety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

As described above in Sections 3.7.1, 3.7.2, and Staff Position 1, Point 2, above for data exchanged between redundant safety divisions and for data exchanged between safety and non-safety portions of the Tricon V10 platform, all data exchanges are done using an interposing communications processor, and the safety function processor processes this data as part of the standard software loop. The Tricon V10 LTR indicates that there will be no data exchange between RXM Chassis in different safety divisions or trains. For this reason, the NRC staff has determined that the data exchange within the Tricon V10 platform complies with Staff Position 1, Point 8.

3.7.3.1.9 STAFF POSITION 1, POINT 9

Staff Position 1, Point 9, states that 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.

As described in Staff Position 1, Point 4, the internal communication path for external devices to and from the Tricon V10 platform is via the TCM and/or RXMs, to the triplicated Communication Bus (COMBUS) and/or I/O bus, and to the TMR 3008N MPs (all are safety related and contained within the SR Main Chassis). The SR 3008N MP contains an application processor, DPRAM, and IOCCOM processor. The application processor executes the SR application program. The IOCCOM handles interactions with the TCM via the COMBUS and the I/O subsystem via the I/O Bus, utilizing dedicated memory locations for communications and I/O data. All communications between the safety function processor and the IOCCOM and/or the RXMs are via the DPRAM. Data received by the Tricon V10 is stored in fixed "aliased" memory locations (an *alias* is a unique identifying integer value, which is automatically assigned by the TriStation 1131 application programming tool to input, output, and system variables), which are utilized by the application processor when computing application logic. Input data is segregated from output data within memory. The DPRAM provides separate memory areas and queues for communication messages and I/O data. The communications processor uses physically different areas (or bins) of the DPRAM for receiving and sending data. The memory locations used for each message is determined at the time of program compilation. The DPRAM includes extensive memory protection via parity checks, CRCs, checksum, and other mechanisms. For these reasons, the NRC staff has determined that the dual-ported memory usage, in terms of separate areas for input and output data and for fixed memory usage within the Tricon V10 platform complies with Staff Position 1, Point 9.

3.7.3.1.10 STAFF POSITION 1, POINT 10

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

A non-safety computer is used to upgrade module firmware and/or reprogram the application program installed on the Tricon V10 controller(s). During these activities the Tricon is taken out of service with site administrative procedures and by taking the Tricon keyswitch out of the RUN mode. The Tricon keyswitch is a physical interlock that controls the mode of the 3008N MPs. It prevents the 3008N MPs from accepting “write” messages when placed in the RUN position. This keyswitch is described in Section 3.3.1.3 of IOM Document No. NTX-SER-10-14, “Tricon V10 Conformance to Regulatory Guide 1.152” (Reference 35). It describes the physical protection of the embedded firmware and the process that must be followed to update the software. The keyswitch is implemented by a three-gang, four-position switch. Each of the gangs is connected to one of the 3008N MPs. The values are read by each of the 3008N MPs as a two bit software value. The position of the keyswitch is continuously monitored by the TMR MPs, with the MPs voting on the detected position of the keyswitch. The Tricon is designed so that an application program output can be provided to activate an annunciator window in the control room when the Tricon keyswitch is not in the RUN position. The application program has access to the voted keyswitch position through specialized function blocks. These specialized function blocks allow monitoring (i.e., read-only capability) of a system variable for the voted keyswitch position. The application can be programmed to perform any required action on a change of the keyswitch position. However, this would be an application specific feature that is beyond the scope of this review. During firmware updates of the Tricon controllers the Tricon module (e.g., 3008N MP, TCM, I/O module) is removed from the chassis. The Tricon controller would have to be taken out of service (keyswitch to STOP) and the module removed from the chassis. These activities would be under site-specific administrative controls and performed in accordance with site-specific procedures.

The keyswitch design mitigates against any single hardware fault. If one of the gangs on the switch goes bad or an input to a 3008N MP fails (e.g., a single bit flip), the error would affect only the 3008N MP that is attached to the failed gang. The other two 3008N MPs would continue to receive good inputs values and out vote the 3008N MP with the bad input. This protects against any single fault in the physical keyswitch or on the 3008N MP. Section 3.1.2 of this SE discusses other administrative control options that may be invoked to ensure on-line changes to safety system software are prevented.

The I/O subsystem, which includes the RXM Chassis, cannot be modified during run time. There is no interface with the operator or TriSation 1131 user that would allow modification of the RXM firmware during run time. Modification or update of RXM firmware requires 1) removal of the RXM from the RXM Chassis, and 2) special tools to interface directly with the single RXM; IOM neither provides nor sells these tools to its customers.

However, the Tricon V10 keyswitch does not provide a physical disconnect or interruption of the connection by means of hardwired logic as required by ISG 4, Staff Position 1, Point 10, but instead sets 2 bits within the software to change the operating mode of the Tricon. Therefore, the Tricon V10 relies on software to effect the disconnection of the TriStation capability to modify the safety system software, a condition specifically stated as not acceptable in this ISG staff position. Based on the information provided in the LTR, the NRC staff determined that the Tricon V10 platform does not meet the NRC staff guidance provided in Staff Position 1, Point 10.

In order for the NRC staff to accept this keyswitch function as compliant with this Staff Position, the NRC staff will have to evaluate an application specific system communications control configuration--including the operation of the keyswitch, the software affected by the keyswitch, and any testing performed on failures of the hardware and software associated with the keyswitch. This is an ASAI associated with the implementation of this keyswitch.

3.7.3.1.11 STAFF POSITION 1, POINT 11

Staff Position 1, Point 11, states that provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.

As discussed in Sections 2.2, 3.2.1, and 3.1 of this SE, the Tricon V10 platform is a qualified TMR system and is not dependent upon interdivisional communications or external systems to perform the safety function. P2P and SAP communication protocols are utilized for safety-critical communications between the SR Tricon V10 controller and other Tricon controllers or SR systems. However, the Tricon P2P and SAP messages support data exchange only. There are no “flow-of-control” message functions in the P2P or SAP protocols.

Moreover, the RXM Chassis provides no means to send software instructions to the SR 3008N MP. The RXM Chassis only provides the capability to handle I/O at remote locations. The I/O Bus protocol is a single-threaded, command-response serial protocol for transferring I/O data as well as I/O module status. By design, software commands allowing remote control of the SR 3008N MP from the RXM Chassis is not possible. Firmware changes are performed while the RXMs are removed from the chassis. Any modifications to the I/O subsystem configuration, such as adding or deleting an I/O module(s) or changing to a different model I/O module, would be a significant hardware change to the Tricon system and could not be performed on line.

Also, the design of the RXMs does not enable data exchanges between RXM Chassis in different safety divisions or channels.

As discussed in Sections 3.1.2.1 and 3.1.3.2 of this SE, with the Tricon Operational Mode Change keyswitch in RUN, each Tricon V10 is independent of other channels/divisions. Any architecture in which one division relies upon data from another division would be site-specific and thus would warrant plant-specific reviews by the NRC staff. The Tricon V10 system Operational Mode Change keyswitch does change operational modes of the 3008N MPs and enables the TriStation 1131 PC to change parameters, software algorithms, etc, related to the application program of the safety channel without the channel or division being in bypass or in trip. As stated in Section 3.1.3.2 of the SE, the TriStation 1131 PC should not normally be connected while the Tricon V10 is operational and performing safety critical functions. However, it is physically possible for the TriStation PC to be connected at all times, and this should be strictly controlled via administrative controls (e.g., place the respective channel out of service while changing the software, parameters, etc). Furthermore, in order to leave the non-safety TriStation 1131 PC attached to the SR Tricon V10 system while the key switch is in the RUN position, a detailed FMEA of the TriStation 1131 PC system will be required to ascertain the potential effects that this non-safety PC may have on the execution of the safety application program/operability of the channel or division. This would be evaluated on an application specific basis.

Based on the design of the Tricon V10 platform as evaluated above and strict administrative controls (as indicated above) over the use of these keys switches the NRC staff has determined that the Tricon V10 platform does comply with Staff Position 1, Point 11.

3.7.3.1.12 STAFF POSITION 1, POINT 12

Staff Position 1, Point 12, states that communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute “single failures” as described in the single failure criterion of 10 CFR Part 50, Appendix A. This section provides 12 examples of credible communication faults, but cautions that the possible communication faults are not limited to the list of 12.

As discussed in Points 2 and 4 above, electrical and functional isolation of the 3008N MPs are provided by the TCM, which has a reliable design, and includes several engineered layers of protection against communication failures. As stated previously, the SR TCM handles all external communications, and thus serves as an isolation or buffer for the TMR 3008N MPs from communications data. Also, as described in Section 3.1.2.8 of this SE, the Tricon communication P2P and SAP protocols provide end-to-end integrity checks of all communications data. The design and operation of the Tricon V10 is intended to prevent communication faults from altering the application program or its performance.

In conjunction with these platform design features, testing was performed by an independent third-party (Wurldtech) to validate the robustness of the Tricon V10 platform against communication failures. Wurldtech performed testing of a number of scenarios testing the communications link in the presence of a communications failure. This testing is discussed in this SE Section 3.8.1.2, and is documented in Appendix A of IOM Document No. NTX-SER-10-14 (Reference 35). This report and the data it contains is proprietary, and will not be discussed in this SE. However, in summary this testing verified the effectiveness of the TCM to cope with various communication failures, such as proper handling of rogue and invalid protocol packets, and continued operation under network storm conditions without adverse impact on the TMR 3008N MP control algorithm. Ethernet, ARP, IP, ICMP, TCP, and UDP protocols were tested. The test configuration included monitoring of digital output signals to confirm that the Tricon application program running on the TMR 3008N MPs was unperturbed. This testing validated that the TCM will discard rogue, invalid, and excessive Ethernet packets (such as during data storms), thereby ensuring the operation of the TMR 3008N MPs was unperturbed during communication failures. The results of the Wurldtech testing validated the added reliability that the TCM provides to the communication link. Furthermore, as discussed in the IOM Document No. NTX-SER-09-10, Revision 2, “Compliance with NRC Interim Guidance ISG-2 & ISG-4,” the P2P and SAP communications protocol design further enhances mitigation of communication faults, including those enumerated in the Staff Position, Point 12. Also, communications data faults emanating from non-safety remote RXMs are mitigated by the data validation features of the master and slave CPUs within the SR primary RXMs and the IOCCOM processor in the MPs.

Based on the robust design of the Tricon V10 platform to mitigate or eliminate communications data errors, and the NRC staff's review of the Wurldtech report (as discussed in Section 3.8.3.1 of this SE) allowed the NRC staff to determine that communications faults, including the 12 examples contained in Staff Position 1, Point 12, will not adversely affect the performance of the required safety functions, and that the Tricon V10 platform complies with Staff Position 1, Point 12.

3.7.3.1.13 STAFF POSITION 1, POINT 13

Staff Position 1, Point 13, states that vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are properly 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.

As discussed in Section 3.1.1 of this SE, each Tricon TMR-channel monitors dedicated sensors allowing bi-stable logic within the Tricon V10 to operate completely independent of other Tricon-channels/divisions. As shown in Figure 2-2, the termination panels pass input signals from the field to an input module or pass signals generated by an output module directly to field wiring. The Tricon V10 LTR does not propose any interchannel/interdivisional communications or input from any external systems to perform the Tricon V10 safety function and therefore, each channel is not dependent upon any information or resource originating from outside its own safety division.

Staff Position 1 Point 1 explains how each Tricon V10 is self-contained. Architectures involving vital communications between channels or divisions, such as for voting trip decisions, are supported using the P2P and SAP SR communication protocols, as explained in Section 3.7.1 of this SE. However, such architectures would be site-specific, and would require staff review and approval on an application specific basis. Also, there are no data exchanges between RXM Chassis in different safety divisions or trains. Furthermore, non-safety Remote RXM Chassis will not be utilized for vital communications.

The NRC staff reviewed the Tricon V10 system as described above and in the LTR and determined that this configuration of the Tricon V10 platform complies with Staff Position 1, Point 13.

3.7.3.1.14 STAFF POSITION 1, POINT 14

Staff Position 1, Point 14, states that vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.

As discussed in Section 3.1.1 of this SE, each Tricon TMR-channel monitors dedicated sensors allowing bi-stable logic within the Tricon V10 to operate completely independent of other Tricon-channels/divisions. The Tricon V10 system is triple redundant from input terminal to output terminal. Figure 2-2 shows the arrangement of the input, main processor, and output modules. The termination panels pass vital input signals directly from the field to an input module or pass signals generated by an output module directly to field wiring. Each input and output module includes three separate and independent input or output circuits or legs. These input/output legs communicate independently in a point-to point manner with the three main processor modules. The Tricon V10 LTR does not propose any interchannel/interdivisional communications or input from any external systems to perform the Tricon V10 safety function and therefore, each channel is not dependent upon any information or resource originating from outside its own safety division. As described in Section 3.8.1.2 of this SE, the LTR and IOM Document No. NTX-SER-10-14 (Reference 35) credit the triplicated communications busses (I/O and COMBUS) as being physically separate. The communications processors (IOCCOM) are autonomous and separate from the safety function (application) processors. Communications between the safety function processor and its IOCCOM is point-to-point using a half-duplex master-slave protocol. IOCCOM is scan based with no interrupts and gives priority to safety I/O communications by design. CRC checks are performed on all data received by IOCCOM through both I/O and COMBUS paths. The Tricon V10 system utilizes point-to-point routed network communications protocol and media, copper and fiber optic cables to communicate data externally. All external communications uses a two-point network, where there is no equipment other than the sending and receiving nodes on the network. All communication protocols for vital communications (i.e., communications that are needed to support a safety function) support redundant communication links. Additionally, there is no data exchange between Remote RXM Chassis in different safety divisions or trains, and non-safety Remote RXM Chassis are not be utilized for vital communications.

The NRC staff has reviewed this information and has determined that the Tricon V10 platform as described above and in the V10 LTR complies with Staff Position 1, Point 14, for point-to-point communications.

3.7.3.1.15 STAFF POSITION 1, POINT 15

Staff Position 1, Point 15, states that communications for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

As described above in Sections 3.1.3.1 and 3.7.3.1.7 of this SE, communications for safety functions have predefined data sets and therefore, communicate a fixed set of data. This data is sent every scan cycle and at regular intervals, whether data in the set has changed or not. NTX-SER-09-10 Section 5.0 discusses the Tricon scan cycle in detail. In summary, at least once every Scan Task the I/O input data is retrieved and I/O data sets are sent to the I/O modules. The I/O Bus message formats are fixed (though data length can vary depending upon the valid command-response sequence).

Communications to external SR applications are limited to Tricon V10-compatible protocols. Each protocol is well-defined and ordered (e.g., number of start and stop bits, timing, data frame format, number of data fields and check sum or CRC field). If an error were to occur, the communication processor would reject the message. Again, message length may vary because an external device may request a different number of data points within each request. Based on this information, the NRC staff has determined that the communications data set and transmission intervals as used in the Tricon V10 platform complies with Staff Position 1, Point 15.

3.7.3.1.16 STAFF POSITION 1, POINT 16

Staff Position 1, Point 16, states that 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, GDC 24, which states, “interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired,” and (2) IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” (Source: NUREG/CR-6082, Section 3.4.3)].

As described in Staff Position 1, Point 1, the Tricon V10 LTR does not propose any interchannel/interdivisional communications or input from any external systems to perform the Tricon V10 safety function and therefore, each channel is not dependent upon any information or resource originating from outside its own safety division. Also, the independence of the Tricon V10 controllers from external devices discussed in Staff Position 1, Points 1 and 2 describe the independence of Tricon V10 controllers from external devices, which includes engineered layers of protection against communication failures. The TCM has been qualified under IOM Appendix B program, and it provides functional and electrical isolation for the TMR 3008N MP safety processors.

As discussed in Section 3.1.2.8 of this SE, the P2P and SAP communications protocols are used for communications of safety critical data between other Tricon platforms and SVDU respectively. End-to-end integrity checking of SR communications links is provided through the use of validation bits and timing within the message, so that the receiving Tricon or SVDU, as appropriate, is “aware” that the messages are current and not static. If the messages are detected to be static, lost, or significantly delayed, the receiving Tricon/SVDU activates an alarm. In the case of a receiving SR Tricon, it will assume the “fail-safe” status of the transmitting Tricon.

The I/O Bus is an "internal system" bus based on RS485. The I/O Bus protocol is single-threaded master-slave serial protocol. By design, one command message is sent from the SR IOCCOM at a time and no other command messages are sent until a valid response from the non-safety I/O module is received, or the message thread times out. Also, every Scan Task, the SR IOCCOM polls a given I/O module at most once every 10 msec. Based upon this information, the NRC staff has determined that the Tricon V10 platform meets the guidance provided by Staff Position 1, Point 16, for network connectivity.

3.7.3.1.17 STAFF POSITION 1, POINT 17

Staff Position 1, Point 17, states that pursuant to 10 CFR 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

The environmental qualification for the Tricon V10 platform is described in the Section 3.3 of this SE. The generic qualification of the Tricon V10 encompasses both the hardware and the software used in the system. The hardware includes termination assemblies, signal conditioners, chassis, power supplies, main processor modules, communication modules, input/output modules, termination assemblies, module interconnecting cables, and Class 1E to Non-Class 1E module Isolation devices. The Tricon V10 platform was qualified in accordance with the EPRI TR-107330 requirements. The medium used for vital communications within the platform was a part of each of the systems qualified and is therefore qualified as described.

The Tricon V10 platform was tested for EMI and RFI to demonstrate its qualification as a SR device with respect to EMI/RFI emissions and susceptibility. The platform was also subjected to Electrical Fast Transient (EFT) and Surge Withstand testing to demonstrate its qualification as a SR device with respect to susceptibility to repetitive EFTs on the power and signal input/output leads, and AC power and signal line electrical surge withstand capability. The NRC staff approved this qualification testing within the qualification limits noted in Section 3.3 of this SE.

However, as noted in Section 3.3.1 of this SE, the qualification of the Tricon V10 does not include the fiber optic cables used to connect external devices to the safety application processor via the TCM or the RXMs. Therefore, an application specific evaluation will be required for plant specific applications of the Tricon V10 system utilizing fiber optic cables to connect external devices to the Tricon V10 platform.

The NRC staff has determined that the Tricon V10 platform meets the guidance provided by Staff Position 1, Point 17. However, as noted above, fiber optic cables used to implement the Tricon V10 system in safety applications will require application specific review to verify these cables are qualified for the environment in which they will be used, in accordance with 10 CFR 50.49 as applicable.

3.7.3.1.18 STAFF POSITION 1, POINT 18

Staff Position 1, Point 18, states that provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

IOM performed a FMEA on the Tricon V10 system in accordance with the applicable requirements of EPRI TR-107330 Section 6.4.1. In general, the techniques of ANSI/IEEE Std 352-1987 were used in the analysis. The results of the FMEA are documented in IOM Document No. 9600164-531, “Failure Modes and Effects Analysis for the Tricon Version 10.2 Programmable Logic Controller” (Reference 28). The FMEA addresses failures of major components and at the module level. The approach was appropriate because sub-components in the Tricon modules are triple-redundant, and no single failure of an individual subcomponent can impact the ability of the Tricon to perform its SR functions.

To summarize, the Tricon Communication Module (TCM) handles all communications protocol, start/stop bits, handshaking, etc. tasks. The 3008M MPs are neither burdened nor interrupted by communications faults. Communication errors and malfunctions do not interfere with the execution of the safety function. Exchange of data between the communication processors and MPs occur once each MP scan cycle. Because all the communication with external devices, systems, and hosts is performed by and localized in the TCM, the 3008N MPs are alleviated of unneeded communications functionality and attendant complications due to complexity. This mitigates any deficiencies in the TCM with regard to performance deficits posed by unneeded functionality.

The I/O Bus is an internal system bus based on RS485. The I/O Bus protocol is single-threaded master-slave serial protocol. By design one command message is sent from the SR IOCCOM, and no other is sent until a valid response from the non-safety I/O module is received, or the data thread times out. Also, every Scan Task, the SR IOCCOM polls a given I/O module at most once every 10 msec. The RXMs are relatively simple modules, because they simply act as I/O Bus repeaters with gatekeeper functionality implemented within the RXM processors.

This analysis included potential failures of communications used within the Tricon V10 system. The NRC staff reviewed and concurred with this FMEA in Section 3.5 of this SE. In addition, the Tricon self-diagnostic features have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate that the diagnostics detect all possible single failures within each module.

