Project:	TRICON v10 NUCLEAR QUALIFICATION PROJECT

TRICON System Accuracy Specifications

Document No.: 9600164-534

Revision 1

January 26, 2010

	Name	Signature	Title
Author:	Frank Kloer		R&D Engineer
Reviewer:	Gary McDonald		Independent Review Engineer
	Alan Sands		Project QA Engineer
Approval:	Naresh Desai	N. Desai per Telecon	Project Manager

Document Change History			
Revision	**Date**	**Change**	**Author**
0	7/26/07	Initial Issue	Frank Kloer
1	01/26/10	Revision to correct typographical error in Date field of document header (Reference ARR 711).	Frank Kloer

TABLE OF CONTENTS

SECTION **PAGE**

1.0 PURPOSE 4
2.0 SCOPE 4
3.0 REFERENCES 4
4.0 SETPOINT ANALYSIS REQUIREMENTS 5
5.0 PERFORMANCE SPECIFICATIONS 5
6.0 SUMMARY / CONCLUSIONS 12

1.0 PURPOSE

EPRI TR-107330, (Reference 3.1), requires that information be provided to support an application specific setpoint analysis per ISA RP 67.04, (Reference 3.2). Section 4.2.4 of the EPRI TR identifies the specific information to be provided.

The purpose of this report is to provide a single concise listing of the accuracy specifications of the Triconex TRICON control system. The specifications documented are those typically used by nuclear industry users for calculating instrument measurement uncertainties and establishing critical control setpoints.

2.0 SCOPE

This report documents the accuracy specifications for the Triconex TRICON PLC system included in the TRICON V10 Nuclear Qualification Project (i.e. the Tricon-Under-Test, or TUT). The specifications cover all components and modules that were subjected to performance and qualification testing. These specific components and modules are identified in the Master Configuration List (Reference 3.3).

3.0 REFERENCES

3.1 EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996.
3.2 ISA RP 67.04.02-2000, "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation."
3.3 Master Configuration List, Triconex Document 9600164-540.
3.4 Radiation Test Report, Triconex Document 9600164-533.
3.5 TRICON Planning & Installation Guide, Triconex Document 9700077-008, August 2006.
3.6 TRICON User's Manual for Field Terminations, Triconex Document 9700052-001, August 2006.
3.7 Performance Proof Test Report, Triconex Document 9600164-530.
3.8 Environmental Test Report, Triconex Document 9600164-525.
3.9 Seismic Test Report, Triconex Document 9600164-526
3.10 EMI / RFI Test Report, Triconex Document 9600164-527, Rev. 0.

3.11 Triconex Quality Assurance Manual (QAM), Section 10.0, Inspection and Testing, Revision 017
3.12 IEEE 381-1977 Standard Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations.
3.13 IEEE 344-1987 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.
3.14 1600024-010 Data Sheet
3.15 1600024-020 Data Sheet
3.16 1600024-030 Data Sheet
3.17 1600024-040 Data Sheet
3.18 1600081-001 Data Sheet
3.19 1600082-001 Data Sheet
3.20 1600083-200 Data Sheet
3.21 1600083-600 Data Sheet

4.0 SETPOINT ANALYSIS REQUIREMENTS

EPRI TR-107330, Section 4.2.4 requires that the following effects on the accuracy of the equipment be addressed by this specification:

- Calibrated Accuracy, including hysteresis and non-linearity.
- Repeatability.
- Temperature Sensitivity.
- Drift Over Time.
- Power Supply Variation Effects.
- Arithmetic Operations Error (based on two additions plus a multiplication on an input value plus a comparison for both integer and floating point calculations).
- Vibration Effect.
- Radiation Effect.
- Relative Humidity Effect.

5.0 PERFORMANCE SPECIFICATIONS

The TRICON is a state-of-the-art fault tolerant programmable logic controller based on a Triple-Modular Redundant (TMR) architecture. The TMR uses three isolated, parallel control systems and extensive online diagnostics integrated into one system. The system uses voting to provide high integrity, error free, uninterrupted process operation with no single point of failure.

The Triple-Modular Redundant architecture of the TRICON along with its continuous diagnostics and self-calibration features eliminates many of the typical error sources found in standard instrumentation. Component / module failure, channel failures, or communication failures at the Input, Output, or Main Processor Module level will be corrected / compensated for by the system's ability to detect transient/steady state errors, and to take appropriate corrective actions online through the system's hardware and software voting mechanisms.

Each channel on the analog output module has two independent current loopback circuits per point that is readable by all other channels. The information from these circuits is used as part of the hardware voting process. The first circuit verifies the accuracy and presence of the analog signal for each point, independent of the load presence or channel selection. The second circuit verifies the actual current flow for each point from the selected channel. If a current flow is detected from any point on a non-selected channel, that channel is immediately shutdown. The Load alarm status indicator is annunciated if the module cannot drive current from any point—for example, by an open load.

The key in the Tricon design is its triplication of all critical processes. By performing continuous cross comparisons between the triplicated process, a true and full verification of actual input and output values is maintained.

5.1 APPLICABLE UNCERTAINTY TERMS

Tables 5-1 and 5-2 document the Reference Accuracy specifications, from References 3.5 and 3.6, for each of the analog I/O modules included in the Triconex Tricon PLC qualification program. Table 5-3 documents the Reference Accuracy specifications, from References 3.14 through 3.21.

Table 5-1
I/O Module Accuracy Specifications

I/O Module Type	Model Number	Reference Accuracy(Note 1)
0-10V Analog Input	3701	< 0.15% of FSR 0° to 60° C (Note 2 & 3)
0-5V or 0-10V Analog Input (16 Inputs)	3703E	< 0.15% of FSR 0° to 60° C (Note 2 & 3)
4-20 mA Analog Output	3805E	< 0.25% (in range of 4-20 mA) of FSR (0-21.2mA) 0° to 60° C
Thermocouple Input J,K,T,E	3708E	See Table 2
Pulse Input	3511	@ 1,000 Hz to 20,000 Hz = ± 0.01% @ 100 Hz to 999 Hz = ± 0.1% @ 20 Hz to 99 Hz = ± 1.0%
0-5V Analog Input or -5 to +5V Differential	3721	< 0.15% of FSR 0° to 60° C (Note 2 & 3)

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis non-linearity, and dead band). The manufacturer guarantees that the performance of the module meets specifications. This performance has been verified by testing performed on all modules during production. Typically, field application of the modules with respect to calibration accuracy's is more stringent than the specified accuracy. Therefore, Reference Accuracy values are considered to be a 95% or better probability value with a 95% or better confidence level.

2. On current loop inputs, a 0.01% precision resistor is used on the input termination to convert the current signal to a voltage reading (250 ohm for 0 -5 VDC or 500 ohm for 0-10 VDC). This is not included in the accuracy of the module.

3. FSR = Full Scale Range

Table 5-2
Reference Accuracy of Model #3708E Thermocouple Input Module

TC Type	Temperature Range	Reference Accuracy (Notes 1 and 2) @0-60°C (32-140°F)	
		T_a=25°C (77°F)	T_a=0-60°C (32-140°F)
		Typical	Maximum
J	-150 to 0°C (-238 to 32°F) 0 to 760°C (>32 to 1400°F)	±1.7°C (±3.0°F)	±5.0°C (±9.0°F) ±3.1°C (±5.5°F)
K	-150 to 0°C (-238 to 32°F) 0 to 1251.1°C (>32 to 2284°F)	±2.3°C (±4.0°F)	±4.5°C (±8.0°F) ±3.9°C (±7.0°F)
T	-161 to 0°C (-250 to 32°F) 0 to 400°C (>32 to 752°F)	±1.7°C (±3.0°F)	±4.8°C (±8.5°F) ±2.5°C (±4.5°F)
E	-200 to 0°C (-328 to 32°F) 0 to 999°C (>32 to 1830°F)	±1.7°C (±3.0°F)	±4.5°C (±8.0°F) ±2.8°C (±5.0°F)

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis, non-linearity, and dead band). The manufacturer guarantees that the performance of the module meets specifications. This performance has been verified by testing performed on all modules during production. Typically, field application of the modules with respect to calibration accuracy's is more stringent than the specified accuracy. Therefore, Reference Accuracy values are considered to be a 95% or better probability value with a 95% or better confidence level.

2. Accuracy specifications account for errors related to reference-junction compensation but do not account for errors caused by temperature gradients between the temperature transducers and thermocouple terminations. The user is responsible for maintaining a uniform temperature across the thermocouple termination module.

Table 5-3
Reference Accuracy of Analog Devices Signal Conditioners

Signal Conditioner Type	Model Number	Reference Accuracy (Note 1)
AD7B34CUSTOM, RTD Signal Converter, 200 ohm Pt., 0 – 600°C	1600083-600	+/- 0.11% span
AD7B34CUSTOM, RTD Signal Converter, 200 ohm Pt., 0 - 200°C	1600083-200	+/- 0.2% span
AD7B340401, RTD Signal Converter, 100 ohm Pt., 0 - 600°C	1600024-040	+/- 0.1% span
AD7B340301, RTD Signal Converter, 100 ohm Pt., 0 - 200°C	1600024-030	+/- 0.15% span
AD7B340201, RTD Signal Converter, 100 ohm Pt., 0 - 100°C	1600024-020	+/- 0.2% span
AD7B340101, RTD Signal Converter, 100 ohm Pt., -100 to +100°C	1600024-010	+/- 0.15% span
AD7B300201, RTD Signal Converter, 0 – 100 mV	1600082-001	+/- 0.1% span

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis, and non-linearity) (See References 3.14 thru 3.21).

5.2 NON-APPLICABLE UNCERTAINTY TERMS

As a result of the TRICON design and based on References 3.5, 3.6, 3.7, 3.8 and 3.9, the following uncertainty terms are considered **Not Applicable** to the TRICON and its modules, thereby establishing their error contribution as zero.

Temperature Sensitivity (i.e. Temperature Effect)

The TRICON has no known temperature induced inaccuracies over its rated temperature range. Per Reference 3.8, the TUT was subjected to environmental testing to meet the requirements of EPRI TR-107330 (Reference 3.1) and IEEE Standard 381-1977 (Reference 3.12). This testing sequence demonstrated that the TUT met all applicable performance requirements during and after application of the environmental profiles.

Drift Over Time (i.e. Drift Effect)

The TRICON analog I/O modules have an auto-calibration feature which maintains the Reference Accuracy rating at all times.

Power Supply Variation Effects (i.e. Power Supply Effect)

The TRICON has internal voltage regulation that eliminates the effects of voltage supply variations within the manufacturer's recommended ratings.

Arithmetic Operation Errors

All arithmetic operations are performed at a bit level that maintains resultant values well within the reference accuracy values. This determination is based on two additions plus a multiplication on an input value, plus a comparison for both integer and floating point calculations.

Vibration Effect (i.e. Seismic/Vibration Effect)

The TRICON has no known seismic or vibratory induced inaccuracies. Per Reference 3.9, the TUT was subjected to seismic testing to meet the requirements of EPRI TR-107330 (Reference 3.1) and IEEE Standard 344-1987 (Reference 3.13). This testing sequence demonstrated that the TUT met all applicable performance requirements during and after application of the seismic test vibration levels.

Radiation Effect

The TRICON has no known radiation induced error components that would prevent the TRICON from performing its function. Per Reference 3.4 the TUT was subjected to a radiation exposure of 1,000 Rads, plus margin.

Relative Humidity Effect (i.e. Humidity Effect)

The TRICON has no known humidity induced inaccuracies. Per Reference 3.8, the TUT was subjected to environmental testing to meet the requirements of EPRI TR-107330 (Reference 3.1) and IEEE Standard 381-1977. This testing sequence demonstrated that the Tricon Test Specimen met all applicable performance requirements during and after application of the environmental profiles. The TRICON's auto-calibration and diagnostic features ensure components maintain their Reference Accuracy rating.

5.3 ADDITIONAL CONSIDERATIONS

A/D and D/A Effects

The effects of analog to digital and digital to analog conversions are included in the reference accuracy values.

Digital Output Modules

Discrete output modules have no affect on the accuracy of programmed discrete outputs.

EMI/RFI Sensitivity

Per Reference 3.10, EMI/RFI effects should not be treated as a systematic, predictable source of instrument error that can be mathematically modeled in instrument uncertainty equations. EMI/RFI effects should be treated as an environmental condition under which the reliable operation of the instrumentation should be demonstrated. The TUT has been subjected to EMI / RFI testing per Reference 3.10.

6.0 SUMMARY / CONCLUSIONS

This report has defined the accuracy specifications for the Triconex TRICON PLC system included in the TRICON V10 Nuclear Qualification Project (i.e. the TUT). The specifications cover all components and modules that were subjected to performance and qualification testing. These specific components and modules are identified in the Master Configuration List (Reference 3.3). The information provided herein satisfies the requirements stated in Section 4.2.4 of TR-107330 (Reference 3.1).

The configuration of the system will be unique for each user depending on the plant specific application of the Triconex TRICON PLC system. The applicability of specified terms and approach to determining overall "system" uncertainty with respect to the data contained herein is the responsibility of the end user. Applicability of uncertainty terms and the methodology for determination of uncertainty shall be in accordance with the plant specific setpoint and uncertainty programs or other administrative guidelines.

invensys
Operations Management

TRICONEX TOPICAL REPORT

Document No.: 7286-545-1

Revision 2

March 31, 2010

	Name	Signature	Title
Author:	Frank Kloer	Signature on file	Engineer
Approvals:	Naresh Desai	Signature on file	Project Manager
	Gary Hufton	Signature on file	Director Control H/W Development

invensys
Operations Management

TRICONEX TOPICAL REPORT

Document Revision History

Revision Number	Date	Description of Changes
0	6/27/2000	Initial Issue
1	9/18/2000	Incorporate Triconex and STP comments
2	03/31/2010	Revised format of document incorporating new document template. Consolidated Revision 1 sections 2.0 thru 7.0 into new Section 2.0. Added new sections 3.0 thru 5.0. Revised report content including Appendices A and B to incorporate changes associated with Tricon V10.

invensys
Operations Management

TRICONEX TOPICAL REPORT

TABLE OF CONTENTS

SECTION		PAGE
1.0	INTRODUCTION	5
2.0	TRICON NUCLEAR QUALIFICATION PROJECT	6
2.1	SYSTEM DESCRIPTION	9
2.1.1	Tricon System Overview	9
2.1.2	Tricon System Hardware	11
2.1.3	Tricon System Software	20
2.1.4	Qualified Tricon Modules	26
2.1.5	Qualification of Newer Versions of the Tricon System	27
2.2	HARDWARE QUALIFICATION	28
2.2.1	Tricon Test Specimen Configuration	30
2.2.2	Radiation Qualification	31
2.2.3	Environmental Qualification	32
2.2.4	Seismic Qualification	35
2.2.5	Electromagnetic and Radio Frequency Interference Qualification	39
2.2.6	Electrical Fast Transient	43
2.2.7	Surge Withstand	44
2.2.8	Electrostatic Discharge	48
2.2.9	Class 1E to Non-1E Isolation	51
2.2.10	Performance Proof Testing	53
2.2.11	Failure Modes and Effects Analysis	55
2.2.12	Reliability and Availability Analysis	56
2.2.13	Cable Similarity Analysis	57
2.2.14	System Accuracy Specifications	57
2.2.15	Component Aging Analysis	58
2.3	SOFTWARE QUALIFICATION	58
2.3.1	Software Documentation	59
2.3.2	Software Development Process	61
2.3.3	Software Verification and Validation Process	62
2.3.4	Safety Analysis	65
2.3.5	Configuration Management and Error Notification	65
2.4	SYSTEM APPLICATION	66
2.5	REFERENCES	82

TRICONEX TOPICAL REPORT

TABLE OF CONTENTS

SECTION	PAGE
3.0 DIFFERENCES BETWEEN V9.5.3 AND V10.2.1 SYSTEMS	87
3.1 BACKGROUND	87
3.2 SYSTEM ARCHITECTURE & SYSTEM LEVEL DIFFERENCES BETWEEN V9.5.3 & V10.2.1	88
3.3 COMPARISON OF V9/V10 DIFFERENCES	88
4.0 TRICON V10.5 UPGRADE	92
4.1 INTRODUCTION	92
4.2 PURPOSE	92
4.3 DISCUSSION	92
4.3.1 Tricon Firmware Changes	96
4.3.2 TriStation 1131 Changes	102
4.3.3 Process Change Review	103
4.4 CONCLUSION	105
5.0 INVENSYS PROCESSES AND POLICIES FOR NUCLEAR PRODUCTS	105
5.1 MAINTENANCE OF QA AND PRODUCT DEVELOPMENT PROCESSES	106
5.1.1 Quality Assurance Program	106
5.1.2 Product Development Process	106
5.2 INVENSYS PROJECT INTEGRATION PROCESSES	107
5.3 SECURITY	108
5.4 DIVERSITY AND DEFENSE-IN-DEPTH ISSUES (ISG-02)	109
5.5 HIGHLY INTEGRATED CONTROL ROOMS – COMMUNICATION ISSUES (ISG-4)	109
5.6 INVENSYS TRICONEX TOPICAL REPORT/SER MAINTENANCE PROCESS	110

APPENDICES

A EPRI TR-107330 REQUIREMENTS COMPLIANCE AND TRACEABILITY MATRIX

B APPLICATION GUIDE

TRICONEX TOPICAL REPORT

1.0 INTRODUCTION

In 1997, EPRI issued TR-107330, which provides an acceptable method for generically qualifying a PLC for safety-related applications in nuclear facilities. After reviewing the technical report, the US Nuclear Regulatory Commission (NRC) issued a favorable Safety Evaluation Report (SER), concluding the methodology acceptable for generically qualifying a PLC for safety-related applications.

Beginning in 1997, Invensys participated in a subsequent EPRI effort to qualify the Tricon V9.5.3 in accordance with elements of TR-107330. Invensys, with the assistance of its contractors and Wyle Labs, completed all analysis and testing of the Tricon V9. After reviewing submitted test procedures, test results, analysis reports, and conducting an audit of the Irvine engineering and manufacturing facilities, the NRC issued a SER in December 2001 (ADAMS Accession # ML013470433), stating:

> *The staff concludes that the Tricon PLC system meets the requirements of 10 CFR 50.55a(a)(1) and 55a(h). It also meets GDC 1, 2, 4, 13, 20-24, and 29, and IEEE Std 603 for the design of safety-related reactor protection systems, engineered safety features systems, and other plant systems, and the guidelines of RG 1.152 and supporting industry standards for the design of digital systems.*
>
> *On that basis, the staff concludes that, when properly installed and used, the Tricon PLC system is acceptable for safety-related use in nuclear power plants.*

As the leading supplier of digital safety systems, Invensys has a responsibility to continue offering new and enhanced products that achieves the evolving demands of the various industries served – Oil and Gas Production, Refining and Petrochemical, Transportation, and Power. The nuclear power industry is no exception. Subsequently, the Tricon has undergone several design changes including the Main Processor, and the TRICON TMR PLC with Version 10 Firmware was selected to be evaluated under the TR-107330 specification and R.G. 1.180. Because of the technical enhancements (surface mount technology, main processor platform change, et. al.), and the addition of new products (NGIO, TCM, Vicor power supplies, R.G. 1.180 External Termination Assemblies) Triconex had determined it necessary to once again undertake nuclear qualification to EPRI TR-107330.

This report is organized as follows:

- Section 2.0 provides a summary of the Tricon nuclear qualification project, including background on the EPRI TR-107330 document and the overall approach used to demonstrate compliance with requirements specified in the EPRI document.
- Section 3.0 is an overview description of the differences between Tricon V9.5.3 and V10.2.1 Systems.
- Section 4.0 describes the Tricon V10.5 System upgrade.
- Section 5.0 describes the Invensys processes and policies for Nuclear Products, including:
  - Maintenance of QA and Product Development Processes
  - Security (ISG-1)
  - Defense in Depth & Diversity (ISG-2)
  - Communications Issues (ISG-4)
  - Project Integration Processes

- SER/Topical Report Maintenance Process

2.0 TRICON NUCLEAR QUALIFICATION PROJECT

This report documents the basis for generic qualification of the Tricon Version V10 programmable logic controller (PLC) system for safety-related applications in nuclear facilities. The basis for qualification is compliance with EPRI TR-107330, Reference 2.5.5, which has been approved by the U.S. Nuclear Regulatory Commission (NRC) as an acceptable approach for qualifying commercial PLCs for safety-related applications. Appendix A documents a detailed compliance matrix demonstrating how the Tricon system complies (Requirement Not Applicable, Fully Complies, Exception Taken, or TR Discrepancy Noted) with each of the requirements specified in EPRI TR-107330.

The Tricon is a mature commercial PLC that has demonstrated more than twenty years of safe and reliable operation in safety critical applications. High reliability and system availability are achieved through the triple-modular-redundant (TMR) architecture. The TMR design enables the Tricon system to be highly fault tolerant, to identify and annunciate faults, and to allow on-line replacement of faulty modules to prevent overall process failure. These features are desirable characteristics of a nuclear safety system, and hence there has been substantial interest in the industry in generic qualification of the Tricon PLC.

Note that the Tricon V10 Programmable Logic Controller (PLC) system is a successor to the Tricon V9 system, which was qualified and approved for nuclear safety related use in nuclear facilities by the Nuclear Regulatory Commission (NRC) in 2001. The Tricon V10 includes the enhanced Main Processor module (model 3008), the next generation differential Analog Input (NGAID) module, the next generation Digital Output (NGDO) module, SMT (Surface Mount Technology) versions of previously qualified I/O modules, and the Tricon Communication Module (TCM). Also included are power supplies with new DC-DC converters, and external termination assemblies (ETAs) with EMC enhancements.

The Tricon V10 has been qualified on a generic basis to provide utilities and other users with a platform that has been shown to comply with the applicable requirements for digital safety systems. Compliance with the applicable requirements is defined in terms of a "qualification envelope." This envelope defines the range of conditions within which the Tricon V10 meets the acceptance criteria. In applying the Tricon V10 to a specific safety-related application, the user must confirm that the qualification envelope bounds the facility-specific requirements. Additional guidance on use of the Tricon system in safety-related applications is provided in the Application Guide, Appendix B. A comparison of the Tricon V10 qualification to the EPRI TR-107330 requirements is documented in Appendix A. Exceptions and clarifications to the requirements and/or test methodology have been summarized in Table 2-2.

The generic qualification of the Tricon V10 encompasses both the hardware and the software used in the system. The hardware includes termination assemblies, chassis, power supplies,

main processor modules, communication modules, input/output modules, signal conditioners, and interconnecting cabling. The specific Tricon modules selected for qualification are defined in the Master Configuration List, Reference 2.5.39. These modules provide the functionality that is typically required for safety-related control and protection systems in nuclear facilities. The Tricon software that has been qualified includes the embedded real time operating system and its associated communication and input/output modules, and the PC-based system configuration software, TriStation 1131.

The process of qualifying the Tricon V10 has involved technical evaluations and qualification tests as type tests. This report summarizes the results of these evaluations and tests and provides references to the applicable documents for more detailed information.

This section provides an overview of the Tricon V10 Nuclear Qualification Project. EPRI TR-107330 provides generic requirements for qualifying commercial PLCs for use in safety-related applications in nuclear facilities. It defines the essential technical characteristics, (e.g., input and output point requirements, scan rates, software features, etc.) that must be included to cover the needs of facility safety applications. Process-oriented considerations, including system and software development and quality assurance, are addressed in this specification primarily by reference to published standards and guidelines. The process-oriented guidance is provided as a means of achieving adequate software and systems quality for safety related applications.

The objective of EPRI TR-107330 is to provide generic requirements for qualifying commercial PLCs for use in safety-related applications in nuclear facilities. It defines the essential technical characteristics, (e.g., input and output point requirements, scan rates, software features, etc.) that must be included to cover the needs of a range of facility safety applications. Process-oriented considerations, including system and software development and quality assurance, are addressed in this specification primarily by reference to published standards and guidelines. The process-oriented guidance is provided as a means of achieving adequate software and systems quality for safety related applications. Triconex has chosen to apply the qualification process documented in this EPRI report to the Tricon, even though the Tricon is maintained under Triconex 10 CFR 50 Appendix B program.

The TR-107330 requirements are intended for qualifying a PLC as a replacement for specific segments of safety systems at existing facilities (for example, using a PLC to perform reactor protection system functions). The envisioned application is to place one or more PLCs in the control logic portion of each channel, division, or train of existing safety actuation systems to perform control actions that are currently performed using electro-mechanical devices, analog circuitry, and loop controllers. In this type of application, the disruption of existing separation and isolation is minimal which, in turn, minimizes the impact of the replacement on the current licensing basis for these systems.

The Tricon Nuclear Qualification Project was initiated by Triconex to qualify the Tricon V10 in accordance with the EPRI TR-107330 requirements. Quality assurance requirements and special procedures that were unique to the Tricon V10 Nuclear Qualification Project are

documented in the Nuclear Qualification Quality Plan, Reference 2.5.37. The major activities completed as part of this project include the following:

- Identifying the specific PLC modules and supporting devices to be qualified. The Tricon hardware included in the qualification are listed in the Master Configuration List, Reference 2.5.39. This hardware was integrated in a complete test system that was intended to demonstrate capabilities typical of various nuclear safety systems. The design of the test system is documented in the System Description, Reference 2.5.41 and associated drawings, References 2.5.43 through 2.5.45.

- Developing an application program to support the required testing. The Test Specimen Application Program (TSAP) was developed to simulate operation of the Tricon in typical nuclear facility applications. Development, including verification and validation (V&V) of the TSAP was done in accordance with the Triconex QA program and a project-specific Software QA Plan, Reference 2.5.40. The TSAP program and associated V&V activities are documented in References 2.5.66 through 2.5.70.

- Specifying the set of qualification tests to be performed on the test specimen, including defining a set of operability tests to be performed at suitable times in the qualification process. Operability tests are required to determine the baseline system performance and to demonstrate satisfactory system operation under the stresses applied during qualification testing. The specific tests performed are defined in the Master Test Plan, Reference 2.5.38. Test procedures are provided in References 2.5.46 through 2.5.54, Reference 2.5.73, and Reference 2.5.74.

- Performing the qualification tests and documenting the results. Results of these tests, documented in References 2.5.55 through 2.5.61 and 2.5.75 through 2.5.79, define the qualification envelope and form the basis for the application guidance contained in this report.

- Performing other technical evaluations as needed to demonstrate compliance with regulatory requirements and other technical requirements in EPRI TR-107330. Evaluation of the embedded operating system and programming software is documented in the Software Qualification Report, Reference 2.5.65. Evaluation of new hardware modules (MP 3008, NGAID 3721, NGDO 3625, and Tricon Communication Module (TCM)) is documented in Critical Digital Review (CDR), Reference 2.5.80. A failure modes and effects analysis evaluating the effects of component failures on Tricon operation is provided in Reference 2.5.63. Reference2.5.62 documents an analysis of Tricon system reliability. Reference 2.5.64 provides a summary of the accuracy specifications for the Tricon system for use in calculating instrument measurement uncertainties and establishing critical control setpoints.

2.1 SYSTEM DESCRIPTION

This section provides a brief description of the Tricon system. A more detailed description of the system is provided in the Tricon Product Guide, Reference 2.5.29, and the Planning and Installation Guide, Reference 2.5.30. The specific hardware and software that has been qualified is identified in the Master Configuration List, Reference 2.5.39. For convenience, Table 3-1 at the end of this section lists the Tricon modules that have been qualified for nuclear safety-related applications.

The Tricon system was designed as a safety-critical system, and all aspects of its design are based on thorough engineering evaluation of potential failure modes, confirmed by substantial testing. All new or revised hardware designs are tested by physically injecting faults and verifying proper error detection. All new or revised software is also tested for backwards compatibility with prior versions of the Tricon system.