IOM also provide a FMEA for the non-safety Remote RXM chassis in Table 3 of NTX-SER-09-10, Revision 2, which is considered an extension of the Tricon V10 FMEA discussed in Section 3.5 of this SE. This assessment identified the mechanisms that could cause the failure modes, and evaluated the consequences of the failures on the operation of the SR portion of the configuration (i.e., SR 3008N MPs, Primary RXM chassis, and I/O modules). Because of the architecture of the Tricon, failure mechanisms that affect a single leg of the triple redundant system generally have no effect on system operation. Therefore, the FMEA considered (1) failure mechanisms that are recognized as being highly unlikely but that could affect multiple components, and (2) the coincident occurrence of otherwise single failures (i.e., multiple failures). Multiple-failure scenarios include failures of all three non-safety Remote RXMs due to software common mode failure, loss of all power, fire, floods, or missiles. These types of multiple-failure scenarios are recognized as being very unlikely, but were included to describe system behavior in the presence of severe failures. Congestion is not a concern, because the I/O Bus is a closed system utilizing a single-threaded master-slave serial protocol based on RS485. By design one command message is sent from the SR IOCCOM and no other messages are sent until a valid response from the non-safety I/O module is received, or the message thread times out. Also, the SR IOCCOM polls a given I/O module at most once every 10 msec. Therefore, data rates are strictly defined and controlled.

The NRC staff determined that these failure modes and effects analyses for the Tricon V10 system meet the guidance provided in Staff Position 1, Point 18.

3.7.3.1.19 STAFF POSITION 1, POINT 19

Staff Position 1, Point 19, states that the communications data rates be such that they will not exceed the capacity of a communications link or the ability of nodes to handle traffic, and that all links and nodes have sufficient capacity to support all functions. To do this, the applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions and that communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

Communications within the Tricon V10 platform is cyclic in nature as described in Sections 3.1.3.1 and 3.7.3.1.4 of this SE. The Communication task runs every 10 msec or when a communication port interrupt occurs. Factors which affect the platform communications performance include: COMBUS speed; the amount of aliased data and scan time; network speed and loading; and the particular communication protocol being used. The COMBUS speed determines the speed at which data is communicated between the 3008N MPs and TCMs. If the amount of aliased data updated by the 3008N MPs is too large for a single scan, then it may take several scans to update the aliased data stored in the TCMs. Network communication speeds with the TCM is 100 megabits-per-second, which means that it is highly unlikely that data transfer between the TCM and remote safety applications will be affected by the physical network. In the event that the 3008N MPs are excessively burdened with data requests, the Tricon continuously monitors system functions and performance, activating an alarm should scan time exceed the predicted performance. Also, as discussed in Sections 3.1.2.9 and 3.7.3.1.7 of this SE, extensive testing was performed by an independent third-party (Wurldtech) to validate the robustness of the Tricon V10 platform against communication failures. The Tricon V10 platform was tested to verify the robustness of the TCM to various communication failures, such as proper handling of rogue and invalid protocol packets, and continued operation under network storm conditions without adverse impact on the TMR 3008N MP control algorithm. Ethernet, ARP, IP, ICMP, TCP, and UDP protocols were tested. The test configuration included monitoring of digital output signals to confirm that the Tricon application program running on the TMR 3008N MPs was unperturbed. Testing validated that the TCM will discard rogue, invalid, and excessive Ethernet packets (such as during data storms), thereby ensuring the operation of the TMR 3008N MPs was unperturbed during communication failures.

However, in order to assess the platform's performance against this Staff Position, the entire safety system application should be available and evaluated. For example, it is necessary to understand the exact communication protocols used to implement communications between the 3008N MPs and external safety and non-SR applications. Based on the safety system design, data transfer time calculations can be used to determine whether safety-critical timing requirements in the plant-specific safety analysis are met by the Tricon V10 communications protocols. Also, thorough program operational testing will need to be conducted to determine the longest scan-time duration, identify the true system data rate, including overhead, and ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions and that communications throughput thresholds and safety system sensitivity to communications throughput issues are confirmed by testing.

Determination that the safety system communications data rates be such that they will not exceed the capacity of a communications link or the ability of nodes to handle traffic and that all links and nodes have sufficient capacity to support all functions is an application-specific activity that requires an assessment of a full system design. Since the LTR does not address a specific application and the scope of the platform does not include this system level information, no evaluation of the Tricon V10 platform against Staff Position 1, Point 19 could be performed. Therefore, implementation of the Tricon V10 platform in safety system applications will require application specific review to verify it meets the guidance of this Staff Position.

3.7.3.1.20 STAFF POSITION 1, POINT 20

Staff Position 1, Point 20, states that 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.

"Response time" is generally defined as the total time elapsed from initiation of a change in process control signal at one end of an instrumentation loop (the detector or sensor) until the end-of-loop actuated device reaches its final desired position. Safety system response time is dependent upon the specific plant process and safety system architecture. The plant safety analysis determines the response time required, including error rate, to prevent exceeding a safety limit. The Tricon V10 processor is only one contributor to the overall response time computation, and this variable is referred to as the "throughput" of the Tricon processor. Throughput is generally referred to as the time required for processing a change in any signal or variable from the input screws to output screws of the Tricon V10 cabinet. Throughput is dependent upon a number of factors, such as the number of variables scanned, size and complexity of the application program, when a change in a signal or variable is detected, number of communications protocol variables being transmitted/received, etc.

Because of the number of factors involved, throughput cannot be exactly predicted for any given configuration without knowing the exact safety system design. However, IOM did perform a calculation of throughput, documented in IOM Document No. 9600164-731, Revision 0, "Maximum Response Time Calculations" (Reference 43), which was used for the Tricon V10 qualification testing as required by Section 4.2.1-A of EPRI TR-107330, "General Functional Requirements," Part A, "Response Time." The TR specifies that, "the overall response time from an input to the PLC exceeding its trip condition to the resulting outputs being set shall be 100 msec or less." IOM analysis determined that the theoretical maximum response time for different combinations of Digital Inputs, Digital Outputs, AIs and AOs. The analysis indicates that none of these combinations of input and output modules comply with the 100 msec requirement (i.e., they all exceed this value). However, this analysis may be useful in determining the overall throughput for a safety system. Actual scan time, throughput, and data error rates will be measured and recorded during the plant-specific Factory Acceptance Tests (FATs).

Determination that 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 is an application-specific activity that requires an assessment of a full system design. Since the LTR does not address a specific application and the scope of the platform does not include this system level information, no evaluation of the Tricon V10 platform against Staff Position 1, Point 20 could be performed. Therefore, implementation of the Tricon V10 platform in safety system applications will require application specific review to verify that it meets the guidance of this Staff Position.

3.7.3.2 DI&C-ISG-04, SECTION 2 - COMMAND PRIORITIZATION

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

The design of field device interfaces and the determination of means for command prioritization is an ASAI. Since the LTR does not address a specific application, no evaluation against this staff position could be performed.

3.7.3.3 DI&C-ISG-04, SECTION 3 - MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS

Section 3 of DI&C-ISG-04 provides guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division, and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

The design of information displays and operator workstations and the determination of information sources and interconnections is an ASAI. Since the LTR does not address a specific application nor include display devices within the scope of the platform, no evaluation against this staff position could be performed.

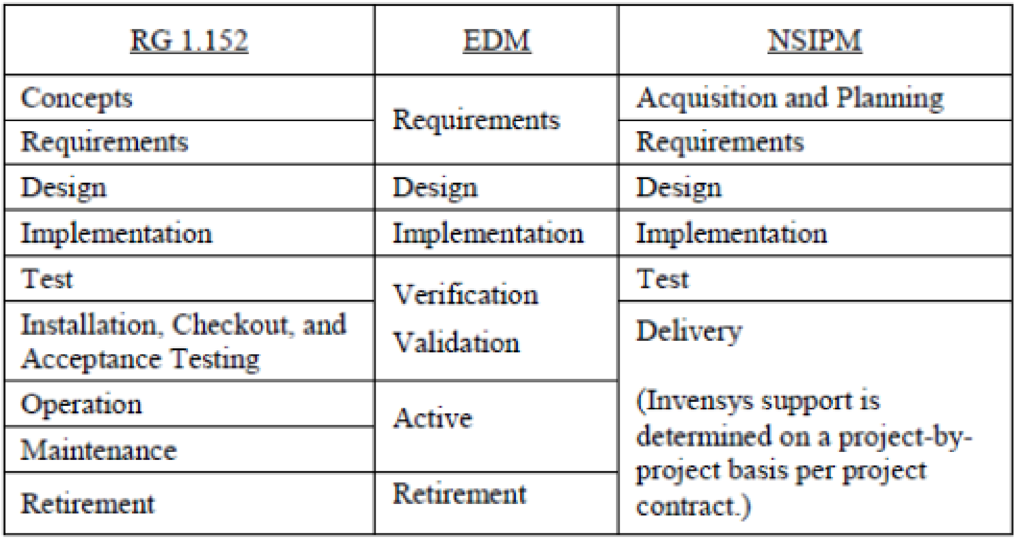
3.8 SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT

RG 1.152, Revision 3, describes a method that the NRC deems acceptable for complying with the Commission's regulations to promote high functional reliability, design quality, and establishment of secure development and operational environments for the use of digital computers in SR systems at nuclear power plants. Specifically, the guidance for secure development and operational environment measures states that potential vulnerabilities should be addressed in each phase of the digital safety system life cycle. The overall guidance provides the basis for physical and logical access controls to be established throughout the digital system development process to address the susceptibility of a digital system to inadvertent access.

IOM submitted a separate document, IOM Document No. NTX-SER-10-14, "Tricon V10 Conformance to Regulatory Guide 1.152" (Reference 35), that provides a detailed description of the Tricon V10 conformance to RG 1.152, Revision 2. The differences between Revision 2 and Revision 3 for Clauses 2.1 – 2.5 are minor and the NRC staff reviewed the information considering both versions. Cyber security elements of Revision 2 and Clauses 2.6-2.9 are not addressed in this SE.

3.8.1 LIFECYCLE PHASES

IOM's lifecycle framework does not match one to one against the lifecycle phases identified in RG 1.152, Revision 3. Table 3.8.1-1 shows a comparison of the phases for platform development outlined in IOM's EDM and application development outlined in the NSIPM.



RG 1.152	EDM	NSIPM
Concepts	Requirements	Acquisition and Planning
Requirements		Requirements
Design	Design	Design
Implementation	Implementation	Implementation
Test	Verification Validation	Test
Installation, Checkout, and Acceptance Testing		Delivery (Invensys support is determined on a project-by-project basis per project contract.)
Operation	Active	
Maintenance		
Retirement	Retirement	

Table 3.8.1-1 Lifecycle Stages Comparison

The lifecycle phases outlined for platform development in the EDM were reviewed and accepted under the Tricon V9 SE (Reference 9) Section 4.2.2. The NRC staff reviewed the changes to the EDM as part of the Tricon V10 evaluation and determined that IOM's commitments were expanded or were unchanged. Because the EDM process changes did not diminish previous commitments, the NRC staff determined that the Tricon V9 conclusions discussed in Section 4.2.2 of the SE sufficiently support the lifecycle requirements of RG 1.152, Revision 3.

The NRC staff did not complete a review of the NSIPM, as stated in Section 2.1 of this SE. Conclusions regarding the NSIPM were left as an ASAI.

IOM describes the development environment in Sections 3.1 and 3.2 of IOM Document No. NTX-SER-10-14, "Tricon V10 Conformance to RG 1.152" (Reference 35), detailing the secure development controls in place. Physical access is controlled through security access cards and is supplemented by the use of photo identification badges. Network access is globally managed at the corporate level where partitioning by responsibility limits access of individual users. Source code access is limited through the configuration management tool. The tool limits write access to developers. Wurldtech, a third party organization that provided independent security testing and review noted that all developer level personnel can access code for projects they are not directly supporting. However, IOM mitigates this through administrative controls in the release process which includes code reviews by multiple reviewers and hard copy offline storage of the final releases. Also, the independent third party review performed by TÜV includes a code review.

Manufacturing occurs at a separate IOM facility outside the U.S. Software and firmware are loaded at the IOM manufacturing site to facilitate testing. However, IOM manufacturing process requires all received subassemblies (modules) to undergo inspection and card level test and verification of all configuration items including firmware and software. IOM also employs automated configuration management systems that help to eliminate human error during verification of configuration items. At final inspection IOM performs a firmware "dump" from the configuration item and compares all firmware version numbers from the dump to the list generated by the automated configuration management system.

The NRC staff observed elements of the secure development environment during the December 2010 audit at IOM's Irvine, California facility (Reference 6). The NRC staff also reviewed Sections 4.2 and 5.1 of the Tricon V9 SE and find that the previous conclusions still apply. Based on a review of IOM document NTX-SER-10-14 Section 3.1 (Reference 35) regarding secure development environment and a comparison to the previously reviewed development environment from the Tricon V9 SE (Reference 9) combined with direct observations of the current development environment at IOM's facility in Irvine, California, the NRC staff finds that IOM meets the requirements for secure development environment in RG 1.152, Revision 3. It is an ASAI to verify that the secure development environment has not changed and to confirm that the application secure development environment is the equivalent or otherwise meets the requirements of RG 1.152, Revision 3.

Without a specific operational environment to assess, the NRC staff cannot reach a final conclusion on the Tricon V10 platform's ability to withstand undesirable behavior of connected systems and preclude inadvertent access. However, the Tricon V10 platform does have features that could be credited by a licensee when demonstrating these protections. Final conclusions regarding protection from undesirable behavior from connected systems and inadvertent access in the operational environment must be an ASAI.

3.8.1.1 CONCEPTS PHASE

Security Capabilities

As stated in the Regulatory Position 2.1 of RG 1.152, Revision 3, the Concepts Phase is the phase in which "the licensee and developer should identify safety system security capabilities that should be implemented."

Development Environment - The NRC staff reviewed the Tricon V10 development documentation and determined that the development process did incorporate several security features that apply to the secure development and operating environment of the system. Even though a formal concepts phase security analysis was not performed, the application development process outlined in the NSIPM supports the security concepts used during the development of the Tricon V10 platform.

IOM has identified the following security capabilities as having been implemented during the Tricon V10 platform development processes.

- network firewall protection,
- server and workstation anti-virus protection,
- password-based access control,
- administrative restrictions on write permissions, and
- control of source code versions and protection of record versions in a source-code repository.

Operational Features - IOM also identified the following security features intended to protect the Tricon V10 system from unauthorized access and modification.

- Tricon keyswitch – The triplicated 3008N MP modules vote on the position of the keyswitch to determine, among other things, whether downloads from the TriStation 1131 are allowed. With the keyswitch in "RUN" mode, downloads from the TriStation 1131 are rejected.

- Runtime memory check – The application (or "control") program is downloaded into flash memory on the 3008N MPs. During runtime, the control program is transferred to and executed from RAM. Periodically the control program in RAM is compared to the control program (i.e., the downloaded application program) in flash memory to ensure system integrity.
- Role-based access – The TriStation 1131 programming tool provides up to ten levels of password protection. Access to TriStation 1131 functionality can then be based on the user's job responsibility, e.g., System Engineer versus Maintenance Technician.
- Communication integrity checking – End-to-end integrity of the communications is ensured through the use of CRCs on the 3008N MPs (i.e., IOCCOM, DPRAM, and the Application Processor). For communication data links utilizing P2P and/or SAP in the fielded system, the application program logic that interfaces with the data link is defined and interpreted in the SR 3008N MP, which adds another layer of security.
- Access control lists – The TCM can be configured to restrict access based on IP addresses.
- Read/Write access control – The TCM can be configured to restrict access by external devices to read-only operations.

The NRC staff concluded that the security concept defined in NTX-SER-10-14 (Reference 35) and the platform capabilities identified in that document comply with this criterion from Regulatory Position 2.1 regarding identification of safety system security capabilities.

<u>Identification of Life Cycle Vulnerabilities</u>

Regulatory Position 2.1 of RG 1.152, Revision 3, also states that "the licensee and developer should perform security assessment to identify potential security vulnerabilities in the relevant phases of the system life cycle. The results of the analysis should be used to establish security requirements for the system (hardware and software)."

<u>Development Environment</u> - Appendix B of NTX-SER-10-14 (Reference 35) also lists the Tricon V10 Potential Vulnerabilities for each phase of the development process for the platform. No vulnerabilities were identified for the Concept or Requirements phases. For other development process phases, the following vulnerabilities were identified:

Design Phase

- Synergy Read Access – All Employees who have access to Synergy have read access to Tricon V10 code.
- Synergy Read/Write Access – All employees with developer privileges are allowed to modify Tricon V10 code.

Implementation Phase

- Build Control – The task of building a release is assigned to one person and there is no secondary verification that the build included the correct source.

Test Phase

- Factory Acceptance Testing – IOM facility has physical access controls and network access controls to network resources, the staging area for system integration testing is located in an open area within the building. There are no controls over physical access to staged nuclear SR systems.

Operational Environment - IOM has identified the security vulnerabilities of systems developed with the Tricon V10 platform as follows:

- Deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the safety system that may degrade the reliability, integrity or functionality of the safety system during operations; or
- Inability of the system to sustain the safety function in the presence of undesired behavior of connected systems.

The vulnerability assessment also identified the following additional platform vulnerabilities:

Tricon Design

- Keyswitch – All Tricon Controllers are shipped with identical keys and there is currently no procedure in place for a customer to order a different key for their systems.
- RXM 4200 – series fiber optic cables – The fiber optic cables to extend the I/O Bus between the RXM chassis can be cut or damaged.

Tricon Communications Module

- TSAA, MODBUS, MODBUS TCP, Peer-to-Peer – Packet injection of valid packets.
- Reboot command from trusted node – The TCM can be re-booted from a non-safety device.
- Network Routing Capability – The TCM can be configured to route network packets.
- Telnet Server – The TCM has a Telnet server that can be accessed in the field. This allows reboot of TCM, placing the TCM in download mode, and allows changing of route tables.
- FTP Server – The TCM has an FTP server that can be accessed in the field. This allows transferring files to and from the TCM.

Tristation 1131

- Security of Tristation 1131 – The Tristation 1131 provides the capability to create, modify, and download application programs to the Tricon controllers. The tool will likely be installed on maintenance workstations and laptops at licensee facilities.
- Default username and password – TriStation 1131 projects are created with default username and password at the highest level of privilege.
- Man-in-the-Middle during download – During download of an application program, the Tricon is placed into the “program” mode. The network connection is susceptible to Man-in-the-Middle attack whereby malicious code could be installed.

The NRC staff determined that the identified vulnerabilities adequately address the potential for tampering with the Tricon V10 platform during the developmental phases associated with either maintenance of IOM developed software or configuration of the platform to support an application. The vulnerabilities identified in the analyses contribute to the basis for security functional requirements for the platform, and support the determination of appropriate security controls for system hardware and software development. Based on the NRC staff review of the vulnerabilities identified and recognition that process and platform requirements to address these vulnerabilities through the various life cycles have been established, the NRC staff has determined that IOM has met this criterion of Regulatory Position 2.1 in RG 1.152, Revision 3, for the Tricon V10 platform.

Remote Access and One-Way Communication

The guidance in Section 2.1 of RG 1.152, Revision 3, states that implementation of remote access to a SR system should not be allowed. In addition, any transfer of data to other systems by computer-based SR systems should be limited to one-way communication pathways.

The LTR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures so this criterion must be evaluated at the application level. This is an ASAI.

IOM stated that the Tricon V10 system allows for and supports bi-directional communications with external devices and hosts. The Tricon V10 has been tested and certified by third-parties that communications errors, including unexpected operation of connected equipment, will not corrupt the safety function of the Triple Modular Redundant (TMR) 3008N MPs. The NRC staff reviewed non-safety to safety communications in Section 3.7.2 of this SE.

3.8.1.2 REQUIREMENTS PHASE

Security Functional Performance Requirements

Section 2.2.1 of RG 1.152, Revision 3, states in part that developers should define the security functional performance requirements and system configuration for a SR system. Security requirements for interfaces external to the system should be established by developers as well. Also, the developers should address security requirements for qualification, human factors engineering, data definitions, documentation of the software and hardware, installation and acceptance practices, operation and execution conditions, and maintenance activities.

The Tricon V10 security concept, as documented in NTX-SER-10-14 (Reference 35), identifies secure operational environment features of the platform that are traceable to functional performance requirements:

> Protection from Undesired Behavior of Connected Systems - All external runtime communications to the Tricon V10 come through the TCM which has two Ethernet ports and four serial ports. IOM did not qualify all of the commercial functionality available via serial port connections and the vulnerability testing performed by Wurldtech documented in Appendix A of NTX-SER-10-14 (Reference 35) applies to Ethernet ports only. However, most of the protection IOM credited pertains to the overall architecture and is not specific to the individual ports.
>
> IOM credited the overall architecture and highlighted specific features of individual elements for protecting the safety function from the undesirable behavior of connected systems in IOM Document No. NTX-SER-10-14, Section 3.3.3 (Reference 35). Other supporting information was supplied in the LTR Section 2.
>
> The NRC staff reviewed the Tricon V9 SE (Reference 9), the LTR, and NTX-SER-10-14 (Reference 35). IOM credits the triplicated communications busses (I/O and COMBUS) being physically separate. The communications processor (IOCCOMM) is autonomous and separate from the application processor. IOCCOMM uses a half-duplex master-slave

protocol with a timeout on every message to communicate over both the I/O and COMBUS. IOCCOM is scan based with limited interrupts and gives priority to safety I/O communications by design. CRC checks are performed on all data received by IOCCOM through both I/O and COMBUS paths.

IOM also credits the TCM access control. A TCM can be programmed via TriStation 1131 to communicate only with predetermined IP addresses and also allows users to dictate specific read and write permissions for each IP address. Although the TCM access control feature seems to provide a one-way communication tool to meet DI&C-ISG-04 safety to non-safety criteria, the NRC staff credits it as an element of protection from connected systems to satisfy this criterion.

The NRC staff also reviewed the Wurldtech Achilles Level One testing criteria. IOM credits the test as a demonstration of the Tricon's ability to maintain the safety function during a period of extreme network traffic or data storm. The test itself has not been endorsed by NRC. However, based on a review of the test criteria on the Wurldtech website and related review details by MPR Associates in the CDR report (Reference 32), the NRC staff accepts the test results as a demonstration of Tricon's ability to protect the safety function.

All IOM modules have a debug or test port that may be used to load updates. Most of these ports are not accessible when the module is plugged into the chassis. However, the TCM and 3008N MP modules both have debug ports on the front panel. These ports can be used to update firmware, but are disabled when the main chassis operating mode keyswitch is in the "RUN" position. Other aspects of controlling access to these ports are covered below under "Inadvertent Access".

A remote RXM chassis may connect to non-safety I/O. The NRC staff finds that connection acceptable as described in Section 3.7.2.2 of this report. The safety to non-safety barrier is at the RXM in the SR primary RXM chassis and safety and non-safety I/O are not connected on the same remote RXM chassis (a requirement of IEEE Std 603-1991).

<u>Protection from Unintended Access</u> - IOM uses several physical methods to prevent inadvertent access including redundant modules, debug port access control and system operating mode keyswitch. The features are intended to mitigate consequences of removing the wrong module during maintenance, prevent unintended application code changes and firmware changes. Redundant 3008N MP modules can maintain the safety function when up to two of the three modules are inadvertently removed or become inoperative. IOM's Triple Modular Redundant (TMR) voting preferences are application specific and are defined in the application program. Redundant I/O modules in hot standby prevent a loss of safety channel if an active module is inadvertently removed or dislodged. However, redundant I/O modules in hot standby are optional and not required for normal operation and must be credited on the application specific review. System operating mode is set using a keyed switch on the faceplate of the main chassis to one of four modes; Stop, Run, Program or Remote. The module can only be reprogrammed by setting the keyswitch to the "Program" mode. Debug ports on the face of all main processor modules and TCM's are deactivated during runtime.

The NRC staff determined that the Tricon V10 platform has met this criterion of Regulatory Position 2.2.1 in RG 1.152, Revision 3.

Security Requirements Verification and Validation (V&V)

Regulatory Position 2.2.1 of RG 1.152, Revision 3, also states that security requirements should be included within the overall system requirements. Therefore, the system security requirements should be subject to treatment under the full V&V process activities of the overall system to assure the correctness, completeness, accuracy, testability, and consistency of those security requirements.

As stated in Section 4.3.3 of the IOM document, "EDM 90.00 Product Verification" (Reference 50), a security analysis will be conducted at every phase of the software life cycle as part of the V&V process applied to a development project. In addition, the V&V process applied to the dedication of PDS was shown to address security requirements. Based on these considerations and the review of the IOM V&V program discussed in Section 3.2 of this SE, the NRC staff determined that the Tricon V10 platform has met this criterion of Regulatory Position 2.2.1 in RG 1.152, Revision 3.

Use of Pre-Developed Software and Systems

Regulatory Position 2.2.1 of RG 1.152, Revision 3, further states that the security vulnerability of a SR system should be addressed in any requirements specifying the use of pre-developed software and systems (e.g., reuse of software and incorporation of commercial off-the-shelf systems). In particular, the use of pre-developed software functions that have been tested and are supported by operating experience is identified.

The pre-developed operating software of the TCM in the Tricon V10 platform underwent dedication for use in SR applications. As described in Section 3.2.2 of this SE, the dedication process indicates the quality and reliability of the PDS is acceptable. In addition, testing performed as part of the CGD effort further established the quality and security characteristics of the PDS. The dedicated operating software is controlled under the Tricon Software Configuration Management program (SCMP) as evaluated in Section 3.2.1 of this SE and is maintained under the Tricon software Quality Assurance program which is evaluated in Section 3.2.1 (SQAP) evaluation of this SE. Based on the review of the CGD evidence for the PDS and its ongoing management under the IOM quality processes, the NRC staff determined that the Tricon V10 platform has satisfied this criterion of Regulatory Position 2.2.1 in RG 1.152, Revision 3.

Development Activities

Regulatory Position 2.2.2 of RG 1.152, Revision 3, states, "The development process should ensure the system does not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted and undocumented functions or applications."

The key vulnerability to the requirements phase of the Tricon V10 platform development was unauthorized changes of the requirements in the requirements specification and unauthorized versions of the requirement specification. If appropriate controls are not placed on handling of the requirements documentation, the opportunity exists for inappropriate requirements to be inserted and/or necessary requirements to be omitted. As described previously, Security Controls are in place at the Irvine facility when developing SR nuclear systems produced. These controls provide assurance that the Tricon V10 platform code and plant-specific application code are protected from unauthorized access and modification. Further, administrative restrictions are implemented on write permissions, control of test procedures and test code versions, and protection of record versions in the Agile repository. Agile is used as the system of record for Tricon product lifecycle information, beginning at conception/planning, through design, source, build, test, and maintenance, to retirement.

IOM procedures for specification of software requirements describe the organization, content and structure of requirements specifications for the Tricon V10 platform. The NRC staff review of these procedures found them to be acceptable, as described in Section 3.2.1. IOM uses Rational Synergy tool for integrated configuration management of Tricon V10 platform software code. IOM engineering procedures for software configuration change control define the Tricon V10 software configuration and change process. The NRC staff reviewed these configuration management controls in IOM document EDM 20.00, “Configuration Management” (Reference 49). IOM procedures also provide assurance that the Tricon V10 does not have undocumented codes (e.g., backdoor coding) and unwanted functions that could adversely impact system reliability. Section 5.6 of IOM document EDM 12.00, “Product Development Process” (Reference 19), states that verification activities occur after each phase of the design lifecycle and that documentation and source code are independently reviewed following the implementation phase.

Also, as described in Section 3.2.1, the software QA program addresses the design, implementation, and commissioning of SR systems based on the Tricon V10 platform. The program provides for measures to ensure the maintenance of records.

In addition, Security Controls that are used for SR nuclear systems produced at IOM facilities include:

- Physical access controls to the building.
- Corporate policy on appropriate use of email and network resources.
- Local policy on the use of computer resources and removable media on nuclear system integration projects and equipment.
- Network access controls. Access to network resources is based upon job responsibility, therefore R&D engineers, for example, do not have access to the Manufacturing network resources. Also, only engineers involved in nuclear system integration projects have access to nuclear projects folders. Furthermore, Irvine employees have limited access to network resources at other IOM locations that is also based upon work responsibilities.
- Managed Virtual Private Networks. Access is granted after special request. Several methods for VPN access are used, such as secure tokens.
- Managed firewalls and DMZs partition the network using current best practices to isolate the corporate network from the outside; Wireless access points for “Guest” accounts are outside the firewall.
- Network server and workstation virus scanning.
- Controls over Tricon V10 source code and build process.
- Controls over the Tricon manufacturing process.

Based on the IOM procedures to reconstitute and trace requirements, as well as the controls in place to protect their requirements documentation, the NRC staff determined that the Tricon V10 platform has met the provisions of Section 2.2.2 of RG 1.152, Revision 3.

3.8.1.3 DESIGN PHASE

Security Design Configuration Items

Regulatory Position 2.3.1 of RG 1.152, Revision 3, states "The safety system security requirements identified in the system requirements specification should be translated into specific design configuration items in the system design description. The safety system security design configuration items should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items incorporating pre-developed software into the safety system should address security vulnerabilities of the safety system."

Regulatory Position 2.3.1 of RG 1.152, Revision 3, also states "Physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life cycle. The results of this assessment may identify the need for more complex access control measures, such as a combination of knowledge (e.g., password), property (e.g., key and smart card), or personal features (e.g., fingerprints), rather than just a password."

As described before, IOM uses Agile repository to maintain records for Tricon product lifecycle information, beginning at conception/planning, through design, source, build, test, and maintenance, to retirement. All firmware/software versions are controlled and released into Agile, as well as Software Requirements Definition (SRD) and the Software Control Specification for the system. Software code is controlled with Synergy.

In this phase, the system security requirements stated in Section 3.8.1.1 of this SE are translated into design configuration items. The secure operational environment requirements for the Tricon V10 platform correspond to security-related features, capabilities, and design elements that serve as design configuration items. In NTX-SER-10-14, IOM documented the security design configuration for the Tricon V10 platform, as well as potential vulnerabilities for each lifecycle phase. Section 3.8.1.2 (above Security Functional Performance Requirements) summarizes the security control implemented in the design of the Tricon V10 platform related to physical and logical access to the system functions. Section 3.8.1.1 (above Platform Security Capabilities) summarizes the security features of the Tricon V10 platform related to use of safety system service and data communication with other systems to protect the Tricon V10 system from unauthorized access and modifications.

IOM has implemented measures to protect the application against inadvertent operator actions and unintended operation of connected equipment. IOM identified the following security features intended to protect the Tricon V10 system from unauthorized access and modification:

- Tricon redundancy – pulling an active module will not shutdown the system, but will cause a system alarm.
- Maintenance/debug front panels – Physical ports are provided in the front panels for debug and firmware update. This requires halting operation of the system, for the ports to be activated.
- Tricon keyswitch – key that determines the system operating mode. To download an application, the key must be in the "Program" position.

Thus, conditions permitting overwrite of the application software cannot be inadvertently triggered and adequate provisions are in place to protect the integrity of the installed application software from alteration. Licensees should identify if and how to protect the Tricon keyswitch as part of their establishment of a secure operational environment for the platform.

In NTX-SER-10-14, IOM stated the necessary security controls will be based on the results of the security assessment performed during the Concept phase of the plant-specific SR implementation of the Tricon V10. The security controls could be a combination of the Tricon V10 security features described previously, plus any controls required by the Licensee's site Cyber Security Plan developed by the Licensee to comply with 10 CFR 73.54. Therefore, additional security features required for the plant-specific application must be an ASAI.

Communication with non-safety systems are evaluated in Section 3.7.2 and conformance to ISG-04 in Section 3.7.3 of this SE. An important design consideration of the Tricon V10 is that communication failures do not adversely affect the safety function of the TMR 3008N MPs.

For plant-specific configurations utilizing the Tricon V10, the development process for SR application software will be controlled under the IOM NSIPM.

The NRC staff determined that the Tricon V10 platform has met the criterion of Regulatory Position 2.3.1 of RG 1.152, Revision 3.

Development Activities

Regulatory Position 2.3.2 of RG 1.152, Revision 3, states, "The developer should delineate the standards and procedures that will conform with the applicable security policies to ensure the system design products (hardware and software) do not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications."

As discussed in Section 3.8.1.1 of this SE (above Concept phase), the licensee identified that the key vulnerability to the design phase of the Tricon V10 platform was improper manipulation of the preliminary or detailed design description documentation. If the IOM's procedures do not properly control the design process, the opportunity exists for insertion of inappropriate features and/or the omission of required features. During the NRC review of the Tricon V9 platform, the NRC staff found that the software development process and lifecycle for the Tricon V9 system was adequate for SR use in nuclear power plants.

The development process for the Tricon V10 system is controlled by the IOM QPM and EDM, which were previously reviewed and approved by the NRC. For plant-specific configurations utilizing the Tricon V10, the development process for SR application software will be governed by the IOM NSIPM.

The NRC staff has determined that the vendor's procedures and processes have adequately protected the design phase of the system lifecycle from tampering by excluding undocumented code, malicious code, and other unwanted or undocumented functions or applications and has met the criterion in Section 2.3.2 of RG 1.152, Revision 3.

3.8.1.4 IMPLEMENTATION PHASE

Regulatory Position 2.4, states that, "In the system (integrated hardware and software) implementation phase, the system design is transformed into code, database structures, and related machine executable representations. The implementation activity addresses hardware configuration and setup; software coding and testing; and communication configuration and set-up [including the incorporation of reused software and commercial off-the-shelf (COTS) products].”

System Features

Regulatory Position 2.4.1 of RG 1.152, Revision 3, states that, “The developer should ensure that the security design configuration item transformations from the system design specification are correct, accurate, and complete.”

During the design of the Tricon V10 and TriStation 1131 software, peer reviews are performed on documents, logic, tests, and other electronic documents to ensure that the contents are complete, logical, correct, and also that the Tricon and TriStation 1131 designs include only the required functionality. EDM 40.50 defines the software code review process. The software design review includes structural walk-through of overall design as well as individual module design. All requirements must be traceable from the system specification to the design, thus accounting for hidden functions. This provides reasonable assurance that IOM has minimized the possibility of inadvertent injection of undesired code into the system and application program logic. The NRC staff review of this process found it to be acceptable and the December 2010 audit at IOM’s Irvine, California facility (Reference 6) supported the conclusion by directly verifying requirements traceability.

The NRC staff has reviewed the implementation controls and determined that the Tricon V10 platform has features that comply with the criterion in Section 2.4.1 of RG 1.152, Revision 3.

Development Activities

Anti-Tampering Provisions During Implementation

Regulatory Position 2.4.2 of RG 1.152, Revision 3, states, “The developer should implement security procedures and standards to minimize and mitigate tampering with the developed system. The developer’s standards and procedures should include testing with scanning as appropriate, to address undocumented codes or malicious functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave beyond the system requirements. The developer should account for hidden functions and vulnerable features embedded in the code, and their purpose and impact on the safety system. If possible, these functions should be disabled, removed, or (as a minimum) addressed (e.g., as part of the failure modes and affects analysis of the application code) to prevent any unauthorized access.”

As discussed in Sections 3.8.1.1, 3.8.1.2, and 3.8.1.3, IOM has implemented security controls for software development environments, security controls over physical and network access to Tricon platform source code and build process, including password-based access control, administrative restrictions on write permissions, and control of source code versions and protection of record versions in a source-code repository (Synergy). Furthermore, the ability to embed undesired code in system or application software would require not only access but also expert knowledge of the programming conventions and tools to avoid immediate detection through erratic behavior or design measures.

For plant-specific configurations utilizing the Tricon V10, the development process for SR application software will be controlled under the IOM NSIPM. IOM will work with the Licensee to identify applicable Tricon V10 security performance requirements that should be incorporated, and, in accordance with the IOM NSIPM, provide traceability of these requirements into the plant-specific implementation of the application software.

Configuration control is maintained for Tricon V10 software. Software development is conducted on development workstations in a controlled environment through authorized project directories. Review and approval processes are enforced before releasing modified software for inclusion in Synergy. Only developers with "developer" access control are allowed to add and/or modify code in Synergy. Only one developer can modify the Tricon V10 code. Changes to the source code are reviewed by cognizant IOM personnel as outlined in IOM process document, EDM 40.50.

The development process for the Tricon V10 system is controlled by the IOM QPM and EDM. In the process of a release of a product, a change impact analysis is performed during which the new source base is compared to the last source base. Any changes have to be documented and justified. NTX-SER-10-14 (Reference 35) identifies a vulnerability – "The task of building a release is currently assigned to one person and there is no secondary verification that the build included the correct source." IOM has implemented process changes to mitigate these as stated in NTX-SER-10-14 (Reference 35). Third party reviewer, TÜV Rheinland, however, performs source code review which can be credited for the verification of the build because it occurs before product rollout. The NRC staff finds the newly implemented process is improved because it occurs before the build is released.

System developer uses TriStation 1131 Developers Workbench to develop the code to be executed on the Tricon controllers. TriStation 1131 uses password protection that may be configured to assign different levels of access to multiple users. Thus, every TriStation 1131 operation is assigned a default security level and each user is assigned a security level that defines what operations a user can perform. Windows security file access rules apply to all TriStation 1131 project files. If an existing TriStation 1131 project was created by a user with restricted or administrator-level rights in Windows, other users must have the same access rights to open that project.

For plant-specific configurations utilizing the Tricon V10, the development process for SR application software will be governed by the IOM NSIPM. In addition to the NSIPM, the "Nuclear Delivery Programming Guide," IOM Document No. 9600380-001, provides guidance on Tricon V10 application programming for nuclear system integration projects.

Based upon the documented efforts to fully inspect their source code for unwanted code and features, as well as the controls currently in place to protect the development environment and developed software products, the NRC staff determined that Tricon V10 platform complies with Section 2.4.2 of RG 1.152, Revision 3.

Use of Commercial-Off-the-Shelf Systems (COTS)

Regulatory Position 2.4.2 states, "[For Commercial-Off-the-Shelf (COTS) systems] unless such systems are modified by the application developer, the security effort should be limited to ensuring that the features within the system do not compromise the security requirements of the system, and the security functions should not be compromised by the other system functions."

All firmware and TriSTation 1131 software was implemented and tested by IOM personnel, with the exception of the third party software in the TCM. The third party software was dedicated by IOM as described in Section 3.2.2. IOM also modified the third party software and performed significant testing on the TCM as part of their validation and verification process. Further, the TCM has been used commercially in the Tricon V10 without incident since 2005.

The NRC staff determined that this criterion of Regulatory Position 2.4.2 of RG 1.152, Revision 3, has been met.

3.8.1.5 TEST PHASE

Section 2.5 of RG 1.152, Revision 3, states that, "The objective of testing security functions is to ensure that the system security requirements are validated by execution of integration, system, and acceptance tests where practical and necessary. Testing includes system hardware configuration (including all external connectivity), software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing."

System Features

Section 2.5.1 of RG 1.152, Revision 3, states that, "The security requirements and configuration items are part of validation of the overall system requirements and design configuration items. Therefore, security design configuration items are just one element of the overall system validation. Each system security feature should be validated to verify that the implemented system does not increase the risk of security vulnerabilities and does not reduce the reliability of safety functions."

IOM EDM requires validation and traceability of all system requirements through design and testing. IOM performed various tests in their Irvine facility. As mentioned before, the Irvine Facilities management maintains physical access controls over the Irvine facility. Although the staging area for system integration testing is located in an open area within the building, it is part of the greater access controlled area.

The dedication of the operating software and the generic qualification of the Tricon V10 platform involved an extensive test program that varied from low level single step testing of software units or components to operability testing for computer qualification of a representative system configuration. The test subjects ranged from application software objects to software components to module prototypes to a fully functional representative system (i.e., the test specimen). Specific tests were implemented to validate the security requirements and corresponding design features that are identified in the previous sections of this SE.

The testing was controlled by IOM test procedures (see Section 3.2.1 of this SE), which address the test requirements, performing the tests, and producing the test report. The test procedures and records are controlled under the IOM configuration management plan, as discussed in Section 3.2.1 of this SE. Test procedures are maintained in Agile.

The various tests conducted under the qualification program for the Tricon V10 platform are discussed in Section 3.3 of this SE. The traceability of the tests to the requirements which they validate is documented in the requirements traceability matrix and associated appendices and discussed in Section 3.2.1 of this SE.

The NRC staff evaluation of these tests (see Sections 3.2.1 and 3.3 of this SE) also involved review of the test procedures and assessment of the traceability to requirements. The NRC staff determined that security-related requirements were validated during these tests and that this criterion of Regulatory Position 2.5.1 of RG 1.152, Revision 3, has been met.

Development Activities

Regulatory Position 2.5.2 of RG 1.152, Revision 3, specifies, “The developer should configure and enable the designed security features correctly. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in OEM [original equipment manufacturer] features.”

As discussed in section 3.8.1.4 of this SE, testing for the Tricon V10 platform operating software was performed at several different levels. Specifically, testing under the dedication and generic qualification activities addressed object, component, module, and system functionality. The results from these tests validated the correct implementation of key security features.

After a system is configured to the customer’s requirements, all of the modules are then scanned into the system by serial number. A system-level test is then performed in accordance with Test Procedure 9600051-001. At the end of the test the technician will do a dump of the firmware that provides a printout that lists each module, its serial number, its location, and the Meta numbers for all programmed parts.

After testing was completed, IOM uses the System Hierarchy Automated File Transfer (SHAFT) program to track configuration of the system (e.g., version of the system, modules requested, etc.) to be installed in a plant specific application. For example, during System Test all firmware is checked for correct Meta numbers per the configuration called out in the SHAFT configuration database.