Throughout its life cycle, a quality assurance program and documented development process has been in place to control the design, verification and validation, and configuration management of the system (including both hardware and software). The quality assurance program and development process have been continually improved since 1985 and are compliant with the requirements of 10 CFR Part 50, Appendix B and 10 CFR Part 21. Demonstration of high quality, robust design, and accurate performance has been required from the first version of the Tricon system because of the safety-critical nature of the applications in which it is used. Qualification of the system for use in safety-critical systems has required evaluation by various safety certification agencies, including Factory Mutual, and TÜV Rheinland. Triconex's commitment to support the nuclear power industry is a natural extension of this corporate history.

2.1.1 Tricon System Overview

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

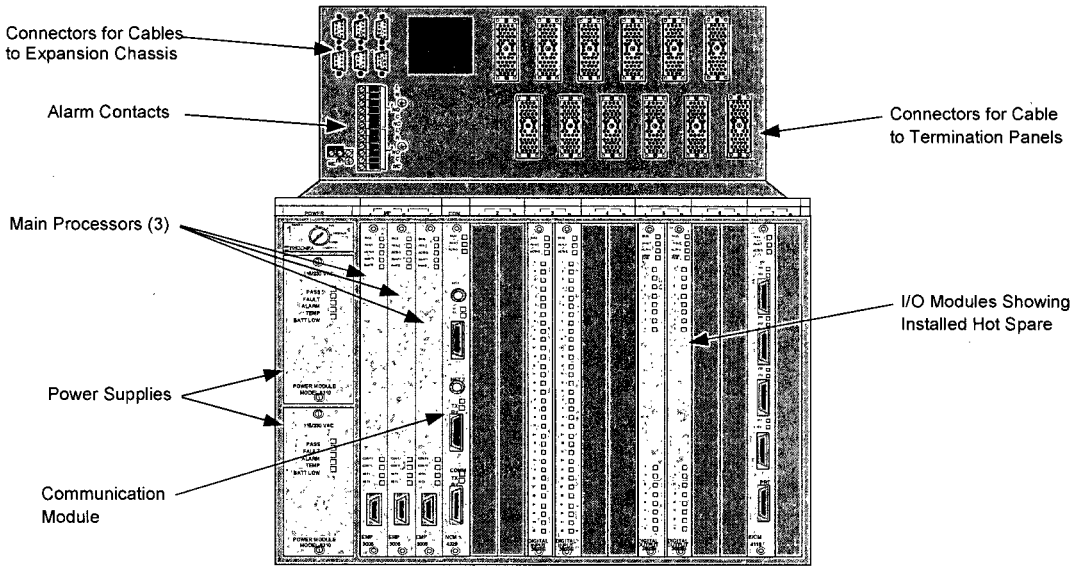


Figure 2-1. Tricon Main Chassis

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 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 to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. In the presence of a fault, the Tricon 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 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.

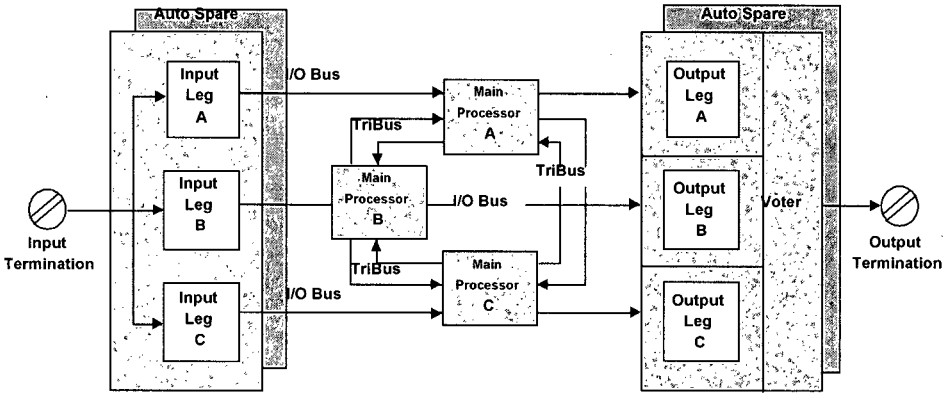


Figure 2--2. Triple Modular Redundant Architecture.

Figure 2-2 shows the arrangement of the input, main processor (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 main processor modules for all three microprocessors as well as on the input and output modules and communication modules (not shown in Figure 2--2).

2.1.2 Tricon System Hardware

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

2.1.2.1 Main Chassis

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

As shown in Figure 2-3, the Tricon 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 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.

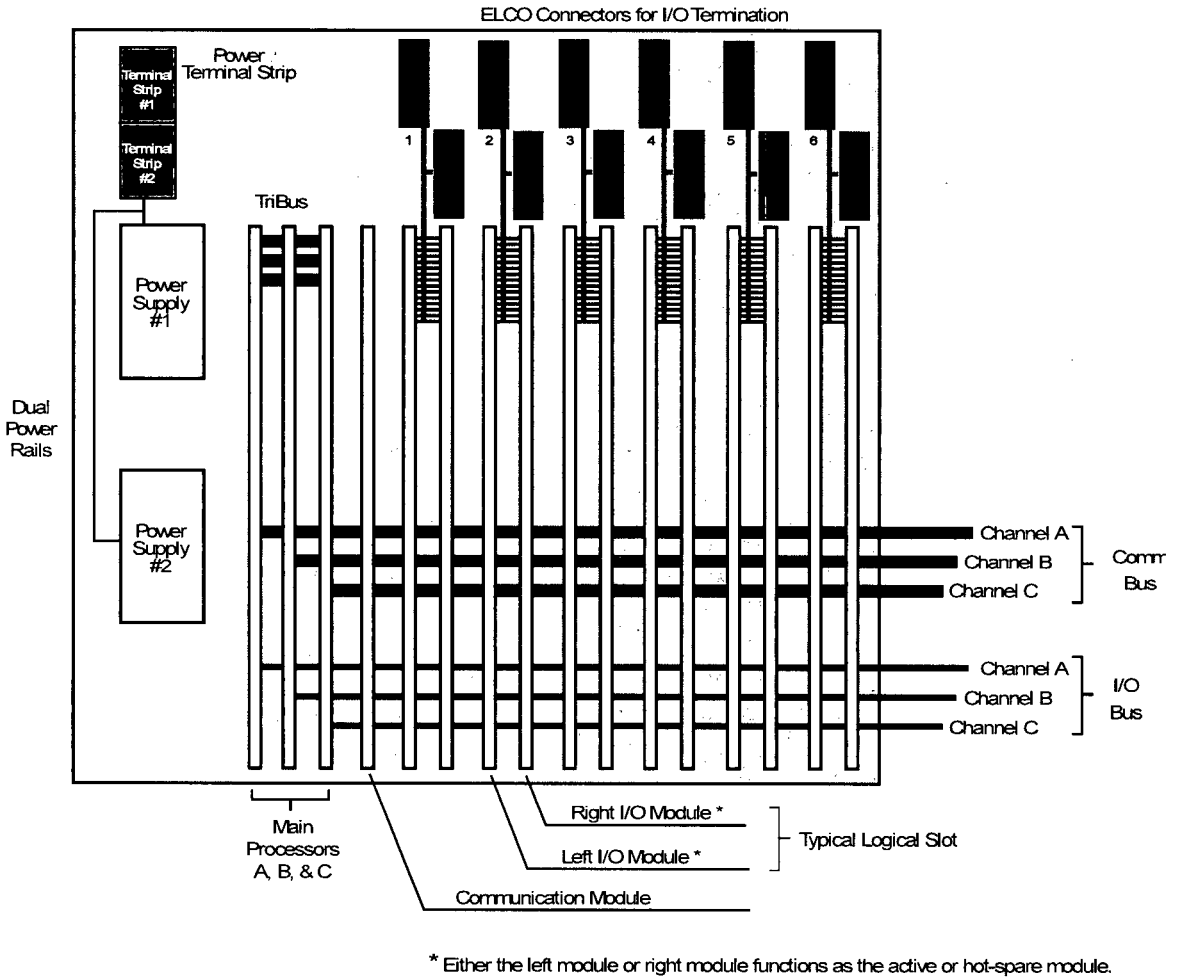


Figure 2-3. Tricon Chassis Backplane Configuration

2.1.2.2 Expansion Chassis

Expansion chassis are interconnected via three separate RS-485 data links, one for each 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

2.1.2.3 Remote Extender Modules

The Remote Extender Modules (RXM) are single-mode fiber optic modules that allow expansion chassis to be located several kilometers 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 module has single channel transmit and receive cabling ports. Each of the three primary RXM modules is connected to the remote RXM modules housed in the remote chassis. Each pair of RXM modules 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 RXM modules provide immunity against electrostatic and electromagnetic interference. Since the RXM modules are connected with fiber optic cables, they may be used as 1E-to-non 1E isolators between a safety-related main chassis and a nonsafety-related expansion chassis.

2.1.2.4 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, analog input, 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 chassis backplane.

2.1.2.5 Power Supply Modules

All power supply modules 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 V ac or V dc, 230 V ac, and 24 V dc.

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 analog output 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.

2.1.2.6 Main Processor Modules

The Tricon system utilizes three main processor modules to control the three separate legs of the system. Each main processor module operates independently with no shared clocks, power regulators, or circuitry. Each module owns and 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 control program and all system diagnostics at the main processor module level. Between the 32-bit primary processors is a dedicated dual port random access memory (RAM) allowing for direct memory access data exchanges.

The operating system, run-time library, and fault analysis for the main processor is fully contained in flash memory on each module. 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. Each main processor has an independent clock circuit and selection mechanism that enables all three main processors to synchronize their operations each scan to allow voting of data and exchange of diagnostic information.

The IOCCOM processors constantly poll respective legs for all the input and output 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 input and output 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 health 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 a neighbor, the local table representing that respective leg data will default to the de-energized state.

For digital inputs, the voted input table is formed by a 2 out of 3 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 analog inputs, a mid-value selection algorithm chooses an analog input 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. Significant errors are alarmed.

The primary processors then execute the application 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 cyclic redundancy code (CRC) to ensure the health of data transmitted between modules. 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 with a certain timeout period. 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 health 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 main processor module, it is annunciated and voted out, and processing continues through the remaining two main processors. When the faulty main processor is replaced, it runs a self-diagnostic to determine its basic health. When the self-diagnostic is successfully completed, the main processor then begins the process of "re-education," where the control program is transferred from each of the working

units into the returning main processor. All three main processors then resynchronize data and voting, and the replacement processor is allowed back in service.

2.1.2.7 Input/Output Modules

As shown in Figure 2-2, all triple modular redundant (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 main processors. Each main processor communicates via an individual I/O bus with one of the triplicated microprocessors on each I/O module. In each main processor, the I/O bus microprocessor reads the data and provides it to the main processor through a dual port RAM interface. For analog inputs, 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, 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 the Planning and Installation Guide, Reference 2.5.30.

After the main processors complete the control algorithm, data is sent out to the output modules. Outputs from the main processors are provided to the I/O bus microprocessors through dual port RAM. The I/O bus 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). Analog outputs 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.
- Analog output 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 2.5.30.

If one of the three legs within an I/O module fails to function, an alarm is raised to the main processors. If a standby module is installed in the paired slot with the faulty module, and that module is itself deemed healthy by the main processors, 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 main processors 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 main processors, each of the modules is exercised on a periodic basis. The main processors 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.

2.1.2.8 Communication Module

Like the I/O modules, the communication modules have three separate communication busses and three separate communication bus interfaces, one for each of the three main processors. 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 main processors 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 main processors.

The communication paths to external systems have appropriate levels of Cyclic Redundancy Checks, handshaking, and other protocol-based features. These features are supported in hardware and firmware. Firmware provides core functionality common to all the communication modules with additional coding to support the specific communication protocol.

The TCM allows the Tricon to communicate with other Tricons and with external hosts over fiber optic networks. The TCM provides two fiber optic port connectors labeled Net 1 and Net 2, which support Peer-to-Peer, time synchronization, and open networking to external systems using Triconex applications. In addition, the TCM contains four serial ports allowing the Tricon to communicate with Modbus master and slaves. Each serial port is uniquely addressed and supports the Modbus protocol.

Invensys has developed a Communication Application Safety Layer which allows safety communication between a client and the Triconex system. The two major types of components are the safety related components and the black channel components. In the Tricon System, the communication subsystem is considered a black channel and cannot be used to provide measures and techniques to insure the integrity of communication. Data integrity assurance is a fundamental component of the safety communication layer to reach a required safety integrity level. The protocol was developed to meet IEC-61784. Application guidance on the safety communication layer is found in Appendix B, Application Guide, sections 3.4 and 5.7.

2.1.3 Tricon System Software

The Tricon system software consists of the operating system that is resident on the various microprocessors within the system, the application programming software that runs on a PC, and the application program itself. Functional requirements for this software are specified in Section 4.4 of EPRI TR-107330. Compliance of the Tricon software with these requirements is summarized in the Compliance Matrix, Appendix A. A brief description is provided below.

2.1.3.1 Tricon Operating System

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

The operating system (ETSX) consists of three tasks: Scan task, Communication Task, and Background Task.

Upon power up (when the MP is inserted in the MP slot of the main chassis), the EMP 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 EMP. Upon successful completion of Power up sequence, the EMP enters the Scan task. Figure 2-4 shows the ETSX tasks and priorities.

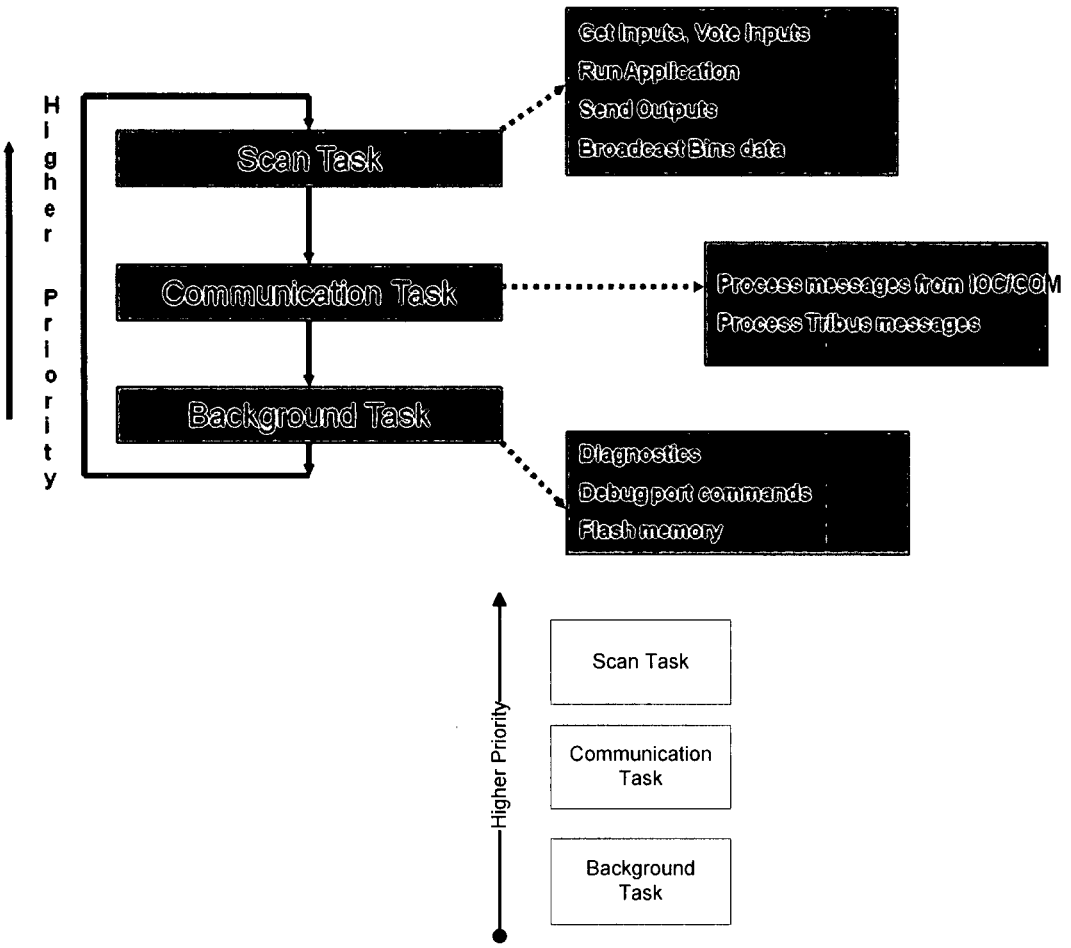


Figure 2-4 - ETSX tasks and priorities

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

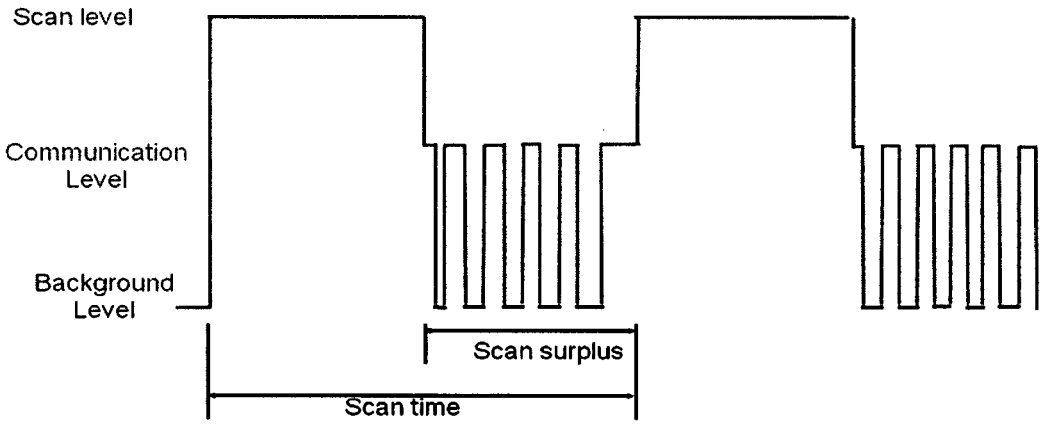


Figure 2-5 - ETSX task scheduling

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 milliseconds 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 is synchronized with the IOCCOM processor at the beginning of every scan. This is illustrated in Figure 2-6.

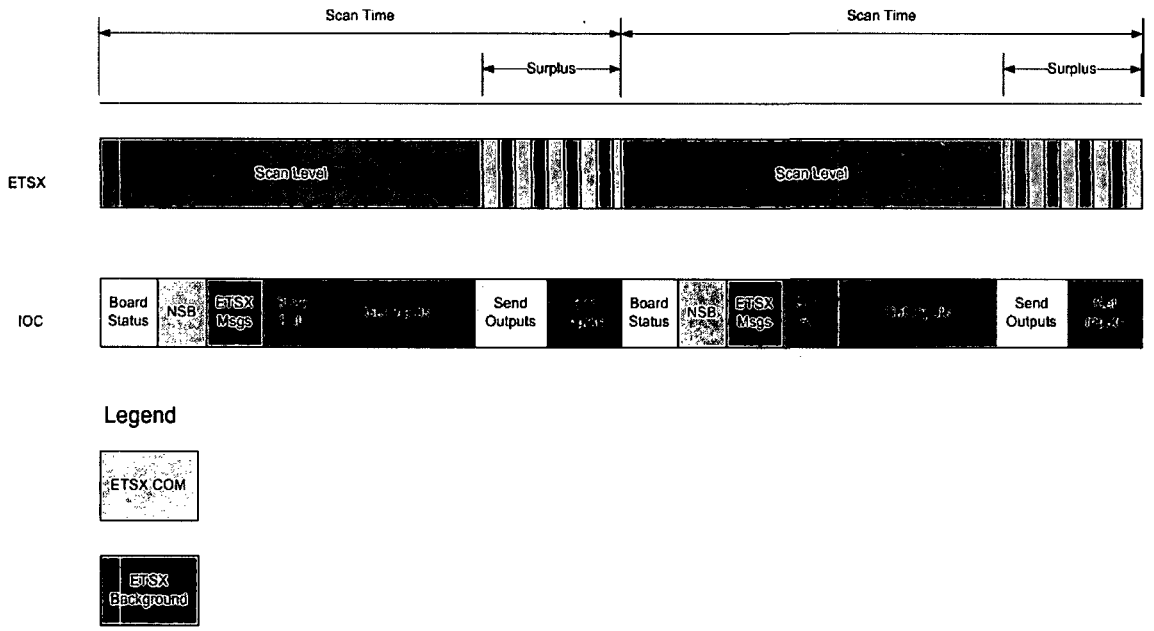


Figure 2-6 - ETSX and IOCCOM synchronization

The system firmware resident on the Input/Output modules is designed around a common core which supports communication with the main processors and processing of the input or output 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 firmware. Each microprocessor interfaces to only one leg of the I/O bus, and thus to only one main processor.

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 extensive diagnostics comply with the requirements established in BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions." The diagnostics are integrated into the base Tricon 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, consistent with the requirements of NUREG-0800 Branch Technical Position 7-17 (BTP 7-17). Thus, requirements imposed on the application program relating to error detection are limited to providing appropriate error recovery and annunciation of faults. Use of several of the diagnostic data inputs are mandated in the application guidelines in this report.

Based on the quality and coverage of the internal diagnostics, surveillance testing requirements could be reduced by taking credit for the extensive system diagnostics.

2.1.3.2 TriStation 1131 Programming Software

Application programming is generated using the TriStation 1131 Developer's Workbench, which runs in a Windows NT environment on a standard PC. The TriStation 1131 does not perform safety-related functions. It is a software tool which allows end-users to develop application programs and download those applications to the target Tricon. While the Tricon is performing safety critical functions, the TriStation 1131 PC would not normally be connected.

The TriStation 1131 software provides three IEC 61131-3 compliant languages, including Structured Text, Function Block Diagrams, and Logic Diagrams, as well as a Triconex-defined Cause and Effect Matrix language, called CEMPLE. The TriStation 1131 software provides language features and functionality in keeping with the recommendations of USNRC guidance documents, such as NUREG/CR-6463. The software implements a Graphical User Interface comprising language editors, compilers, linkers, emulation, communication, and diagnostic capabilities for the Tricon.

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 Structure Text is translated into an emulated code. The emulated code is then translated into native mode assembly language. This is then assembled and linked with native mode code libraries to generate a program. Up to this point, all application development may be performed off line, with no physical connection between the TriStation PC and the Tricon.

The TriStation 1131 Developer's Workbench also provides emulation capabilities for the Tricon. 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. This simulation can be used as part of the validation process for new or modified application code.

Compiled application programs are downloaded to the Tricon through a communication module. Programs and translated code are protected by 32-bit Cycle Redundancy Checks (CRC). During the download process, the individual communication blocks have CRC protection. Communication blocks where the computed CRC 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.

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

2.1.3.3 Application Program

The application program implements the desired 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.

The TriStation 1131 software offers various support functions for security, change detection, and documentation or comments integrated with the programming. These features should provide a basis on which a utility could build a workable software control and configuration management process. Various programmatic requirements are provided in the Applications Guidelines, Appendix B of this report.

In addition to the support features offered by the TriStation 1131, the standardized language features will aid in 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 as well as software common cause failures.

2.1.4 Qualified Tricon Modules

For convenience, the specified Tricon modules that are qualified for nuclear safety-related use are listed in the table below. For more information on the specific revision levels of these modules and on other qualified hardware and software, refer to the Master Configuration List, Reference 2.5.39. Section 2.2 of this report summarizes the qualification testing of these modules and the specific qualification envelope applicable to each one.

Table 2-1. Qualified Tricon Modules

MODULE TYPE	MODEL NO.	MODULE TYPE/DESCRIPTION
Main Processor	3008	Enhanced Main Processor III, V10, 16 Mb
High Density (HD) Main Chassis	8110	Main Chassis # 1
HD Expansion Chassis	8111	I/O expansion chassis
HD Remote Expansion Chassis	8112	Remote I/O expansion chassis
Remote Extender	4200	Remote Extender Module (Primary)
	4201	Remote Extender Module (Remote)
Communication	4352A	Tricon Communication Module, Fiber
Analog Input	3701	AI Module, 0-10 VDC
	3703E	EAI Module, Isolated
	3721	NGAI, -5-5 VDC
Analog Output	3805E	Analog Output Module, 4-20 mA
Digital Input	3501E	EDI Module, 115V AC/DC
	3502E	EDI Module, 48V AC/DC
	3503E	EDI Module, 24V AC/DC
Digital Output	3601T	EDO Module, 115 VAC
	3603T	EDO Module, 120 VDC
	3607E	EDO Module, 48 VDC
	3623T	SDO Module, 120 VDC
	3625	NGDO Module, 24 VDC
Pulse Input	3511	Pulse Input Module
Thermocouple Input	3708E	ITC Thermocouple Input Module
Relay Output	3636T	ERO Module, N.O., Simplex
Blank I/O slot Panel	8105	Blank I/O slot Panel
Seismic balance Module	8107	Seismic balance Module
Power Supply	8310	120 VAC/VDC Power Supply
	8311	24 VDC Power Supply
	8312	230 VAC Power Supply

Note: Specific termination panels, cable assemblies, and RTD signal conditioners that have also been qualified are listed in the Master Configuration List, Reference 2.5.39.

2.1.5 Qualification of Newer Versions of the Tricon System

Hardware qualification tests were performed on Version 10.2.1 of the Tricon system. Subsequent to this testing, Triconex has released Version 10.5 of the Tricon system. The software qualification effort evaluated Version 4.1.437 of the TriStation 1131 Developer's

Workbench software. This version of the software was released for use with Version 10.2.1, but has since been extended to Version 4.6.134.

To accommodate ongoing product evolution and maintenance activities, Triconex will extend all qualification results to the current Tricon product offering through established quality assurance program procedures. The current listing of nuclear qualified product hardware and software is maintained on the Nuclear Qualified Equipment List (NQEL), which is a living document. To facilitate customer licensing of Tricon system applications, Triconex procedures assure that all nuclear products, as reflected on the NQEL, are consistent with, and represented by, the existing NRC SER.

2.2 HARDWARE QUALIFICATION

This section describes the qualification of the Tricon system hardware for nuclear safety-related applications. Qualification activities were performed as required by EPRI TR-107330, Reference 2.5.5. These activities conform to the requirements of IEEE Standard 323 for qualifying Class 1E equipment.

The requirements for acceptance and operability tests are specified in Section 5 of EPRI TR-107330 and requirements for qualification tests are specified in Section 6 of the EPRI TR. Compliance of the Tricon hardware and the Tricon qualification program with the detailed EPRI test requirements is summarized in the Compliance Matrix, Appendix A.

Qualification of the Tricon hardware was demonstrated primarily by conducting a series of qualification tests in accordance with EPRI TR-107330. The tests specified in the EPRI TR are required in order to comply with the applicable regulatory requirements and industry standards. For Tricon qualification, the required tests and their sequence was defined in the Master Test Plan, Reference 2.5.38. A test sequence was chosen in which irradiation exposure was prior to environmental exposure. Sequencing of testing implies the existence of a significant aging mechanism. The Tricon is intended for use in mild environments, where aging is not required. Additionally, IEEE Standard 627-1980 states that significant aging mechanisms must satisfy a number of criteria including: "In the normal service environment, the aging mechanism causes degradation during the design life of the equipment that is appreciable compared to degradation caused by the design basis events." Radiation exposure to the TR-107330 levels does not meet this criterion. Results of the qualification testing on the Tricon test specimen demonstrate this.

The test sequence included pre-qualification performance testing, qualification testing, and post-qualification performance proof testing.

Pre-qualification testing included the following:

- System setup and checkout test are described in Reference 2.5.46, which documented proper configuration and operation of the test system. This test was performed after

manufacturing and assembly of the test specimen and test system, and as required, throughout the qualification process. This test includes verification of hardware, software, and cabling including interconnections to all equipment.