Following review and acceptance for release, source code is to be placed in Synergy to preclude unauthorized modification. The source code, associated derived products, and design documentation are to be retained as controlled items in Agile. Manufacturing never ships a Tricon V10 system with application software installed. Virus Scan is run daily on all workstations used to execute test programs. Installation of the operating software is accomplished by downloading through the TCM using a Windows platform running IOM’s TriStation 1131. Administrative controls will be required when downloading in the operational environment. Revision and checksum information are embedded into the firmware to serve as identification. Nevertheless, it is important to ensure that the identification of the code installed is correct to avoid inadvertent usage of incorrect software.

For plant-specific configurations utilizing the Tricon V10, the test-phase activities for SR application software will be controlled under the IOM NSIPM. IOM will work with the licensee to identify applicable plant-specific security performance requirements that should be incorporated into the Tricon V10 system, and, in accordance with the NSIPM, provide traceability of these requirements through testing and V&V of plant-specific application software. The NRC staff has not reviewed the NSPIM, as stated in Section 2.1 of this SE.

Based upon the defined testing procedures and the measures taken to verify correct software installation, the NRC staff determined that IOM has mitigated the potential for unauthorized versions of the Tricon V10 platform software to be released. The NRC staff concluded that IOM has met the criteria of Section 2.5.2 of RG 1.152, Revision 3.

3.9 DIVERSITY AND DEFENSE-IN-DEPTH

The Staff Requirements Memorandum on SECY 93-087, dated July 21, 1993, describes the NRC position on diversity and defense-in-depth (D3) requirements to compensate for potential common-cause programming failure. This requires that the applicant assess the D3 of the proposed instrumentation and control system, and if a postulated common cause failure (CCF) could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, shall be required to perform either the same function or a different function.

Guidance on the evaluation of D3 is provided in SRP BTP 7-19. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 31, 1994, summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses.

Additional guidance on evaluation of the need for D3, and acceptable methods for implementing the required D3 in DI&C system designs, is contained in "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues."

Since both diversity and defense-in-depth are plant specific topics, the LTR did not address these topics, and therefore are not within the scope of this SE. Sections 3.6.2 and 3.6.3 of Appendix B, "Applications Guide," to IOM Document No. 7286-545-1 (Reference 4), provides guidance in the preparation of a plant specific D3 evaluation. A review of the differences between the Tricon V10 system and the safety/non-safety control system and indications implemented at a particular nuclear power plant, and the determination that plant specific required diversity and defense-in-depth continue to be maintained must be addressed in a plant-specific D3 evaluation. Thus, the performance of a plant-specific D3 analysis is an ASAI for SR applications of the Tricon V10 platform. These determinations will be reviewed during the plant-specific safety evaluation.

3.10 CONFORMANCE WITH IEEE STD 603-1991

For nuclear power generating stations, 10 CFR 50.55a(h) requires that safety systems must meet the requirements stated in IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" and the correction sheet dated January 30, 1995. The subsections below document the evaluation of the Tricon V10 platform against those regulatory requirements. The generic SRP acceptance criteria contained in NUREG-0800, Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," were used in evaluating conformance of the Tricon V10 platform with the applicable IEEE Std 603-1991 requirements. This evaluation supports conclusions regarding adherence of the Tricon V10 platform to the relevant regulatory requirements.

IEEE Std 603-1991 is written from a system perspective, which defines criteria (i.e., contains requirements) that a safety system must meet. The evaluation documented below is performed in accordance with this system perspective. Consistent with accepted industry guidance on generic qualification of PLCs, the LTR documents evidence that the Tricon V10 PLC platform is suitable for use in SR applications rather than present a complete safety system design. Consequently, it is not possible to provide a complete assessment of conformance with system requirements on the basis of the platform alone. In the absence of a specific system design for a particular SR application, the determination of conformance with the IEEE Std 603-1991 requirements is necessarily limited to the evaluation of features and characteristics of the platform that support fulfillment of system requirements. Thus, this evaluation addresses the capabilities and qualifications of the platform that are relevant in assuring that a safety system based on the Tricon V10 platform satisfies regulatory requirements.

IEEE Std 603-1991 contains five clauses (Clause 4, 5, 6, 7, and 8), described in the five major subsections below, that must be considered in the evaluation of the platform.

Each of these major subsections contains subordinate subsections that address the individually identifiable requirements of these clauses. Consideration is given to the degree to which each requirement can be evaluated in whole or in part within the scope of a platform review. While a number of the requirements cannot be assessed or cannot be assessed fully on the basis of the platform, each of the main requirements of IEEE Std 603-1991 is presented. This evaluation provides a means for subsequent plant specific submittals to account for those elements of review that are contained in this document.

3.10.1 IEEE 603-1991 CLAUSE 4, "SAFETY SYSTEM DESIGNATION"

Clause 4 of IEEE Std 603-1991 states that a specific basis shall be established for the design of each safety system of the nuclear power generating station. The sub-clauses of this requirement can be characterized as follows:

Clause 4.1	Identification of the Design Basis Events
Clause 4.2	Safety Functions and Corresponding Protective Actions
Clause 4.3	Permissive Conditions for Each Operating Bypass Capability
Clause 4.4	Identification of Variables Monitored
Clause 4.5	Minimum Criteria for Manual Initiation and Control Of Protective Actions
Clause 4.6	Identification of the Minimum Number and Location Of Sensors
Clause 4.7	Range Of Transient and Steady State Conditions
Clause 4.8	Identification of Conditions Which May Degrade Performance
Clause 4.9	The Methods to Be Used To Determine Reliability
Clause 4.10	The Critical Points in Time After The Onset Of A Design Basis Event
Clause 4.11	The Equipment Protective Provisions
Clause 4.12	Any Other Special Design Basis

SRP Chapter 7, Appendix 7.1-C, Section 4, "Safety System Designation" provides acceptance criteria for these requirements.

The determination and documentation of the design basis for a safety system is an application-specific activity that is dependent on the plant design. Since the LTR does not address a specific application of the platform, the design basis for a safety system is not available for review and no evaluation of the Tricon V10 platform against these regulatory requirements could be performed. Nevertheless, in regard to Clause 4.9, a platform-level assessment of reliability was performed by IOM and the analysis is reviewed in Section 3.6 of this SE. Based on the NRC staff's review of this analysis, IOM used an acceptable method to perform this reliability analysis (IEEE Std 352-1987).

3.10.2 IEEE STD 603-1991 CLAUSE 5, "SAFETY SYSTEM CRITERIA"

Clause 5 of IEEE Std 603-1991 requires that safety systems maintain plant parameters, with precision and reliability, within acceptable limits established for each design basis event. The power, instrumentation and control portions of each safety system are required to be comprised of more than one safety group (or division) of which any one safety group can accomplish the safety function. The establishment of a safety group that can accomplish a given safety function is an application-specific activity. Since the LTR does not address a specific application, the evaluation against the following regulatory requirements addresses the capabilities and characteristics of the Tricon V10 platform that are relevant for adherence to each requirement.

3.10.2.1 IEEE STD 603-1991 CLAUSE 5.1, "SINGLE FAILURE CRITERION"

Clause 5.1 of IEEE Std 603-1991 requires that the safety system be able to perform its safety function required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. SRP Chapter 7, Appendix 7.1-C, Section 5.1, "Single Failure Criterion," provides acceptance criteria for the single failure criterion. In addition, RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," endorses IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," as providing an acceptable method for satisfying this requirement.

Determination that no single failure within the safety system can prevent required protective actions at the system level is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those features and capabilities that support adherence to the single failure criterion by a system design based on the platform. Since the LTR does not address a specific application for approval, the evaluation against this requirement is limited to consideration of the means provided within the platform to address failures.

As discussed in Section 3.5 of this SE, the NRC staff reviewed the Tricon V10 FMEA and determined that the analysis provides a thorough assessment of the potential failure modes and the effect of those failures based on a generic reference system composed of a single Tricon V10 platform. The FMEA concludes that there are no undetectable single failures of the platform based on the use of redundancy, diagnostics and self-tests as means of failure detection and indication. The NRC staff finds that the FMEA supports a conclusion that the Tricon V10 platform is suitable for use in SR applications in a nuclear power plant. The analysis and results of the FMEA for the Tricon V10 platform can be incorporated into application-specific FMEAs for system designs based on the platform.

The use of redundancy at the platform level (triple modular redundant processors) supplements the conventional use of redundancy at the system level to satisfy the single failure criterion. The Tricon V10 platform provides diagnostic and self-test capabilities to detect and enable indication of hardware faults and module component failures during power up and runtime as described in IOM Document No. 9600164-531 (Reference 28). These platform-level capabilities satisfy Clause 5.1 by providing the means to detect postulated component failures.

3.10.2.2 IEEE STD 603-1991 CLAUSE 5.2, "COMPLETION OF PROTECTIVE ACTION"

Clause 5.2 of IEEE Std 603-1991 states that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion, and that deliberate operator action shall be required to return the safety systems to normal. SRP Chapter 7, Appendix 7.1-C, Section 5.2, “Completion of Protective Action,” provides acceptance criteria for this requirement.

Determination that protective actions of the execute features of a safety system will continue to completion after initiation is an application-specific activity that requires an assessment of a full system design. Since the LTR does not address a specific application and the scope of the platform does not include execute features for a safety system, no evaluation of the Tricon V10 platform against this regulatory requirement could be performed.

3.10.2.3 IEEE STD 603-1991 CLAUSE 5.3, “QUALITY”

Clause 5.3 of IEEE Std 603-1991 states that the components and modules within the safety system must be of a quality that is consistent with minimum maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program. SRP Chapter 7, Appendix 7.1-C, Section 5.3, “Quality,” provides acceptance criteria for the quality requirement. This acceptance criteria states that the QA provisions of 10 CFR Part 50, Appendix B, apply to a safety system.

GDC 1 states that structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A QA program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

The regulation at 10 CFR 50.55a(a)(1), “Quality Standards,” requires that the “structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.”

The current processes and procedures contained in the IOM QAM, QPM, and EDM documents have previously been audited by the Nuclear Procurement Issues Committee (NUPIC). As a consequence of the most recent audits performed in May 2010, IOM is a qualified supplier of Class 1E nuclear safety systems.

The Tricon V10 product line is based on a foundation of products that were designed for commercial grade industrial systems, rather than specifically for use in SR systems in nuclear power plants. As a result, the design process that led to the Tricon V10 platform was not governed by Appendix B of 10 CFR Part 50. The Tricon V10 platform has undergone commercial grade dedication (by IOM) of its system software and been subjected to Class 1E equipment qualification (see Sections 3.2.1 and 3.3, respectively, of this SE). The platform is now maintained under a software QA program that satisfies the requirements of Appendix B in all aspects of the product life cycle going forward with regard to the Tricon V10 platform (Reference 48), including the design control process, purchasing, fabricating, handling, shipping, storing, building, inspecting, testing, operating, maintaining, repairing, and modifying the platform. As such, the Tricon V10 platform hardware and software is designed for Class 1 E equipment applications at nuclear power plants.

Application software and its specific life cycle processes are outside the scope of this review and will be reviewed in plant-specific reviews. The operating software and communications module software are commercial grade PDS that was dedicated by IOM using their CGD procedure, EDM 76.00 (Reference 18). As stated previously in this SE (Sections 3.2.1 and 3.7) the NRC staff reviewed these CGD activities and based on the review of the associated development history, operating experience, life cycle design output documentation, and testing and review activities, the NRC staff finds the dedication evidence for the PDS of the Tricon V10 platform to be acceptable for demonstrating built-in quality. In addition, the NRC staff determined that the IOM QA processes for software maintenance provides reasonable assurance that the quality characteristics of the PDS can be preserved. Consequently, the NRC staff concludes that the Tricon V10 hardware and software is of sufficient quality to satisfy Clause 5.3 and is suitable for use in SR applications.

3.10.2.4 IEEE STD 603-1991 CLAUSE 5.4, "EQUIPMENT QUALIFICATION"

Clause 5.4 of IEEE Std 603-1991 states that safety system equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting the performance requirements as specified in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.4, "Equipment Qualification" provides acceptance criteria for IEEE Std 603-1991 Clause 5.4. This acceptance criteria states that the applicant/licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. This clause of IEEE Std 603-1991 also states that qualification of Class 1E equipment be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980, "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations." RG 1.89 endorses and provides guidance on compliance with IEEE Std 323-1974 for qualification of SR electrical equipment installed in harsh environment locations (i.e., locations subject to design basis-accident conditions). RG 1.209 endorses and provides guidance for compliance with IEEE Std 323-2003 for qualification of SR computer-based I&C systems installed in mild environment locations.

EPRI TR-107330 was used to establish the bases for the Tricon V10 platform equipment qualification. As such, it consists of the maximum (i.e., extremes) environmental and service conditions for which qualification was validated and the range of performance characteristics for the PLC that were demonstrated under exposure to environmental stress conditions. Subsequent plant-specific applications are obligated to verify that the qualification envelope provided by qualification to the guidance of EPRI TR-107330 bounds the requirements of the application.

The environmental qualification program for the new/modified components for the Tricon V10 platform addressed the generic qualification envelope that is specified in EPRI TR-107330. The evaluation of the environmental qualification that was demonstrated is contained in Section 3.3 of this SE. Based on that evaluation, the NRC staff determined that an acceptable qualification envelope for the Tricon V10 platform was demonstrated for radiation, temperature and humidity, seismic withstand, electromagnetic capability (EMC), electrical fast transient response, power surge withstand, electrostatic discharge, and Class 1E to Non-Class 1E isolation capabilities for use in SR application in nuclear power plants, and satisfies this clause. However, the NRC staff concludes that some EQ tests (e.g., EMC qualification of the Tricon V10 platform for radiated magnetic field, low frequency conducted interference, and high frequency conducted interference emissions) have been demonstrated, up to the respective EQ limitations noted in Section 3.3 of this SE. It remains as an ASAI to verify that the generic equipment qualification envelope for the Tricon V10 platform, as approved by this SE, bounds the corresponding plant-specific conditions for these environmental stressors and that the performance characteristics demonstrated for the Tricon V10 platform under the tested service conditions are adequate for the specific application. Furthermore, applications of the Tricon V10 platform at nuclear power plants should verify that the equipment qualification limitations observed during testing (as noted in Section 3.3 of this SE) are adequate for the specific application, or additional EQ testing should be performed to address this ASAI.

3.10.2.5 IEEE STD 603-1991 CLAUSE 5.5, "SYSTEM INTEGRITY"

Clause 5.5 of IEEE Std 603-1991 states that the safety systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," provides acceptance criteria for system integrity. This guidance on acceptance criteria states that the NRC staff should confirm that tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady state conditions of both the energy supply and the environment. Furthermore, the NRC staff should confirm that if tests show that the system does fail, it fails in a safe state. Also, the NRC staff should verify that failures detected by self-diagnostics also place a protective function into a safe state. Finally, confirmation that system real-time performance is adequate to ensure completion of protective action within critical time frames is identified as a special concern for digital computer-based systems.

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

As discussed above and in Section 3.3 of this SE, the Tricon V10 platform underwent testing to demonstrate qualification for installation in mild environment locations in a nuclear power plant. Pending satisfactory resolution of the equipment limitations in certain environmental qualification testing as noted in Section 3.3 of this SE, the IOM qualification program provides reasonable assurance that SR systems based on the Tricon V10 platform will be capable of performing safety functions over the full range of environmental stressors that correspond to those expected worst case design basis events bounded by the qualification envelope for the Tricon V10 platform.

As described in Section 3.5 of this SE, IOM performed a failure modes and effects analysis (FMEA) on the Tricon V10 platform. The NRC staff reviewed the FMEA (Reference 28) to confirm that if the system does fail, it fails in a safe state. Failure mechanisms that affect a single leg of the triple-redundant system generally have no effect on system operation, therefore, the FMEA also considered (1) failure mechanisms that are recognized as being highly unlikely but could affect multiple components, and (2) the coincident occurrence of otherwise single failures (i.e., multiple failures). The results of the analysis show that, in general, failure modes that could prevent a Tricon V10 system from performing its safety function are detected by the built-in system diagnostics or by periodic testing. Also, the NRC staff concludes that the system is designed to fail into a safe mode.

The evaluation of response time and deterministic performance is discussed in Sections 3.4.1 and 3.4.2 of this SE. Although the Tricon V10 platform did not satisfy the response time criteria from EPRI TR-107330 for the test specimen executing the TSAP application, the platform did demonstrate credible response time characteristics that are suitable to support SR applications and satisfy the criteria of this clause at the platform level. The actual response times for particular safety functions are application specific and acceptable performance depends on the system design and safety function requirements. Thus, it is an ASAI to confirm the suitability of the response time characteristics of the Tricon V10 platform for particular safety functions and to demonstrate acceptable response times for each combination of input and output modules and system configurations that are relevant to the specific design. Consequently, evaluation for full conformance against this portion of the acceptance criteria remains for a plant-specific review.

Based on the review items discussed above, the NRC staff finds that the integrity characteristics (e.g., response time, deterministic performance, failure detection and response, fault tolerance, environmental withstand) of the Tricon V10 platform, when appropriately implemented, are suitable for SR applications at nuclear power plants and satisfy Clause 5.5 for the platform.

3.10.2.6 IEEE STD 603-1991 CLAUSE 5.6, "INDEPENDENCE"

Clause 5.6 of IEEE Std 603-1991 requires in part independence between: (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence" provides acceptance criteria for system integrity. This acceptance criteria states that three aspects of independence: (1) physical independence, (2) electrical independence, and (3) communications independence, should be addressed for each of the previously listed cases. Guidance for evaluation of physical and electrical independence is provided in RG 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems," which endorses IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. Transmission of signals between independent channels should be through isolation devices.

SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence," provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system.

Establishing independence for a safety system is an application-specific activity that requires an assessment of a full system design. Since the LTR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to promote independence. The Tricon V10 platform provides features to address electrical and communications independence. Physical independence is solely dependent on the design and implementation of the full safety system.

Independence between redundant portions of a safety system is addressed in Sections 3.1.2.8 and 3.7.1 of this SE. IOM has developed a Communication Application Safety Layer for SR communication between external processors (e.g., redundant channel Tricon V10 platforms) and the Tricon V10 system. This is an additional layer of protection provided by the communication protocols at the Application Layer of the network stack. The P2P and SAP protocols ensure end-to-end integrity of safety-critical messages. System architectures requiring data transfer between SR Tricons over a network would use the P2P protocol over an electrically and data isolated, point-to-point network. Architectures requiring safety-critical data exchange with SR video display units would utilize the SAP.

Independence between the SR Tricon V10 platform and other NSR systems is discussed in Sections 3.1.2.3 and 3.7.2 of this SE. There are two means of digital communications provided between the Tricon V10 platform and other NSR systems: Communications via the TCM and communications with RXMs.

Communications with NSR systems via the TCM is implemented in the same manner as described above for SR inter-channel communications, except the communications protocol would be different. However, electrical isolation is still accomplished via fiber optic communication links between the Tricon V10 and the NSR system. Data isolation between the Tricon V10 platform and the NSR systems is accomplished via communications through the IOCCOM processor and using dual ported RAM as a buffer as discussed in Section 3.7 of this SE.

Communications with NSR systems via remote extender chassis/modules extend the Tricon V10 PLC I/O bus to allow communications with the main chassis and expansion chassis. The RXMs are single-mode fiber optic modules that also provide ground loop isolation, which are suitable Class 1E to Non-Class 1E isolators between a SR main chassis and a NSR expansion chassis. Data isolation between the Tricon V10 platform and the NSR RXMs is accomplished via communications through the IOCCOM processor and using dual ported RAM as a buffer as discussed in Section 3.7 of this SE.

Therefore, on the basis of the electrical isolation design features of the TCM and RXM modules (as described in this SE), the NRC staff concludes that the electrical isolation provided between the Tricon V10 platform and attached systems/equipment via these modules satisfy the electrical independence requirement of Clause 5.6. Section 3.1.2.6 of this SE discusses the use of interposing processors (IOCCOM) to buffer the execution of the safety function by the MP (3008N) from the management of communications transactions via the TCM and RXMs. Section 3.7 of this SE addresses the evaluation of communications independence with respect to the guidance in DI&C-ISG-04. The NRC staff has determined that the platform communication capabilities of the Tricon V10 platform provide features that support communications independence, but the specific interconnections defined in an application must be determined and evaluated in an application-specific review. Thus, the review items cited above indicate provisions for electrical isolation and communications circuitry and protocols to promote communications independence. Consequently, the NRC staff concludes that the Tricon V10 platform complies with the electrical and communications provisions of Clause 5.6 at the platform level.