- Operability tests are defined in Reference 2.5.47, to establish the baseline performance and to demonstrate the functionality of the Tricon in accordance with its specifications. The operability test procedure included tests for analog module accuracy, system response time, operation of discrete inputs and outputs, performance of timer functions, failover tests (due to failure of redundant components), loss of power, detection of failure to complete a scan, power interruption, and power quality tolerance.

- Prudency testing is described in Reference 2.5.48, to establish baseline performance and to demonstrate the ability of the Tricon 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.

EPRI TR-107330 Section 5.2.F requires a burn-in test, to check for early component failures. However it was concluded that the normal elevated temperature burn-in test performed by Triconex as part of the manufacturing process is considered to meet the EPRI TR-107330 requirements and sufficient to detect early component failures. An additional burn-in test was therefore not conducted.

Qualification testing included the following:

- Radiation Exposure testing, Reference 2.5.76, is performed to demonstrate the ability of the Tricon V10 PLC to operate properly after being exposed to radiation. The operability tests and prudency tests were performed immediately after to demonstrate proper operation of the system.

- Environmental testing, Reference 2.5.50, is performed to demonstrate the ability of the Tricon to operate properly under the extremes of temperature and humidity. The operability test was performed at the high and low temperature and humidity conditions and also immediately after the environmental test (at ambient conditions) to demonstrate proper system operation. The prudency test was also performed at the high temperature conditions.

- Seismic testing, Reference 2.5.51, is performed to demonstrate the ability of the Tricon to operate properly during and after design basis seismic events, and therefore demonstrate the suitability of the device for qualification as Seismic Category I equipment. The operability and prudency tests were performed immediately after the seismic test to demonstrate continued proper operation of the system.

- Electromagnetic interference (EMI) and radio frequency interference (RFI) testing, Reference 2.5.58, is performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility

- Electrical Fast Transient (EFT) testing, Reference 2.5.73, is performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to susceptibility to repetitive electrical fast transients on the power and signal input/output leads.

- Surge testing, Reference 2.5.52, is performed to demonstrate the suitability of the Tricon for qualification as a safety-related device with respect to AC and DC power, signal and communication line electrical surge withstand capability.

- Electrostatic Discharge (ESD) testing, Reference 2.5.78,, is performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to immunity to electrostatic discharge exposure

- Class 1E-to-non 1E electrical isolation testing, Reference 2.5.53, is performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related, Class 1E device with respect to providing electrical isolation at Non-1E field connections.

After the qualification tests, the following post-qualification performance tests were done:

- Operability test as described above.

- Prudency test as described above.

Results of these tests are summarized in the following sections of this report. Refer to the individual test reports for full discussion of the detailed qualification envelope defined by the test results.

Engineering analyses were also performed to demonstrate compliance with additional hardware and system requirements specified in EPRI TR-107330. A failure modes and effects analysis, Reference 2.5.63, and a reliability and availability analysis, Reference 2.5.62, were performed.

2.2.1 Tricon Test Specimen Configuration

The Tricon Under Test (TUT) consisted of four Tricon chassis populated with selected input, output, communication, and power supply modules. The TUT also included external termination assemblies provided for connection of field wiring to the Tricon input and output modules.

The System Description (Reference 2.5.41) shows the general arrangement and interconnection of the Tricon Test Specimen chassis. The System Description, Reference 2.5.41, provides an overview and description of the test specimen and test system. A detailed identification of the tested equipment is provided in the project Master Configuration List, Reference 2.5.39.

During testing, the test specimen was executing an application program (the TSAP) developed specifically for the qualification project and designed to exercise the test specimen in a manner that supported data collection requirements during testing. The TSAP is described in

Reference 2.5.66. The Master Configuration List identifies the revision level of all test specimen software and firmware.

Analog and digital inputs to the test specimen were generated using a two-chassis simulator TUT. This system was configured with a simulator application program that was used to create a variety of static and dynamic input signals as described in Reference 1.1.1. Appropriate test equipment was used to provide additional analog inputs 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. 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 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 data was monitored for deviations or trends from normal performance.

2.2.2 Radiation Qualification

Radiation qualification testing of the TUT was performed as described in the Radiation Test Procedure, Reference 2.5.49. This testing was performed in accordance with the requirements of EPRI TR-107330, Reference 2.5.5 and IEEE Standard 381-1977, Reference 2.5.9. The objective of radiation testing was to demonstrate that the Tricon does not experience failures upon exposure to Co60 gamma radiation at the levels expected in mild environments. Requirements for radiation withstand capability are specified in EPRI TR-107330, Section 4.3.6, which requires that the PLC be able to withstand a radiation exposure of up to 1000 rads.

Compliance of the Tricon radiation qualification testing with these requirements is described in the Radiation Test Procedure, Reference 2.5.49.

The radiation test acceptance criteria are as given below based on Appendix 4 of the Master Test Plan, Reference 2.5.38, and EPRI TR-107330, Section 4.3.6, Reference 2.5.5:

- 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 at the University of Massachusetts, -Lowell, Massachusetts. The testing complied with the specific requirements of EPRI TR--107330, Sections 4.3.6 as described above, and the general requirements of IEEE Standard 381-1977, Reference 2.5.9. Results of the testing are described in the Radiation Test Report, Reference 2.5.76. Review of the post-radiation operability and prudency test results shows that exposure to the radiation test conditions had no adverse effect on the TUT.

Conclusions from this test are as follows:

1. Radiation Exposure Testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977. All of the tested TUT components were exposed to Co60 gamma radiation doses of 1000 rads, plus margin.
2. The TUT met all applicable acceptance requirements of the post-radiation exposure visual inspections performed as part of Radiation Exposure Testing.
3. Results of the post-radiation operability and prudency tests demonstrate that the applied Radiation Exposure Test conditions had no adverse effect on the TUT performance.
4. The Radiation Exposure Test results demonstrate that the Tricon V10 PLC will not experience failures due to normal and abnormal service conditions of gamma radiation exposure. 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.

2.2.3 Environmental Qualification

Environmental qualification testing of the TUT was performed as described in the Environmental Test Procedure, Reference 2.5.50. This testing was performed in accordance with the requirements of IEEE Standard 381-1977, Reference 2.5.9. The objective of environmental testing was to demonstrate the Tricon V10 PLC will not experience failures due to abnormal service conditions of temperature and humidity.

Requirements for environmental testing are specified in EPRI TR-107330, Sections 4.3.6 and 6.3.3, and include the following:

- The PLC under qualification shall meet its performance requirements during and following exposure to abnormal environmental conditions of 40°F to 140°F and 5% to 95% relative humidity (non-condensing) according to a time varying profile (see Figure 4-4 of 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 half of the discrete and relay outputs ON and loaded to their rated current. In addition, all analog outputs shall be set to between 1/2 and 2/3 of full scale.

Section 4.3.6.2 of EPRI TR-107330 (Reference 2.5.5) requires that the generic PLC meet its performance requirements over abnormal environmental conditions of 40°F to 120°F and 10% to 95% relative humidity (non-condensing). Section 4.3.6.3 of EPRI TR-107330 (Reference 2.5.5) 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% relative humidity (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% 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 (Reference 2.5.5) requires that Environmental Testing be performed with margins of 5°F and 5% applied to the temperature and humidity values given above.

Compliance of the Tricon environmental qualification testing with these requirements is described in the Environmental Test Procedure, Reference 2.5.50.

In addition to the modules that were installed and operating in the Test Specimen chassis at the start of environmental testing, a spare of each input, output, and communication module was put in the test chamber in an open container. Being inside the test chamber, these modules were maintained at thermal equilibrium with the chamber temperature throughout the test process, and were therefore readily available to be used as replacements for any modules installed in the chassis. In accordance with IEEE Standard 381-1977, Section 5.9.8, replacement of faulted or failed modules using these spare modules would constitute a replacement with a similarly tested component, which allows continuation of the test from the point of replacement (i.e., the test does not have to be restarted from the beginning).

The environmental test acceptance criteria are as given below based on Appendix 4 of the Master Test Plan, Reference 2.5.38, and EPRI TR-107330, Section 4.3.6, Reference 2.5.5.

- 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 at National Technical Systems in Boxborough, Massachusetts. The testing complied with the specific requirements of EPRI TR-107330, Sections 4.3.6 and 6.3.3, as described above, and the general requirements of IEEE Standard 381-1977, Reference 2.5.9. Results of the testing are described in the Environmental Test Report, Reference 2.5.56.

As described in the Test Report, 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% relative humidity over an 4 hour period.
- Hold at 140°F and 95% RH for a 1 hour period.
- Troubleshoot test system for a 1 hour period.
- Hold at 140°F and 95% 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% relative humidity 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% RH over a 6 hour period.
- Hold at 35°F and 5% humidity for an 8 hour period.
- Low temperature Operability Test performed over a 9 hour period
- Ramp-up to ambient temperature and humidity over a 5 hour period.
- Hold at ambient temperature and humidity for a 2 hour period.
- Ambient temperature Operability Test performed over a 13 hour period

Review of the data collected during the test shows that the TUT operated as intended. A number of module diagnostic messages were indicated at the Enhanced Diagnostic Monitor (EnDM) Console during testing. These messages included two indications of TUT hardware faults and other indications that were due to operation of the system under abnormal conditions. A description of all diagnostic messages received during the testing is provided in the test report, Reference 2.5.56. It is important to note that the diagnostic messages <u>did not indicate failures</u> of the system, only faults. The system met its safety function throughout testing.

Review of the post-test operability and prudency test results shows that exposure to the environmental test conditions had no adverse effect on the TUT performance.

Conclusions from this test are as follows:

1. Environmental testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977.

2. The TUT met all applicable performance requirements during and after application of the environmental test conditions.

3. One digital output module fault occurred during environmental. The fault indication was cleared through the Enhanced Diagnostic Monitor (EnDM) and did not return for the remainder of the Environmental Test. Because of the fault tolerant design of the Tricon V10 PLC, the monitored digital output point of the module (Model 3623T) continued to perform as expected during the fault condition.

4. The environmental test results demonstrate that the Tricon V10 PLC will not experience failures due to abnormal service conditions of temperature and humidity. 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.

2.2.4 Seismic Qualification

Seismic qualification of the Tricon was accomplished by performing the seismic test as described in Reference 2.5.51. The objective of seismic testing is to demonstrate the suitability of the Tricon V10 PLC for qualification as a Category 1 seismic device.

EPRI TR-107330, Sections 4.3.9 and 6.3.4, requires that the test PLC be seismically tested in accordance with IEEE Standard 344, Reference 2.5.8. The testing is required to include a resonance search followed by five simulated Operating Basis Earthquakes (OBEs) and one simulated Safe Shutdown Earthquake (SSE) at 9.75 g's and 14 g's respectively, based on 5% damping. The simulation vibrations are required to be applied triaxially (in three orthogonal directions), with random frequency content.

Additional requirements include the following:

- The test PLC shall meet its performance requirements during and following the application of the SSE.

- The test PLC shall be mounted on a structure whose configuration meets the manufacturer's mounting requirements. The structure is required to be stiff enough so there are no resonances below 100 Hz.

- Seismic testing shall be performed with the power sources to the test PLC power supply modules set to operate at minimum AC and DC source voltages and frequencies

- The test PLC shall be powered with its TSAP operating during seismic testing, with 1/2 of its solid-state discrete outputs ON and loaded to their rated current, 1/2 of its relay outputs ON, and 1/2 of its relay outputs OFF. In addition, 1/4 of its relay outputs shall transition from OFF to ON and 1/4 shall transition from ON to OFF during the OBE and SSE tests.

- The seismic test table shall be instrumented with a control accelerometer, and each chassis of the test PLC shall be instrumented with one or more response accelerometers located to establish maximum chassis accelerations.

- The test PLC shall operate as intended during and following the application of an SSE, all connections and parts shall remain intact and in-place, and relay output contacts shall not chatter.

The extent to which Tricon seismic qualification testing of the TUT complied with these requirements is described in the Seismic Test Procedure, Reference 2.5.51.

The TUT was mounted to the seismic test table in accordance with mounting details provided on Triconex Drawing No. 9600164-102. The seismic test mounting simulated a typical 19" rack mount configuration using standard Tricon front and rear chassis mounting brackets and fastener hardware, and standard Tricon external termination panel mounting plates. All fastener torque values indicated on Triconex Drawing 9600164-102 were verified. Additional details on the equipment arrangement for seismic testing are provided in the Seismic Test Report, Reference 2.5.57.

The seismic test acceptance criteria are as given below. These criteria were developed based on EPRI TR-107330, Section 4.3.9, and the Master Test Plan.

- 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.

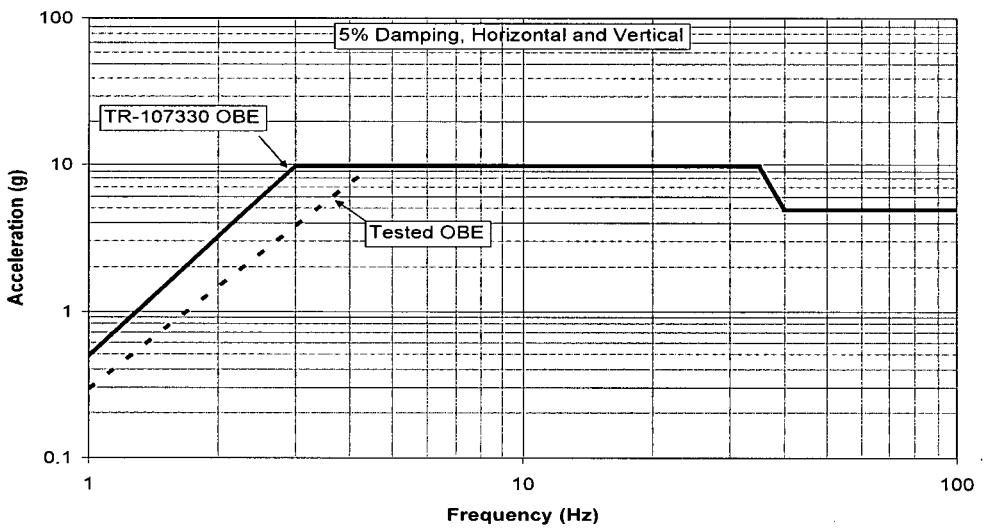
- The operation of the chassis power supply normally open alarm relay contacts and the Model 3636T electromechanical relay module output contacts shall be monitored during application of the OBE and SSE vibrations. The relay contacts shall change state in accordance with the TSAP. Any spurious change of state of the relay contacts shall not exceed 2 milliseconds in duration. Any spurious change of state of the power supply alarm relay contacts from open to closed shall not exceed 2 milliseconds in duration.

- The TUT shall pass the Operability Test following completion of the seismic testing.

Seismic testing of the TUT was performed at National Technical Systems in Acton, Massachusetts. Tests were performed in accordance with the Triconex Seismic Test Procedure, Reference 2.5.51. The following tests were performed in the order given:

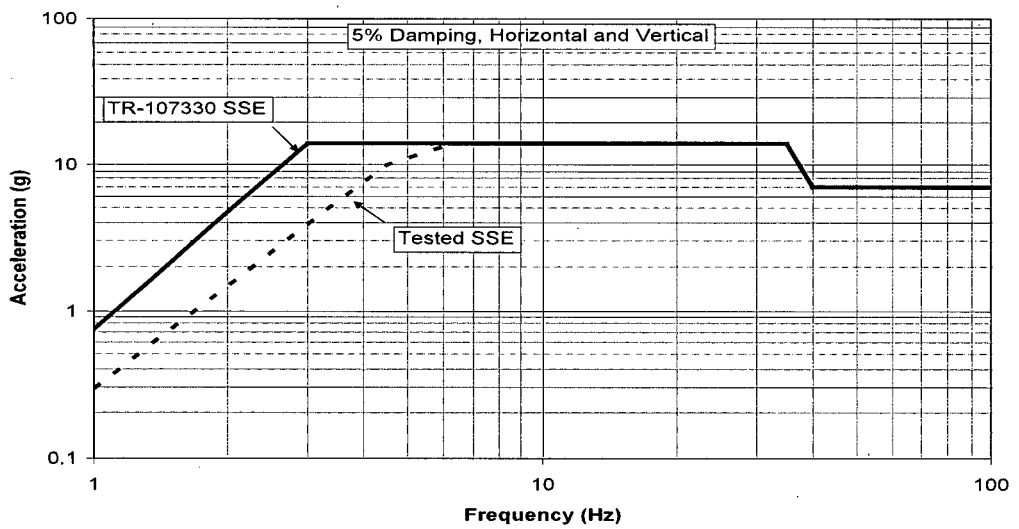
- Resonance search testing was performed as described in IEEE Standard 344, Section 7.1.4. The tests were performed to provide information on the dynamic response of the equipment mounted on the seismic test table. Over most of the 1 Hz to 10 Hz test frequency range, the accelerations experienced at the response accelerometer attachment points equaled or exceeded the acceleration applied to the seismic test table (as measured by the control accelerometers) in each of the three orthogonal directions.

- Five OBE tests and one SSE test were performed using the test response spectrum (TRS) which are shown in Figures 2-7 and 2-8.



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 2-7: OBE 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 2-8: SSE Test Acceleration

The TUT performance was monitored at the start of, during, and for a short period following each OBE and SSE test. During testing the TUT was operating in accordance with execution of the Test Specimen Application Program (TSAP).

Results of the testing are described in the Seismic Test Report, Reference 2.5.57. Data collected during and after each OBE and SSE test demonstrate that the TUT operated as intended throughout the testing. The TUT was visually inspected for damage or degradation following each OBE and SSE test. Results of these inspections showed no physical damage or degradation of the test specimen.

The results of the seismic test show that:

1. Seismic testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 344-1987.

2. The TUT met all applicable performance requirements during and after application of the seismic test vibration levels

3. Results of the Operability Test performed after Seismic Testing show that exposure to the Seismic Test conditions had no adverse effect on the TUT performance.

4. The seismic test results demonstrate that the Tricon PLC platform is suitable for qualification as Category 1 seismic equipment.

5. The horizontal and vertical seismic withstand response spectrum of the TUT as determined by testing is shown in Figures 2-7 and 2-8. The figures are based on a damping value of 5% used in the data analysis.

6. The seismic test results demonstrate that the equipment mounting configurations shown in Triconex Drawing No. 9600164-102 are adequate to support seismic qualification of the Tricon V10 PLC.

7. The manner in which the TUT chassis alarm relay contacts were monitored was determined to have the potential to mask contact chatter during Seismic Testing. Therefore, the TUT chassis alarm relays were not seismically qualified as part of Seismic Testing. It is important to note that these contacts do not provide a safety function.

2.2.5 Electromagnetic and Radio Frequency Interference Qualification

Electromagnetic interference (EMI) and radio frequency interference (RFI) testing was performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related 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 a shielded enclosure. The testing was performed in accordance with the EMI/RFI Test Procedure, Reference 2.5.54, and in accordance with the EPRI TR-107330 and NRC RG 1.180 test method requirements.

The specific tests conducted include the following MIL-STD-461E and IEC test methods:

Test Type	Test Method	Frequency Range
Conducted Emissions	CE101	30 Hz to 10 kHz
Conducted Emissions	CE102	10 kHz to 2 MHz
Radiated Emissions, Magnetic Field	RE101	30 Hz to 100 kHz

Radiated Emissions, Electric Field	RE102	2 MHz to 1 GHz
Radiated Susceptibility	IEC 61000-4-3	26 MHz to 1 GHz
Conducted Susceptibility	IEC 61000-4-6	150 kHz to 80 MHz
Radiated Susceptibility	IEC 61000-4-8	Power Line Frequency Magnetic Field
Radiated Susceptibility	IEC 61000-4-9	Pulsed Magnetic Field
Radiated Susceptibility	IEC 61000-4-10	Damped Oscillatory Magnetic Field
Conducted Susceptibility	IEC 61000-4-13	Harmonics and Interharmonics
Conducted Susceptibility	IEC 61000-4-16	Common-Mode Disturbances

Where necessary, testing was also performed at levels lower than the NRC RG 1.180, Rev. 1 specified levels to establish the envelope of acceptable performance.

The TUT was installed in the EMI/RFI chamber in open-frame racks as required by 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 Tricon Test Specimen 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 specific configuration of the TUT is described in the EMI/RFI Test Procedure, Reference 2.5.54.

During EMI/RFI testing, operation of the TUT was monitored by the DAS. The status of the Tricon diagnostic indicating LED's was also recorded to demonstrate continued correct operation.

EPRI TR-107330 requires that a portion of the Operability and Prudency tests be performed during the EMI/RFI testing. However, the test system as configured for EMI/RFI testing did not support Operability or Prudency testing. Instead, the Operability and Prudency tests were run at the completion of all qualification testing to demonstrate acceptable system performance following EMI/RFI, EFT, Surge Withstand, ESD and Isolation testing. The data recorded during the EMI/RFI tests were intended to demonstrate acceptable system performance during EMI/RFI exposure.

The EMI/RFI test acceptance criteria are as follows, based on Appendix 7 of the Master Test Plan, Reference 2.5.38, and RG 1.180, Revision 1, Reference 2.5.4:

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

Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) demonstrated operation as intended, including the following specific operational performance 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% of their current reading.

EMI/RFI testing of the TUT was performed at National Technical Systems in Boxboro, Massachusetts. The TUT successfully passed all of the EMI/RFI susceptibility tests. The main processors continued to function correctly throughout testing. The transfer of input and output data was not interrupted. There were no interruptions or inconsistencies in the operation of the system or the software.

For the emissions tests, the TUT was found to comply with the allowable equipment emissions levels defined in NRC RG 1.180, Rev. 1 for MIL-STD-461E, RE101 and RE102 testing. The TUT does not fully comply with the allowable equipment emissions levels defined in NRC RG 1.180, Rev. 1 for MIL-STD-461E, CE101 and CE102 testing.

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

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

The TUT main processor, chassis power supply, remote extender, and communication modules fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for all EMI/RFI susceptibility tests.

The TUT discrete and analog input/output hardware does not fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 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 V ac) with ETA 9663-610N

Detailed results of all the EMI/RFI tests are described in the EMI/RFI Test Report, Reference 2.5.58. In addition, the conclusions from additional tests to determine the impact of the Tricon V10 PLC input and output module EMI/RFI susceptibilities are detailed in the EMI/RFI Test Report.

2.2.6 Electrical Fast Transient

Electrical fast transient (EFT) testing of the TUT was performed as described in the EFT Test Procedure, Reference 2.5.77, to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to susceptibility to repetitive electrical fast transients on the power and signal input/output leads.

NRC RG 1.180, Rev. 1, Section 5.3, requires that the PLC under qualification be tested for EFT susceptibility in accordance with the requirements of IEC 61000-4-4. Section 5.3 and 4.2 of NRC RG 1.180, Rev. 1 includes the requirements for EFT testing of the AC and DC power supplies and signal leads respectively.

As described in the EFT Test Procedure, Reference2.5.73, the TUT was subjected to the following EFT tests:

- 120 V ac Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
- 230 V ac Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
- 24 V dc 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 are based on Appendix 8 of the Master Test Plan, Reference 2.5.38, and EPRI TR-107330, Section 4.3.7, Reference 2.5.5:, which require:

- 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 NRC RG 1.180, Rev. 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 2**	**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% (of full scale).

EFT testing of the TUT was performed at National Technical Systems in Boxboro, Massachusetts. 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 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 described in the EFT Test Report, Reference 2.5.77. Data collected during and after each voltage test demonstrate that the TUT operated as intended throughout the testing.

Conclusions from this test are as follows:

1. EFT Testing of the TUT was performed in accordance with the applicable requirements of NRC Regulatory Guide 1.180, Rev. 1 and IEC 61000-4-4. The following EFT tests were performed:
   - 120 V ac Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
   - 230 V ac Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
   - 24 V dc 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
2. The TUT met all applicable operational and performance requirements during and after each application of the EFT Tests voltages.
3. 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.

2.2.7 Surge Withstand

Surge withstand testing was performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to AC and DC power line, signal line and communication line electrical surge withstand capability.

EPRI TR-107330, Section 4.6.2, requires that surge withstand testing of the PLC be conducted in accordance with EPRI TR-102323, Reference 2.5.6, NRC RG 1.180, Rev. 1, Reference 2.5.4

provides an NRC approved alternative to the Surge Withstand Testing specified in EPRI TR--102323. Surge Withstand Testing of the TUT AC and DC power supplies, signal lines and communication lines was performed in accordance with IEC 61000-4-5 and IEC 61000-4-12 requirements.

As described in the Surge Withstand Test Procedure, Reference 2.5.52, the Tricon Test Specimen chassis power supplies, signal lines and communication lines were subjected to the following surge tests:

IEC 61000-4-5 Combination Wave: ± 2.0 kV (common mode and differential)

- 120 V ac and 230 V ac Chassis Power Supplies
- 24 V dc Chassis Power Supplies,

IEC 61000-4-12 Ring Wave: ± 2.0 kV (common mode), ± 1.0 kV (differential)

- 120 V ac and 230 V ac Chassis Power Supplies,
- 24 V dc 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 testing was performed at National Technical Systems in Boxborough, Massachusetts. Prior to the start of testing, all of the TUT modules (Main Processors (MPs), communication, and input/output) 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. Change-out of the modules was appropriate because surge withstand tests are design tests as opposed to conditioning (or aging) tests and therefore do not have to be performed on aged hardware.

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.

Operation of 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. The test details are described in the Surge Withstand Test Report, Reference 2.5.59. Data collected during and after each surge withstand test demonstrates that the TUT operated as intended throughout the testing.

The Surge Withstand Test acceptance criteria are as follows, based on Appendix 6 of the Master Test Plan, Reference 2.5.38, and EPRI TR-107330, Section 4.6.2, Reference 2.5.5:

- Applying the surge test voltages to the specified 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 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 Tricon Test Specimen following application of the surge test voltage. 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 Tricon Test Specimen to operate as intended.

Test results described in the Surge Withstand Test Report, Reference 2.5.59, show that:

1. Surge withstand testing of the Tricon Test Specimen 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:

   <u>IEC 61000-4-5 Combination Wave</u>: ± 2.0 kV
   - 120 V ac and 230 V ac Chassis Power Supplies,
     - Line to Neutral
     - Line to AC Ground
     - Neutral to AC Ground
     - Line and Neutral to AC Ground
   - 24 V dc Chassis Power Supplies,
     - High Side (+) to Low Side (-)
     - Low Side (-) to AC Ground

IEC 61000-4-12 Ring Wave: ± 2.0 kV

- 120 V ac and 230 V ac Chassis Power Supplies,
  - Line to AC Ground
  - Neutral to AC Ground
  - Line and Neutral to AC Ground
- 24 V dc Chassis Power Supplies,
  - Low Side (-) to AC Ground

IEC 61000-4-12 Ring Wave: ± 1.0 kV

- 120 V ac and 230 V ac Chassis Power Supplies,
  - Line to Neutral
- 24 V dc 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. In all cases, the Tricon Test Specimen continued to operate in accordance with the test acceptance criteria following application of the surge test voltages with no damage to components.

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.

2.2.8 Electrostatic Discharge

Electrostatic Discharge (ESD) testing was performed as described in the ESD Test Procedure, Reference 2.5.74, to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to immunity to electrostatic discharge exposure.

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, Reference 2.5.6. 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.

As described in the Electrostatic Discharge Test Procedure, Reference 2.5.74, the TUT was subjected to the following ESD tests:

<u>ESD Direct Contact Discharges:</u> ± 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 (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 2.5.38, and EPRI TR-107330, Section 4.3.7 and 4.3.8, Reference 2.5.5:

- 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.
  - The applied EFT disturbances shall not cause the discrete I/O to change state.
  - Analog I/O levels shall not vary more than 3% (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 at National Technical Systems in Boxboro, Massachusetts. 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 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, Reference2.5.78. 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 (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)
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 data links continued to operate correctly.

2.2.9 Class 1E to Non-1E Isolation

Class 1E to Non-1E isolation testing was performed to demonstrate the suitability of the Triconex Tricon V10 PLC for qualification as a safety-related, Class 1E device with respect to providing electrical isolation at Non-1E field connections.

The qualification of the Tricon V10 PLC is based on a system design that connects Non-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-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-1E electrical isolation capability (if these module are used to interface to Non-1E communication equipment). Accordingly, the TCM Module, RS-232 (MODBUS) was tested for Class 1E isolation capability.

In addition, the Tricon Model 3636T Relay Output Module was tested for electrical isolation capability. This allows interface to Non-1E circuits (such as alarms or annunciators) without having to install a separate, fiber optically isolated chassis.

Class 1E to Non-1E electrical isolation testing of the PLC was performed in accordance with the requirements of IEEE Standard 384-1981, Reference 2.5.10. In particular, IEEE Standard 384 requires that (a) the isolation device prevents shorts, grounds, and open circuits on the Non-1E side from unacceptably degrading the operation of the circuits on the 1E side, and (b) the isolation device prevents application of the maximum credible voltage on the Non-1E side from degrading unacceptably the operation of the circuits on the 1E side.

Communication port testing performed as part of the Prudency Test Procedure, Reference 2.5.48, addresses the item (a) isolation requirements for the Tricon communication modules. During prudency testing, the Tricon response time was monitored and shown not to degrade. These results are documented in the Triconex Performance Proof Test Report, Reference 2.5.61.

The Class 1E to Non-1E Isolation Test Procedure, Reference 2.5.53, addresses the item (b) isolation requirements for the communication modules and both the item (a) and item (b) isolation requirements for the relay output module.

The isolation testing was performed at National Technical Systems in Boxboro, Massachusetts. During 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 isolation testing was the same as for the EMI/RFI tests.

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 2.5.60.

Isolation test acceptance criteria are as follows based on Appendix 6 of the Master Test Plan, Reference 2.5.38, and EPRI TR-107330, Section 4.6.4, Reference 2.5.5:

- Applying the isolation test voltages for the required time to the specified TUT test points shall not disrupt the operation of any other module in the Test Specimen, or cause disruption of the Test Specimen backplane signals or any other data acquisition signals.
- Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate satisfactory operation of the TUT during and after application of the isolation 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 6.3.6 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.

Test results described in the Isolation Test Report, Reference 2.5.60, show that:

1. Class 1E to Non-1E isolation testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 384-1981.
2. The TUT met all applicable performance requirements during and after application of the Class 1E to Non-1E isolation test voltages Furthermore, during application of the isolation test voltages, functional isolation was demonstrated by: continued operation of the main processors; no interruptions of I/O data transfer; discrete I/O data maintaining expected states; analog I/O remaining with ranges; and normal operation of the NET1 and serial port peripheral communications.
3. The isolation test results (together with the Prudency Test communication port fault tests) demonstrate that the Tricon Model 4352A TCM Module MODBUS serial communication ports provide adequate electrical isolation per IEEE 384-1981 between the safety related portions of the Tricon and connected non-safety related communication circuits.

   The testing demonstrated electrical isolation capability of the communication ports to applied voltages of 250 V ac (at 10 amps maximum) and 250 V dc (at 5 amps maximum) for 30 seconds. The fiber optic module is considered an acceptable Class 1E to Non-1E isolation device by design, and was not tested.
4. The Class 1E to Non-1E isolation test results demonstrate that the Tricon PLC relay output module Model 3636Tprovides adequate electrical isolation per IEEE Standard 384-1981 between the safety related portions of the Tricon and connected non-safety related field circuits. The testing demonstrated electrical isolation capability of the relay output points to applied voltages of 600 Vac (at 5 amps maximum) and 250 Vdc (at 10 amps maximum).

5. The remote RXM chassis connection to the primary RXM chassis is essentially the I/O Bus over fiber optic cable, and no network protocols are utilized. Adding another remote RXM chassis would be a hardware change and would cause the system to become non-functional without first performing a Download All configuration change to the 3008N MPs in the Main chassis. The remote RXM chassis by design is physically remote from the Main chassis, and it is electrically isolated from the rest of the system (i.e., 3008N MPs running the application program) via the triplicated fiber optic cables. Therefore, the Tricon V10 Model 4201 Remote RXM fiber optic module is considered an acceptable Class 1E to Non-1E isolation device by design, and was not tested. The fiber optic cables are incapable of transmitting electrical faults from the remote Non-1E RXM module to the primary RXM module (which would be installed in the safety related Tricon chassis), and therefore meet IEEE Standard 384-1981 electrical isolation requirements. In addition, hardware faults in the remote RXM chassis would not impair the safety function, thus satisfying the physical, electrical, and communications isolation requirements in IEEE Standard 603, Clause 5.6, "Independence."

2.2.10 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 exposure to the various qualification test conditions. The operability and prudency tests were performed as part of performance proof tests. These procedures were developed in accordance with Sections 5.3 and 5.4 of EPRI TR-107330. Results of these tests are documented in the Performance Proof Operability Test Report, Reference 2.5.61 and Performance Proof Prudency Test Report, Reference 2.5.79. These test reports serve as an evaluation and summary of the Operability and Prudency test data collected throughout the qualification testing process. The data evaluation included comparison of the performance proof test data to Operability and Prudency test data collected during pre-qualification, environmental, and seismic testing. Conclusions from the testing are provided in the reports, including a summary of the specific manufacturer's performance specifications that were verified throughout qualification testing.

Conclusions from the performance proof testing are summarized below. Important results that affect the application of the Tricon in nuclear safety-related systems are described in the Application Guide, Appendix B.

1. Analog Input/Output Module Accuracy – For all Operability Test runs, the accuracy of each analog input/output module was demonstrated to meet the published Triconex product 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 – Response times for digital input to digital output, analog input to digital output, and "round robin" sequences of the TUT were measured during all runs of the Operability Test procedure. Triconex provides a method for calculating the maximum expected digital input to digital output, analog input to digital output, and analog output and "round-robin" response time for a specific Tricon hardware configuration and application

program scan time. The test data demonstrates that the Triconex equation provides a reliable upper bound on the maximum expected response times for a specific hardware configuration and an appropriately structured application program.

3. Discrete Input Operation – For all Operability Test runs, the OFF to ON and ON to OFF voltage switching levels of each digital input module were demonstrated to meet the published Triconex product 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 – For all Operability Test runs, each discrete output module was demonstrated to operate ON and OFF at the manufacturer's published product 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 – 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% of the time out period or three application program scan cycles. In addition, the test results show no degradation in timer function variation from pre-qualification testing throughout qualification and performance proof testing.

6. Failover Performance – Tests were done to demonstrate automatic failover to redundant components on simulated failures of a main processor module, an RXM module, 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 – Each run of the Operability Test procedure included tests to demonstrate performance of the TUT 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 – Each run of the Operability Test procedure included tests to demonstrate power hold-up time performance of the Tricon PLC chassis power supplies on an interruption of source power for approximately 40 milliseconds. The test results demonstrated:

   - The 120 V ac and 230 V ac chassis power supplies meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 milliseconds when installed as the only

chassis power supply or when installed in combination with a second chassis power supply.

- The 24 V dc chassis power supplies do not meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 milliseconds. The measured hold-up time capability of the 24 VDC chassis power supplies was less than 3 milliseconds.

9. Power Quality Tolerance – Tests to demonstrate tolerance of the Tricon V10 PLC power supplies to changes in the quality (voltage and frequency) of AC and DC source power were performed. Tests were performed over the manufacturer's 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.

10. Burst of Events Performance – Burst of Events testing demonstrated the ability of the PLC to process rapidly changing input and output signals based on the control logic of the TSAP.

11. Communication Port Failure Performance – Communication port failure testing demonstrated no effect on digital input to digital output and analog input to analog output response times during simulated failures of communication lines connected to communication ports on the TCM.

2.2.11 Failure Modes and Effects Analysis

As part of the Tricon V10 PLC qualification effort, a failure modes and effects analysis (FMEA) was performed as documented in Reference 2.5.63. The FMEA was performed in accordance with the guidelines of Section 6.4.1 of EPRI TR-107330, Reference 2.5.5.

The system analyzed by the FMEA is identical to the Test Specimen configuration that was used in the Qualification Test Program. The intent of the FMEA is to identify potential failure states of a typical Tricon PLC in a single train system and to provide data for use in the application-specific FMEA for a particular system.

This FMEA was performed using a macroscopic approach, addressing failures on a major component and module level. This approach is appropriate because sub-components in the Tricon modules are triple redundant and no single failure of an individual sub-component would impact the ability of the PLC to perform its safety related functions. The Tricon self-diagnostic features have been specifically designed to detect and alarm failures of sub-components within each module.

Because all single, internal failures are detected and alarmed, the FMEA focused on credible failure modes of major components and modules in a typical Tricon PLC system. The

components considered include the following:

- Power Supplies (including chassis power supplies and I/O loop power supplies)
- PLC Chassis (including internal power and communication buses)
- Main Processors and Communications Modules
- PLC Cables
- PLC I/O Modules
- Termination Panels

The approach used in the FMEA was to postulate credible failures of these components, identify the mechanisms that could cause these failures, and evaluate the consequences of these failures on the operation of the Tricon system. 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 also considers (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).

For this FMEA, multiple failures are considered to include scenarios such as failure of all three main processors due to software common cause failure, loss of all power, fire, floods, or missiles. These types of multiple failure scenarios are recognized as being very unlikely but are included to describe system behavior in the presence of severe failures and to provide guidance for application design.

The detailed results of the FMEA are tabulated in Reference 2.5.63. The results show that failure modes that can prevent the Tricon system from performing its function are detected by proper application-specific design, the built-in system diagnostics or by periodic testing. Provided the results of this FMEA are applied to specific control system designs, there will be no undetectable failure modes associated with safety-related functions.

The Tricon system design information presented in References 2.5.29 and 2.5.30 includes recommendations for periodic testing of field inputs and outputs. These recommendations establish general surveillance techniques and surveillance intervals intended to maintain the high reliability of the overall control system. It is strongly recommended that specific nuclear facility safety-related applications incorporate the manufacturer's recommended methods and frequencies to maximize system reliability and operability.

2.2.12 Reliability and Availability Analysis

Section 4.2.3 of EPRI TR-107330 requires that analyses be performed to determine the *availability* and *reliability* of a PLC in safety-related applications. The *availability* is defined in the EPRI TR as the probability that the system will operate on demand, and, in particular, that it will initiate a protective action when required. The *reliability* is defined in the EPRI TR as the probability that the system will perform its required mission under specified conditions for a specified period of time. Section 4.2.3 of the EPRI TR defines the hypothetical system configuration and conditions under which these probabilities must be determined.

The reliability and availability analysis for the Tricon system is documented in Reference 2.5.62. This analysis complies with the applicable requirements of EPRI TR-107330.

For the Tricon analysis, the two probabilities calculated include: (1) the probability that the system will fail in a given period of time (reliability), and (2) the probability that the system will fail on demand in a given period of time (availability). As required by the EPRI TR, the analysis was performed with the assumption that periodic testing of the system will uncover faults that are not normally detected by the system. As the periodic test interval is lengthened, the probability of failure increases. 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%, which exceeds the recommended goal of 99.0% 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% and the availability is 99.9990%.

2.2.13 Cable Similarity Analysis

As part of the Tricon V10 PLC qualification effort, a cable similarity analysis was performed as documented in Reference 2.5.81. The analysis was performed in accordance with the guidelines of IEEE 381-1977, Reference 2.5.9.

The cables used in a Tricon system are all of similar construction and rating. The difference between the cables is the insulation and jacketing material. The insulating material consists of either polyvinylchloride (PVC) or cross-linked polyethylene (XLPE). The XLPE cables use non-halogenated flame retardant polyethylene (NHFRPE) jacketing material. Both types of cables are mated with the same types of connectors to create an Interface Cable Assembly.

The similarity analysis establishes the basis for extending the qualification of Interface Cable Assemblies that utilize PVC and XLPE cables in the TUT. Only one specimen of each XLPE and PVC cable assembly type underwent all aspects of testing, including radiation testing. The analysis qualified the non-tested XLPE cable assemblies by comparison to the tested XLPE assembly and the non-tested PVC cable assemblies by comparison to the tested PVC assembly.

The analysis concluded that all XLPE and PVC Interface Cable Assemblies in the Tricon V10 Nuclear Qualification Project are qualified.

2.2.14 System Accuracy Specifications

As part of the Tricon V10 PLC qualification effort, system accuracy specifications for the Tricon V10 were established as documented in Reference 2.5.64. The accuracy specifications are documented in accordance with the Section 4.2.4 of EPRI TR-107330, Reference 2.5.5.

`The design of the Tricon enables it to maintain its rated reference accuracy specifications indefinitely. If the rated reference accuracy specifications are not met, 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 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. The effects of temperature sensitivity, drift over time, 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 system accuracy specifications cover all the components and modules subjected to qualification testing.

2.2.15 Component Aging Analysis

EPRI TR-107330, Section 4.7.8.2 requires the qualifier to perform an aging analysis of the PLC hardware based on the normal and abnormal environmental conditions to which it is exposed. This analysis must identify significant aging mechanisms, establish a qualified life for the hardware based on the significant aging mechanisms, and/or specify surveillance, maintenance and replacement activities to address the significant aging degradation.

Per IEEE Standard 323-1983, Section 6.2.1, "An aging mechanism is significant if in the normal and abnormal service environment, it causes degradation during the installed life of the equipment that progressively and appreciably renders the equipment vulnerable to failure to perform its safety function."

Based on review of the components used to assemble a Tricon PLC, and recognizing the extensive self monitoring and diagnostic features of the Tricon system, the components which are susceptible to significant, undetected aging mechanisms were determined to include only the chassis power supplies. The decreased capacity of the backup batteries is detected and alarmed before the decreased capacity can affect the ability of the batteries to maintain the Tricon program during an extended power failure.

The chassis power supplies are subject to gradual loss of performance (in particular, hold-up time capability on interruption of power) due to aging electrolytic capacitors. The lithium backup batteries are subject to gradual loss of capacity. Aging degradation of these components can be effectively addressed through periodic replacement prior to onset of significant loss of performance. A qualified life for the Tricon hardware is therefore not specified. Section 6.3 of Appendix B to this report (the Application Guide) provides recommended replacement intervals for the chassis power supplies and backup batteries.

2.3 SOFTWARE QUALIFICATION

Ultimately, the basis for the qualification of the Tricon system software is the U.S. Nuclear Regulatory Commission Standard Review Plan (SRP), provided in NUREG-0800, Section 7,

"Instrumentation and Controls." The approach used to demonstrate compliance with the requirements of the SRP is based on the guidance provided in EPRI TR-107330 and EPRI TR-106439. This approach, including the activities performed as part of the software qualification effort and the acceptance criteria established for these activities, is described in the Software Qualification Report, Reference 2.5.65.

The software qualification approach involved evaluating the processes, procedures, and practices used to develop the software, analyzing the software architecture, and assessing the history of the software and its associated documentation and operating experience. The objective of this approach is to develop the confidence necessary to assure that the product being qualified is of at least the same quality as would be expected of a product developed under a nuclear quality assurance program (i.e., complying with the quality assurance requirements of 10 CFR 50, Appendix B).

Criteria were established for determining the acceptability of the software based on the following:

- SRP, Section 7.1, "Instrumentation and Controls – Introduction"
- SRP, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems"
- Branch Technical Position 7-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems"
- Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- NRC Regulatory Guide 1.152, which endorses IEEE Std 7-4.3.2 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations"

The Tricon and TriStation 1131 software, including documentation, development practices, and operating history were evaluated against these criteria. Detailed results from this evaluation are provided in the Software Qualification Report, Reference 2.5.65. Key results are summarized in the following sections.

2.3.1 Software Documentation

EPRI TR-107330, Section 8.7 lists the minimum documents that are needed to support software verification and validation and the related software quality processes. This list is based on NUREG/CR-6241, which BTP 7-18 describes as an acceptable process for qualifying existing

software, and ASME NQA-1-1994. The minimum documents are:

- Software quality assurance plan
- Software requirements specification
- Software design description
- Software V&V plan
- Software V&V report
- User documentation (Manuals)
- Software configuration management plan

The Tricon is an evolutionary product. New releases do not necessarily alter the functional requirements, or even the design specifications (e.g. fixing "bugs"). Therefore, the Tricon software documentation is not necessarily updated with each revision. In addition, the Triconex development process maintains tight integration between hardware and software design activities. This integration of hardware and software design processes is based on the unique design philosophy inherent in a triple redundant, fault tolerant controller. Finally, the Tricon is the principal product of Invensys Triconex. Consequently, the required software documentation listed above is embodied in several sets of Triconex documents:

- Triconex quality and engineering procedures which provide planning requirements for quality assurance, V&V, configuration management, and test activities,
- The original Tricon System Functional Requirements Specifications,
- A series of Tricon Software Design Specifications that define the incremental changes to the system,
- Test procedures and test reports applicable to each system revision (whether it includes changes to hardware, software, or both),
- The Tricon Software Release Definition documents that identify software changes made in each revision, and
- The Tricon user documentation.

The documentation associated with Version 10.2.1 of the Tricon software was extensively reviewed as part of the qualification effort. As described in the Software Qualification Report, Reference 2.5.65, this review establishes that there are sufficient documents, as well as sufficiently mature product, to accept the Tricon PLC and TriStation 1131 as acceptable for nuclear safety related use. This acceptance is based on certain compensatory actions and evaluations defined in the proprietary appendix to the Software Qualification Report.

2.3.2 Software Development Process

As expressed in SRP Appendix 7.0-A, the use of digital systems presents the concern that minor errors in design and implementation can cause them to exhibit unexpected behavior. To minimize this potential problem, the design qualification for digital systems needs to focus on a high quality development process that incorporates disciplined specification and implementation of design requirements. Potential common-mode failures caused by software errors are also a concern. Protection against common-mode software failures is also accomplished by an emphasis on a quality development process.

For Commercial-Off-The-Shelf (COTS) software, there needs to be a reasonable assurance that the equipment will perform its intended safety function and is deemed equivalent to an item designed and manufactured under a 10 CFR 50 Appendix B quality assurance program. To accomplish this, the SRP emphasizes the implementation of a life cycle process and an evaluation of the COTS software development process.

Triconex was originally established to develop and manufacture triple-redundant fault-tolerant controllers. The triple-redundant fault-tolerant controller continues to be the primary focal point of Triconex. While some custom programs have been written for specialized applications, those efforts are performed by the applications group and are separate from the processes used to develop and maintain the Tricon system itself.

The Tricon system was initially developed in 1986, evolving into the present day configuration. When the Tricon operating system was conceived, there was very little guidance in the way of industry standards to base the software development and design. Good programming practices were used based on the objective of producing a highly reliable safety system.

The QA program was updated in March of 1998 to be in full compliance with 10 CFR 50 Appendix B as well as ISO 9001-1994. The current QA program and departmental procedures satisfy the following:

- ISO 9001-1994 in the Version 9.3.1 qualification
- ISO 9001-2000 in the Version 10.2.1 qualification
- 10 CFR 50 Appendix B for both the Version 9.3.1 and 10.2.1 qualifications
- TÜV Certification for DIN V VDE 19250, resp. DIN V VDE 0801 Class 6 in the Version 9.3.1 qualification
- TÜV Certification for IEC 61508, Part 1-7:2000, IEC 61511-1:2004, EN 50156-1:2004, EN 61131-2:2005, EN 61000-6-2:2005, EN 61000-6-4:2001, EN 54-2:1997, NFPA 72:2002, NFPA 85:2001.

Triconex quality manuals and procedures have been developed specifically for the development, enhancement, maintenance, certification, manufacture, and servicing of the Tricon. These manuals provide the requirements for the Triconex life cycle process planning, which includes software.

Three sets of processes and procedures describe the various aspects of software life cycle process planning:

- Triconex Quality Assurance Manual (QAM), Reference 2.5.26.
- Triconex Quality Procedures Manual (QPM), Reference 2.5.27.
- Triconex Engineering Department Manual (EDM), Reference 2.5.28.

The Quality Assurance Manual provides the overall corporate QA requirements. The Quality Procedures Manual contains specific procedures for the QA organization including validation testing. The Engineering Manual provides the procedures specific to the development, verification, configuration control, maintenance, and enhancement of the Tricon. All manuals have been improved, expanded, and enhanced during the period of time in which the Tricon has been produced.

These engineering procedures define a product life cycle that includes the following phases:

- Requirements Phase
- Design Input Phase
- Design Output Phase
- Verification Phase
- Product Validation Phase
- Certification and Agency Approvals
- Active Phase
- Product Obsolescence and Deactivation

To assess the processes used to produce the Tricon software, including pre-existing code from the initial release, the QAM, QPM, and EDM procedures were reviewed at various points in time between 1986 and 2006. The evolution of the various Engineering Procedures described in the Software Qualification Report, Reference 2.5.65, demonstrates the continual refinement and improvement of the procedures.

2.3.3 Software Verification and Validation Process

An essential issue for acceptability is a defined, controlled process for software verification and validation (V&V). The requirements specified in IEEE Standard 1012-1998 provide an approach that is acceptable to the NRC for meeting the requirements of 10 CFR 50, Appendix B and the guidance given in Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." NRC Regulatory Guide 1.168 endorses IEEE Standard 1012-1998 as an acceptable methodology for implementing the verification and validation of safety system software, subject to certain exceptions listed in that Regulatory Guide.

Triconex verification and validation activities do not strictly follow the ANSI/IEEE Standard 1012 model. However, a life cycle process is defined in the engineering procedures and this process includes verification and validation processes. A detailed assessment of the Triconex process is provided in the Software Qualification Report, Reference 2.5.65.

Verification techniques used by Triconex include design document review, and code walk through to verify the correctness of code modifications and functionality enhancements.

Validation activities include functional tests (with regression testing) of the integrated system in accordance with written test procedures. In addition, hardware and software design upgrades and enhancements are tested using the automated fault insertion test system (AFITS) to validate the diagnostic capability and operating software associated with diagnostics.

AFITS is a robotic tool for physically injecting faults into individual Tricon modules operating in a system environment, monitoring the system response, and collecting objective evidence. For every fault condition introduced, the system is required to detect the fault, exhibit correct error handling behavior, and continue to operate without any safety critical loss of functionality. Typical faults reported include 1) fault not masked (e.g. outputs were driven incorrectly), 2) fault not detected internally, 3) fault not detected externally, and 4) faults that cause a permanent loss of TMR (Triple Modular Redundancy). The scope of testing varies according to the complexity and scope of the change being applied to the version revision. The results of a CIA (change impact analysis) are used to determine the extent of FI regression testing required for each system modification. A major version revision could include the following test parameters:

- Modules tested in 'Spared' mode
- Modules tested in 'Non-Spared' mode
- Dead hardware leg testing to test dual-mode capability at the module level.
- MP modules tested in TMR and Dual modes, as specific hardware is active in Dual Mode that is not active in TMR Mode. Both logical and physical paths are tested.

The TriStation software is tested by manual and automated tests in accordance with written functional test procedures. These tests validate correct operation of both the TriStation and the Tricon. Functional outputs, boundary conditions, value conversions, and other essential functions are validated in this test. Since the test is automated and runs in a PC Windows environment, any changes to the TriStation operator interface will be explicitly uncovered in the testing process.

The Triconex V&V activities are supplemented by the independent certification activities performed by TÜV-Rheinland. TÜV-Rheinland is a German third party certification agency that validates equipment to existing international standards. In 1992, TÜV-Rheinland first certified the Tricon Version 6.2.3 to meet standard DIN V VDE 19250, resp. DIN V VDE 0801 requirements for safety equipment, class 5 (Test Report 945/EL 366/91, Reference 2.5.71).

Each new version has been tested by TÜV-Rheinland, with Version 10.2.1 being certified in October of 2006 to the IEC standard (968/EZ105.06/06, Reference 2.5.72). The testing preformed by TÜV-Rheinland examines both the hardware and the software. Both the system software (main processors and associated communication and I/O support modules) and the application development tools software (TriStation 1131) are reviewed and tested with each new version. The TÜV Rheinland driven development, release, and maintenance procedures are effective for control of the Tricon development process.

The three aspects of software review and testing by TÜV-Rheinland are software analysis, software testing, and integrated system (software/hardware) testing.

The TÜV-Rheinland software analysis consists of examination of the code and support documentation to ensure that specifications are met and good practices are used during the development. The key element is the software specification from which the coding is generated. The software / firmware modules are checked to verify that their functions are sufficiently described in the module's specification. From the specification, the source code is examined to ensure that the source code implements the specification. The analysis also evaluates measures taken to avoid systematic failures in the software (common mode failures). Here the emphasis is placed on examining the software development process and quality controls used by Triconex.

TÜV-Rheinland testing of the TriStation software consists of the following:

- The Triconex life cycle and life cycle documentation was evaluated, including verification and validation at the unit, module, and system levels. TÜV Rheinland concluded that the development life cycle meets the expectations of IEC 61508.
- TÜV Rheinland performed a Functional Safety Assessment at Triconex facilities. TÜV Rheinland engineers evaluated the application and effectiveness of Triconex measures to avoid failures, as well as the measures taken to detect and control failures within the hardware, and concluded that Triconex complies with expectations. TÜV Rheinland does take credit for Triconex system, module, automated fault insertion, and unit level hardware and software verification and validation tests. TÜV Rheinland engineers evaluated the module level Failure Modes and Effects Analysis and found the Triconex FMEA acceptable.
- TÜV Rheinland reviewed the software and hardware life cycle documentation, as well as the configuration management and change control applied to that documentation, and concluded that Triconex documentation and processes are appropriate and meet the software and hardware life cycle expectations established in IEC 61508.
- TÜV Rheinland engineers inspected the average Probability of Failure on Demand (PFDavg) and Mean Time To Spurious Failure (MTTF spurious) spreadsheet prepared by Triconex, and concluded that the spreadsheets used accepted methodologies and reasonably conservative failure data (Bellcore, Issue 6).
- TÜV Rheinland engineers inspected the Triconex upgrades of many of the previously accepted modules. These upgrades included changing through-hole components for surface mount components. The TÜV Rheinland engineers concluded that the surface mount

modules are 100% plug-compatible, and are form, fit, and function replacements for the through-hole modules. The firmware was slightly modified to support the new microprocessor model used on the new modules.

Software and integrated system testing is performed to verify external communication and fault detection capabilities.

Since Version 6.2.3, the TÜV certification process has provided a second layer of classically independent verification and validation. While the TÜV certification process is focused on obtaining a "safety" certification, the process requires a set of verification and validation activities. Together, the internal Triconex review, combined with the TÜV reviews provides an equivalent level of confidence to that obtained in an IEEE 1012 compliant program.

2.3.4 Safety Analysis

The Safety Analysis as described in BTP 7-14 is most applicable to applications where specific hazards can be identified (e.g. control rods are not driven into the core). Until a user application is defined with inputs and outputs, there are no "hazards" in the sense that no set of conditions can be defined that will lead to an accident or loss event.

The Tricon – or any programmable controller – can be considered from the viewpoint of being a potential initiator of events through failures of hardware components or through design errors that are manifested as faults in the execution of software.

Unlike most controllers, the Tricon was conceived, designed, and developed specifically for safety applications and applications where high availability is required. From this perspective, all design activities have inherently included safety analysis. For example, the triple redundant architecture and the resultant fault tolerant capability are in themselves the result of a safety analysis. Therefore, the Tricon architecture should be viewed as an output of the safety analysis that occurred in the design phase of the system. These safety analysis activities continue to be the driving force in the engineering design decisions that are made.

2.3.5 Configuration Management and Error Notification

Triconex has always had a formal configuration control, change control, and error tracking system. Software and documents, once placed under configuration control, are retrievable and changes are controlled.