3.10.2.7 IEEE STD 603-1991 CLAUSE 5.7, "CAPABILITY FOR TEST AND CALIBRATION"

Clause 5.7 of IEEE Std 603-1991 states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. This clause further states that the testing of Class 1E systems be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station; however, appropriate justification must be provided; acceptable reliability of equipment operation must be demonstrated; and the capability shall be provided while the generating station is shut down.

SRP Chapter 7, Appendix 7.1-C, Section 5.7, "Capability for Test and Calibration," provides acceptance criteria for IEEE Std 603-1991 Clause 5.7. First, it states that guidance on periodic testing of the safety system is provided in RG 1.22, "Periodic Testing of Protection System Actuation Functions," and in RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," that endorses IEEE Std 338-1987. Section 5.7 acceptance criteria states that periodic testing should duplicate, as closely as practical, the overall performance required of the safety system, and that the test should confirm operability of both the automatic and manual circuitry. This capability should be provided to permit testing during power operation and that when this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Section 5.7 further states that test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation. Section 5.7 further states that for digital computer based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup.

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

The regulation at 10 CFR 50.36(c)(3), "Technical specifications," states that surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met. RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," which endorses IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," states that the protection system must be capable of accomplishing the required protective function in the presence of any single detectable failure concurrent with all identifiable, but non-detectable, failures. Consequently, self-testing and periodic testing are important elements in the design's ability to meet the single-failure criterion. SRP BTP 7-17 describes additional considerations in the evaluation of test provisions in digital computer based systems.

Determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements (e.g., accuracy) that apply. In addition, the establishment of the types of surveillance necessary for the safety system to ensure detection of identifiable single failures that are only announced through testing is an application-specific activity as well. Since the LTR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to enable testing and calibration for a redundant portion of a safety system (i.e., channel).

The Tricon V10 FMEA (see Section 3.5 of this SE) provided a systematic analysis of a representative (single-channel) system based on the Tricon V10 platform to determine the effect on the system (i.e., platform) of credible single failures. For each postulated failure mode, the FMEA determined ways in which the failure could be detected via platform automated diagnostics and self-testing. Diagnostics and self-test capabilities of the Tricon V10 platform are described in Section 3.4.3 of this SE. The level of diagnostic self-test capabilities of new modules in the Tricon V10 platform, including the 3008N MP module, is similar to the level of capabilities reviewed on the Tricon V9 platform. The NRC staff determined the diagnostic self-test capabilities are thorough and provide automatic detection of most identified failure modes at the platform level. The diagnostics are integrated into the Tricon V10 operating system software and data is made available to the application program concerning program operation, results of arithmetic operations, and other internal faults. Thus, requirements imposed on the application program relating to error detection are limited to providing appropriate error recovery and annunciation of faults. IOM also performs fault detection verification testing that verifies fault detection capabilities of the platform. Faults were injected into a live card connected to an operational Tricon V10 platform via extender cables. Faults were assessed through a maintenance terminal connected to a TCM module in the main chassis. The LTR describes acceptable use of software watchdog timers, memory checks, processing time checks, communications checks, and other tests in each type of component (or module) as appropriate to verify normal operation and detection of potential subtle system failures such as data errors and computer lockup (see Sections 3.4.3, 3.1.2.7, and 3.1.3.1 of this SE).

The Tricon V10 diagnostic and self-test features satisfy this requirement for test and calibration capabilities and are acceptable at the platform level. These capabilities may be cited in support of specific applications. Furthermore, the testing and calibration capabilities of the Tricon V10 platform have been demonstrated to be in compliance with RG 1.22, RG 1.118, and IEEE Std 338. The capability exists to permit testing of redundant channels during power operation. The design does not require disconnecting wires, installing jumpers, or otherwise modifying the installed equipment. Therefore, the Tricon V10 platform conforms to the requirements of Clause 5.7.

3.10.2.8 IEEE STD 603-1991 CLAUSE 5.8, "INFORMATION DISPLAYS"

Clause 5.8 of IEEE Std 603-1991 has four sub-clauses, 5.8.1, "Displays for Manually Controlled Actions," 5.8.2, "System Status Indication," 5.8.3, "Indication of Bypasses," and 5.8.4, "Location." Appendix 7.1-C, Section 5.8, "Information Displays," provides acceptance criteria for IEEE Std 603, Clause 5.8. This guidance states that the information displays for manually controlled actions should include confirmation that displays will be functional, and that safety system bypass and inoperable status indication should conform to the guidance of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

The design and location of information displays and operator workstations is an application specific activity. Since the LTR does not address a specific application nor include display devices permanently connected to the V10 platform (other than local platform LEDs) within the scope of the platform, no evaluation against this regulatory requirement could be performed.

3.10.2.9 IEEE STD 603-1991 CLAUSE 5.9, "CONTROL OF ACCESS"

Clause 5.9 of IEEE Std 603-1991 states that the safety system must be designed to permit administrative control of access to safety system equipment. SRP Chapter 7, Appendix 7.1-C, Section 5.9, "Control of Access," provides acceptance criteria for IEEE Std 601-1991, Clause 5.10. This acceptance criteria states that administrative control is acceptable to assure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access, and that digital computer based systems need to consider controls over electronic access, including access via network connections and maintenance equipment, to safety system software and data.

Establishing the particular approach for control of access to safety system equipment is an application-specific activity that depends on the system design. Physical access mechanisms depend on the specific implementation. The extent and nature of authorized human-system interactions depend on the allocation of function, operations and maintenance procedures, and human-machine interface capabilities addressed in a safety system design. In addition, the communication interconnections that may be provided between the safety system and other safety related or non-safety systems or equipment are generally dependent on the application. Since the LTR does not address a specific application, the evaluation against this requirement is limited to consideration of the means provided within the platform to control access to both hardware and software.

As described in Section 3.1.2.1 of this SE, the main chassis has a key switch that sets the following system operating modes:

- RUN – Normal operation with read-only capability by externally connected systems, including TriStation. Normally, the switch is set to this position and the key is removed and stored in a secure location.
- PROGRAM – Allows for control of the Tricon V10 system using an externally connected PC running the TriStation software, including application program downloads.
- STOP – Stops application program execution.
- REMOTE – Allows writes to application program variables by a TriStation PC or by MODBUS masters and external hosts.

The Tricon V10 is a modular, rack mounted platform that is housed in cabinets. However, the cabinets themselves are not identified as part of the base platform and thus are not within the scope of this review. Consequently, the mechanisms for physical access control cannot be evaluated in this review.

Although the Tricon V10 product line includes display and peripheral component (e.g., operator work stations) interface modules that can support online human-system interactions via the TCM, these modules are not within the scope of the platform under review. As submitted for review, the base architecture does contain provisions for external communication to the Tricon V10 platform across via the TCM by other devices (e.g., operator or testing/maintenance workstations). However, control of electronic access through provisions associated with HMIs is not within the scope of the LTR and cannot be evaluated in this review.

Application programming is generated using the TriStation 1131 Developer's Workbench, which runs on a standard PC. The TriStation 1131 serves as a maintenance workstation that supports the offline, out-of-service management (i.e., develops application programs and download those applications to the target Tricon V10 processor) of application software. The TriStation 1131 PC does not perform SR functions and would not normally be connected while the Tricon V10 is performing safety critical functions. However, it is physically possible for the TriStation PC to be connected at other times, and this should be prevented or controlled in such a manner so that the TriStation tool cannot affect the safety functions of the Tricon PLC via administrative control. Any such connection that may be established in a specific application would require additional review.

The NRC staff has evaluated the Tricon V10 platform features to provide control of access and finds that they are sufficient at the platform level. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.9.

3.10.2.10 IEEE STD 603-1991 CLAUSE 5.10, "REPAIR"

Clause 5.10 of IEEE Std 603-1991 states that safety systems must be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Chapter 7, Appendix 7.1-C, Section 5.10, "Repair" provides acceptance criteria for IEEE Std 601-1991 Clause 5.10. This acceptance criteria states that while digital safety systems may include self-diagnostic capabilities to aid in troubleshooting, the use of self-diagnostics does not replace the need for the capability for test and calibration systems as required by Clauses 5.7 and 6.5 of IEEE Std 603-1991.

The timely identification and location of malfunctioning Tricon V10 components is facilitated by platform and application-specific (hardware and software) features. Any diagnostic and self-test functions developed as part of the application software are outside the scope of this evaluation and will be evaluated in an application-specific review. The majority of Tricon V10 hardware is rack mounted and is replaced rather than repaired, which greatly facilitates timely repair. The Tricon V10 is triple redundant from input terminal to output terminal, as shown in Figure 2-2. The triple modular redundant (TMR) architecture is designed to allow continued system operation in the presence of any single point of failure within the system. The TMR architecture is also intended to allow the Tricon to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. The Tricon V10 boards contain board-edge LEDs to provide a visual indication of functional status of the platform hardware and software. In the presence of a fault, the Tricon V10 will alarm the condition, remove the affected portion of the faulted module from operation, and continue to function normally in a dual redundant mode. The affected module can be replaced and the system returns to the fully triple redundant mode of operation. To facilitate module replacement, the Tricon chassis includes provisions for a spare module, logically paired with a single input or output module. This design allows on-line, hot replacement of any module, under power while the system is running, with no impact on the operation of the application.

The platform software for the Tricon V10 includes diagnostic and self-test functions (see Section 3.4.3 of this SE). The Tricon V10 FMEA identifies failure modes that are automatically detected by diagnostic and self-test functions.

Based on the provision of automatic diagnostics and self-tests to detect and identify most failures of the platform, the NRC staff evaluation finds that the Tricon V10 platform complies with the requirements of Clause 5.10. However, it is necessary for an application-specific design to provide additional diagnostics or testing functions either as part of the application or as manually-conducted testing to address those system-level failures that are identified as detectable only through periodic surveillance. Thus, a plant-specific review would be necessary to address physical configuration and plant-specific installation conditions that impact safety system maintenance or to evaluate any necessary diagnostic, testing, or surveillance functions implemented in application software.

3.10.2.11 IEEE STD 603-1991 CLAUSE 5.11, "IDENTIFICATION"

Clause 5.11 of IEEE Std 603-1991 states that (1) safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," and IEEE Std 420-1982, "IEEE Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations," (2) identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes, (3) identification of safety system equipment and its divisional assignment shall not require frequent use of reference material, and (4) the associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 (R1990), "IEEE Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations." Clause 5.11 further states that components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification. SRP Chapter 7, Appendix 7.1-C, Section 5.11, "Identification," provides acceptance criteria for Clause 5.11 and cites the guidance in RG 1.75, "Criteria for Independence of Electric Systems," which endorses IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."

Identification of cabinets and cabling for a safety system is an application-specific activity. In addition, the particular means for identifying safety equipment according to redundant portions of a safety system (i.e., channels or divisions) is an application-specific activity. However, component identification for the Tricon V10 platform can contribute to fulfillment of this requirement. The IOM QA Program Manual defines requirements for the identification and control of items and provides procedures for establishing and maintaining system configuration management (Reference 49). Under its Configuration Management Program, IOM has established labeling, tracking and record keeping practices and capabilities to control the identification of components. In addition to faceplate identification of module type, IOM provides physical labels on the printed circuit board of each module to uniquely identify the hardware module and installed firmware. As part of the regulatory audits conducted at the IOM facility (Reference 6), the NRC staff observed component identification based on the physical labels applied to representative modules. Software identification includes version, revision and maintenance identifiers (e.g., V10.5.1) as described in EDM 24.00, "Software Configuration and Change Control." EDM 25.00, "Hardware Identification," describes the identification of components and sub-assemblies. Document control and numbering are described in EDM 22.00 and EDM 23.00.

The NRC staff finds that the identification procedures and methods for the Tricon V10 platform complies with this Clause 5.11 and are suitable to support fulfillment of this clause by a SR system. As noted above, identification of the redundant portions of a safety system (i.e., channels or divisions) is a plant specific activity. Any supplementary identification approach employed at the system-level will be addressed in a plant-specific review to assure satisfaction of Clause 5.11.

3.10.2.12 IEEE STD 603-1991 CLAUSE 5.12, "AUXILIARY FEATURES"

Clause 5.12 of IEEE Std 603-1991 states that auxiliary supporting features meet all requirements of this standard, and that auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions and are not isolated from the safety system shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. SRP Chapter 7, Appendix 7.1-C, Section 5.12, "Auxiliary Features," provides acceptance criteria for Clause 5.12 and cites SRP BTP 7-9, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," as providing specific guidance for the review of anticipatory trips that are auxiliary features of a reactor protection system.

Determination of auxiliary supporting features for a safety system is an application-specific activity. Since the LTR does not address a specific application, no evaluation of the Tricon V10 platform against this regulatory requirement could be performed.

3.10.2.13 IEEE STD 603-1991 CLAUSE 5.13, "MULTI-UNIT STATIONS"

Clause 5.13 of IEEE Std 603-1991 states that the sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired, and that guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1980 "IEEE Standard Criteria for Class IE Power Systems for Nuclear Power Generating Stations," and guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1988, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems." SRP Chapter 7, Appendix 7.1-C, Section 5.13, "Multi Unit Stations," provides acceptance criteria for Clause 5.13. This acceptance criterion states that the shared user interfaces must be sufficient to support the operator needs for each of the shared units. Implementation of a safety system in a multi-unit station and determination of components can be shared is an application-specific activity. Since the LTR does not address a specific application, no evaluation of the Tricon V10 platform against this regulatory requirement could be performed.

3.10.2.14 IEEE STD 603-1991 CLAUSE 5.14, "HUMAN FACTORS CONSIDERATIONS"

Clause 5.14 of IEEE Std 603-1991 states that human factors be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operators and maintainers can be successfully accomplished to meet the safety system design goals. SRP Chapter 7, Appendix 7.1-C, Section 5.14, "Human Factors Considerations," provides acceptance criteria for Clause 5.14, and states that safety system human factors design should be consistent with the applicant/licensee's commitments documented in Chapter 18 of the Updated Safety Analysis Report (USAR).

Implementation of human factors considerations to address functional allocation is an application-specific activity. Since the LTR does not address a specific application nor include display devices within its scope, no evaluation of the Tricon V10 platform against this regulatory requirement could be performed.

3.10.2.15 IEEE STD 603-1991 CLAUSE 5.15, "RELIABILITY"

Clause 5.15 of IEEE Std 603-1991 states that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved, and that IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis. SRP Chapter 7, Appendix 7.1-C, Section 5.15, "Reliability," provides acceptance criteria for Clause 5.15. This acceptance criterion states that the applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed and that for computer systems, both hardware and software reliability should be analyzed. The acceptance criteria further states that software that complies with the quality criteria of IEEE Std 603-1991 Clause 5.3 and that is used in safety systems that provide measures for defense against common cause failures, as previously described for IEEE Std 603-1991 Clause 5.1, are considered by the NRC staff to comply with the fundamental reliability requirements of GDC 21, IEEE Std 279-1971, and IEEE Std 603-1991.

SRP Chapter 7, Appendix 7.1-C, Section 5.15 further states that the assessment of reliability should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures, and that hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common cause failures, cascading failures, and undetected failures. SRP Chapter 7, Appendix 7.1-C, Section 5.15 also references SRP Chapter 7, Appendix 7.1-D, and states quantitative reliability goals are not sufficient as a sole means of meeting the Commission's regulations for the reliability of digital computers used in safety systems. The regulation at 10 CFR Part 50, Appendix A, GDC 21, "Protection system reliability and testability," requires in part that the protection system be designed for high functional reliability commensurate with the safety functions to be performed.

Determination of the reliability of a safety system is an application-specific activity that requires an assessment of a full system design. Since the LTR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures, the evaluation against this requirement is limited to consideration of the reliability characteristics of the Tricon V10 platform and its components.

An FMEA was performed in accordance with IEEE Std 352-1987 based on a generic reference system architecture. The NRC staff's evaluation of the FMEA determined that it provides an effective assessment of the potential failure modes and the effect of those failures at the platform level. Based on the use of redundancy, diagnostics and self-tests, no undetectable single failures of the Tricon V10 platform were identified in the FMEA. However, an extension of the analysis to address the effects of software CCF is necessary for an application-specific FMEA to support a conclusion about defense against CCFs in a digital safety system based on the Tricon V10 platform.

IOM performed a reliability and availability analysis of the Tricon V10 platform as specified in Section 4.2.3 of EPRI TR-107330 and documented the results in IOM Document No. 9600164-532, "Reliability / Availability Study for the Tricon V10" (Reference 47). Calculations were done for periodic test intervals ranging from 6 to 30 months. In all cases, the calculated reliability and availability were greater than 99.9 percent, which exceeds the recommended goal of 99.0 percent from the EPRI TR. For a periodic test interval of 18 months (corresponding to the typical nuclear power plant refueling outage cycle), the reliability is 99.9987 percent and the availability is 99.9990 percent.

The NRC staff reviewed this study, and agrees that the results of the reliability and availability analysis of the Tricon V10 platform satisfy the criteria of Clause 5.15.

Based on the evaluation, the NRC staff finds that the results of the IOM reliability and availability analysis provide supporting evidence to indicate that the Tricon V10 platform is suitable for use in SR applications in a nuclear power plant. However, an application-specific reliability and availability analysis must be developed to demonstrate full compliance with this Clause.

3.10.3 IEEE STD 603-1991 CLAUSE 6, "SENSE AND COMMAND FEATURES – FUNCTIONAL AND DESIGN REQUIREMENTS"

The requirements of this clause, in addition to the requirements of Clause 5, apply to the Sense and Command Features of a safety system. The sub-clauses of this requirement are given by the following:

Clause 6.1	Automatic Control
Clause 6.2	Manual Control
Clause 6.3	Interaction between Sense and Command Features and other Systems
Clause 6.4	Deviation of System Inputs
Clause 6.5	Capability for Testing and Calibration
Clause 6.6	Operating Bypass
Clause 6.7	Maintenance Bypass
Clause 6.8	Setpoints

SRP Chapter 7, Appendix 7.1-C, Section 6, "Sense and Command Features – Functional and Design Requirements," provides acceptance criteria for Clause 6.

The functional and design requirements for the sense and command features of a safety system are dependent solely on the specific application. Since the LTR does not address a specific application of the platform, include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the Tricon V10 platform against these regulatory requirements could be performed.

Although the requirement for setpoints primarily addresses factors beyond the scope of the digital platform (i.e., plant design basis limits, modes of operation, and sensor accuracy), the contribution of the Tricon V10 platform to setpoint uncertainty must be addressed in an application-specific analysis. The "Tricon V10 EQ Summary Report," IOM Document No. 9600164-545 (Reference 24), describes the Tricon V10 system accuracy, which is documented in the "Tricon System Accuracy Specifications," IOM Document No. 9600164-534 (Reference 58). As part of the Tricon V10 platform qualification effort, system accuracy specifications for the Tricon V10 system were established. The accuracy specifications are documented in accordance with Section 4.2.4 of EPRI TR-107330 and provide information required by EPRI TR-107330 to support an application specific setpoint analysis per the International Society of Automation Recommended Practice 67.04, "Setpoints for Nuclear Safety-Related Instrumentation," standard. Section 4.2.4 of the EPRI TR identifies the specific information to be provided. The System Accuracy report provides a single concise listing of the accuracy specifications of the IOM Tricon V10 platform. The specifications documented are those typically used by nuclear industry users for calculating instrument measurement uncertainties and establishing critical control setpoints.

As stated in the System Accuracy Specifications, the Tricon will maintain its rated reference accuracy specifications over extended periods. As stated in the Failure Modes and Effects Analysis, failure of components affecting the rated reference accuracy are detected, and the system will generate an alarm and the faulted module will be indicated. Response to the alarm would require replacement of the faulted module and restoration of normal operation. No field adjustments or calibrations of the Tricon are required or possible. The key in the Tricon design is its TMR architecture. By performing continuous cross comparisons between the triplicated values, a true and full verification of actual input and output values is maintained. The effects of calibrated accuracy including drift over time, hysteresis and non-linearity, and repeatability are applicable to the Tricon system and I/O modules, and their error contributions are specified in the System Accuracy Specifications document. The effects of temperature sensitivity, power supply variations, arithmetic operations errors, vibration, radiation and relative humidity are not applicable to the Tricon system and I/O modules and their error contribution is zero.

The specifications cover all Tricon V10 components and modules that were subjected to performance and qualification testing. The information provided satisfies the requirements stated in Section 4.2.4 of TR-107330 and therefore satisfies Clause 6.8 at the platform level. The configuration of the safety system will be unique for each user depending on the plant specific application of the Tricon V10 platform. The applicability of specified terms and approach to determining overall "system" uncertainty with respect to the data contained within this report is the responsibility of the end user and will be reviewed on an application specific basis. Applicability of uncertainty terms and the methodology for determination of uncertainty should be in accordance with the plant specific setpoint and uncertainty programs or other administrative guidelines.

3.10.4 IEEE STD 603-1991 CLAUSE 7, "EXECUTE FEATURES – FUNCTIONAL AND DESIGN REQUIREMENTS"

The requirements of this clause, in addition to the requirements of Clause 5, apply to the Execute Features of a safety system. The sub-clauses of this requirement are given by the following:

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

SRP Chapter 7, Appendix 7.1-C, Section 7, "Execute Features - Functional and Design Requirements," provides acceptance criteria for Clause 7.

The functional and design requirements for the execute features of a safety system are dependent solely on the specific application. Since the LTR does not address a specific application of the platform, include the actuators or other execute features, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the Tricon V10 platform against these regulatory requirements could be performed.

Although the requirement for automatic control addresses the execute features are outside the scope of the digital platform, the acceptance criteria guidance in SRP Chapter 7, Appendix 7.1-C, Section 7.1, “Automatic Control,” states that the evaluation should also confirm that real-time performance of a digital safety system is deterministic and known. The evaluation of deterministic performance characteristics of the Tricon V10 platform is contained in Section 3.4.2 of this SE and is acceptable for demonstrating that the Tricon V10 platform complies with this requirement.

3.10.5 IEEE STD 603-1991 CLAUSE 8, “POWER SOURCE REQUIREMENTS”

Clause 8 of IEEE Std 603-1991 states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems, and that specific criteria unique to the Class 1E power systems can be found in IEEE Std 308-1980. This clause also states that for power systems with a degree of redundancy, the safety functions and acceptable reliability must be retained while power sources are in maintenance bypass. SRP Chapter 7, Appendix 7.1-C, Section 8, does not provide acceptance criteria for IEEE Std 603-1991 Clause 8.

Determination of the power sources to be provided to a safety system is an application specific activity. Since the LTR does not address a specific application of the platform, the evaluation against this regulatory requirement is limited to the capabilities and characteristics of the Tricon V10 platform that are relevant for adherence to Clause 8 and its sub-clauses.

Clauses 8.1 and 8.2 address requirements for electrical power sources and nonelectrical power sources, respectively to the safety system. The Tricon V10 platform only uses electrical power and the platform scope does not include the AC power source(s), which is application-specific. Thus, no evaluation of the Tricon V10 platform against these regulatory requirements could be performed.

Clause 8.3 addresses the capability of the safety system to accommodate maintenance bypass of redundant power sources. The Tricon V10 platform employs power supply modules that are rated for 175 watts, which is sufficient to supply the power requirements of a fully populated chassis. Two different power supply modules can be used in a single chassis. Three qualified models are available to support different power sources: 120 VAC or VDC, 230 VAC, and 24 VDC. The power supply modules possess built in diagnostic circuitry to check for out-of-range voltages and/or over temperature conditions. Indicator light emitting diodes (LEDs) on the front face of each power module provide module status.

As shown in Figure 2-3, the Tricon V10 backplane is designed with dual independent power rails. Both power rails feed each of the three legs on each I/O module and each main processor module residing within the chassis. Power to each of the three legs is independently provided through dual voltage regulators on each module. Each power rail is fed from one of the two power supply modules residing in the chassis. Under normal circumstances, each of the three legs on each I/O module and each main processor module draw power from both power supplies through the dual power rails and the dual power regulators. Should one of the power supplies or its supporting power line fails (or is removed for maintenance), the other power supply will increase its power output to support the requirements of all modules in the chassis. Thus, the platform provides suitable capability to enable the safety system to function while one redundant AC power source is failed or in bypass. While this evaluation indicates the suitability of the platform to satisfy this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 8.

Therefore, the NRC staff has determined that the Tricon V10 platform satisfies the requirements of 10 CFR 50.55a(h) with regard to IEEE Std 603-1991.

3.11 CONFORMANCE WITH IEEE STD 7-4.3.2-2003

RG 1.152, Revision 2, “IEEE Standard Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” states that conformance with the requirements of IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” is a method that the NRC staff has deemed acceptable for satisfying the Commission’s regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. SRP Chapter 7, Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std 7-4.3.2,” contains guidance for the evaluation of the application of the requirements of IEEE Std 7-4.3.2-2003. This section documents the evaluation of the Tricon V10 platform against this guidance.

The Regulatory Position in RG 1.152 provides guidance that establishment of a secure environment be addressed in the development process. SRP acceptance criteria for this guidance can be found in SRP Chapter 7, Appendix 7.1-D, Section 9 and DI&C-ISG-01. The evaluation of the Tricon V10 platform against this guidance is contained in Section 3.8 of this SE.

The requirements of IEEE Std 7-4.3.2-2003 supplement the requirements of IEEE Std 603-1991 by specifying criteria that address hardware, software, firmware, and interfaces of computer based safety systems. Consequently, the structure of IEEE Std 7-4.3.2-2003 parallels that of IEEE Std 603-1991. For those clauses where IEEE Std 7-4.3.2-2003 contains no requirements beyond those found in IEEE Std 603-1991 and SRP Chapter 7, Appendix 7.1-D contains no additional guidance, no review for compliance with IEEE Std 7-4.3.2-2003 is required. Thus, the subsections below are limited to those clauses where further evaluation is warranted. The review against the driving clauses of IEEE Std 603-1991 is documented in the corresponding subsections of Section 3.10 in this SE.

3.11.1 IEEE STD 7-4.3.2-2003 CLAUSE 5, “SAFETY SYSTEM CRITERIA”

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

The implementation of a computer-based safety system is an application-specific activity. Since the LTR does not address a specific application, the evaluation against the following requirements addresses the capabilities and characteristics of the Tricon V10 platform that are relevant for adherence to each requirement.

3.11.1.1 IEEE STD 7-4.3.2-2003 CLAUSE 5.3, “QUALITY”

Clause 5.3 states that computer development activities must include the development of computer hardware and software. In addition, Clause 5.3, also states that the integration of computer hardware and software and the integration of the computer with the safety system must be addressed in the development process. SRP, Chapter 7, Appendix 7.1-C, Section 5.3, states that SRP, BTP 7-14 contains SRP acceptance criteria for software development processes.

The computer development activities of the Tricon platform were reviewed and approved as part of the Tricon V9 LTR (Reference 34); these activities included the development of the computer hardware and platform software. Changes to the Tricon platform computer development process were evaluated in Section 3.2 of this SE, and determined to be acceptable. The NRC staff found that the integration of computer hardware and software is a planned activity in the Tricon V10 platform software development process.

The subsections below contain the evaluation of the Tricon V10 platform against the specific criteria of the sub-clauses of IEEE Std 7-4.3.2-2003, Clause 5.3.

3.11.1.1.1 IEEE STD 7-4.3.2-2003 CLAUSE 5.3.1, "SOFTWARE DEVELOPMENT"

Clause 5.3.1 of IEEE Std 7-4.3.2-2003 requires an approved QA plan consistent with the requirements of IEEE/EIA 12207.0-1996 for all software that is resident at runtime. EPRI TR-106439, as accepted by the NRC SE dated July 17, 1997, and EPRI TR-107330, as accepted by the NRC SE dated July 30, 1998 provide guidance for the evaluation of existing commercial computers and software.

The Tricon platform SQAP was evaluated and approved as part of the review of the Tricon V9 LTR (Reference 34), and changes to this SQAP were determined to be acceptable (see Section 3.2 of this SE). Based on these evaluations, the NRC staff has determined that the Tricon V10 platform conforms to Clause 5.3.1.

3.11.1.1.1.1 IEEE STD 7-4.3.2-2003 CLAUSE 5.3.1.1, "SOFTWARE QUALITY METRICS"

Clause 5.3.1.1 of IEEE Std 7-4.3.2-2003 states that the use of software quality metrics requirements are being met. SRP Appendix 7.1 -D, Section 5.3.1.1, states that metrics are considered in the review of the software development process in accordance with SRP, BTP 7-14.

Since the platform pre-developed software was dedicated rather than developed under the current IOM software QA program, this requirement does not apply within the context of the scope of the LTR. An evaluation of metric usage for application software development will be conducted as part of a plant-specific review for any system based on the Tricon V10 platform.

3.11.1.1.2 IEEE STD 7-4.3.2-2003 CLAUSE 5.3.2, "SOFTWARE TOOLS"

Clause 5.3.2 of IEEE Std 7-4.3.2-2003 states that software tools used to support software development processes and V&V processes shall be controlled under configuration management, and that the tools shall either be developed to a similar standard as the safety related software, or that the software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities. SRP, Chapter 7, Appendix 7.1-D, provides guidance for the evaluation of software tool use.

IOM does not credit any software tools in the development of the Tricon V10 platform other than the TriStation 1131 as described in Sections 3.1.3.2 and 3.1.3.4 of this SE. The TriStation 1131 software has undergone changes as described in the Tricon V10 LTR, and the NRC staff has evaluated and approved the new version (see Section 3.1.3.2). The TriStation 1131 software is maintained under the IOM Configuration Management Program described in EDM 20.00 (Reference 49). Software developed with this tool is manually verified (i.e., independently verified and validated) by IOM to ensure that any defects not detected by the tool will be detected. The software validation program for the TriStation 1131 was reviewed and approved in the Tricon V9 LTR (Reference 34), which has not changed since then.

Based on the above, the NRC staff determined that the use of the TriStation 1131 tool for software development is consistent with the requirements in this clause and is therefore acceptable.

3.11.1.1.3 IEEE STD 7-4.3.2-2003 CLAUSE 5.3.3, "VERIFICATION AND VALIDATION"

Clause 5.3.3 states that a V&V program must address hardware, software, integration of digital components, and interaction with the nuclear power plant. The V&V program must exist throughout the entire system life cycle. SRP Appendix 7.1-C states that the software V&V effort should be performed in accordance with IEEE Std 1012-1998, which is endorsed by RG 1.168, Revision 1.

The NRC staff used RG 1.168 and IEEE Std 1012 to evaluate the V&V process used for the Tricon V9 SER (Reference 9). During this review, the NRC staff concluded that although IOM did not strictly follow IEEE Std 1012 guidelines, the combination of the internal IOM review, the TÜV certification, and the review by external consultants, provided confidence that the verification and validation activities related to the Tricon V9 platform software were adequate. The NRC staff further concluded that the Tricon V9 platform verification and validation activities are acceptable for software that is intended for SR use in nuclear power plants. However, acceptance of the Tricon V9 platform was based to a large degree on the TÜV-Rheinland independent review, and the SER noted that any future version of the Tricon system will require an equivalent level of independent V&V in order to be considered acceptable for SR use in nuclear power plants.

As stated in Section 3.2.1 of this SE, the hardware and software changes developed to support the Tricon V10 were dedicated for SR service. The V&V process used for the Tricon V10 platform, as documented in IOM documents EDM 90.00, "Product Verification" (Reference 50), and EDM 90.10, "Product Validation" (Reference 51), is essentially the same as was used for the Tricon V9 software with exception of the changes noted and approved in Section 3.2.1 of this SE. The IOM V&V evaluations document that the Tricon V10 platform underwent a combination of the internal IOM review, the TÜV certification, and the review by external consultants. Furthermore, the NRC staff audited (Reference 6) the V&V process and results that were implemented for the Tricon V10 platform. The combination of these activities provide confidence that the verification and validation activities related to the Tricon V10 software were adequate and the Tricon V10 platform verification and validation activities are acceptable for software that is intended for SR use in nuclear power plants. However, acceptance of the Tricon V10 PLC system is based to a large degree on the TÜV-Rheinland independent review, and any future version of the Tricon system will require an equivalent level of independent V&V in order to be considered acceptable for SR use in nuclear power plants. Based on these evaluations the NRC staff has determined that the Tricon V10 platform V&V program conforms to Clause 5.3.3.

3.11.1.1.4 IEEE STD 7-4.3.2-2003 CLAUSE 5.3.4, "INDEPENDENT V&V REQUIREMENTS"

Clause 5.3.4 of IEEE Std 7-4.3.2-2003 defines the levels of independence required for the V&V effort, in terms of technical independence, managerial independence, and financial independence. SRP, Chapter 7, Appendix 7.1-D, Section 5.3.4, provides detailed guidance to assist the reviewer in determining the extent of independence of the V&V activities from the design activities in terms of technical, managerial, and financial aspects.

The independence provided by the V&V activities and QA organization for the Tricon V10 software QA program is discussed in Section 3.2 of this SE. As discussed above, the V&V process used for the V10 platform (References 50 and 51) does not comply with IEEE Std 1012 guidelines and is essentially the same as was used for the V9 software with exception of the changes noted and approved in Section 3.2.1 of this SE. However, the IOM V&V evaluations document that the Tricon V10 platform underwent a combination of the internal IOM review, and a review by three independent external organizations; TÜV, MPR and Associates, and JLM Digitech Digital Licensing Services. The results of these independent reviews are documented in References 52, 32, and 25, respectively. The combination of these activities provide confidence that the verification and validation activities related to the Tricon V10 platform software were performed with sufficient independence to satisfy the concepts of IEEE Std 1012. However, acceptance of the Tricon V10 platform V&V independence is based on the TÜV-Rheinland independent review, and any future version of the Tricon PLC system will require an equivalent level of independent V&V in order to be considered acceptable for SR use in nuclear power plants. Based on these evaluations the NRC staff has determined that the Tricon V10 platform V&V program conforms to Clause 5.3.4.

3.11.1.1.5 IEEE STD 7-4.3.2-2003 CLAUSE 5.3.5, "SOFTWARE CONFIGURATION MANAGEMENT"

Clause 5.3.5 of IEEE Std 7-4.3.2-2003 states that software configuration management (SCM) shall be performed in accordance with IEEE Std 1042-1987, and that IEEE Std 828-1998 provides guidance for the development of software configuration management plans. IEEE Std 828-1990 and IEEE Std 1042-1987 are endorsed by RG 1.169. SRP, Chapter 7, Appendix 7.1-D, states that BTP 7-14 and RG 1.169 provide SRP acceptance criteria for SCMPs and activities.

The SCM program as described in EDM 20.00, "Configuration Management," EDM 24.00 , "Software Configuration and Change Control", EDM 40.50 "Software Development Guidelines," and IOM Document No. 7286-545-1 (Reference 4) was used for Tricon V10 software components (see Section 3.2.1 of this SE). The IOM CMP has undergone some changes from the approved Tricon V9 program. These changes were reviewed and approved in Section 3.2.1. The NRC staff found that the current configuration management program and practices of IOM comply with the guidance identified in IEEE Std 828 and IEEE Std 1042, which are endorsed by RG 1.169. Furthermore, the NRC staff concludes that the QAM, QPM, and EDM meet the configuration management provisions outlined in BTP-14 and are, therefore, acceptable for satisfying the regulatory criterion of Clause 5.3.5.

3.11.1.1.6 IEEE STD 7-4.3.2-2003, CLAUSE 5.3.6, SOFTWARE PROJECT RISK MANAGEMENT

Clause 5.3.6 defines the risk management required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.3.6, "Software Project Risk Management" provides acceptance criteria for software project risk management. This section states that software project risk management is a tool for problem prevention, and be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. It also states that software project risks may include technical, schedule, or resource related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform SR functions.

The Tricon V10 upgrade project used a standardized project management process to assess project risks. This methodology is documented in EDM 20.10, "Project Planning, Revision 7.1," as documented in the LTR (Reference 4) and is used to identify, assess, monitor, and control areas of risk that arise during the software development project. The project risks are identified in the Engineering Project Plan (EPP) regarding any risks with which or assumptions without which, the project would be in jeopardy of not meeting its stated objectives. Measures taken to mitigate risks are described in the EPP. During execution of the project, project risks are monitored, and measures are taken to mitigate or eliminate the risk to the project in accordance with the EPP. The NRC staff has reviewed the IOM Project Planning process and determined that the Tricon V10 platform conforms to Clause 5.3.6.

3.11.1.2 IEEE STD 7-4.3.2-2003 CLAUSE 5.4, "EQUIPMENT QUALIFICATION"

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

3.11.1.2.1 IEEE STD 7-4.3.2-2003 CLAUSE 5.4.1, "COMPUTER SYSTEM TESTING"

Clause 5.4.1 of IEEE Std 7-4.3.2-2003 discusses the software that should be operational on the computer system while qualification testing is being performed. SRP Chapter 7, Appendix 7.1-D, Section 5.4.1, "Computer System Testing," provides acceptance criteria for computer equipment qualification testing. This section states that computer equipment qualification testing should be performed while the computer is functioning, with software and diagnostics that are representative of those used in actual operation. Section 3.3 of this SE discusses the evaluation of the environmental qualification program for the Tricon V10 platform. IOM complied with the guidance of EPRI TR-107330 for the generic qualification of a PLC platform. EPRI TR-107330, Section 6.2.2, "Test Specimen Application Program Configuration Requirements," specifies development of a synthetic application program to verify the PLC functionality under the full range of service conditions (i.e., normal conditions as well as environmental extremes). In addition, Table 5.1 of EPRI TR-107330 specifies the testing conditions under which specific tests must be executed. Section 3.3 of this SE discusses the TSAP developed by IOM for its generic qualification program. The TSAP was specifically designed to support qualification testing of the Tricon V10 platform while providing functionality representative of SR applications.

Based on evaluation in Section 3.3 of this SE and review of the design, testing, and qualification test plans and procedures for the TSAP (IOM Document Nos. 9600164-513, Revision 2, and 9600164-536, Revision 0 (References 39 and 40)), the NRC staff concludes that the IOM qualification program meets the requirement for computer testing of the Tricon V10 platform and satisfies the requirements of this Clause.

3.11.1.2.2 IEEE STD 7-4.3.2-2003 CLAUSE 5.4.2, "QUALIFICATION OF EXISTING COMMERCIAL COMPUTERS"

Clause 5.4.2 defines the Qualification of Existing Commercial Computers for use in SR applications in nuclear power plants. SRP Chapter 7, Appendix 7.1-D, Section 5.4.2, "Qualification of Existing Commercial Computers," provides acceptance criteria for equipment qualifications. This section states that EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications", and EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants," provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

The qualification of the Tricon V9 equipment was addressed in the Tricon V9 LTR and associated SE (References 34 and 9). Changes to this approved system that were invoked to develop the Tricon V10 platform have been evaluated in Sections 3.2.1, 3.3, and 3.7.1 of this SE and found to comply with the regulations. Therefore, the Tricon V10 platform conforms to Clause 5.4.2.

3.11.1.3 IEEE STD 7-4.3.2-2003, CLAUSE 5.5, "SYSTEM INTEGRITY"

Clause 5.5 states that in addition to the system integrity criteria provided by IEEE Std 603-1998, the digital system shall be designed for computer integrity, test and calibration, and fault detection and self-diagnostics activities. These attributes are further defined in IEEE Std 7-4.3.2-2003, Clause 5.5.1, "Design for computer integrity," Clause 5.5.2, "Design for test and calibration," and Clause 5.5.3, "Fault detection and self-diagnostics"; these sub-clauses are evaluated in the subsections below. There are no specific acceptance criteria shown in SRP Chapter 7, Appendix 7.1-D, Section 5.5, "System Integrity."

3.11.1.3.1 IEEE STD 7-4.3.2-2003 CLAUSE 5.5.1, "DESIGN FOR COMPUTER INTEGRITY"

Clause 5.5.1 of IEEE Std 7-4.3.2-2003 states that the computer must be designed to perform its safety function when subjected to conditions, either external or internal, that have significant potential for defeating the safety function.

The Tricon V10 system is triple redundant from input terminal to output terminal (as described in Section 3.1 of this SE). The TMR architecture is intended to allow continued system operation in the presence of any single point of failure within the system. The TMR architecture is also intended to allow the Tricon V10 to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. In the presence of a fault, the Tricon V10 will alarm the condition, remove the affected portion of the faulted module from operation, and continue to function normally in a dual redundant mode. The system returns to the fully triple redundant mode of operation when the affected module is replaced.

The Tricon V10 platform has redundant power supplies and backup batteries that supply the TMR system. The redundant features of the Tricon V10 system are described in Section 3.1.1 of this SE. The TMR design redundancy provides fault tolerant capabilities which, coupled with diagnostics and self-testing as discussed in Section 3.4.3 of this SE, provides a high-level of computer integrity. Furthermore, the computer qualification activities documented by IOM, which are discussed in Sections 3.2, 3.2.1, and 3.3, provide suitable evidence that the Tricon V10 platform is capable of handling conditions, external or internal, that have the potential to defeat implemented safety functions. Specifically, the NRC staff review of the platform's capability to withstand single failures in Section 3.5 of this SE, the demonstration of environmental withstand (subject to noted generic open items) in Section 3.3, and the provisions for security (SDOE) in Section 3.6, supports the determination that the Tricon V10 platform satisfies Clause 5.5.1.