The Tricon contains several firmware sets, on several modules. A Tricon version is defined in a formally released, configuration controlled Software Release Definition. These documents define the unique compilation number for each firmware set in a Tricon and TriStation 1131 release. The firmware defined in each Software Release Definition has been validated by both Triconex Product Assurance and by TÜV Rheinland. The minimum supported hardware, software, and firmware levels are defined in the Product Release Notice.

Versions of the Tricon system are controlled with a numbering system that provides the major, minor, and maintenance version data. Major versions, such as 6.0, 7.0, 8.0, 9.0, and 10.0, typically involve extensive hardware and/or software changes. As an example, Version 9.0 reflected a change in the system chassis, removing the terminations from plug-in modules with the Input/Output modules to Elco connectors on the top of the chassis.

Included in the configuration control system is a complete customer history tracking system. This system lists each Tricon system and module, by serial number, defining where the module is, when it was installed, and any repairs done by Triconex. It is used to monitor product operating experience, to facilitate technical support, and to support customer notification.

Triconex also has an established error tracking and reporting program that is consistent with the requirements established in 10 CFR 21. Errors are classified according to severity, with Product Alert Notices (PAN) being the most significant. Only fifteen PANs have been issued against the Tricon since the release of the system over 21 years ago. All of the Product Alert Notices were evaluated as part of this qualification process. An extremely conservative approach to customer notification was found. Most of the Product Alert Notices affected only a very small subset of users. Instead of attempting to determine which customers might be at risk, Triconex chose to notify all customers. None of the notices affect this qualification effort. In addition to this safety critical issue notification system, other notification systems exist which are used to disseminate technical data.

Errors, once entered into the automated error tracking system, are retrievable, changes are controlled, appropriate resolutions are generated, and all data is available. After review for risk of implementation by the Change Control Board, errors may be held for future implementation, released for immediate resolution, or indefinitely postponed. Customer notification is also addressed in this decision. Immediate customer notification will result if possible safety implications exist.

2.4 SYSTEM APPLICATION

This summary report describes tests, evaluations, and analyses that were performed to demonstrate generic qualification of the Tricon system for use in safety-related nuclear facility applications. In any actual nuclear facility application, facility-specific conditions must be evaluated to ensure that they are within the qualification envelope of the Tricon system as described in this summary report. System-specific performance requirements must also be evaluated to ensure that the Tricon system accuracy, response time, and other performance attributes are adequate. Other important considerations for application of the Tricon system to specific facility applications include design, operation, and maintenance requirements needed to ensure high reliability. These requirements include, for example, annunciation of system faults and periodic testing to check for the limited number of abnormal conditions not detectable by the built-in self-diagnostics.

A summary of exceptions to the EPRI TR-107330 requirements and/or test methodology is summarized in Table 2-2. Appendix A contains a compliance traceability matrix of the EPRI requirements versus the Tricon V10 Qualification with appropriate references.

To assist the user with facility-specific application of the Tricon system, an Application Guide is included as Appendix B to this report. The Application Guide is intended to capture all aspects of the Tricon qualification envelope, as well as additional guidance on appropriate design, operation, programming, and maintenance of the system.

Table 2-2 Summary of Exceptions/Clarifications to EPRI TR-107330 Requirements

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.2.1.1.A	Analog Voltage Input Module Ranges. The PLC shall include analog voltage input modules with ranges of: 0 to 10 VDC, -10 to 10 VDC, and 0 to 5 VDC.	Partial Exception	Tricon analog voltage input modules do not include a –10 to 10 VDC range.
4.3.2.1.1.D	Analog Voltage Input Module Common Mode Voltage. The common mode voltage capability shall be at least 10 volts with a common mode rejection ratio of at least 90 dB.	Partial Exception	Common mode rejection rating of Module 3701 is 80 dB, Module 3721 is 85dB, and Module 3703 is 90dB.
4.3.2.1.1.A	Analog Current Input Module Ranges. The PLC shall include analog current input modules with ranges of: 4 to 20 mA and 10 to 50 mA or 0 to 50 mA.	Partial Exception	Tricon analog current input modules do not include a 10 to 50 mA range or 0 to 50 mA range.
4.3.2.1.1.E	Analog Current Input Module Common Mode Rejection Ratio. The common mode rejection ratio shall be at least 90 dB.	Partial Exception	Common mode rejection rating of Module 3701 is 80 dB, Module 3721 is 85dB, and Module 3703 is 90dB.
4.3.2.1.3.A	RTD Input Module Types. The PLC shall include RTD input modules for use with 2, 3 or 4 wire European (DIN 43 760) or US standard 100 ohm RTDs.	Partial Exception	Tricon RTD input signal conditioners are for use with 2 or 3 wire, 100 ohm platinum RTDs.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.2.1.3.B	RTD Input Module Ranges. The PLC shall include RTD input modules with a range of at least 0 to 800°C (32 to 1472°F).	Exception	Tricon RTD input signal conditioners span the -100°C to 600°C (32 to 1112°F) range.
4.3.2.1.3.D	RTD Input Module Resolution. The minimum resolution shall be 0.1° or less for both °C or °F scaling.	Exception	Tricon RTD input signal conditioners (32 to 1112°F max. span = 1 to 5 V output) are interfaced with a 12 bit, 0 to 5 V analog input module. The resulting minimum resolution is 0.33°F (0.19°C).
4.3.2.1.3.G	RTD Input Module Response Time. The overall response time of the RTD input modules must support the response time requirement given in Section 4.2.1.A.	Exception	See Table Section 4.2.1.A. For large step changes (0 to 90% of full scale range), RTD's and input signal conditioners have a relatively long input update rate, and were not considered in qualification response time testing.
4.3.2.1.4.A	T/C Input Module Types. The PLC shall include T/C input modules for use with type B, E, J, K, N, R, S, and T thermocouples over the specified temperature ranges.	Partial Exception	Tricon T/C input modules are for use with type E, J, K, and T thermocouples. Type J input range is –250 to 2000°F (vs. TR requirement of 32 to 2192°F).
4.3.2.1.4.D	T/C Input Module Resolution. The minimum resolution shall be 0.1° or less for both °C or °F scaling.	Exception	Minimum resolution is 0.125°F (0.07°C).

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.2.2.2.A	Discrete DC Input Module Types. The PLC shall include discrete DC input modules for nominal inputs of 125, 24, 15, and 12 V dc.	Partial Exception	Tricon discrete DC input modules are for nominal inputs of 115, 48 and 24 V dc.
4.3.2.2.3	TTL Input Requirements. Requirements for TTL level input modules.	Exception	There is no TTL level input module available for use with the Tricon PLC.
4.3.2.3.1.D	Pulse Input Module Count Accuracy. The module shall have up and down count modes with a range of at least 9999. The accuracy of the count shall be ≤ 0.1%.	Exception	The Tricon pulse input module provides speed or RPM measurement only.
4.3.2.3.1.E	Pulse Input Module Frequency Accuracy. The module shall have a frequency mode with a range of at least 20 to 5000 Hz. The accuracy of the frequency measurement shall be ≤ 0.1%.	Partial Exception	Accuracy is ± 1.0% of reading from 20 to 99 Hz. Accuracy is ± 0.1% of reading from 100 to 999 Hz. Accuracy is ±0.01% from 1000 to 20,000 Hz
4.3.3.1.1	Analog Voltage Output Requirements. Requirements for analog voltage output modules.	Exception	There is no analog voltage output module available for use with the Tricon PLC.
4.3.3.1.2.A	Analog Current Output Module Ranges. The PLC shall include analog current output modules with ranges of 4 to 20 mA or 0 to 20 mA, and 10 to 50 mA or 0 to 50 mA.	Partial Exception	Tricon analog current output module output range is 4 to 20 mA.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.3.2.1.A	Discrete AC Output Module Types. The PLC shall include discrete AC output modules for nominal outputs of 120 and 24 V ac.	Partial Exception	Tricon discrete AC output modules do not include 24 V ac nominal outputs.
4.3.3.2.2.A	Discrete DC Output Module Types. The PLC shall include discrete DC output modules for nominal outputs of 125, 48, 24, 15 and 12 V dc.	Partial Exception	Tricon discrete DC output modules include 120, 48 and 24 V dc nominal outputs.
4.3.3.2.2.C	Discrete DC Output Module ON State Voltage Drop. The ON state voltage drop shall not exceed 2 V dc at 0.5 amps.	Exception	Module Model 3607E ON state voltage drop is < 3 V.
4.3.3.2.2.D	Discrete DC Output Module OFF State Leakage. The OFF state leakage current shall not exceed 2 mA.	Exception	Module Models 3625 OFF state load leakage is 4 mA maximum
4.3.3.2.2.E	Discrete DC Output Module Operating Range. The module points must operate for source inputs of 90 to 140 V dc min. (125 V dc output), 35 to 60 V dc min. (48 V dc output), and 20 to 28 V dc min. (24 V dc output).	Exception	Module Model 3607E (48 V dc output) operates from 44 to 80 V dc. Module Model 3625 (24 V dc output) operates from 22 to 45 V dc.

TRICONEX TOPICAL REPORT

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.3.2.3.A	Relay Output Module Types. The PLC shall include relay output modules that provide normally open and normally closed contacts.	Partial Exception	Tricon relay output module contacts are normally open.
4.3.3.2.4	TTL Output Requirements. Requirements for TTL level output modules.	Exception	There is no TTL level output module available for use with the Tricon PLC.
4.3.4.4.E	Communication Port Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	Exception	Tricon TCM serial communication ports tested for Class 1E to Non-1E isolation capability at 250 V ac (vs. 600 V ac required by TR) and 250 V dc. Test level is based on maximum credible voltage.
4.3.6.1	Normal Environmental Basic Requirements. The normal PLC operating environment is: Temperature Range: 16 to 40°C (60 to 104°F). Humidity Range: 40 to 95% (non-condensing)	Comply	Tricon is rated for 0 to 60°C (32 to 140°F), 5% to 95% humidity (non-condensing).
	Power Source Range: As given in Section 4.6.1.1	Exception	See Table Section 4.6.1.1 for exceptions to power source range.
	Radiation Exposure: Up to 1000 Rads	Comply	Tricon has been tested to a 1000 Rad dose of Co60 gamma radiation.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.6.2	Abnormal Environmental Basic Requirements. The abnormal PLC operating environment is: Temperature Range: 4 to 50°C (40 to 120°F). Humidity Range: 10 to 95% (non-condensing)	Comply	Tricon is rated for 0 to 60°C (32 to 140°F), 5% to 95% humidity (non-condensing).
	Power Source Range: As given in Section 4.6.1.1	Exception	See Table Section 4.6.1.1 for exceptions to power source range.
	Radiation Exposure: Up to 1000 Rads	Comply	Tricon has been tested to a 1000 Rad dose of Co60 gamma radiation.
4.3.7	EMI/RFI Withstand Requirements. The PLC shall withstand EMI/RFI levels given in EPRI TR--102323. When exposed to the radiated and conducted test levels, the PLC processors shall continue to function, I/O data transfer shall not be interrupted, discrete I/O shall not change state, and analog I/O shall not vary more than 3%.	Exception	Tricon showed some susceptibilities to NRC RG 1.1.80 Rev. 1 (CE101).

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
	Power Sources. AC sources shall operate from at least 90 to 150 V ac and 57 to 63 Hz.	Exception	Model 8310 AC power supply modules are rated for 85 to 140 V ac input.
4.6.1.1.A	AC sources shall operate at the temperature and humidity range given in Section 4.3.6.	Comply	Model 8310 AC power supply modules were tested as per required temperature and humidity range (see Table Section 4.3.6.3).
	Power Sources. DC sources shall operate from at least 20.4 to 27.6 V dc.	Exception	Model 8311 DC power supply modules are rated for 22 to 31 V dc input.
4.6.1.1.B	DC sources shall operate at the temperature and humidity range given in Section 4.3.6.	Comply	Model 8311 DC power supply modules were tested as per required temperature and humidity range (see Table Section 4.3.6.3).

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
	Surge Withstand Capability Requirements. PLC platform shall withstand IEEE Standard C62.41 ring wave and combination wave, 3000 volt peak surges.	Comply	Power sources meet surge withstand criteria. Circuits were tested to IEC 61000-4-5 and IEC 61000-4-12 using 1 kV Ring wave, and combination waves at 1kV open circuit/0.5kA short circuit per RG 1.180, Rev. 1, Level 2. All circuits met TR Section 4.6.2 acceptance criteria.
4.6.2	Withstand capability applies to power sources, analog and discrete I/O interfaces, and communication port interfaces. Per Section 6.3.5, surge testing shall be conducted per IEEE Standard C62.45.	Partial Exception	Power Sources were tested per Reg. Guide 1.180 Rev. 1 for category B low exposure installations to 2KV. IEEE Standards 62.41 and 62.45 do not address testing of I/O and communication circuits; these circuits were tested per Reg. Guide 1.180 Rev. 1 for low exposure level 2 installations at 1KV. Tests were performed to IEC61000-4-5 for combination wave and 61000-4-12 for Ring Wave.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.6.4	Class 1E/Non-1E Isolation Requirements. The PLC modules shall provide isolation of at least 600 V ac and 250 V dc applied for 30 seconds. Isolation features shall conform to IEEE Standard 384. Isolation testing shall be performed on the modules.	Exception	Only relay output modules, communication ports, and fiber optic chassis inter-connections are intended to provide Class 1E to Non-1E isolation. Isolation tests were performed on relay output module and communication ports. Relay output module meets TR Section 4.6.4 isolation requirements. Communication ports provide isolation to 250 V ac and 250 V dc for 30 seconds. Fiber optic chassis connections inherently provide isolation through non-conducting fiber optic cables.
5.2.A	Application Objects Testing. Testing of the software objects in the PLC library shall be performed. This testing shall be in addition to any testing performed by the manufacturer.	Exception	Triconex and TÜV Rheinland have performed extensive testing of the Tricon PLC application software. Results of this testing are documented in Ref. 58. Accordingly, this testing was not performed.
5.2.F	Burn-In Test. A minimum 352 hour burn-in test shall be performed during acceptance testing.	Exception	Triconex routinely conducts burn-in tests on all Tricon hardware as part of manufacturing process. This testing meets TR requirements for burn-in testing. Accordingly, this test was not performed.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
5.3.B	Response Time. Response time of analog input to digital output and digital input to digital output sequences shall be measured. For baseline (acceptance) testing the acceptance criteria is that the measured response time shall not vary more than 20% from the value calculated from manufacturer's data. For all subsequent testing, the measured value shall not vary more than 10% from the baseline.	Exception	Based on Tricon design, it is not practicable to perform a test that provides consistent (within ±20%) measured response times. Instead, manufacturer's data is used to calculate maximum expected AI to DO and DI to DO response times. The acceptance criterion for all tests is that the calculated response times are not exceeded.
5.3.E	Communication Operability. If any communication functions are included in the qualification envelope, then operability of the ports shall be tested. Tests shall look for degradation in bit rates, signal levels and pulse shapes of communication protocol.	Partial Exception	The TCM Module NET1 port and NET2 ports are included in the qualification envelope. Test equipment to measure degradation of bit rates, pulse shapes, and signal levels was not available at the time testing was performed. The port protocol is proprietary and not amenable to TR specified tests. Port operation is monitored for correct performance throughout all qualification tests.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
5.4	Prudency Testing Requirements. The Prudency tests shall be performed with the power supply sources at the minimum values specified in Section 4.6.1.1.	Partial Exception	To accommodate power frequency changes, external power to the 230Vac230 V ac chassis power supplies was provided through a step-up transformer which was fed by the same external power supply for the 115Vac115 V ac chassis power supplies. This limited the voltage to the 115Vac115 V ac chassis power supplies to 97Vac.97 V ac.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
5.5	Operability/Prudency Testing Applicability Requirements. As a minimum, Operability and Prudency tests shall be performed: - During acceptance testing: Operability – All, Prudency – All - During environmental testing: Operability – All, Prudency – All - During seismic testing: Operability – All, Prudency – All - After seismic testing: Operability – All, Prudency – None - During EMI/RFI testing: Operability – All except analog I/O checks, Prudency – Only burst of events test - After ESD testing: Operability – All, Prudency – None	Partial Exception	Due to short duration of seismic SSE tests, and special set-up required for EMI/RFI tests, it is not practicable to perform Operability and Prudency tests at those times. The testing complied with the other requirements of Section 5.5.
5.6	Application Software Objects Acceptance (ASOA) Testing. Requirements for ASOA testing.	Exception	See Table Section 5.2.A

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
6.2.1.E	Power Supplies. The test specimen shall include the power supplies needed to meet the TR requirements. Additional resistive loads shall be placed on each power supply output so that the power supply operates at rated conditions.	Exception	The Tricon design does not allow for adding resistive load on the power supplies without altering design and operation. To demonstrate significant power supply loading, one chassis of the test specimen was fully populated with one module in each slot.
6.2.1.F	Dummy Modules. Dummy modules shall be used to fill all remaining slots in the main chassis and at least one expansion chassis. The dummy modules shall provide a power supply and weight load approximately equal to an eight point discrete input module.	Exception	Seismic Balance Modules (SBMs) were installed in two test specimen chassis to increase the weight loading to that representative of a fully module populated chassis. Dummy modules did not provide a load on the power supplies.
6.3.2	EMI/RFI Test Requirements. EMI/RFI testing to be performed as described in Section 4.3.7. Susceptibility tests to be performed at 25%, 50%%, and 75% of specified levels in addition to the specified levels.	Exception	EMI/RFI testing performed per R.G. 1.180, R1. Testing performed at levels lower than specified levels only as needed to establish susceptibility threshold.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
6.3.2.1	EMI/RFI Mounting Requirements. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	Due to space limitations of NTS Labs EMI/RFI chamber, the test specimen was mounted less than six feet above the floor. The test specimen was mounted in a Rittal cabinet with sides and doors removed. Cabinets provided no significant shielding.
6.3.5.1	Surge Withstand Test Mounting Requirements. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	Due to space limitations of NTS Labs EMI/RFI chamber, the test specimen was mounted less than six feet above the floor. The test specimen was mounted in a Rittal cabinet with the sides and doors removed.
6.3.6	Class 1E to Non-1E Isolation Testing. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	Due to space limitations of NTS Labs EMI/RFI chamber, the test specimen was mounted less than six feet above the floor. Test The test specimen was mounted in a Rittal cabinet with the sides and doors removed.
6.4.4.G	ASOA Test Compliance. Results shall be evaluated for compliance to Section 5.6 requirements.	Exception	ASOA testing not performed.

2.5 REFERENCES

2.5.1 NUREG-800; Standard Review Plan, Section 7.0, "Instrumentation and Controls – Overview of Review Process," Rev. 5, March 2007

2.5.2 NUREG/CR-6241, "Using Commercial-Off-the-Shelf (COTS) Software in High-Consequence Safety Systems," November 10, 1995

2.5.3 NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," October 1997

2.5.4 U.S. Nuclear Regulatory Commission Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," October 2003

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

2.5.6 EPRI Report TR-102323-R1, "Guidelines for Electromagnetic Interference Testing in Power Plants"

2.5.7 IEEE Std. 323-1983, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"

2.5.8 IEEE Std. 344-1987, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"

2.5.9 IEEE Std. 381-1977, "Standard Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations"

2.5.10 IEEE Std. 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits"

2.5.11 IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

2.5.12 IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation Plans"

2.5.13 IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

2.5.14 IEC 61000-4-2 "Electromagnetic Compatibility (EMC), Part 4-2: Testing and Measurement Techniques, Electrostatic Discharge Immunity Test," April 2001

2.5.15 IEC 61000-4-3, "Electromagnetic Compatibility (EMC), Part 4-3: Testing and Measurement Techniques, Radiated, Radio-Frequency, Electromagnetic Field Immunity Test," September 2002

2.5.16 IEC 61000-4-4, "Electromagnetic Compatibility (EMC), Part 4-4: Testing and Measurement Techniques, Electrical Fast Transient/Burst Immunity Test," 2004

2.5.17 IEC 61000-4-5, "Electromagnetic Compatibility (EMC), Part 4-5: Testing and Measurement Techniques, Surge Immunity Test," April 2001

2.5.18 IEC 61000-4-6, "Electromagnetic Compatibility (EMC), Part 4-6: Testing and Measurement Techniques, Immunity to Conducted Disturbances, Induced by Radio-Frequency Fields," November 2004

2.5.19 IEC 61000-4-8, "Electromagnetic Compatibility (EMC), Part 4-8: Testing and Measurement Techniques, Power Frequency Magnetic Field Immunity Test," March 2001

2.5.20 IEC 61000-4-9, "Electromagnetic Compatibility (EMC), Part 4-9: Testing and Measurement Techniques, Pulse Magnetic Field Immunity Test," March 2001

2.5.21 IEC 61000-4-10, "Electromagnetic Compatibility (EMC), Part 4-10: Testing and Measurement Techniques, Damped Oscillatory Magnetic Field Immunity Test," March 2001

2.5.22 IEC 61000-4-12, "Electromagnetic Compatibility (EMC), Part 4-12: Testing and Measurement Techniques, Oscillatory Waves Immunity Test," April 2001

2.5.23 IEC 61000-4-13, "Electromagnetic Compatibility (EMC), Part 4-13: Testing and Measurement Techniques, Harmonics and Interharmonics Including Mains Signaling at A.C. Power Port, Low Frequency Immunity Tests," March 2002

2.5.24 IEC 61000-4-16, "Electromagnetic Compatibility (EMC), Part 4-16: Testing and Measurement Techniques, Test for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz," July 2002

2.5.25 IEC 61784-3, "Industrial Process Measurement and Control – Digital Communications," July 2005

TRICONEX DOCUMENTS

2.5.26 Triconex Quality Assurance Manual (QAM)

2.5.27 Triconex Quality Procedures Manual (QPM)

2.5.28 Triconex Engineering Department Manual (EDM)

2.5.29 Tricon Product Guide, Triconex Document No. 9791007-013

2.5.30 Tricon Planning and Installation Guide, Triconex Document No. 9720077-008

2.5.31 Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System, Invensys Document No. NTX-SER-09-05

2.5.32 Triconex Development Processes for PLDs in Nuclear Qualified Products, Invensys Document No. NTX-SER-09-06

2.5.33 Nuclear System Integration Program Manual, Invensys Document No. NTX—SER-09-021

2.5.34 Invensys Security Program Plan, Invensys Licensing Topical Report 7286-545-2

2.5.35 Tricon Applications in Nuclear Reactor Protection Systems – Compliance with NRC ISG-2 and ISG-4, Invensys Document No. NTX-SER-09-10

2.5.36 Safety Evaluation Report (SER) Maintenance Process, Invensys Document No. NTX-SER-09-20

TRICONEX NUCLEAR QUALIFICATION PROJECT DOCUMENTS

2.5.37 Triconex Nuclear Qualification Quality Plan, Triconex Document No. 9600164--002.

2.5.38 Master Test Plan, Triconex Document No. 9600164-500

2.5.39 Master Configuration List, Triconex Document No. 9600164-540

2.5.40 Software QA Plan, Triconex Document No. 9600164-537

2.5.41 Tricon System Description, Triconex Document No. 9600164-541

2.5.42 Equipment Qualification Summary Report, Triconex Document No.. 9600164--545

2.5.43 Function Diagrams, Triconex Drawing Nos. 9600164-500 to 515

2.5.44 Wiring Schedule, Triconex Drawing No. 9600164-700

2.5.45 Test System Wiring Drawings, Triconex Drawing Nos. 9600164-100 to 300

2.5.46 Setup and Checkout Test Procedure, Triconex Document No. 9600164-502

2.5.47 Operability Test Procedure, Triconex Document No. 9600164-503

2.5.48 Prudency Test Procedure, Triconex Document No. 9600164-504

2.5.49 Radiation Test Procedure, Triconex Document No. 9600164-511

2.5.50 Environmental Test Procedure, Triconex Document No. 9600164-506

2.5.51 Seismic Test Procedure, Triconex Document No. 9600164-507

2.5.52 Surge Withstand Test Procedure, Triconex Document No. 9600164-508

2.5.53 Class 1E to Non-1E Isolation Test Procedure, Triconex Document No. 9600164-509

2.5.54 EMI/RFI Test Procedure, Triconex Document No. 9600164-510

2.5.55 Pre-qualification Operability Test Report, Triconex Document No. 9600164-560

2.5.56 Environmental Test Report, Triconex Document No. 9600164-525

2.5.57 Seismic Test Report, Triconex Document No. 9600164-526

2.5.58 EMI/RFI Test Report, Triconex Document No. 9600164-527

2.5.59 Surge Test Report, Triconex Document No. 9600164-528

2.5.60 Class 1E to Non-1E Isolation Test Report, Triconex Document No. 9600164-529

2.5.61 Performance Proof Operability Test Report, Triconex Document No. 9600164-566

2.5.62 Reliability/Availability Study for Tricon PLC Controller, Triconex Document No. 9600164-532

2.5.63 Failure Modes and Effects Analysis (FEMA) for TRICON V10 PLC, Triconex Document No. 9600164-531

2.5.64 Tricon System Accuracy Specifications, Triconex Document No. 9600164-534

2.5.65 Software Qualification Report, Triconex Document No. 9600164-535

2.5.66 TSAP Software Requirements Specification, Triconex Document No. 9600164-517

2.5.67 TSAP Software Design Description, Triconex Document No. 9600164-518

2.5.68 TSAP Software V&V Plan, Triconex Document No. 9600164-513

2.5.69 TSAP Final V&V Report, Triconex Document No. 9600164-537

2.5.70 Software Traceability Analysis, Triconex Document No. 9600164-720

2.5.71 TÜV-Rheinland Microelectronic and Process Automation, "Type Approval for the Tricon Triple Modular Redundant (TMR) Controller Tricon," Report No. 945/EL 336/91, April 19, 1991

2.5.72 TÜV-Rheinland Microelectronic and Process Automation, "Type Approval of TriconVersion10.2.1," Report No. 968/EZ 105.06/06, October 31, 2006

2.5.73 EFT Test Procedure, Triconex Document No. 9600164-514

2.5.74 ESD Test Procedure, Triconex Document No. 9600164-512

2.5.75 Pre-Qualification Prudency Test Report, Triconex Document No. 9600164-670

2.5.76 Radiation Test Report, Triconex Document No. 9600164-533

2.5.77 EFT Test Report, Triconex Document No. 9600164-521

2.5.78 ESD Test Report, Triconex Document No. 9600164-522

2.5.79 Performance Proof Prudency Test Report, Triconex Document No. 9600164-573

2.5.80 Critical Digital Review, Triconex Document No. 9600164-539

2.5.81 Cable Similarity Analysis, Triconex Document No. 9600164-538

3.0 DIFFERENCES BETWEEN V9.5.3 AND V10.2.1 SYSTEMS

3.1 BACKGROUND

This section provides an overview of the basic hardware and software differences between the Tricon V9.5.3 system (the current V9 system identified in the existing SER) and the Tricon V10.2.1 system. A more complete and detailed discussion of the platform differences between V9.5.3 to V10.2.1 systems is provided in Triconex document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System" (Reference 2.5.31).

As noted in section 2.0, Invensys initiated the Tricon V10.2.1 Nuclear Qualification Upgrade Project to address the contingencies identified for V9.5.3 in *Triconex Topical Report 7286-545-1-A, Qualification Summary Report* and the *NRC Safety Evaluation Report (SER)* dated December 12, 2001 (ADAMS Accession Number ML013470433). NRC staff noted that the Tricon PLC system did not fully meet the guidance of TR-107330 for seismic, EMI/RFI conducted and radiated emissions, surge withstand, and ESD withstand, requiring the nuclear facility engineering staff to verify that reported results envelop the specific facility application. Recognizing that such requirements increase facility contingencies, Invensys initiated modifications of the Tricon platform to elevate its performance to that required in EPRI TR-107330 and the recently issued R.G. 1.180, Revision 1. In addition to EMC hardening of components, Invensys also introduced new processors and features, which required evaluation, verification and validation testing.

The Tricon V10.2.1 system added the following new modules:

- A new Main Processor - Model 3008N
- New SMT-based "Next Generation I/O modules" - AI 3721N and DO 3625N
- A new Communication Module - TCM 4325AN (Fiber Optic)

Upgraded/redesignated versions of existing modules:

- A new Analog Input Module - AO 3805HN (4-20 mA) (from AO 3805EN)
- A new Pulse Input Module - PI 3511N (from PI 3510N)
- Existing Through Hole I/O modules converted to SMT modules:
  (Form, fit, and function compatible)
  - 3701N (0-10 VDC) - Through Hole to 3701N2 (0-10 VDC) – SMT
  - 3501TN 115V AC/DC – Through Hole to 3501TN2 115V AC/DC – SMT
  - 3502EN 48V AC/DC – Through Hole to 3502EN2 48V AC/DC – SMT
  - 3503EN 24V AC/DC – Through Hole to 3503EN2 24V AC/DC – SMT

Miscellaneous support hardware units added:

- New Remote Extender Modules – RXM 4200N, 4201N
- New upgraded Power Supply Modules – PS 8310N2, 8311N2, 8312N2
- New I/O Module termination panels – (various for new modules & EMC levels)
- New Signal Conditioners (various to support new modules)

3.2 SYSTEM ARCHITECTURE & SYSTEM LEVEL DIFFERENCES BETWEEN V9.5.3 & V10.2.1

Section 2 of the V9 SER describes the Tricon V9.5.3 system architecture. The Tricon V10.2.1 system architecture is the same as that of the previously qualified Tricon V9.5.3 system. Figure 3-1, also in the SER, shows the Triple Modular Redundant (TMR) architecture of all Tricon systems:

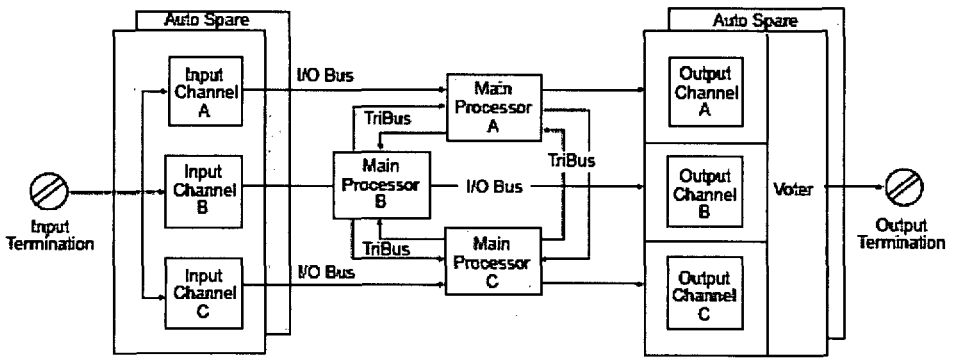


Figure 3-1: Triple Modular Redundant (TMR) architecture

The TriStation 1131 application programming model architecture for the Tricon V10.2.1 system is the same as that of the previously qualified Tricon V9.5.3 system.

The V10.2.1 system is the result of the evolutionary platform improvement of the V9.5.3 system. Since the time the SER was issued, the Tricon V9.5.3 has undergone a number of enhancements as well as maintenance upgrades. The Critical Digital Review (Triconex Report 9600164-539, Reference 2.5.80) provides additional details on the history of upgrades from V9.5.3 to V10.2.1. The stepwise progression of platform change releases between V9.5.3 and V10.2.1 is also described in Reference 2.5.31 (Triconex document NTX-SER-09-05).

3.3 COMPARISON OF V9/V10 DIFFERENCES

Section 1.0 of the V9 SER contains a list of Tricon V9.5.3 modules approved for use in safety-related applications. The SER also contains a table titled "Safety-related Software" in Section 2.2.1 that lists software for each Tricon V9.5.3 module, including version numbers. Tables 3-1 and 3-2 compare Tricon V9.5.3 and V10.2.1 hardware modules and associated software modules. It can be seen that a number of previously qualified modules were deleted from the V10.2.1 qualification. This is primarily a result of replacement by newer modules or changes in market demand.

See section 2.1.4 of this report for the full list of components that went through qualification testing for Tricon V10.2.1.

Table 3-1 Hardware

Module	Tricon V9.5.3 System	Tricon V10.2.1 System
Main Processor	3006N Hardware floating point processor	3008N 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,
	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

Table 3-1 Hardware

Module	Tricon V9.5.3 System	Tricon V10.2.1 System
Remote Extender Modules: **Primary Remote**	4210N (Single Mode Fiber Optic cable) 4211N (Single Mode Fiber Optic	4200N (Multi Mode Fiber Optic cable) 4201N (Multi Mode Fiber
I/O Module Term Panels	Version 8 Term Panels Version 9 Term Panels (various)	Removed Additional Version 9 Term Panels to support new I/O modules
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: ▪ Signal Conditioner (0 to 200 °C) Pt (7B34-CUSTOM) ▪ Signal Conditioner (0 to 600 °C) Pt (7B34-CUSTOM) ▪ Signal Conditioner (0 to 100 mV) (7B30-02-1) ▪ Signal Conditioner (0 to 120 °C) Cu (7B14-C-02-1)
Power Supplies: **120 V** **24 VDC** **230 VAC**	ASTEC Power Modules 8310N 8311N	Alternate Vicor Power Modules 8310N2 8311N2 8312N2
Chassis: **Main Expansion** **Remote Expansion**	8110N 8111N 8112N	8110N2 8111N 8112N

Table 3-2 Software

Module	Tricon V9.5.3 System Software Version	Tricon V10.2.1 System Software Version
TriStation 1131 Developer's Workbench *(Application Development Software)*	V3.1	V4.1.437
Main Processor Software:		
Application Processor	TSX 5211	ETSX 6198 (Build 92)
I/O Processor	IOC 5212	IOCCOM 6054 (Build 92)
COM Processor	COM 5206	
Communication Module Software:		
TCM	Not Applicable	TCM 6136 (Build 92)
Common V9.5.3 COM	ICM 4930	Not Applicable
EICM	IICX 5276	Not Applicable
NCM	NCMX 5028	Not Applicable
ACM	ACMX 5203	Not Applicable
I/O Module Software		
AI 3721N	Not Applicable	AI 6200 (Build 92)
DO 3625N	Not Applicable	DO 6213 (Build 92)
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	Same
DO 3623TN	TSDO 5502	TSDO2 5940
DO 3624N	TSDO 5502	Not Applicable
Remote Extender Modules	RXM 3310	Same

4.0 TRICON V10.5 UPGRADE

4.1 INTRODUCTION

Triconex has completed a Nuclear Qualification Program for its Tricon Triple Modular Redundant (TMR) PLC for safety related (1E) applications in nuclear facilities. The qualification program was performed and documented in accordance with NRC-approved EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." Triconex report 9600164-545, "Qualification Summary Report" (Reference 2.5.42) presented the final results of all testing and analyses performed in accordance with this EPRI specification. Section 2.0 of this Topical Report incorporates the summary information of the Qualification Summary Report.

The focus of the qualification effort was Tricon product version V10.2.1, and TriStation V4.1.437, which were the prevailing versions being marketed at the time the qualification project was being organized. As with any high-tech product, during the extended period of qualification testing and evaluation, the Tricon products continued to evolve such that upgraded versions beyond V10.2.1 and V4.1.437 are now being manufactured and provided to industry. For business reasons, it is now desired to obtain NRC approval of the current Tricon product offering, specifically Tricon V10.5 and its associated support software.

4.2 PURPOSE

All data pertaining to testing and analysis of Tricon V10.2.1 have been provided to the NRC for review. The purpose of this Section of the report is to provide a listing of any pertinent differences between the V10.2.1 product discussed in section 2.0 and the current product upgrades (represented by V10.5). A discussion of impact to qualification testing already completed is also provided. This additional information is provided for the NRC's consideration for inclusion in the SER approval.

4.3 DISCUSSION

No new hardware modules have been added since V10.2.1, i.e., the module listings and hardware descriptions applicable to V10.5 are the same as in section 2.1.4 of this report. Routine component and board changes to maintain production needs are ongoing and are reviewed by the Configuration Control Board (CCB) in accordance with Triconex Appendix B QA procedures. This review confirms that no significant changes have been made to modules or which would adversely affect performance specifications or qualification characteristics (e.g. seismic, environmental, electrical, etc.) as specified in EPRI TR 107330.

V10.5 essentially represents the further evolutionary upgrades and bug fixes made to platform software since V10.2.1 was released. Triconex document NTX-SER-09-05 (Reference 2.5.31)

provides a development tree and table showing the stepwise progression of platform change releases between V9.5.3 and V10.2.1. Figure 4-1 provides an update to this platform history to reflect the further progression of operating software from V10.2.1 to V10.5. Table 4-1 shows the software differences between V10.2.1 and subsequently issued Versions (V10.2.2, V10.2.4 and V10.5) that have been evaluated and qualified for nuclear use (placed on the NQEL) in accordance with Triconex QA procedures. As seen in Table 4-1, there are five software modules in V10.5 that are different from the modules qualified for the V10.2.1 release, i.e.:

ETSX 6271 (versus ETSX 6198)
TCM 6272 (versus TCM 6136)
AI 6256 (versus AI 5661)
DO 6255 (versus DO 6213)
TSDO/HVDO 6273 (versus TSDO 5502)

In addition, the TriStation 1131 programming software revision level for Tricon V10.5 is different. A discussion of these software changes between Tricon V10.2.1 and V10.5 and TriStation 4.1.437 and 4.6.134 is provided below in Sections 4.3.1 and 4.3.2, respectively. Evaluations have determined that the routine product upgrades have not altered the critical characteristics of the product, i.e., current modules have the same functional and environmental characteristics as the V10.2.1 Test Specimen (or better).

The interim revisions between V10.2.1 and V10.5 (i.e., V10.3, V10.4, V10.4.1, and V10.4.2) in the development tree shown in Figure 4-1 have not been released for use in nuclear modules. However, any changes in these releases affecting V10.5 operating software modules were reviewed to assure that these revisions had no negative impact on V10.5 software integrity. A discussion of each of these interim (non-nuclear) releases is provided in Section 4.3.1.4.

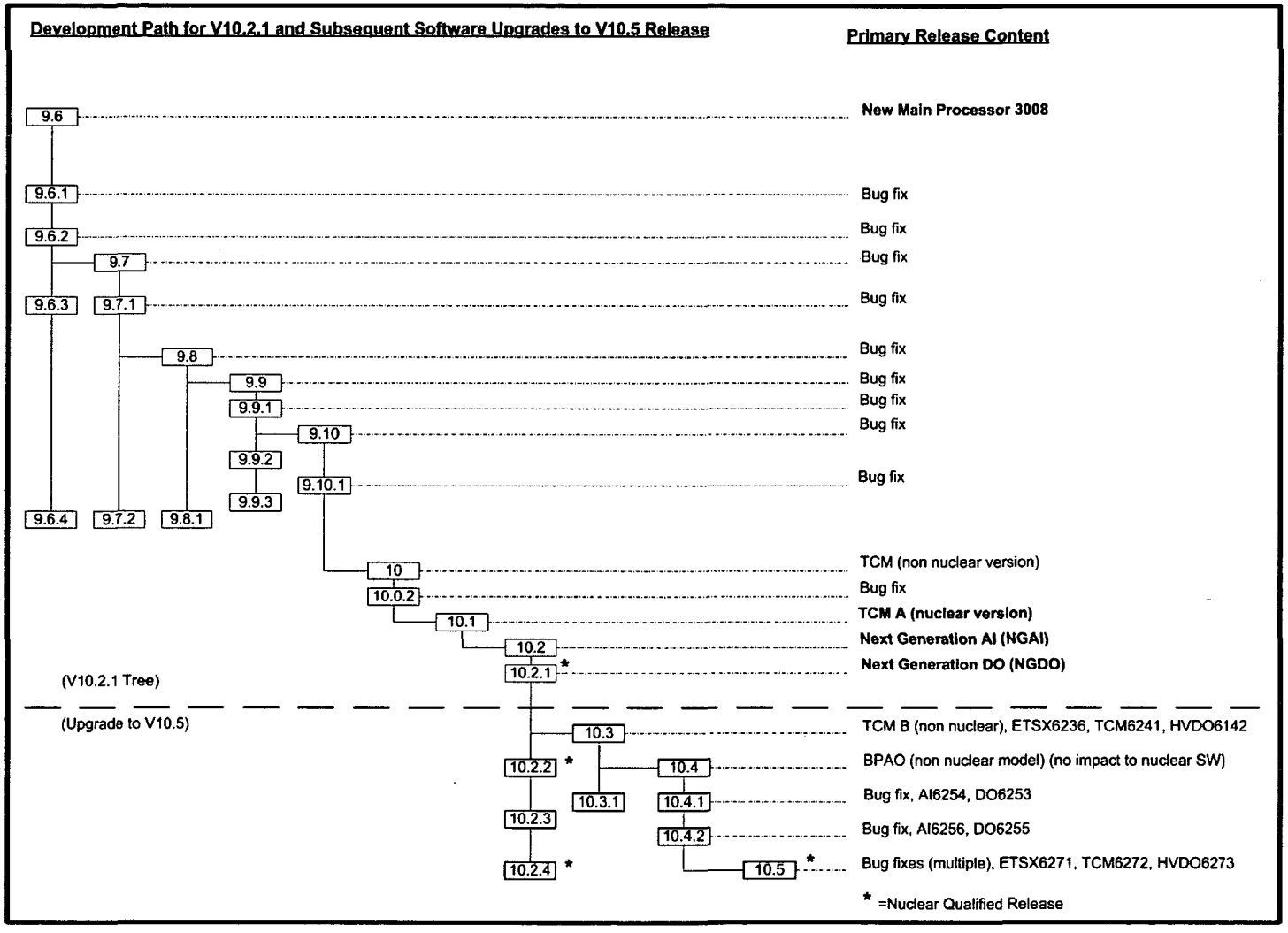


Figure 4-1: V10.2.1 to V10.5 Software Development Tree – Evolutionary Changes

Table 4-1: V10.5 Module Software Development History – Changes in Nuclear Released (NQEL) Software

TYPE	IDENTIFICATION	VERSION (for V10.2.1)	VERSION (for V10.2.2)	VERSION (for V10.2.4)	VERSION (for V10.5)	USED IN
Main Processors	ETSX	6198	6198	6198	**6271***	3008N
	IOCCOM	6054	6054	6054	6054	3008N
Communication Module	TCM	6136	6136	6136	**6272***	4352AN
I/O Modules	AI/NITC	5661	5661	5661	5661	3701N2
	EIAI/ITC	5916	5916	5916	5916	3703EN(AI), 3708EN (TC)
	AI	6200	6200	**6256**	6256*	3721N
	DO	6213	6213	**6255**	6255*	3625N
	PI	5647	5647	5647	5647	3511N
	EDI	5909	5909	5909	5909	3501TN2, 3502EN2, 3503EN2
	EAO	5897	5897	5897	5897	3805HN
	EDO	5781	5781	5781	5781	3601TN, 3607EN
	ERO	5777	5777	5777	5777	3636TN
	TSDO/HVDO	5502	6142	6142	**6273***	3603TN
	TSDO2	5940	5940	5940	5940	3623TN
	RXM	3310	3310	3310	3310	4200N, 4201N
Application Program Development Software	TriStation 1131, Developer's Workbench Suite (Model No./PN)	4.1.437 (7255-4/3000755-802)	4.1.437 (7255-4/3000755-802)	4.1.437 (7255-4/3000755-802)	**4.6.134*** (7255-9/3000755-817)	TriStation Workstation

(**Bold**=new revision released; * = V10.5 Software different from V10.2.1)

4.3.1 Tricon Firmware Changes

4.3.1.1 Upgrade Tricon version from V10.2.1 to V10.2.2

The V10.2.2 incorporates the latest revised TSDO firmware for the 3603TN module. Based on a Product Discrepancy Report and a Technical Advisory Bulletin (TAB), a firmware maintenance update was made to correct a condition of random Output Voter Diagnostic faults on certain PCB board levels.

4.3.1.1.1 Detailed Review of Changes

No additional hardware is being qualified. This change provides newer firmware for the 3603TN Module, which incorporates resolution to the TAB. Only the 3603TN firmware was changed in V10.2.2. Specifically, V10.2.2 consists of a patch to the TSDO 5502 firmware used for the 3603TN, released as the HVDO 6142. Firmware changes were developed and implemented in accordance with EPP 9100135-001. Verification and validation activities were performed in accordance with V&V Plans 9600195-001 and 9600211-001. Firmware was validated as part of V9.52 as documented in the V&V Test Report dated 9/17/2007 and in the 3603T (HVDO) System and I/O Functional Test Report dated 9/17/07.

The new firmware (HVDO 6142) replacing the TSDO 5502 was released together with the V10.2.2 Software Release Definition 6200003-211.

4.3.1.1.2 Impact of Differences on Tricon Qualification

The upgrade to existing qualified 3603TN firmware fixed the problem noted in PDR 2028 and maintained its existing required functionality. The SRD confirms continuing compatibility with the same Tricon modules and other existing software. No functional differences in specified performance or properties were made to the Tricon for V10.2.2.

4.3.1.1.3 Conclusion

It is concluded that this firmware maintenance fix did not introduce any adverse changes to the Tricon system properties or performance. V10.2.2 is considered equivalent to previously qualified V10.2.1 in all aspects of its qualified characteristics.

All software changes were developed in accordance with Triconex Engineering procedures under the Triconex Appendix B QA program. Changes have been provided to and accepted by TÜV Rheinland, in accordance with procedure requirements.

Firmware HVDO 6142 and V10.2.2 are considered to be qualified for nuclear safety related (Class 1E) applications.

4.3.1.1.4 References

6200003-211 Software Release Definition (SRD) – V10.2.2
9791006-143 TAB #143
9100135-001 EPP for 3603T Module Firmware Fix
9100136-001 Change Impact Analysis – High Voltage TSDO Module 3603T Firmware Fix
9600195-001 Tricon V9.52 V&V Plan
9600211-001 3603T (HVDO) Backward Compatibility Software V&V Plan
V9.52 V&V Test Report, dated 9/17/07
3603T HVDO System and I/O Functional Test Report, dated 9/17/07
TUV Certification dated 6/22/08

4.3.1.2 Upgrade Tricon version from V10.2.2 to V10.2.4

The V10.2.4 incorporates the latest revised DO firmware for the 3625N module and AI firmware for the 3721N module. Based on a Product Alert Notice (PAN), a firmware maintenance update was made to correct a condition of the NGIO Core which does not Fault the module when a leg goes down.

4.3.1.2.1 Detailed Review of Changes

No additional hardware is being qualified. This change provides newer firmware for the 3625N and 3721N Modules, which incorporates resolution to the PAN. Only the 3625N and 3721N firmware were changed in V10.2.4. Specifically, V10.2.4 consists of a recompile to the DO 6213 firmware used for the 3625N, released as the DO 6255, and the AI 6200 firmware used for the 3721N, released as AI 6256. Firmware changes were developed and implemented in accordance with EPP 9100234-001. Verification and validation activities were performed in accordance with V&V Plans 9600168-600 and 9100246-001. Firmware was validated as part of V10.2.4 as documented in the V&V Test Report dated 01/19/2009, which includes a system functional test.

The new firmware (DO 6255) replacing the DO 6213 and (AI 6256) replacing the AI 6200 were released together with the V10.2.4 Software Release Definition 6200003-217.

4.3.1.2.2 Impact of Differences on Tricon Qualification

The upgrade to existing qualified 3625N and 3721N firmware fixed the problem noted in the PAN and maintained their existing required functionality. The SRD confirms continuing compatibility with the same Tricon modules and other existing software. No functional differences in specified performance or properties were made to the Tricon for V10.2.4.

4.3.1.2.3 Conclusion

It is concluded that this firmware maintenance fix did not introduce any adverse changes to the Tricon system properties or performance. V10.2.4 is considered equivalent to previously qualified V10.2.2 in all aspects of its qualified characteristics.

All software changes were developed in accordance with Triconex Engineering procedures under the Triconex Appendix B QA program. Changes have been provided to and accepted by TUV Rheinland, in accordance with procedure requirements.

Firmware DO 6255, AI 6256 and V10.2.4 are considered to be qualified for nuclear safety related (Class 1E) applications.

4.3.1.2.4 References

6200003-217 Software Release Definition (SRD) – V10.2.4
9791010-019 PAN #19
9100234-001 EPP for Tricon V10.2.4
9100234-002 Change Impact Analysis – Tricon V10.2.4
9100246-001 Tricon V10.2.4 V&V Plan
9600168-600 NGIO Software Verification and Validation Plan (SVVP)
V10.2.4 V&V Test Report, dated 1/19/09
TUV Certification dated 3/16/09

4.3.1.3 Upgrade Tricon version from V10.2.4 to V10.5

The V10.5 provides a more current version of Tricon System that incorporates a collection of enhancements to operating software and error corrections, as tabulated in SRD 6200003-220.

4.3.1.3.1 Detailed Review of Changes

No additional hardware is being qualified. This change provides newer firmware for the 3008N, 3603TN, and 4352AN Modules, which incorporate resolutions to various PDR's. Changes included correction of conditions noted in TABs 166 and 170. V10.5 also provided common firmware for TCM versions 4352A and 4352B to support alternate board components. Due to the large number of PDRs encompassed in the 10.5 update, other specific changes are not described here, but are tabulated in Software Release Definition (SRD) 6200003-220. Firmware changes were developed and implemented in accordance with V10 EPP 9100218-001. Verification and validation activities were performed in accordance with V&V Plans referenced below. Firmware was validated as documented in the V&V Test Reports listed. V10.5 was approved and released by the Change Control Board (CCB) on 8/13/09.

Table 4-2 provides a summary of affected firmware releases between V10.2.4 and V10.5.

Table 4-2: Affected Firmware Releases

Tricon Firmware Versions			
Firmware module	*Used In:*	*V10.2.4*	*V10.5*
ETSX	3008N	6198	**6271**
TCM	4352AN	6136	**6272**
TSDO/HVDO	3603TN	6142	**6273**

ETSX 6271, TCM 6272, TSDO/HVDO 6273

ETSX 6271, TCM 6272, and TSDO/HVDO 6273 were released in the V10.5 update in August, 2009

Reference documents:

- Software Release Definition (SRD) for V10.5, 6200003-220
- Tricon V10.5 Validation Plan 9600310-001
- V10.5 Validation and Verification Report

Description of change:

The ETSX, TCM, and TSDO/HVDO firmware modules were revised to fix several PDRs affecting the 3008N, 4352AN, and 3603TN modules (see SRD 6200003-220 for details).

Validation:

ETSX 6271, TCM 6272, TSDO/HVDO 6273 were validated as part of the Tricon V10.5 Verification & Validation Plan 9600310-001. This plan included the validation and verification requirements for changes made to the ETSX, TCM, and TSDO/HVDO firmware. The firmware was released in V10.5 per SRD 6200003-220. The results of the V & V are documented in the Tricon V10.5 Validation and Verification Report.

4.3.1.3.2 Impact of Differences on Tricon Qualification

Functional Characteristics

None. The functional characteristics of previously qualified revisions of the Firmware: ETSX, TCM, and TSDO/HVDO have not been changed. This was confirmed in

validation testing. Maintenance release V10.5 removed previously identified errors and/or provided product enhancements for added functionality in the operating and programming software.

Physical Characteristics:

None. No hardware or printed circuit board changes were made. No physical characteristics changed that would affect the radiation, environmental, seismic, or electrical qualification. Revised software is compatible with all associated hardware.

Quality Characteristics:
No differences. All software changes were developed, tested, and released in accordance with the Triconex 10CFR50 Appendix B QA program. Changes have been provided to and approved by TUV Rheinland, in all cases.

Based on the above, it is concluded that changes made in V10.5 did not introduce any changes to the TRICON system's

- Safety Function
- Acceptance Criteria (Performance Specifications)
- Dielectric Stress Levels
- Mechanical Stresses, or
- Postulated Service Conditions

4.3.1.3.3 Conclusion

V10.5 is considered equivalent to V10.2.4, which was previously qualified 1E. No changes were made to the basic functionality or reliability. Triconex has no reason to believe that any of the changes made from V10.2.4 to V10.5 invalidate the findings and results of the generic qualification of the Tricon in accordance with EPRI TR-107330.

No additional qualification steps are required to consider Tricon V10.5 qualified. TRICON V10.5 is considered to be qualified for nuclear safety related (Class 1E) application.

4.3.1.3.4 References

EPP 9100218-001
SRD for V10.5, 6200003-220
Tricon V10.5 Validation Plan 9600310-001
V10.5 Validation and Verification Report
TAB 166
TAB 170
TUV Certification for V10.5, dated 7/22/09

4.3.1.4 Other Releases potentially affecting V10.5 Software

The Software development path from V10.2.1 to V10.5 shown in Figure 4-1 reflects the release of interim versions 10.3, 10.4, 10.4.1, and 10.4.2. These were commercial releases that were not specifically qualified for nuclear facility applications. However, two of the releases (V10.3 and V10.4.1) made changes to software modules that are used in nuclear qualified V10.5 but not described above. Records for these releases were reviewed to confirm that software changes were developed, controlled, and validated accordance with approved EDM development processes.

Release V10.3 was initiated to support new commercial versions of the TCM modules (in addition to the 4352AN). V10.3 included an upgrade to Main Processor software module (ETSX 6236) and Communication Module software module (TCM 6241), both of which were superseded by later V10.5 upgrades ETSX 6271 and TCM 6272, discussed above. V10.3 was approved and released by the Change Control Board (CCB) on 4/26/07. This release was also reviewed and approved by TUV.

Reference documents:

- Engineering Project Plan, 9100109-001
- Software Release Definition (SRD) for V10.3, 6200003-200
- Tricon V10.3 Validation Plan 9600186-001/9600190-001
- V10.3 Validation and Verification Report
- V10.3 TUV approval dated 5/14/07

Release V10.4.1 was primarily initiated to support an interim fix to a software bug (PAN 19). This release included an interim upgrade to NGDO software module (DO 6253) and NGAI software module (AI 6254), both of which were superseded by later V10.2.4 upgrades AI 6271 and TCM 6272, discussed above. V10.4.1 was approved and released by the Change Control Board (CCB) on 9/15/08. This release was also reviewed and approved by TUV.

Reference documents:

- Engineering Project Plan, 9100227-001
- 9791010-019, PAN #19
- Software Release Definition (SRD) for V10.4.1, 6200003-214
- Validation Plan/Section 7.0 of 9100227-001
- PAN 19 Validation and Verification Report (V10.4.1/V10.3.1/V10.2.3)
- V10.4.1 TUV approval dated 11/12/08

Conclusion: The referenced interim changes to the ETSX, TCM, AI, and DO software modules in V10.3 and V10.4.1 (between V10.2.1 and V10.5) were developed, controlled, and validated in accordance with approved EDM procedures, as evidenced in development records and TUV approvals, and therefore had no adverse impact on subsequent revisions of these modules in V10.5.

4.3.2 TriStation 1131 Changes

4.3.2.1 Upgrade TriStation version from V4.1.437 to V4.6.134

The TRICON PLC System Version 10.2.1 was qualified for use in safety related (1E) applications in nuclear facilities. The original qualification included TriStation 1131 Application Software V4.1.437. The parameters of the V10.2.1 system that was qualified were documented in the Master Configuration List, Triconex document 9600164-540 (Reference 2.5.39). This document defines the modules and operating software, which are qualified for 1E service. Evolutionary changes to Triconex products that do not affect the basic operating characteristics are a routine occurrence. The V4.6.134 provides support for Tricon V10.5 and Emulator Support for the TriSim application.

The purpose of this evaluation is to review the impact of the change from TS1131 V4.1.437 to V4.6.134. A discussion of the relevant changes is provided below.