3.11.1.3.2 IEEE STD 7-4.3.2-2003 CLAUSE 5.5.2, "DESIGN FOR TEST AND CALIBRATION"

Clause 5.5.2 of IEEE Std 7-4.3.2-2003 states that test and calibration functions shall not adversely affect the ability of the computer to perform its safety function, and that it shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change. The clause further states that V&V, configuration management, and QA be required for test and calibration functions on separate computers such as test and calibration computers that provide the sole verification of test and calibration data, but that V&V, configuration management, and QA is not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

Determination of the test and calibration requirements for a safety system that must be fulfilled depends upon the plant-specific safety requirements that apply and establishment of the types of surveillance necessary for the safety system to ensure that the identifiable single failures only identified through testing are application-specific activities. Since the LTR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to enable testing and calibration of an implemented system. Online diagnostics and self-tests are provided by the Tricon V10 to support test and calibration requirements in general. The methods for calibration of Tricon V10 platform in the field are not within the scope of the LTR so this capability is not reviewed in this SE. The qualification tests performed for the Tricon V10 platform were conducted with diagnostics executing in conjunction with a TSAP application program simulating safety system functions (see Section 3.3 of this SE). The performance of these tests demonstrated that the diagnostics and self-tests did not adversely affect the ability of the computer to perform its simulated safety functions. Therefore, the NRC staff concludes that the diagnostic and self-test capabilities provided by the Tricon V10 platform conform to the requirements of Clause 5.5.2.

3.11.1.3.3 IEEE STD 7-4.3.2-2003 CLAUSE 5.5.3, "FAULT DETECTION AND SELF-DIAGNOSTICS"

Clause 5.5.3 of IEEE Std 7-4.3.2-2003 discusses fault detection and self-diagnostics, and states that if reliability requirements warrant self-diagnostics, then computer programs should contain functions to detect and report computer system faults and failures in a timely manner, and that these self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function.

The software-based Tricon V10 diagnostics and self-test capabilities provide extensive and thorough coverage of the identified failure modes from the FMEA performed by IOM (see Sections 3.4.3 and 3.5 of this SE for discussions of diagnostic and test software and the Tricon V10 FMEA, respectively). The Tricon V10 PLC system provides continuous self-testing, including monitoring memory and memory reference integrity, using watchdog timers, monitoring communication channels, monitoring central processing unit status, and checking data integrity. The Tricon V10 PLC system performs self-tests and I/O validation on each module. The Tricon V10 PLC system TMR architecture provides continuous self-testing to detect, tolerate, and alarm on single internal failures. The internal self-test functions are transparent to the application program and are an integral part of the base platform operating software. These diagnostics check each main processor, as well as each I/O module and communication channel. Transient faults are recorded and masked by the hardware majority-voting circuit. Persistent faults are diagnosed, and the faulted module can be replaced or operated in a fault-tolerant manner until replacement is completed.

The NRC staff reviewed these self-test capabilities, and finds them acceptable to satisfy Clause 5.5.3 at the platform level. However, implementation of the Tricon V10 platform into an application specific safety system may require additional fault-detection and diagnostic capabilities be implemented as part of the application or system design to provide more comprehensive coverage of identified failures with automatic tests and diagnostics. Therefore, a plant-specific evaluation is necessary to establish full conformance with Clause 5.5.3.

3.11.1.4 IEEE STD 7-4.3.2-2003 CLAUSE 5.6, "INDEPENDENCE"

Clause 5.6 of IEEE Std 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std 603-1991, data communications between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function. In addition, if safety and non-safety software reside on the same computer and use the same computer resources, then the non-safety software functions shall be developed in accordance with SR software development practices. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence," provides acceptance criteria for communication between the safety systems and non-safety systems. This section states that the regulation at 10 CFR Part 50, Appendix A, GDC 24, "Separation of protection and control systems," requires the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired. The ISG 4 was developed to address communication independence.

Establishment of communications among redundant portions of a safety system or between the safety system and other non-safety systems in a plant is an application specific activity. The base platform architecture identified in the LTR does not specify any direct connections or bi-directional communications between the Tricon V10 platform and any other system external to the Tricon V10 system. Since the LTR does not address a specific application or provide a definitive safety system design, the evaluation of the Tricon V10 platform against the communications independence aspect of this regulatory requirement is limited to features and capabilities of its communication interfaces.

The Tricon V10 platform does not contain any NSR software. The description of the communications independence and interconnections for the Tricon V10 platform is contained in Sections 3.7 and 3.7.1 of this SE. Section 3.4.2 of this SE discusses the deterministic performance characteristics.

The NRC staff evaluated data independence between redundant portions of a safety system or between non-safety systems in Sections 3.1.2.3, 3.1.2.8, 3.7.1, and 3.7.2 of this SE.

Section 3.7.3 provides the NRC staff's evaluation of the Tricon V10 platform data communication features independence per DI&C ISG-04. Based on these evaluations the NRC staff has determined that the digital Tricon V10 platform conforms to Clause 5.6. However, the specific interconnections defined for a plant specific safety application must be determined and evaluated in a plant-specific review.

3.11.1.5 IEEE STD 7-4.3.2-2003 CLAUSE 5.11, "IDENTIFICATION"

Clause 5.11 of IEEE Std 7-4.3.2-2003 states that: (1) identification requirements specific to software systems (i.e., firmware and software identification) shall be used to assure the correct software is installed in the correct hardware component, (2) means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools, and (3) physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std 603-1991 Clause 5.11. SRP Chapter 7, Appendix 7.1-D, Section 5.11, "Identification" provides acceptance criteria and adds that the identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation that identifies the changes made by that revision for computer equipment qualification.

The IOM QA Program Manual defines requirements for the identification and control of items and provides procedures for establishing and maintaining system configuration management in EDM 20.00 (Reference 49). Under this Configuration Management Program (CMP), IOM has established labeling, tracking and record keeping practices and procedures to control the identification of hardware and software components. All documents, drawings, and source code identified as deliverables in the Engineering Project Plan (EPP) are maintained under strict configuration management. The Tricon V10 platform configuration management measures began early in the Tricon V10 platform development cycle, at the subcomponent/module level, to assure an orderly and controlled development process. Configuration management was applied to software, hardware, and design documentation at an appropriate point in the process when the item was given a unique identity and baseline, and when subsequent configuration tracking of the item was required by the project plan. CM tools (Agile and CM Synergy) are used to support configuration management activities (i.e., control check in and check-out of software modules). Each document, part, or software component is assigned a unique number per Engineering Document Numbering System standard (IOM procedure EDM 23.00). Each document shows the revision and issue update history and the current "as designed" revision that also defines the latest "to be built" hardware configuration. Each product, up to the system level, is defined by material lists at the appropriate number of indenture levels. These material lists identify the parts (including software and hardware), assemblies, and supporting documentation, along with their respective version/revision numbers, required to construct and sustain the product. Pursuant to their CMP, IOM provides physical labels on the printed circuit board of each module to uniquely identify the hardware module and installed firmware. As part of the regulatory audits conducted at the IOM facility (Reference 6), the NRC staff observed component identification based on the physical labels applied to representative modules.

The IOM software CMP for application software is outside of the scope of this review. Tricon V10 source code is an identified CMP component so version management and change control mechanisms are applied. The platform software components for the Tricon V10 platform are controlled based on assigned part numbers. The configuration information of each software component is securely maintained as part of the IOM system configuration management records and can be referenced by part number for a specific project. Software versions for the assemblage of software components are defined in terms of a formally released, configuration controlled software project. The IOM CMP used to develop the Tricon V9 platform was previously approved by the NRC in its Tricon V9 SE. The IOM CMP has undergone some changes from the approved Tricon V9 program. These changes were reviewed and approved in Section 3.2.1. The NRC staff found that the current configuration management program and practices of IOM comply with the guidance identified in IEEE Std 828 and IEEE Std 1042, which are endorsed by RG 1.169.

The compiled system software for each processor contains embedded information and an internal checksum. Identification of the system software can be checked using special equipment at the factory as described in Section 3.8.1 of this SE. Based on this evaluation and the findings regarding hardware identification in Section 3.10.2.11 of this SE, the NRC staff determined that the Tricon V10 platform complies with the guidance of IEEE Std 7-4.3.2-2003 Clause 5.11 for its system software. Evaluation of application software is outside the scope of this review and will be addressed as part of an application-specific review.

3.11.1.6 IEEE STD 7-4.3.2-2003 CLAUSE 5.15, "RELIABILITY"

Clause 5.15 states that, in addition to the requirements of IEEE Std 603-1991, when reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing. Additional guidance is provided in SRP Chapter 7, Appendix 7.1-C, Section 5.15, and Appendix 7.1-D, Section 5.15.

SRP Appendix 7.1-D, Section 5.15, identifies RG 1.152, containing guidance regarding digital computer reliability. The SRP, Appendix 7.1-C, Appendix 7.1-D, and RG 1.152, states that quantitative reliability goals are not sufficient as a sole means of meeting the NRC's regulations for the reliability of digital computers used in safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system. However, since there is not a widely accepted view on software reliability value, determining a failure probability and therefore a reliability value for software is not possible. Therefore, NRC relies on the use of a high quality process of software design to obtain high quality software.

Determination of the reliability of a digital safety system is an application-specific activity that requires an assessment of a full system design, its application and system software, and the software life cycle processes. Since the LTR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures, the evaluation against this requirement is limited to consideration of the reliability characteristics of the digital platform and the quality of its system software.

Evaluation of the hardware reliability for the Tricon V10 platform is addressed in Section 3.10.2.15 of this SE. IOM performed a quantitative reliability and availability analysis for the Tricon V10 platform (see Section 3.6 of this SE) as specified by EPRI TR-107330.

No quantitative reliability goals are specified for the Tricon V10 platform software. A qualitative evaluation of software reliability for a safety system involves consideration of the quality of the software as demonstrated through its life cycle processes, testing, and operating experience. Acceptable software reliability of the Tricon V10 platform was achieved by a combination of the following factors:

- High quality development processes that minimize the introduction of errors,
- High quality verification and validation processes that maximize the detection any errors introduced, and
- Design and architectural features.

The Tricon V10 platform software has undergone commercial grade dedication pursuant to EPRI TR-107330 and EPRI TR-106439 as pre-developed software and the associated development history, operating experience, life cycle documentation, and testing and review activities have been reviewed and approved by the NRC (see Section 3.2.1 of this SE). The platform software processes were reviewed in accordance with BTP 7-14 to ensure that they will produce reliable software (i.e., will produce high quality software). The impact of software common cause failures was not provided in the LTR and therefore, will have to be reviewed as an application specific item. The reliability impact of potential security (SDOE) vulnerabilities was addressed in Section 3.8 of this SE. Based on these evaluations the NRC staff has determined that the digital Tricon V10 platform conforms to the guidance of Clause 5.15. However, demonstration of the hardware and software reliability of the implemented system is necessary to fully comply with this clause for digital safety system reliability. Specifically, an evaluation of system reliability, including the contribution of application software, will be required in a plant-specific review.

3.12 SUMMARY OF REGULATORY COMPLIANCE

This SE discusses the acceptability of the Tricon V10 platform for use as the basis for a SR DI&C system in nuclear power plants. Each of the findings or conclusions summarized below may be subject to the satisfactory resolution of generic open items identified in the foregoing sections and documented in Section 4.1 of this SE. Careful attention must also be given to the plant-specific items listed in Section 4.2 of this SE.

This SE discusses the acceptability of the Tricon V10 PLC system. The GDC listed in Appendix A to 10 CFR Part 50 establish the minimum requirements for the design of nuclear power plants; 10 CFR 50.55a(h) incorporates IEEE Std 603-1991. The RGs and endorsed industry codes and standards listed in the SRP, Table 7-1, are the guidelines used as the basis for this evaluation.

Section 50.55a(a)(1), "Quality Standards for Systems Important to Safety," is addressed by conformance with the codes and standards listed in the SRP. In the development of the Tricon V10 PLC system, IOM used codes and standards that are the same as or equivalent to the standards identified in the SRP. Therefore, the NRC staff concludes that the Tricon V10 PLC system conforms to this requirement.

Section 50.55a(h) incorporates by reference IEEE Std 603-1991, which addresses both system-level design issues and quality criteria for qualifying devices. The NRC staff has determined that the Tricon V10 PLC system satisfies the requirements of 10 CFR 50.55a(h) with regard to IEEE Std 603-1991 as described in Section 3.10 of this SE.

The NRC staff determined that the following GDCs specified in Appendix A to 10 CFR Part 50 are the applicable design criteria for this review:

GDC 1:	Quality Standards and Records
GDC 2:	Design Basis for Protection against Natural Phenomena
GDC 4:	Environmental and Missile Design Bases

GDC 13: Instrumentation and Control
GDC 20: Protection System Functions
GDC 21: Protection System Reliability and Test ability
GDC 22: Protection System Independence
GDC 23: Protection System Failure Modes
GDC 24: Separation of Protection and Control Systems
GDC 25: Protection System Requirements for Reactivity Control Malfunctions
GDC 29: Protection against Anticipated Operational Occurrences

The NRC staff reviewed the equipment descriptions in the LTR for conformance to the guidelines in the regulatory guides and industry codes and standards that apply to this equipment. The NRC staff concludes that IOM adequately identified the guidelines that apply to this equipment. Given the review of the equipment designs for conformance to the guidelines, the staff finds that there is reasonable assurance that the Tricon V10 system conforms to the applicable guidelines. Therefore, the NRC staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included identifying those components and assemblies of the Tricon V10 that are designed to survive the effects of earthquakes and abnormal environments. On the basis of this review, the NRC staff concludes that IOM has identified those components and assemblies consistent with the design bases for the intended SR applications of the Tricon V10 system and has demonstrated their environmental qualification is adequate to cope with abnormal environments (as discussed in Section 3.3 of this SE). Therefore, the NRC staff finds that the identification and qualification of those components and assemblies satisfies the requirements of GDC 2 and GDC 4.

On the bases of its review of the Tricon V10 system status information, manual interface capabilities, and provisions to support safe shutdown, the NRC staff concludes that information is provided to monitor the Tricon V10 system over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions so as to ensure adequate safety. Appropriate controls can be provided for manual initiation of a reactor trip. The Tricon V10 platform can appropriately support actions to safely operate a nuclear power unit under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the NRC staff finds that the Tricon V10 system design satisfies the requirements of GDC 13.

Given its review of the LTR, the NRC staff concludes that the Tricon V10 system conforms to the design-basis requirements of 10 CFR 50.34(f), and to the guidance of IEEE Std 603 and RG 1.105. The NRC staff also concludes that the Tricon V10 system includes the necessary provisions to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown consistent with the accident analysis presented in Chapter 15 of a licensee's SAR. Licensee evaluation of plant-specific accident analyses is required. Therefore, the NRC staff finds that the Tricon V10 system satisfies the requirements of GDC 20.

The Tricon V10 system conforms to the guidelines for periodic testing in RG 1.22 and RG 1.118. Bypassed and inoperable status indication can be supported to conform to the guidelines of RG 1.47. A Tricon V10 system installation can also conform to the guidelines regarding the application of the single-failure criterion in IEEE Std 379. On the basis of this review, the NRC staff concludes that the Tricon V10 system satisfies the guidance of IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 with regard to system reliability and testability. Therefore, the NRC staff finds that the Tricon V10 system satisfies the requirements of GDC 21.

On the basis of its review, the NRC staff concludes that the Tricon V10 system satisfies the guidance of IEEE Std 603-1991, IEEE Std 7-4.3.2-2003, and the guidance in RG 1.75 with regard to protection system independence. Therefore, the NRC staff finds that the Tricon V10 system satisfies the requirements of GDC 22.

On the basis of its review of the FMEA for the Tricon V10 PLC system, the NRC staff concludes that the Tricon V10 platform/system is designed to fail into a safe mode if conditions such as disconnection of the system, loss of energy, or adverse environment are experienced. Therefore, the NRC staff finds that the Tricon V10 system satisfies the requirements of GDC 23.

Based on its review of the interfaces between the Tricon V10 system and plant operating control systems, the NRC staff concludes that the Tricon V10 system satisfies the guidance of IEEE Std 603 with regard to control and protection system interactions at the platform level. Therefore, the NRC staff finds that the Tricon V10 system satisfies the requirements of GDC 24.

Plant-specific safety I&C systems implemented on a Tricon V10 platform have the capability to comply with GDC 25. The specific variables to be monitored and the associated processing logic must be determined on a plant-specific basis.

On the basis of its review of all GDCs listed above, the NRC staff concludes that the Tricon V10 system satisfies the requirements of GDC 29, “Protection against Anticipated Operational Occurrences.”

On the basis of its review of software development plans and inspections of the computer development process and design outputs, the NRC staff concludes that the Tricon V10 PLC system meets the guidance of RG 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the NRC staff finds that the Tricon V10 system satisfies the requirements of GDC 1 and 21.

The NRC staff determined that the Tricon V10 PLC system meets the relevant requirements of GDCs 1, 2, 4, 13, 20-25, and 29.

4.0 LIMITATIONS AND CONDITIONS

On the basis of the review documented in this SE report, the NRC staff concludes that the Tricon V10 platform is acceptable for use in the development, installation, and operation of SR systems in nuclear power plants, pending acceptable resolution of the generic open items identified in Section 4.1 and subject to the plant-specific conditions and limitations listed in Section 4.2.

4.1 GENERIC OPEN ITEMS

Chassis alarm relays were not seismically qualified as part of Seismic Testing as noted in Section 3.3.5.

4.2 PLANT-SPECIFIC ACTION ITEMS

The following plant-specific actions must be performed by an applicant when requesting NRC approval for installation of a SR system based on the Tricon V10 platform.

1. As noted in Section 2.1, IOM also submitted the Nuclear Safety Integration Program Manual (NSIPM). The NSIPM governs application specific development activities that occur at IOM's facility. The NRC staff reviewed this document, but made no safety determinations and it is not approved by this SE. It is an ASAI for the NRC staff to perform a review of any application specific development activities governed by the NSIPM when requesting NRC approval for the installation of a SR system based on the Tricon V10 platform.

2. Section 3.2 of this SE discusses the software development processes for the Tricon V10 platform. Although the NRC staff has approved the IOM software development and lifecycle planning program (Plans), the NRC staff determined that some of these Plans are also the responsibility of the licensee, and must be developed before the Tricon V10 platform software can be used for SR applications in nuclear power plants. Therefore, the following Plans must be developed and submitted with any license specific application referencing the Tricon V10 platform:

   - Software Installation Plan
   - Software Maintenance Plan
   - Software Operations Plan
   - Software Safety Plan

   The NRC staff will evaluate these plans in accordance with BTP 7-14 when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

3. Section 2.2 of this SE discusses the regulatory criteria used as the basis for this review. Determination of full compliance with the applicable regulations remains subject to plant specific licensing review of a full system design based on the Tricon V10 platform. Licensees must make a determination of full compliance with the design criteria and regulations identified in SRP Chapter 7, Table 7-1, which are relevant to specific applications of DI&C systems. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

4. Section 3.1.3.2 of this SE discusses the use of the TriStation 1131. That section noted that the Tricon V10 platform is designed such that the Tricon V10 platform would not normally be connected to a TriStation PC during SR operation. The plant-specific procedures which disconnect or control the connection of the TriStation PC such that the TriStation tool cannot affect the safety related functions of the Tricon PLC system during operation will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform. In addition, the testing of the operational software produced by the TriStation 1131, and these test plans, procedures, and results will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

5. Section 3.2 of this SE discusses verification and validation. Although IOM did not strictly follow guidelines of IEEE Std 1012, the NRC staff determined that the combination of the internal IOM review, the TÜV certification, and the review by independent consultants provided acceptable verification and validation for software that is intended for SR use in nuclear power plants. However, the NRC staff noted that a significant portion of its

acceptance is predicated upon the independent review by TÜV-Rheinland, and licensees using any Tricon PLC system beyond Tricon V10.5.1 must ensure that similar or equivalent independent V&V is performed; without this, the Tricon PLC system will not be considered acceptable for SR use at nuclear power plants. Should licensees use future Tricon PLC systems beyond Tricon V10.5.1 which have not received TÜV-Rheinland certification, the NRC staff will review the acceptability of the independent V&V during the plant-specific safety evaluation.