4.3.2.1.1 Detailed Review of Changes

TS1131 v4.6.134 provides support for Tricon V10.5 and support for the TriSim application. It also adds several product enhancements and fixed 10 problems (PDRs), listed in the SRD.

Reference documents:

- 6200097-032 Software Release Definition for V4.6.134
- TS 1131, V4.6 Project Verification and Validation Report -- archived by QA
- 9100220-001 Change Impact Analysis for V4.6.100
- 9100255-001 Change Impact Analysis for V4.6.134

Description of change:
The major changes in v4.6.134 include

- Support for Tricon 10.5
- Emulator Support for TriSim application
- Support Download Change to emulator
- Support UDP Peer-to-Peer with other emulator instances

For change descriptions, see "TS1131 V4.6 Build 100 Change Impact Analysis" and "TS1131 V4.6 Build 134 Change Impact Analysis."

4.3.2.1.2 Impact of Differences on Tricon Qualification

Based on the above, it is concluded that changes made in V4.6.134 did not introduce any negative impact changes to the TRICON systems

- Safety Function

- Acceptance Criteria (Performance Specifications)
- Dielectric Stress Levels
- Mechanical Stresses, or
- Postulated Service Conditions

4.3.2.1.3 Conclusion

V4.6.134 is considered an improvement to V4.1.437, which was previously qualified 1E. No negative impact changes were made to the basic functionality or reliability. Triconex has no reason to believe that any of the changes made from V4.1.437 to V4.6.134 invalidate the findings and results of the generic qualification of the Tricon in accordance with EPRI TR-107330.

All software changes were developed, tested, and released in accordance with the Triconex 10CFR50 Appendix B QA program. Changes have been provided to and approved by TÜV Rheinland, in all cases.

No additional qualification steps are required to consider TS1131 qualified. TS1131 v4.6.134 is considered to be qualified for nuclear safety related (Class 1E) application.

4.3.2.1.4 References

9100186-001 TriStation V4.6 EPP
6200097-032 Software Release Definition for V4.6.134
9100220-001 Change Impact Analysis for V4.6.100
9100255-001 Change Impact Analysis for V4.6.134
TS 1131, V4.6 Project Verification and Validation Report
TUV Certification for V10.5 (including TriStationV4.6.134), dated 7/22/09

4.3.3 Process Change Review

Changes to the Triconex Quality Assurance program and development processes between V9.5.3 and V10.2.1 were reviewed in document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System." This section reviews changes to processes from V10.2.1 to V10.5 (developed during the period of 2006 to 2009) for any impact on the V10.5 software changes described in sections 4.3.1 and 4.3.2 above.

4.3.3.1 QA program and procedures

For the period of 2001 to 2006, the "Differences Document" (NTX-SER-09-05) tabulated the changes to QA Manual (QAM) sections and Quality Procedure Manual (QPM) procedures to demonstrate that the Appendix B QA program continued to be consistent with QA program commitments, i.e., 10CFR50 Appendix B, 10CFR21, and NQA-1-1994. While ongoing procedure revisions occurred as part of the normal Triconex QA program maintenance, reflecting changes in implementation details and ongoing process

improvements, the QA program continued to be compliant with nuclear industry commitments. This was independently confirmed by nuclear customer and agency audits over the period of 2001 to 2006.

Similarly, during the period from 2006 to 2009 (spanning development of software upgrades to V10.5), commitments to nuclear industry QA regulations and standards did not change. This can be seen by comparing the documented QA Program commitments contained in the 2006 version of the QA Manual (rev 029) and the 2009 QA Manual (revision 040). All revisions to the QAM continued to cite 10CFR50 Appendix B, 10CFR21, and NQA-1-1994 as governing regulations and standards. In addition, all QAM revisions contained reference to the Invensys Corporate Nuclear Quality Assurance Manual (IOM-Q2), which commits to the nuclear industry regulations and standards. Continuing compliance with nuclear quality program requirements during the 2006-2009 period was confirmed by internal and external audits, including customer (NUPIC) and NRC audits that reflected continuing Triconex status as an approved nuclear supplier. QA processes and commitments have remained stable and compliant in the period spanning the development and production release of Tricon V10.5.

Details of individual procedure changes during this period will not be tabulated. However, a change to the Triconex Quality Assurance Program that occurred in 2009 warrants discussion. A restructuring of the QA program document hierarchy was implemented as part of an Invensys management goal to establish consistency in Quality Assurance Programs at the corporate level. Effective August 7, 2009, the Corporate Quality Assurance Manuals IOM-Q1 (ISO 9000) and IOM-Q2 (Invensys Nuclear Quality Assurance Manual) were formally adopted as the Top level QA program documents for Triconex activities. The Triconex QA Manual (QAM) was made redundant by this change and was formally cancelled and superseded by IOM-Q1 and IOM-Q2. Prior to cancellation of the QAM, any significant procedural detail that previously existed in the QAM sections was confirmed to be adequately covered in the following department procedure manuals that implement the Triconex QA program:

- Quality Procedures Manual (QPM)
- Manufacturing Department Manual (MDM)
- Engineering Department Manual (EDM)
- Project Procedures Manual (PPM)

While the document structure underwent a change in 2009, the requirements and process content previously reflected in the QAM remained unchanged. A description and detailed mapping of the Quality System Restructuring Project can be found in the current QPM Manual.

4.3.3.2 Engineering/Software Development Processes

Document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System" reviewed Product Development Processes in the EDM for the entire period from 2001 through 2009 and concluded that no reductions or adverse changes to the previously approved development processes were made. This review encompassed the period of development and release of Tricon V10.5.

4.3.3.3 Conclusion

No changes were made to the Quality Assurance or Development processes that reduced commitments or effectiveness of processes affecting the product upgrade from V10.2.1 to V10.5.

4.4 CONCLUSION

The Tricon V10.5 products and TriStation V4.6.134 Application Software continue to meet EPRI TR 107330 and IEEE requirements for Class 1E service and accurately represent the Tricon Qualification Test results as presented in the V10.2.1 Qualification Summary Report, 9600164-545. Changes made to the Tricon product since V10.2.1 and TriStation 4.1.437 are considered minor and evolutionary and have no adverse effect on qualification program results previously submitted for review.

5.0 INVENSYS PROCESSES AND POLICIES FOR NUCLEAR PRODUCTS

As a supplement to the Tricon Platform description and product qualification information in this Topical Report, a discussion is provided below on Invensys processes and policies as they relate to nuclear safety related activities. Invensys maintains a strong ongoing commitment to consistency with nuclear industry regulations, standards, and NRC guidance in implementation of nuclear product design, manufacture, and nuclear application project delivery.

Invensys commits to maintaining these programs and policies, based on process elements contained in the governing documents referenced below, as part of the Topical Report. Changes to processes that are not consistent with these documents will be evaluated for impact on the SER and need for topical report revision (see section 5.6).

5.1 MAINTENANCE OF QA AND PRODUCT DEVELOPMENT PROCESSES

5.1.1 Quality Assurance Program

At the time of the V9 Triconex Platform SER (December 2001), Triconex was operating under a 10CFR50 Appendix B Quality Assurance Program. The program had been established and approved by nuclear utility audits in early 1998. The V9 Tricon System, with existing legacy hardware and software, was not fully developed under the Appendix B program, as noted in the SER. However, all nuclear related activities, including hardware and software development, since 1998 have been implemented under 10CFR50 Appendix B controls. The Appendix B nuclear QA program has been maintained since the V9 qualification timeframe as evidenced by continued nuclear utility approvals of Invensys Triconex as a nuclear safety-related system supplier. Further discussion of audits by nuclear utilities (including NUPIC audits) and the NRC is found in Invensys document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System," (Reference 2.5.31).

All processes listed in this section are contingent on compliance with the Invensys Nuclear Quality Assurance Manual and documented approval of the program by nuclear customer and NRC audits. Any changes to the Quality Assurance Program status shall be evaluated for impact on the SER and the need for topical report revision (see section 5.6).

5.1.2 Product Development Process

The V9 SER documented the NRC's review of Triconex procedures and process for hardware and software development. The SER concluded that procedures in the Engineering Department Manual (EDM), as part of the Appendix B Quality Assurance Program, were suitable for production of safety related hardware and software, with the caveat that an independent second level V&V review (such as by TÜV) would be required for future software to be considered acceptable.

Triconex development processes continue to be equivalent to (or better than) the processes reviewed as part of the V9 Qualification. Product development processes and software development activities continue to be controlled by procedures found in the Engineering Department Manual (EDM). All changes in engineering procedures since the 2001 timeframe were reviewed for any significant changes that may be construed to be a reduction in the rigor or effectiveness development processes as previously reviewed. No reductions were found. To the contrary, an ongoing improvement in process rigor and procedure completeness is evident. Significant improvements in the quality and formality of the EDM procedures have taken place since the SER was issued for Tricon V9.5.3, but no basic changes (reductions in commitment) were made to the design process. For more details, see further discussion of process changes in Invensys document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System," (Reference 2.5.31).

Invensys intends to assure that, going forward, the basic Triconex Development Process continues to remain stable and consistent with previously approved processes. However, one

aspect of the development process is being changed to reflect the evolution of programmable logic devices (PLDs) such as FPGAs. Historically, Triconex has used relatively simple PLDs in selected Tricon hardware modules and has treated these devices as hardware under its product development and design verification activities. Due to the growth in complexity of these devices, current industry expectation is that PLDs should be treated with a process similar to the software development process rather than the hardware development process, including application of appropriate software standards and techniques. For future nuclear products (developed subsequent to the V10 SER), Triconex will specifically address measures for development of PLDs in a new process distinctively tailored to development of software used in designing and maintaining the PLD. This refinement of process detail is considered to be an improvement. Invensys Triconex document NTX-SER-09-06, "Triconex Development Processes for PLDs in Nuclear Qualified Products," (Reference 2.5.32) provides a thorough discussion of design control processes historically applied to PLDs in Triconex products and describes planned development program changes related to these devices. Process modifications, where indicated, will be incorporated into EDM 12.00 and supporting EDM hardware development procedures.

EDM procedure 12.00, Product Development Process, is the governing procedure defining the Triconex Product Development Process at the system level. This procedure documents the established process flow, product lifecycle phases (hardware and software) and the primary elements of the NRC approved processes, including the requirement for ongoing review by an independent organization. EDM 12.00 is the development process standard and will be maintained as such going forward.

Any changes to the process described in EDM 12.00 (or any supporting procedures that deviate from the requirements of this procedure) shall be evaluated for impact on the SER and the need for topical report revision (see Section 5.6).

5.2 INVENSYS PROJECT INTEGRATION PROCESSES

In addition to designing and producing nuclear qualified digital control systems, Invensys develops and delivers entire application projects for nuclear customers under its Project Integration (Delivery) organization. An application project is defined as any project that incorporates standard Tricon products into a fully operational integrated system in accordance with customer specified requirements.

A summary of the administrative controls for Invensys nuclear and commercial application project activities conducted at the Invensys Irvine CA facility is presented in Invensys document NTX-SER-09-21, "Nuclear System Integration Program Manual," (Reference 2.5.33). A description of the project processes and the basis for implementing project procedures is provided in this document. NTX-SER-09-21 includes a process flowchart of a typical application project implementation.

Project procedures supporting the Nuclear System Integration Program Manual (NSIPM) govern all quality-affecting Project activities performed by personnel at the Irvine facility. The

NSIPM implements the requirements of the Invensys Nuclear Quality Assurance Manual, 10CFR50 Appendix B, NQA-1, and applicable Regulatory Guides and industry Standards. Specific standards associated with software activities include, but are not limited to Regulatory Guide 1.168 and IEEE Standards 830 and 1012. The NSIPM may also be used by other Invensys facilities.

The Irvine facility project procedures represented by the NSIPM and their implementation have been audited and deemed to be satisfactory by several outside organizations including nuclear customers, NUPIC, and the Quality & Vendor Branch of the NRC Office of New Reactors (See Inspection Report identified as ADAMS Accession # ML082460540).

The Project Integration Process for all safety related application projects will be implemented utilizing procedures consistent with NTX-SER-09-21 and as audited/approved by nuclear customers.

Any significant changes to the process described in this document (or procedures deviating from the requirements of this document) shall be evaluated for impact on the SER and need for topical report revision (see Section 5.6).

5.3 SECURITY

The increasing use of computers for various functions at nuclear facilities brings forth new technical challenges that must be addressed in a rigorous and balanced manner. Digital computers in nuclear facilities are used in safety-related and non-safety systems, where non-availability or malfunction could affect nuclear safety and continuity of power. Computers are also used to store important and sensitive data, where malfunction could lead to the loss or unavailability of data. As the complexity of these computer systems increases, comprehensive methods to assure computer system dependability and reliability need to be employed.

As a supplier of digital control systems for safety related applications in nuclear facilities, Invensys is committed to implementing a Program to mitigate relevant security risks during the applicable life cycle phases of the digital computer systems. Invensys Licensing Topical Report 7286-545-2, "Invensys Security Program Plan," (Reference 2.5.34), describes the Invensys security program, including Wurldtech certification, designed to be consistent with the policy and guidance provided by United States NRC Regulatory Guide 1.152 and NRC guidance for security matters found in DI&C-ISG-01. This program will be implemented using approved Invensys procedures that are consistent with the requirements of this document.

Any significant changes to the process described in this document (or procedures deviating from the requirements of this document) shall be evaluated for impact on the SER and need for topical report revision (see Section 5.6).

5.4 DIVERSITY AND DEFENSE-IN-DEPTH ISSUES (ISG-02)

The Invensys position and application philosophy in regard to NRC Interim Staff Guidance ISG-02 and related regulatory standards and guidance is described in Invensys Document NTX-SER-09-10, "Tricon Applications in Nuclear Reactor Protection Systems – Compliance with NRC ISG-2 and ISG-4," (Reference 2.5.35).

The philosophy of Diversity and Defense-in-Depth (D3) analysis is a multi-layered approach to safe facility operation. It includes multiple physical boundaries between the fuel and environment, redundant paths and equipment to provide core cooling, and qualified control and monitoring systems for safe shutdown and long term cooling of the reactor, as defined in Nuclear Regulatory Commission BTP-7-19 (Reference 3), with additional details and clarifications provided in ISG-02.

Document NTX-SER-09-10 describes how Invensys develops and applies Tricon safety related systems nuclear facilities in the USA, in accordance with NRC regulations and guidelines. It is intended to be generic in the application of Tricons in safety-related applications. It does not include site specific acceptance, pre-operation, or surveillance testing requirements. It also does not include site-specific life cycle hardware and software configuration management, or quality assurance activities following installation. These topics are addressed in site-specific submittals.

In Section 1.0 of the document, a typical example illustrates the flexibility and many of the features of Tricons configured for RPS and/or ESFAS applications. While not proposed for any specific facility architecture, the example is presented for discussion purposes of how Tricons may be applied in reactor protection applications in compliance with regulatory requirements and to industry standards.

Section 2.0 of the document provides a matrix with a detailed tabulation of ISG-2 "Diversity and Defense-in-Depth Issues." This section compares NRC ISG-2 position and Invensys compliance and comments in a point-by-point matrix.

As the document is a generic guide for use in customer-specific applications, no specific Invensys hardware or system is being licensed. However, any changes made to this Invensys policy document with respect to Diversity and Defense-in-Depth will be evaluated for impact on the SER and need for topical report revision (see section 5.6).

5.5 HIGHLY INTEGRATED CONTROL ROOMS – COMMUNICATION ISSUES (ISG-4)

The Invensys position and application philosophy in regard to NRC Interim Staff Guidance ISG-04 and related regulatory standards and guidance is described in Invensys Document NTX-

SER-09-10, "Tricon Applications in Nuclear Reactor Protection Systems – Compliance with NRC ISG-2 and ISG-4," (Reference 2.5.35).

Document NTX-SER-09-10 describes how Invensys develops and applies the Tricon systems to safety-related systems in nuclear facilities in the USA in accordance with NRC regulations and guidelines. It is intended to be generic in the application of Tricon controllers in safety-related applications. It does not include site specific acceptance, pre-operation, or surveillance testing requirements. It also does not include site-specific life cycle hardware and software configuration management, or quality assurance activities following installation. These topics are addressed in site-specific submittals.

In Section 1.0 of the document, a typical example illustrates the flexibility and many of the features of Tricon controllers configured for RPS and/or ESFAS applications. While not proposed for any specific facility architecture, the example is presented for discussion purposes of how Tricon controllers may be applied in reactor protection applications in compliance with regulatory requirements and to industry standards.

Section 3.0 of the document provides a matrix with a detailed tabulation of ISG-4 "Highly Integrated Control Rooms – Communications Issues." This section compares NRC ISG-4 positions and Invensys compliance and comments in a point-by-point matrix. Each of the Staff Positions for Interdivisional Communication, Command Prioritization, and Multidivisional Control and Display Stations is tabulated and addressed. Appendix 1 of the document addresses the Tricon system relative to Staff Positions on Non-Safety to Safety Communications.

As this document is a generic guide for use in customer-specific applications, no specific Invensys hardware or system is being licensed. However, any changes made to this Invensys policy document with respect to Communication Issues will be evaluated for impact on the SER and need for topical report revision (see Section 5.6).

5.6 INVENSYS TRICONEX TOPICAL REPORT/SER MAINTENANCE PROCESS

Invensys has established a process for ongoing maintenance of the Triconex system Topical Report (7286-545-1-A), including measures to assure nuclear licensees that the Tricon Platform provided for their application is always within the boundaries of the current US Nuclear Regulatory Commission's Safety Evaluation Report (SER).

Triconex procedures include standard measures for evaluation of evolutionary upgrades and general product maintenance to maintain nuclear qualification status (change impact analysis). New or upgraded equipment is added to the Nuclear Qualified Equipment List (NQEL), as necessary, provided it has been evaluated or undergone further testing in accordance with applicable Engineering Department procedures. Similarly, new or upgraded software for the Triconex platform is added to the NQEL in accordance with the evaluation process defined in the Engineering Department procedures.

The V9 SER permitted licensees to take credit for the NRC approval of the equipment only as listed in the SER. Therefore, the burden of licensing subsequent Tricon system upgrades fell to the licensees as part of the site-specific application licensing process. The SER Maintenance Process changes that. An additional review process is being added to Triconex procedures to further evaluate platform changes that could impact the basis of the existing NRC SER. The intent of this expanded evaluation process is to identify any safety issues related to platform or quality program changes that have not been reviewed by the NRC (similar to a 10CFR50.59 evaluation). This documented evaluation uses a checklist and a set of criteria for identifying significant platform or program changes relative to their impact on the SER.

To the extent that product or process changes are confirmed to be within the established criteria, the Triconex platform will be considered consistent and current with the latest SER/Topical Report and marketed as such. Where the SER Impact Review identifies unreviewed safety issues, i.e., issues considered to be outside the basic elements credited in the SER, the process will assure NRC review and approval of the changes by Topical Report revision. Similar to a 10CFR50.59 process, summary reports on Triconex SER impact reviews will be provided to the NRC on a 24 month basis.

This SER Maintenance Process will permit licensees to consider all current Triconex products pre-approved by the NRC, potentially eliminating any further NRC platform reviews other than the facility-specific aspects of the application project.

38The Invensys SER Maintenance Process is described in more detail in Invensys document NTX-SER-09-20, "Safety Evaluation Report (SER) Maintenance Process," (Reference 2.5.36).

Any significant changes to the process described in this document (or procedures deviating from the requirements of this document) shall be evaluated for impact on the SER and need for TR revision as discussed above.

invensys
Operations Management

TRICON TOPICAL REPORT

EPRI TR-107330 REQUIREMENTS COMPLIANCE AND TRACEABILITY MATRIX

Document No.: 7286-545-1

Revision 2

Appendix A

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
1	Scope. Description of TR scope.	---	No requirements.
2	Definitions, Abbreviations, Acronyms. List of definitions, abbreviations, and acronyms used in the TR.	---	No requirements.
3	Reference Documents. List of documents referenced in the TR.	---	No requirements.
4	System Requirements. (section heading)	---	No requirements.
4.1	Overview of Performance Basis. Descriptive information.	---	No requirements.
4.2	Functional Requirements. (section heading)	---	No requirements.
4.2.1	General Functional Requirements. Descriptive information.	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.2.1.A	Response Time. The overall response time from an analog or discrete input exceeding its trip condition to the resulting discrete outputs being set shall be 100 milliseconds or less. Response time shall include time required for input filtering, input module signal conversion, main processor input data acquisition, two scan times of an application program containing 2000 simple logic elements, main processor output data transmission, digital output module signal conversion, and performance of self-diagnostics and redundancy implementation.	Comply	Ref 7, Section 4.0 gives a summary of calculated maximum response time. However, the as tested Maximum response times were 83.0 milliseconds (for a DI to DO loop), 119.0 milliseconds (for an AI to DO loop), and 126.0 milliseconds (for an AI to AO loop). See Ref. 53, Section 6. The test specimen application program included 3946 simple logic elements, and 175 simple and complex logic elements, almost twice that required by the TR. This effectively resulted in almost double the scan time associated with 2000 elements.
4.2.1.B	Discrete I/O. The PLC shall have the capability to provide a total of at least 400 discrete I/O points.	Comply	See Ref. 45, Chapter 3, Table 62
4.2.1.C	Analog I/O. The PLC shall have the capability to provide a total of 100 analog I/O points.	Comply	See Ref. 45, Chapter 3, Table 62
4.2.1.D	Combined I/O. The PLC shall have the capability to provide a total of 50 analog and 400 discrete I/O points.	Comply	See Ref. 45, Chapter 3, Table 62
4.2.2	Control Function Requirements. The PLC shall provide a high -level language designed for control algorithms.	Comply	See Ref. 46 and 47.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.2.3	Availability/Reliability and FMEA. (section heading)	- - -	No requirements.
4.2.3.1	Availability/Reliability Overview. Descriptive information.	- - -	No requirements.
4.2.3.2	Availability/Reliability and Basic Requirements. The overall availability goal of the PLC is 0.99.	Comply	See Ref. 11.
4.2.3.3	Availability/Reliability Calculation Requirements. An availability calculation shall be prepared which conforms to IEEE 352.	Comply	See Ref. 11.
4.2.3.3.1	Availability/Reliability Calculation Requirements Applicable to Redundant PLCs. For PLCs that include redundancy, the availability calculation shall address additional, redundancy-specific considerations.	Comply	See Ref. 11.
4.2.3.4	PLC Fault Tolerance Requirements. Fault tolerance capability shall be addressed in the availability calculation, and included as part of the qualification envelope definition.	Comply	See Ref. 11 and Appendix B of this report.
4.2.3.5	Failure State/FMEA Requirements. An FMEA analysis shall be performed in accordance with IEEE 352. The analysis shall evaluate the effects of failures of components in the PLC modules on the PLC performance.	Comply	See Ref. 10.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.2.3.6	Failure Detection Requirements. The PLC shall contain features to permit generating an alarm when the on-line fault detection detects a failure. Processor-to-processor communication for fault detection shall meet the given specific performance requirements.	Comply	See Ref. 45, Chapter 4, Table 74 to Table 86 and Ref. 10. The Tricon does not require loopback of output to input signals for fault detection.
4.2.3.7	Recovery Capability Requirements. The PLC shall include a watchdog timer and power bus monitoring features. Output modules shall initialize to a known state.	Comply	See Ref. 20, Sections 8.0 and 10.0.
4.2.3.8	Requirements for Use of Operating Experience. If operating experience is used as a basis for establishing module failure rates, the PLC manufacturer must have a problem reporting and tracking program.	Comply	See Table Section 7.8 for reference to manufacturer Problem Reporting and Tracking Program procedures.
4.2.4	Setpoint Analysis Support Requirements. An analysis shall be prepared to provide the information needed to support an application specific set point analysis per ISA RP 67.04.	Comply	See Ref. 9.
4.3	Hardware Requirements. (section heading)	---	No requirements.
4.3.1	General. (section heading)	---	No requirements.
4.3.1.1	Background. Descriptive information.	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.1.2	Requirements Common to All Modules. All modules shall meet or support the general requirements given in Section 4.2.1, and shall meet the range of environmental conditions given in Section 4.3.6. Special requirements apply to single module assemblies that include both inputs and outputs.	Comply	See Table Sections 4.2.1 and 4.3.6. No Tricon modules include Input and Output points on the same assembly.
4.3.1.3	External Device Requirements. External devices used to meet I/O module requirements shall meet the given specific requirements.	Comply	Qualification testing did not include use of external devices.
4.3.1.4	General Redundancy Requirements. Redundant components may be included in the generic PLC platform.	Comply	Tricon test specimen included redundant main processors and chassis power supplies.
4.3.2	Input Requirements. (section heading)	- - -	No requirements.
4.3.2.1	Analog Input Requirements. The PLC shall include modules that provide analog inputs.	Comply	See Ref. 45, Chapter 2.0. See Ref. 56 for list of Tricon analog input modules included in the qualification program.
4.3.2.1.A	Monotonicity. The analog inputs shall be monotonic to ±1/2 LSB.	Comply	The DACs used by Triconex are monotonic by design.
4.3.2.1.B	Number of Channels. Each analog input module shall provide a minimum of four input channels.	Comply	See Ref. 45, Chapter 2.0.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.C	Over Range. The converted value of each analog input module shall remain at its maximum value for over range inputs up to twice rated.	Comply	See Ref. 45, Chapter 2.0. Analog input module A/D converters remain at their maximum value regardless of the input value once the input is ≥ the specified over range value.
4.3.2.1.D	Under Range. The converted value of each analog input module shall remain at its minimum value for low range inputs up to the negative of the rated input value.	Comply	See Ref. 45, Chapter 2.0. Analog input module A/D converters remain at their minimum value regardless of the input value once the input is ≤ the specified under range value.
4.3.2.1.E	Out of Range Indication. Over and under range conditions shall be indicated in a manner available to the application program.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.1	Voltage Input Requirements. (section heading)	- - -	No requirements.
4.3.2.1.1.A	Analog Voltage Input Module Ranges. The PLC shall include analog voltage input modules with ranges of: 0 to 10 VDC, -10 to 10 VDC, and 0 to 5 VDC.	Partial Exception	See Ref. 45, Chapter 2.0. Tricon analog voltage input modules do not include a –10 to 10 VDC range.
4.3.2.1.1.B	Analog Voltage Input Module Accuracies. Overall accuracies shall be ≤ ± 0.32% of the specified range.	Comply	See Ref. 45, Chapter 2.0, and Ref. 9.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.1.C	Analog Voltage Input Module Resolution. The minimum resolution shall be 12 bits.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.1.D	Analog Voltage Input Module Common Mode Voltage. The common mode voltage capability shall be at least 10 volts with a common mode rejection ratio of at least 90 dB.	Partial Exception	See Ref. 45, Chapter 2.0. Common mode rejection rating of Module 3701 is 80 dB, Module 3721 is 85dB, and Module 3703 is 90dB.
4.3.2.1.1.E	Analog Voltage Input Module Response Time. The overall response time of the analog voltage input modules must support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3.0 and Table Section 4.2.1.A.
4.3.2.1.1.F	Analog Voltage Input Module Group-to-Group Isolation. The group-to-group isolation shall be at least ± 30 volts peak.	N/A	See Ref. 45, Chapter 2.0. Tricon analog voltage input module points are not grouped.
4.3.2.1.1.G	Analog Voltage Input Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	Analog input modules are not intended for use as a Class 1E to Non-1E isolation device.
4.3.2.1.1.H	Analog Voltage Input Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.1.I	Analog Voltage Input Module Input Impedance. The input impedance shall be at least 1 megohm.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.2	Current Input Requirements. (section heading)	- - -	No requirements.
4.3.2.1.1.A	Analog Current Input Module Ranges. The PLC shall include analog current input modules with ranges of: 4 to 20 mA and 10 to 50 mA or 0 to 50 mA.	Partial Exception	See Ref. 45, Chapter 2.0. Tricon analog current input modules do not include a 10 to 50 mA or 0 to 50 mA range.
4.3.2.1.1.B	Analog Current Input Module Accuracies. Overall accuracies shall be $\leq \pm$ 0.35% of the specified range.	Comply	See Ref. 45, Chapter 2.0, and Ref. 9.
4.3.2.1.1.C	Analog Current Input Module Resolution. The minimum resolution shall be 12 bits.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.1.D	Analog Current Input Module Common Mode Voltage. The common mode voltage capability shall be at least 10 volts.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.1.E	Analog Current Input Module Common Mode Rejection Ratio. The common mode rejection ratio shall be at least 90 dB.	Partial Exception	See Ref. 45, Chapter 2.0. Common mode rejection rating of Module 3701 is 80 dB, Module 3721 is 85dB, and Module 3703 is 90dB..

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.1.F	Analog Current Input Module Response Time. The overall response time of the analog current input modules must support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 2.0 and Table Section 4.2.1.A.
4.3.2.1.1.G	Analog Current Input Module Group-to-Group Isolation. The group-to-group isolation shall be at least ± 30 volts peak for 4 to 20 mA inputs.	N/A	See Ref. 45, Chapter 2.0. Tricon analog current input module points are not grouped.
4.3.2.1.1.H	Analog Current Input Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	Analog input modules are not intended for use as a Class 1E to Non-1E isolation device.
4.3.2.1.1.I	Analog Current Input Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and Ref. 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.2.1.1.J	Analog Current Input Module Input Impedance. The input impedance shall be 250 ohms maximum.	Comply	See Ref. 48, Chapter 7.0. 0 to 5 VDC analog voltage input modules are used for 4 to 20 mA current inputs with a 250 ohm resistor supplied by Triconex.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.3	RTD Input Requirements. (section heading)	- - -	No requirements.
4.3.2.1.3.A	RTD Input Module Types. The PLC shall include RTD input modules for use with 2, 3 or 4 wire European (DIN 43 760) or US standard 100 ohm RTDs.	Partial Exception	See Ref. 48, Chapter 5, Table 135. Tricon RTD input signal conditioners are for use with 2 or 3 wire, 100 ohm platinum RTDs.
4.3.2.1.3.B	RTD Input Module Ranges. The PLC shall include RTD input modules with a range of at least 0 to 800°C (32 to 1472°F).	Exception	See Ref. 48, Chapter 5, Table 135. Tricon RTD input signal conditioners span the -100°C to 600°C (32 to 1112°F) range.
4.3.2.1.3.C	RTD Input Module Accuracies. Overall accuracies shall be ≤ ± 2°C.	Comply	See Ref. 45, Chapter 2.0 and Ref. 9. Tricon RTD input signal conditioners are interfaced with a 0 to 5 VDC analog input module. Combined accuracy is ≤ ± 2°C.
4.3.2.1.3.D	RTD Input Module Resolution. The minimum resolution shall be 0.1° or less for both °C or °F scaling.	Exception	See Ref. 45, Chapter 2.0, and Ref. 9. Tricon RTD input signal conditioners (32 to 1112°F max. span = 1 to 5 V output) are interfaced with a 12 bit, 0 to 5 V analog input module. The resulting minimum resolution is 0.33°F (0.19°C).

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.3.E	RTD Input Module Common Mode Voltage. The common mode voltage capability shall be at least 10 volts.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.3.F	RTD Input Module Common Mode Rejection Ratio. The common mode rejection ratio shall be at least 90 dB.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.3.G	RTD Input Module Response Time. The overall response time of the RTD input modules must support the response time requirement given in Section 4.2.1.A.	Exception	See Ref. 20, Section 3.0 and Table Section 4.2.1.A. For large step changes (0 to 90% of full scale range), RTD's and input signal conditioners have a relatively long input update rate, and were not considered in qualification response time testing.
4.3.2.1.3.H	RTD Input Module Group-to-Group Isolation. The group-to-group isolation shall be at least ± 30 volts peak.	N/A	See Ref. 48, Chapter 5. Tricon RTD input signal conditioner points are not grouped.
4.3.2.1.3.I	RTD Input Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	RTD input signal conditioners are not intended for use as a Class 1E to Non-1E isolation device.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.3.J	RTD Input Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.2.1.3.K	RTD Input Module Input Impedance. The input impedance shall be 1 megohm minimum.	Comply	The Analog Devices signal conditioner has a two-pole output filter and subsequent buffer to ensure that a low noise, low impedance (<1Ω) signal is available at the output to drive loads to 2 kΩ minimum (Ref. 55). Input impedance of RTD signal conditioning modules is not relevant. Modules are compatible with specific RTD types via the Analog Devices signal conditioners.
4.3.2.1.4	Thermocouple Input Requirements. Thermocouple (T/C) input modules must meet performance requirements with 1000 feet of 20 AWG extension wire connected to input.	Comply	Comparison of the input impedance to load impedance indicates there is no effective maximum limit.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.4.A	T/C Input Module Types. The PLC shall include T/C input modules for use with type B, E, J, K, N, R, S and T thermocouples over the specified temperature ranges.	Partial Exception	See Ref. 45, Chapter 2.0. Tricon T/C input modules are for use with type E, J, K and T thermocouples. Type J input range is –250 to 2000°F (vs. TR requirement of 32 to 2192°F).
4.3.2.1.4.B	T/C Input Module Accuracies. Overall accuracies shall be: Type E: ≤ ± 4.5°F, Type J: ≤ ± 6.3°F, Type K: ≤ ± 7.2°F, Type T: ≤ ± 4.5°F.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.4.C	T/C Input Module Accuracies. Cold junction compensation shall support Section 4.3.2.1.4.B accuracies for the environmental temperature range given in Section 4.3.6.	Comply	See Ref. 45, Chapter 2.0, for T/C termination module (cold junction) temperature in range of 32 to 140°F, and over TR temperature ranges for each T/C type.
4.3.2.1.4.D	T/C Input Module Resolution. The minimum resolution shall be 0.1° or less for both °C or °F scaling.	Exception	See Ref. 45, Chapter 2.0, minimum resolution is 0.125°F (0.07°C).
4.3.2.1.4.E	T/C Input Module Common Mode Voltage. The common mode voltage capability shall be at least 10 volts.	Comply	See Ref. 45, Chapter 2.0.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.4.F	T/C Input Module Common Mode Rejection Ratio. The common mode rejection ratio shall be at least 90 dB.	Comply	See Ref. 45, Chapter 2.0. T/C input module Model 3708E common mode rejection ratio is 90 dB (0 to 60 Hz) minimum.
4.3.2.1.4.G	T/C Input Module Open Detection. The module shall provide open thermocouple detection.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.1.4.H	T/C Input Module Response Time. The overall response time of the T/C input modules must support the response time requirement given in Section 4.2.1.A.	Clarification	The input response time is the same as the analog input module 3708; they both use the same PCBA. This module was successfully tested during the SER testing and there have not been any design changes.
4.3.2.1.4.I	T/C Input Module Group-to-Group Isolation. The group-to-group isolation shall be at least ± 30 volts peak.	N/A	See Ref. 45, Chapter 2.0. Tricon T/C input module points are not grouped.
4.3.2.1.4.J	T/C Input Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	T/C input modules are not intended for use as a Class 1E to Non-1E isolation device.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.4.K	T/C Input Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.2.1.4.L	T/C Input Module Input Impedance. The input impedance shall be 1 megohm minimum.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.2	Discrete Input Requirements. The PLC shall include modules that provide discrete inputs. Each module shall provide a minimum of 8 input channels and include indicators that show the ON/OFF status of each point.	Comply	See Ref. 45, Chapter 2.0. See Ref. 3 for list of Tricon discrete input modules included in the qualification program.
4.3.2.2.1	Discrete AC Input Requirements. (section heading)	- - -	No requirements.
4.3.2.2.1.A	Discrete AC Input Module Types. The PLC shall include discrete AC input modules for nominal inputs of 120 VAC and 24 VAC.	Comply	See Ref. 45, Chapter 2.
4.3.2.2.1.B	Discrete AC Input Module ON Transition. The input must transition to ON at 90 VAC max. (120 VAC input) or 20 VAC max. (24 VAC input).	Comply	See Ref. 45, Chapter 2.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.2.1.C	Discrete AC Input Module OFF Transition. The input must transition to OFF between 65 to 25 VAC (120 VAC input) or 15 to 6 VAC (24 VAC input).	Comply	See Ref. 45, Chapter 2.
4.3.2.2.1.D	Discrete AC Input Module Operating Range. The module must operate for inputs up to at least 150 VAC (120 VAC input) or 40 VAC (24 VAC input).	Comply	See Ref. 45, Chapter 2.
4.3.2.2.1.E	Discrete AC Input Module Response Time. The overall response time of the discrete AC input modules must support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3.0 and Table Section 4.2.1.A.
4.3.2.2.1.F	Discrete AC Input Module Group-to-Group Isolation. The group-to-group isolation shall be at least 600 volts peak for 120 VAC inputs or 100 volts peak for 24 VAC inputs.	Comply	The Triconex design utilizes point to point and ETP isolation at 1500Vac (Ref. 45)
4.3.2.2.1.G	Discrete AC Input Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	Discrete AC input modules are not intended for use as a Class 1E to Non-1E isolation device.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.2.1.H	Discrete AC Input Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.2.2.2	Discrete DC Input Requirements. (section heading)	- - -	No requirements.
4.3.2.2.2.A	Discrete DC Input Module Types. The PLC shall include discrete DC input modules for nominal inputs of 125, 24 , 15 and 12 Vdec.	Partial Exception	See Ref. 45, Chapter 2.0. Tricon discrete DC input modules are for nominal inputs of 115, 48 and 24 Vdc.
4.3.2.2.2.B	Discrete DC Input Module ON Transition. The input must transition to ON at 90 VDC max. (125 VDC input) or 20 VDC max. (24 VDC input).	Comply	See Ref. 45, Chapter 2.0.
4.3.2.2.2.C	Discrete DC Input Module OFF Transition. The input must transition to OFF between 65 to 25 VDC (125 VDC input) or 15 to 6 VDC (24 VDC input).	Comply	See Ref. 45, Chapter 2.0.
4.3.2.2.2.D	Discrete DC Input Module Operating Range. The module must operate for inputs up to at least 150 VDC (125 VDC input) or 40 VDC (24 VDC input).	Comply	See Ref. 45, Chapter 2.0.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.2.2.E	Discrete DC Input Module Response Time. The overall response time of the discrete DC input modules must support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3.0 and Table Section 4.2.1.A.
4.3.2.2.2.F	Discrete DC Input Module Group-to-Group Isolation. The group-to-group isolation shall be at least 600 volts peak for 125 VDC inputs or 40 volts peak for 24 VDC inputs.	Comply	The 120 Vdc DI module is the same as the 115 Vac module. They are commen in groups of 8 because of "stuck-on" diagnostics.
4.3.2.2.2.G	Discrete DC Input Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	Discrete DC input modules are not intended for use as a Class 1E to Non-1E isolation device.
4.3.2.2.2.H	Discrete DC Input Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.2.2.3	TTL Input Requirements. Requirements for TTL level input modules.	Exception	There is no TTL level input module available for use with the Tricon PLC.
4.3.2.3	Other Inputs. (section heading)	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.3.1	Pulse Input Requirements. The PLC shall include modules that provide pulse inputs.	Comply	See Ref. 45, Chapter 2.0. See Ref. 9 for identification of Tricon pulse input module included in the qualification program.
4.3.2.3.1.A	Pulse Input Module Input Number. The module shall have at least two inputs.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.3.1.B	Pulse Input Module Range. The module input count frequency range shall be at least 20 to 5000 Hz.	Comply	See Ref. 45, Chapter 2.0.
4.3.2.3.1.C	Pulse Input Module Operation. The input must operate for a pulse range of at least 3 to 28 VDC and a duty cycle of at least 20 microseconds at 90%.	Comply	The PI Module clocks on a falling edge and does not care about duty cycle.
4.3.2.3.1.D	Pulse Input Module Count Accuracy. The module shall have up and down count modes with a range of at least 9999. The accuracy of the count shall be ≤ 0.1%.	Exception	See Ref. 45, Chapter 2.0. The Tricon pulse input module provides speed or RPM measurement only.
4.3.2.3.1.E	Pulse Input Module Frequency Accuracy. The module shall have a frequency mode with a range of at least 20 to 5000 Hz. The accuracy of the frequency measurement shall be ≤ 0.1%.	Partial Exception	See Ref. 45, Chapter 2.0. Accuracy is ± 1.0% of reading from 20 to 99 Hz. Accuracy is ± 0.1% of reading from 100 to 999 Hz. Accuracy is ±0.01% from 1000 to 20,000 Hz

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.3.1.F	Pulse Input Module Response Time. The overall response time of the pulse input module must support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3.0. Pulse Input Modules were not used for Response Time Analyses. Module selection was based on update rates; the selection of digital and analog output modules to include in the test is not significant.
4.3.2.3.1.G	Pulse Input Module Group-to-Group Isolation. The group-to-group isolation shall be at least 40 VDC.	N/A	See Ref. 45, Chapter 2.0. Tricon pulse input module points are not grouped.
4.3.2.3.1.H	Pulse Input Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	Pulse input modules are not intended for use as a Class 1E to Non-1E isolation device.
4.3.2.3.1.I	Pulse Input Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.3	Output Requirements. (section heading)	- - -	No requirements.
4.3.3.1	Analog Output Requirements. The PLC shall include modules that provide analog outputs.	Comply	See Ref. 45, Chapter 2. See Ref. 3 for identification of Tricon analog output module included in the qualification program.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.1.A	Monotonicity. The analog outputs shall be monotonic to ±1/2 LSB.	Comply	The DACs used by Triconex are monotonic by design.
4.3.3.1.B	Number of Channels. Each analog output module shall provide a minimum of four output channels.	Comply	See Ref. 45, Chapter 2.0.
4.3.3.1.1	Analog Voltage Output Requirements. Requirements for analog voltage output modules.	Exception	There is no analog voltage output module available for use with the Tricon PLC.
4.3.3.1.2	Current Output Requirements. (section heading)	- - -	No requirements.
4.3.3.1.2.A	Analog Current Output Module Ranges. The PLC shall include analog current output modules with ranges of: 4 to 20 mA or 0 to 20 mA, and 10 to 50 mA or 0 to 50 mA.	Partial Exception	See Ref. 45, Chapter 2.0. Tricon analog current output module output range is 4 to 20 mA.
4.3.3.1.2.B	Analog Current Output Module Accuracy. Overall accuracy shall be ≤ ± 0.32% of full range.	Comply	See Ref. 45, Chapter 2.0, and Ref. 9.
4.3.3.1.2.C	Analog Current Output Module Resolution. The minimum resolution shall be 12 bits.	Comply	See Ref. 45, Chapter 2.0.
4.3.3.1.2.D	Analog Current Output Module Load Impedance. The 4 to 20 mA outputs shall support a load impedance of 1 Kohm or less.	Comply	See Ref. 45, Chapter 2.0.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.1.2.E	Analog Current Output Module Response Time. The overall response time of the analog current output modules must support the response time requirement given in Section 4.2.1.A.	Comply	Section 4.2.1.A bases response time on AI to DO or DI to DO configurations. Analog outputs are not addressed.
4.3.3.1.2.F	Analog Current Output Module Isolation. The group-to-group, module-to-module and module to backplane isolation shall meet the requirements of Section 4.6.4.	N/A	Section 4.6.4 provides requirements for Class 1E to Non-1E isolation capability. Tricon analog current output modules are not intended for use as a Class 1E to Non-1E isolation device.
4.3.3.1.2.G	Analog Current Output Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.3.2	Discrete Output Requirements. The PLC shall include modules that provide discrete outputs.	Comply	See Ref. 45, Chapter 2.0. See Ref. 9 for list of Tricon discrete output modules included in the qualification program.
4.3.3.2.A	Number of Channels. Each module shall provide a minimum of 8 output channels.	Comply	See Ref. 45, Chapter 2.0.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.2.B	Leakage Current. Leakage current in the OFF state of non-supervised (no internal ringback) modules shall be less than 80% of the minimum current needed to turn ON any digital input module.	Comply	See Ref. 45, Section 2.0. Minimum digital input module turn ON current is 3 mA. Maximum non-supervised digital output module leakage current is 2 mA which is < 0.8 x 3 mA.
4.3.3.2.C	Output Circuit Interrupter. Outputs must include a circuit interrupter.	Comply	See Ref. 48, Chapter 4.
4.3.3.2.D	Status Indication. Modules must include indicators that show the ON/OFF status of each point.	Comply	See Ref. 45, Chapter 2.0.
4.3.3.2.1	Discrete AC Output Requirements. (section heading)	- - -	No requirements.
4.3.3.2.1.A	Discrete AC Output Module Types. The PLC shall include discrete AC output modules for nominal outputs of 120 and 24 Vac.	Partial Exception	See Ref. 45, Chapter 2.0. Tricon discrete AC output modules do not include 24 Vac nominal outputs.
4.3.3.2.1.B	Discrete AC Output Module Output Current. The output must operate with an output current between 50 mA and 0.5 amps with an inrush capability of at least 2 amps.	Comply	See Ref. 45, Chapter 2.0
4.3.3.2.1.C	Discrete AC Output Module ON State Voltage Drop. The ON state voltage drop shall not exceed 2 VAC at 0.5 amps.	Comply	See Ref. 45, Chapter 2.0, Table 31.
4.3.3.2.1.D	Discrete AC Output Module OFF State Leakage. The OFF state leakage current shall not exceed 2 mA.	Comply	See Ref. 45, Chapter 2.0. Based on load leakage specifications.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.2.1.E	Discrete AC Output Module Operating Range. The modules must operate for point source inputs at 47 Hz to 63 Hz over the range 90 to 130 VAC min. (120 VAC output).	Comply	See Ref. 45, Chapter 2.0
4.3.3.2.1.F	Discrete AC Output Module Response Time. The overall response time of the discrete AC output modules must support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3.0 and Table Section 4.2.1.A.
4.3.3.2.1.G	Discrete AC Output Module Group-to-Group Isolation. The group-to-group isolation shall be at least 600 volts peak for 120 VAC outputs.	N/A	See Ref. 45, Chapter 2.0. Tricon discrete AC output module points are not grouped.
4.3.3.2.1.H	Discrete AC Output Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	Discrete AC output modules are not intended for use as a Class 1E to Non-1E isolation device.
4.3.3.2.1.I	Discrete AC Output Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.3.2.2	Discrete DC Output Requirements. (section heading)	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.2.2.A	Discrete DC Output Module Types. The PLC shall include discrete DC output modules for nominal outputs of 125, 48, 24, 15 and 12 Vdc.	Partial Exception	See Ref. 45, Chapter 2.0. Tricon discrete DC output modules include 120, 48 and 24 Vdc nominal outputs.
4.3.3.2.2.B	Discrete DC Output Module Output Current. The outputs must operate with an output current between 50 mA and 0.5 amps with an inrush capability of at least 2 amps.	Comply	See Ref. 45, Chapter 2.0.
4.3.3.2.2.C	Discrete DC Output Module ON State Voltage Drop. The ON state voltage drop shall not exceed 2 Vdc at 0.5 amps.	Exception	See Ref. 45, Chapter 2.0. Module Model 3607E ON state voltage drop is < 3 V.
4.3.3.2.2.D	Discrete DC Output Module OFF State Leakage. The OFF state leakage current shall not exceed 2 mA.	Exception	See Ref. 45, Chapter 2.0. Module Models 3625 OFF state load leakage is 4 mA maximum.
4.3.3.2.2.E	Discrete DC Output Module Operating Range. The module points must operate for source inputs of 90 to 140 Vdc min. (125 Vdc output), 35 to 60 VDC min. (48 Vdc output), and 20 to 28 Vdc min. (24 Vdc output).	Exception	See Ref. 45, Section 2.0. Module Model 3607E (48 Vdc output) operates from 44 to 80 Vdc. Module Model 3625 (24 Vdc output) operates from 22 to 45 Vdc.
4.3.3.2.2.F	Discrete DC Output Module Response Time. The overall response time of the discrete DC output modules must support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3.0 and Table Section 4.2.1.A.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.2.2.G	Discrete DC Output Module Group-to-Group Isolation. The group-to-group isolation shall be at least twice nominal output.	N/A	See Ref. 45, Chapter 2.0. Tricon discrete DC output module points are not grouped.
4.3.3.2.2.H	Discrete DC Output Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	Discrete DC output modules are not intended for use as a Class 1E to Non-1E isolation device.
4.3.3.2.2.I	Discrete DC Output Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.3.2.3	Relay Output Requirements. (section heading)	- - -	No requirements.
4.3.3.2.3.A	Relay Output Module Types. The PLC shall include relay output modules that provide normally open and normally closed contacts.	Partial Exception	See Ref. 45, Chapter 2.0. Tricon relay output module contacts are normally open.
4.3.3.2.3.B	Relay Output Module Output Current. The continuous current carrying capacity must be at least 2 amps with make and break switching capability of at least 750 VA for AC and 150 watts for DC.	Comply	See Ref. 45, Chapter 2.0

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.2.3.C	Relay Output Module Contact Resistance. The contact resistance shall not exceed 2 ohms.	Comply	Per the vendor published catalog information, the contacts have a maximum resistance of 30 milli-ohms.
4.3.3.2.3.D	Relay Module Operating Range. The contacts must operate from a source of up to 30 VDC or 150 VAC.	Comply	See Ref. 45, Chapter 2.0
4.3.3.2.3.E	Relay Output Module Response Time. The overall response time of the relay output module must support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3.0 and Table Section 4.2.1.A.
4.3.3.2.3.F	Relay Output Module Group-to-Group Isolation. The group-to-group isolation shall be at least 600 volts peak.	N/A	See Ref. 45, Section 2. Tricon relay output module points are not grouped.
4.3.3.2.3.G	Relay Output Module Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	Comply	See Ref. 41. Isolation test voltage levels selected per IEEE-384, Section 7.2.2.1.
4.3.3.2.3.H	Relay Output Module Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.3.2.4	TTL Output Requirements. Requirements for TTL level output modules.	Exception	There is no TTL level output module available for use with the Tricon PLC.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.4	Processor/Other System Component Requirements. (section heading)	- - -	No requirements.
4.3.4.1	Processor Loop Time Requirements. Processor loop time shall support the response time requirement given in Section 4.2.1.A. Also, processor loop time shall be faster than the longer of the analog input conversion time or the period associated with 2.5 times the analog filter cutoff frequency.	Comply	See Ref. 20, Section 3.0 and Reference 52, Section 4. The processor loop time is included in the overall application program scan time, which is set by the user. For each nuclear plant application, the actual set scan time must be evaluated and demonstrated acceptable based on the data acquisition rates and response time requirements of the plant application.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.4.2	Memory Capacity and Data Retention Capability Requirements. The memory capacity of the main processor shall provide sufficient memory to execute a single application program with the number of program elements given.	Comply	See Ref. 45. A four chassis, 24 module Tricon system programmed as described in TR Section 4.3.4.2 has over 90% remaining free memory. See Ref. 46 for number of supported program elements.
	The memory used to contain the program shall be capable of retaining the information for a minimum of 6 months with no power applied.	Comply	See Ref. 45, Chapter 2, Page 28.
	Any memory used for field modifiable constants shall be capable of at least 100,000 write cycles.	Comply	Memory used for field modified constants is battery backed up ram on the 3008 main processors. There is no limit on the number of write cycles on this memory.
4.3.4.3	Data Acquisition Requirements. The PLC shall be capable of transferring information between the main processor and I/O modules mounted in the same or expansion chassis. The data transfer rate shall support the response time requirement given in Section 4.2.1.A, and 4.3.4.1.	Comply	See Ref. 45, Chapter 2, page 38-41.See Ref. 7, Section 4.0 and Table Section 4.2.1.A.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.4.3.A	Main Chassis Interconnect Device Operation. Devices used to interface remote or expansion chassis to the main chassis shall meet the range of environmental conditions given in Section 4.3.6. Failures of the chassis interconnect devices shall not defeat the ability to transfer data on the main chassis.	Comply Comply	See Ref. 35. Remote and expansion chassis interface devices were included in environmental testing. See Ref. 20, Section 7. Fault simulations of interconnect hardware performed during Operability tests showed that main chassis data transfer is not interrupted.
4.3.4.3.B	Main Chassis Interconnect Device Failure. Failures of the chassis interconnect devices shall not affect memory capacity or main processor data retention.	Comply	This attribute is inherent in the design of the Tricon. Local & Remote I/O operate independent of the MP memory.
4.3.4.3.C	Main Chassis Interconnect Device Loss of Power. Loss of power to chassis interconnect devices shall not defeat the ability to transfer data on the main chassis or I/O on any other chassis.	Comply	See Ref. 20, Section 7. Fault simulation of chassis power supplies performed during Operability tests showed that main chassis data transfer is not interrupted to local I/O or any other chassis.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.4.3.D	Main Chassis Interconnect Device Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	N/A	See Ref. 41, Section 3. Multi-pin cable connectors in-between Tricon Chassis are not intended for use as a Class 1E to Non-1E isolation device. Fiber optic cable and interface (RXM) module connectors inherently provide Class 1E to Non-1E isolation through non-conducting fiber optic cables.
4.3.4.3.E	Main Chassis Interconnect Device Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	N/A	See Ref. 27, Section 3.2. No interposing devices are used on multi-pin cable connectors and therefore surge testing is not required. Fiber optic cable and interface (RXM) module connectors inherently provide surge protection through non-conducting fiber optic cables.
4.3.4.3.F	Main Chassis Interconnect Device Data Acquisition Time. Data acquisition time shall be deterministic or manufacturer shall provide information to establish timing effect.	Comply	See Ref. 45, Chapter 2, Page 31 and 44. All expansion or remote chassis communication is at same rate as main chassis communication.
4.3.4.3.G	Redundant Inter-Processor Data Acquisition Backplane Busses. Descriptive information.	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.4.3.G.1	Redundant Inter-Processor Data Acquisition Backplane Busses. Busses shall be at least dual redundant.	Comply	See Ref. 42.
4.3.4.3.G.2	Redundant Inter-Processor Data Acquisition Backplane Busses. Loss of one bus shall not cause misoperation.	Comply	See Ref. 42.
4.3.4.3.G.3	Redundant Inter-Processor Data Acquisition Backplane Busses. Loss of all busses shall not result in an indeterminate operation.	Comply	See Ref. 42.
4.3.4.3.G.4	Redundant Inter-Processor Data Acquisition Backplane Busses. External alarm shall be activated on loss of one bus.	Comply	See Ref. 42.
4.3.4.3.G.5	Redundant Inter-Processor Data Acquisition Backplane Busses. Data acquisition time shall be deterministic.	Comply	See Ref. 42.
4.3.4.3.G.6	Redundant Inter-Processor Data Acquisition Backplane Busses. Operation of busses shall support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3.0. Redundant busses are always operational. Therefore, response time determination and qualification testing was performed with redundant busses operational.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.4.4	Communication Port Requirements. The main processor shall provide at least one communication port.	Comply	See Ref. 45, Chapter 2, Page 148. TCM Module.
4.3.4.4.A	Communication Port Data Rate. The port shall support data rates up to 9600 baud.	Comply	See Ref. 45, Table 60
4.3.4.4.B	Communication Port Interface. The port shall support RS-232, RS-422, RS-485 or other widely used protocol.	Comply	See Ref. 45, Table 61.
4.3.4.4.C	Communication Port Connector. The port shall provide positive hold down of connectors.	Comply	See Ref. 50, Appendix A. Standard DB-9 connectors provided on TCM ports.
4.3.4.4.D	Communication Port Isolation. For multiple ports, the port-to-port isolation shall be at least 300 volts peak.	Comply	See Ref. 50, Appendix A
4.3.4.4.E	Communication Port Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	Exception