6. Sections 3.3 and 3.10.2.4 of this SE discuss environmental qualification. EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," which was accepted by NRC SE dated July 30, 1998, presents a set of requirements to be applied to the generic qualification of PLCs for application to SR I&C systems in nuclear power plants. It is intended to provide a qualification envelope for a plant-specific application. As noted in section 3.3 of this SE, several EQ tests did not fully meet the acceptance criteria of TR-107330 (e.g., EMC and Seismic Withstand). The licensee must make a determination that the as-tested envelope bounds the requirements of the specific application. Also, licensees must verify that the maximum test voltages cited in Section 3.3 envelop the maximum credible voltages applied to Non-Class 1E interfaces at their facility. Furthermore, licensees must provide further testing or mitigations for equipment that does not meet plant specific requirements such as the multi-mode fiber optic cable noted in Section 3.3.1. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

7. Sections 3.4.1 and 3.10.2.5 of this SE discuss response time. On the basis of the measured response times for the baseline testing, the Tricon V10 platform is not in compliance with Section 4.2.1, Item A, of EPRI TR-107330. However, the NRC staff determined that the response time characteristics are suitable to support SR applications in nuclear power plants. The licensee must make a determination regarding the response time performance of a SR system based on the Tricon V10 platform to ensure that it satisfies its plant- and application-specific requirements for system response time presented in the accident analysis in Chapter 15 of the safety analysis report for the plant. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

8. Section 3.4.3 of this SE discusses diagnostics and self-test capabilities. The NRC staff reviewed these self-test capabilities, and finds them to be suitable for a digital system used in SR applications in nuclear power plants. It may also be possible to use some of these diagnostic capabilities to modify or eliminate certain TS-required periodic surveillance tests; however this is a plant specific, application-dependent issue and, therefore, is not addressed in this SE. The licensee must provide any such surveillance test modifications or eliminations as part of plant-specific licensing amendment requests. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

9. Section 3.7.2.1 of this SE discusses communications interconnections. All external communications connections will require justification of the deterministic quality of TCM routed data in the application specific review. The licensee must provide a justification that should include the minimum guaranteed throughput on the COMBUS based on application specific scan time and number of I/O and the selected protocol. The

justification should also include an assessment of TCM vulnerabilities based on the application specific design (reference CDR Report (Reference 32) and ISG 2&4 NTX-SER-09-10 (Reference 29)). This justification will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

10. Section 3.7.2.2 of this SE discusses non-safety I/O connected to a remote RXM chassis. The NRC staff concluded that adequate protection is provided to the safety side I/O bus and the overall safety function. All data received from a non-safety remote RXM must be treated as non-safety data. The licensee must make a determination that adequate isolation is maintained in the design and that no data received from the non-safety I/O is used to make a safety determination. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

11. Section 3.7.3.1 of this SE discusses the 20 individual points of DI&C-ISG-04, Section 1, Interdivisional Communications. The LTR does not provide a specific safety system design. The licensee must make a determination regarding interdivisional communication including justifications as noted in the individual subsections of Section 3.7.3.1 of this SE report. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

12. Section 3.7.3.2 of this SE discusses DI&C-ISG-04, Section 2 - Command Prioritization. The design of field device interfaces and the determination of means for command prioritization are application-specific activities. Since the LTR does not address a specific application, no evaluation against this NRC staff position could be performed. The licensee must provide the design of field device interfaces and the determination of means for command prioritization. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

13. Section 3.7.3.3 of this SE discusses DI&C-ISG-04, Section 3, Multidivisional Control and Display Stations. The design of information displays and operator workstations and the determination of information sources and interconnections are application-specific activities. Since the LTR does not address a specific application nor include display devices within the scope of the platform, the licensee must provide the design of information displays and operator workstations and the determination of information sources and interconnections. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

14. Section 3.8.1 of this SE discusses the secure development environment. The NRC staff observed elements of the secure development environment during the December 2010 audit at IOM's Irvine, California facility. The NRC staff also reviewed Sections 4.2 and 5.1 of the Tricon V9 SE and find that the previous conclusions still apply. Based on a review of "Tricon V10 Conformance to R.G. 1.152," IOM document NTX-SER-10-14 (Reference 35), Section 3.1, regarding secure development environment and a comparison to the previously reviewed development environment from the Tricon V9 SE combined with direct observations of the current development environment at IOM's facility in Irvine, California, the NRC staff determined that IOM meets the requirements

for secure development environment in RG 1.152, Revision 3. The licensee must make a determination that the secure development environment has not changed and confirm that the application secure development environment is the equivalent or otherwise meets the requirements of RG 1.152, Revision 3. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

15. Section 3.8.1 of this SE discusses the secure operational environment. Without a specific operational environment to assess, the NRC staff could not reach a final conclusion on the Tricon V10 platform's ability to withstand undesirable behavior of connected systems and preclude inadvertent access. However, the Tricon V10 platform does have features that could be credited by a licensee when demonstrating these protections. Licensees must provide a description of the secure design and operational environment for the application software and hardware at their facility, which will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

16. Section 3.9 of this SE discusses diversity and defense-in-depth (D3). Since both diversity and defense-in-depth are plant specific topics, the LTR did not address these topics, and therefore are not within the scope of this SE. Sections 3.6.2 and 3.6.3 of Appendix B, "Application Guide," to IOM Document No. 7286-545-1, provide guidance in the preparation of a plant specific D3 evaluation. A review of the differences between the Tricon V10 system and the non-safety control system implemented at a particular nuclear power plant, and the determination that plant specific required diversity and defense-in-depth continue to be maintained must be addressed in a plant-specific D3 evaluation. These determinations will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

17. Section 3.10.3 of this SE discusses conformance with IEEE Std 603-1991, including setpoint determination. IOM has performed an analysis of accuracy, repeatability, thermal effects and other necessary data for use in a plant-specific setpoint analysis. Licensees must ensure that, when the Tricon V10 is installed, setpoint calculations are reviewed and, if required, setpoints are modified to ensure that the Tricon V10 platform will perform within system specifications. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

18. Section 3.7.1 of this SE discusses communications with SR equipment. The documentation confirms testing of the TriStation 1131 library with the SAP protocol. However, the protocol will also be implemented at the application layer of the connected SR equipment, presumably an SVDU. The documentation does not confirm that the protocol has been tested with any specific external SR devices. Therefore, it is an ASAI for the applicant to verify that the SAP library is tested in any proposed application specific SR devices. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

19. Section 3.7.3.1.10 of this SE discusses protection of safety division software. In order for the NRC staff to accept this keyswitch function as compliant with this Staff Position, the NRC staff will have to evaluate an application specific system communications

control configuration including the operation of the keyswitch, the software affected by the keyswitch, and any testing performed on failures of the hardware and software associated with the keyswitch when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

5.0 CONCLUSION

Based on the findings of Section 3.0 that are summarized above, the NRC staff concludes that, when properly installed and used, the Tricon V10 platform is acceptable for SR use in nuclear power plants, subject to satisfactory licensee compliance with the Limitations and Conditions identified in Section 4.0 and further described in Section 3 of this SE.

6.0 REFERENCES

1. Brian Haynes, Invensys Operations Management, letter to U.S. Nuclear Regulatory Commission, “Nuclear Safety-Related Qualification of the Tricon TMR Programmable Logic Controller (PLC) – Update to Qualification Summary Report Submittal and “Application for Withholding Proprietary Information from Public Disclosure", September 9, 2009 (Agencywide Document Access and Management System (ADAMS) Accession No. ML092870628).

2. Brian Haynes, Invensys Operations Management, letter to U.S. Nuclear Regulatory Commission, “Nuclear Safety-Related Qualification of the Tricon TMR Programmable Logic Controller (PLC) – Update to Qualification Summary Report Submittal and “Application for Withholding Proprietary Information from Public Disclosure", November 13, 2009 (ADAMS Accession No. ML093370293).

3. Brian Haynes, Invensys Operations Management, letter to U.S. Nuclear Regulatory Commission, “Nuclear Safety-Related Qualification of the Tricon TMR Programmable Logic Controller (PLC) – Update to Qualification Summary Report Submittal and “Application for Withholding Proprietary Information from Public Disclosure", July 11, 2010 (ADAMS Accession No. ML102040050).

4. Invensys Operations Management, “Triconex Topical Report,” Document No. 7286-545-1, Revision 4, December 20, 2010 (ADAMS Accession No. ML110140443).

5. Brian Haynes, Invensys Operations Management, letter to U.S. Nuclear Regulatory Commission, “Nuclear Safety-Related Qualification of the Tricon TMR Programmable Logic Controller (PLC) – Update to Qualification Summary Report Submittal and “Application for Withholding Proprietary Information from Public Disclosure", August 5, 2010 (ADAMS Accession No. ML102230299).

6. Jonathan Rowley, U.S. Nuclear Regulatory Commission, letter to Brian Haynes, Invensys Operations Management, “Audit Report Regarding the Invensys Triconex V10 Upgrade Topical Report,” March 14, 2011 (ADAMS Accession No. ML111650198).

7. Melissa S. Ash, U.S. Nuclear Regulatory Commission, letter to Brian Haynes, Invensys Operations Management, “Request for Additional Information for Review of Invensys

Triconex V10 Upgrade Topical Report," December 8, 2010 (ADAMS Accession No. ML103350091).

8 Brian Haynes, Invensys Operations Management, letter to U.S. Nuclear Regulatory Commission, "Invensys Response to Request for Additional Information (RAI) Ref: Letter dated December 8, 2010, NRC to Invensys, Enclosure 3," January 5, 2011 (ADAMS Accession No. ML110140448).

9 U.S. Nuclear Regulatory Commission, "Review of Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 To Qualification Summary Report," Revision 1," December 11, 2001 (ADAMS Accession No. ML013470433).

10 Invensys Operations Management, "Differences between the Tricon V9.5.3 and the Tricon V10.2.1 System," Document No. NTX-SER-09-05, Revision 2, April 7, 2010 (ADAMS Accession No. ML101100651, Page 21).

11 U.S. Nuclear Regulatory Commission, "Final Safety Evaluation by the Office of Nuclear Reactor Regulation for Topical Report HFC-6000 Safety System, Doosan HF Controls Corporation, Project No. 731," April 27, 2011 (ADAMS Accession No. ML110831014).

12 U.S. Nuclear Regulatory Commission, "Safety Evaluation by the Office of Nuclear Reactor Regulation, Siemens Power Corporation Topical Report EMF-2110(NP), "Teleperm XS: A Digital Reactor Protection System," Project No. 702," May 5, 2000 (ADAMS Accession No. ML003732662).

13 U.S. Nuclear Regulatory Commission, "Acceptance for Referencing of Topical Report CENPD-396-P, Revision 1, "Common Qualified Platform" and Appendices 1, 2, 3 and 4, Revision 1 (TAC No. MA1677)," August 11, 2000 (ADAMS Accession No. ML003740165).

14 U.S. Nuclear Regulatory Commission, "Wolf Creek Generating Station, Issuance of Amendment No. 181, Revise Licensing Basis, Modification of the Main Steam and Feedwater Isolation System Controls (TAC No. MD4839)," March 31, 2009 (ADAMS Accession No. ML090610317).

15 Invensys Operations Management, "Technical Product Guide, Tricon Systems," Document No. 9791007-013, Revision 22, August, 2006 (ADAMS Accession No. ML093290424).

16 Invensys Operations Management, "Planning and Installation Guide for Tricon v9-v10 Systems," Document No. 9700077-012, February, 2009 (ADAMS Accession No. ML093290420).

17 Invensys Operations Management, "Master Configuration List," Document No. 9600164-540, Revision 22, August 7, 2009 (ADAMS Accession No. ML100190961).

18 Invensys Operations Management, "Dedication of Products for Nuclear Service," EDM 76.00, Revision 1.0, July 18, 2008 (ADAMS Accession No. ML101121019, Page 140).

19 Invensys Operations Management, “Product Development Process,” EDM 12.00, Revision 4.6, September 30, 2009 (ADAMS Accession No. ML101121019, Page 32).

20 Invensys Operations Management, “Invensys QA Documentation Package of Wind River, Commercial Grade Survey,” August 23, 2010 (ADAMS Accession No. ML110960534).

21 Invensys Operations Management, “Invensys/Triconex Special Dedication Parts Evaluation,” Document No. 9100055-501, Revision 1, March 31, 2011 (ADAMS Accession No. ML110960519).

22 Invensys Operations Management, “Tricon System Description,” Document No. 9600164-541, Revision 0, July 24, 2007 (ADAMS Accession No. ML093370352).

23 Invensys Operations Management, “Master Test Plan,” Document No. 9600164-500, Revision 5, May 10, 2008 (ADAMS Accession No. ML100190963).

24 Invensys Operations Management, “Equipment Qualification Summary Report,” Document No. 9600164-545, Revision 3, August 3, 2009 (ADAMS Accession No. ML100190967).

25 Jerry L. Mauck, “Independent Tricon V10 Equipment Qualification Assessment,” July 31, 2007 (ADAMS Accession No. ML093370329, Page 1).

26 Invensys Operations Management, “EMI/RFI Test Report,” Document No. 9600164-527, Revision 3, February 10, 2012 (ADAMS Accession No. ML120470212).

27 Invensys Operations Management, “Seismic Test Report,” Document No. 9600164-526, Revision 0, July 17, 2007 (ADAMS Accession No. ML100190964).

28 Invensys Operations Management, “Failure Modes and Effects Analysis (FMEA) for the Tricon V10.2 Programmable Controller,” Document No. 9600164-531, Revision 1, January 17, 2012 (ADAMS Accession No. ML12047A152).

29 Invensys Operations Management, “Compliance with Interim Guidance ISG-2 & ISG-4,” Document No. NTX-SER-09-10, Revision 3, February 6, 2012 (ADAMS Accession No. ML12047A032).

30 Invensys Operations Management, “Nuclear System Integration Program Manual,” Document No. NTX-SER-09-21, Revision 1, July 9, 2010 (ADAMS Accession No. ML102040078).

31 Invensys Operations Management, “Invensys Triconex Safety Evaluation Report (SER) Maintenance Process,” Document No. NTX-SER-09-20, Revision 1, April 7, 2010 (ADAMS Accession No. ML101100642, Page 8).

32 Invensys Operations Management, “Critical Digital Review of the Triconex Tricon V10.2.1,” Document No. 9600164-539, Revision 1, August 4, 2009 (ADAMS Accession No. ML092070715).

33 Invensys Operations Management, “Tricon V10 System Safety Concepts,” Document No. 9100112-001, Revision 1, June 22, 2006 (ADAMS Accession No. ML101110709, Page 302).

34 Invensys Operations Management, Triconex Topical Report 7286-545-1-A, “Qualification Summary Report,” March 8, 2002 (ADAMS Accession No. ML020730573).

35 Invensys Operations Management, “Tricon V10 Conformance to R.G. 1.152,” Document No. NTX-SER-10-14, Revision 0, July 11, 2010 (ADAMS Accession No. ML102040062).

36 Invensys Operations Management, “TCM System Requirements Specification,” Document No. 6200152-001, Revision 3.1, March 7, 2007 (ADAMS Accession No. ML101110711, Page 689).

37 Invensys Operations Management, “TCM Traceability Matrix,” Revision 1.0, January 6, 2006 (ADAMS Accession No. ML101121019, Page 319).

38 Invensys Operations Management, “TCM TSAA Software Test Description,” Document No. 6500155-011, Revision 2.6, March 24, 2007 (ADAMS Accession No. ML101110709, Page 718).

39 Invensys Operations Management, “TSAP Software V&V Plan,” Document No. 9600164-513, Revision 2, December 1, 2006 (ADAMS Accession No. ML093370355).

40 Invensys Operations Management, “TSAP Software V&V Report,” Document No. 9600164-536, Revision 0, December 7, 2006 (ADAMS Accession No. ML093370328).

41 Invensys Operations Management, "Software Qualification Report," Document No. 9600164-535, Revision 1, August 5, 2009 (ADAMS Accession No. ML100192059).

42 Invensys Operations Management, "ETSX Software Architecture Specification," Document No. 6200106-001, Revision 2.1, September 13, 2006 (ADAMS Accession No. ML101110711, Page 734).

43 Invensys Operations Management, "Maximum Response Time Calculations," Document No. 9600164-731, Revision 0, December 5, 2006 (ADAMS Accession No. ML093280316).

44 Invensys Operations Management, "Test Report Operability Test Procedure Performance Proof Test," Document No. 9600164-566, Revision 0, July 26, 2007 (ADAMS Accession No. ML093280298).

45 Invensys Operations Management, "Radiation Test Report," Document No. 9600164-533, Revision 2, September 26, 2008 (ADAMS Accession No. ML100191819).

46 Invensys Operations Management, "Environmental Test Report," Document No. 9600164-525, Revision 0, July 17, 2007 (ADAMS Accession No. ML100192034).

47 Invensys Operations Management, "Reliability/Availability Report," Document No. 9600164-532, Revision 0, May 23, 2007 (ADAMS Accession No. ML093280312).

48 Invensys Operations Management, "Quality Assurance Manual," QAM 0.0, Revision 29, September 15, 2006 (ADAMS Accession No. ML093370329, Page 14).

49 Invensys Operations Management, "Configuration Management," EDM 20.00, Revision 8.0, October 26, 2009 (ADAMS Accession No. ML101121019, Page 79).

50 Invensys Operations Management, "Product Verification," EDM 90.00, Revision 4.2, September 15, 2009 (ADAMS Accession No. ML101121019, Page 159).

51 Invensys Operations Management, "Product Validation," EDM 90.10, Revision 1.0, February 20, 2008 (ADAMS Accession No. ML101121019, Page 193).

52 TÜV Rheinland Group, "Tricon V10 Test Report," 968/EZ 105.06/06, October 31, 2006 (ADAMS Accession No. ML093280230).

53 Invensys Operations Management, "Electrical Fast Transient Test Report," Document No. 9600164-521, Revision 1, April 30, 2008 (ADAMS Accession No. ML100191817).

54 Invensys Operations Management, "Surge Withstand Test Report," Document No. 9600164-528, Revision 1, April 30, 2008 (ADAMS Accession No. ML100191815).

55 Invensys Operations Management, "Electrostatic Discharge Test Report," Document No. 9600164-522, Revision 1, April 30, 2008 (ADAMS Accession No. ML100192048).

56 Invensys Operations Management, "Test Report Prudency Test Procedure Performance Proof Test," Document No. 9600164-573, Revision 0, July 26, 2007 (ADAMS Accession No. ML100192038).

57 Invensys Operations Management, "Class 1E to Non-1E Isolation Test Report," Document No. 9600164-529, Revision 1, April 30, 2008 (ADAMS Accession No. ML100191814).

58 Invensys Operations Management, "Tricon System Accuracy Specifications," Document No. 9600164-534, Revision 3, February 10, 2012 (ADAMS Accession No. ML12047A151, Page 9).

59 Invensys Operations Management, "Supplementary Information-Selected Topics," Letter No. NRC-V10-10-007, August 5, 2010 (ADAMS Accession No. ML102230297, Page 8).

60 Invensys Operations Management, "Safety Application Protocol Library Software Requirements Specification," Document No. 6200260-001, Revision 1.2, April 21, 2010 (ADAMS Accession No. ML11278A006, Page 49).

61 Invensys Operations Management, "Communication Application Safety Layer Interface Requirements Specification," Document No. 6200154-099, Revision 1.1, March 24, 2010 (ADAMS Accession No. ML11278A006, Page 81).

62 Invensys Operations Management, “TS1131 Libraries Software Verification and Validation Plan,” Document No. 9600355-001, Revision 1.2, June 29, 2010 (ADAMS Accession No. ML11278A006, Page 2).

63 Invensys Operations Management, “SAP Library Verification and Validation Test Report,” Revision 1.0, October 26, 2010 (ADAMS Accession No. ML11278A006, Page 69).

64 U.S. Nuclear Regulatory Commission, “Oconee Nuclear Station, Units 1, 2, and 3, Issuance of Amendments Regarding Acceptance of the Reactor Protective System and Engineered Safeguard Protective System (RPS/ESPS) Digital Upgrade,” January 28, 2010 (ADAMS Accession No. ML10020016).

65 Dave Baxter, Duke Energy Corporation, letter to U.S. Nuclear Regulatory Commission, "Duke Energy Carolinas, LLC Oconee Nuclear Station, Units 1, 2, and 3, Docket Nos. 50-269, 50-270, 50-287, Supplemental Response to Request for Additional Information Associated with Cyber Security Features of the Oconee Nuclear Station Reactor Protective System and Engineered Safeguards Protective System Digital Upgrade," November 25, 2008 (ADAMS Accession No. ML083450717).

66 Dave Baxter, Duke Energy Corporation, letter to U.S. Nuclear Regulatory Commission, "Duke Energy Carolinas, LLC Oconee Nuclear Station, Units 1, 2, and 3, Docket Nos. 50-269, 50-270, 50-287, Response to Supplemental Request for Additional Information Associated with Cyber Security Features of the Oconee Nuclear Station Reactor Protective System and Engineered Safeguards Protective System Digital Upgrade," April 3, 2009 (ADAMS Accession No. ML091000660).

67 John Jolicoeur, U.S. Nuclear Regulatory Commission, “Acceptance for Review of Invensys Operations Management Topical Report, “Triconex Topical Report 7286-545-1, Revision 3”,” August 11, 2010 (ADAMS Accession No. ML102220073).

Principle Contributors: S. Wyman
R. Stattel
W. Kemper

Date: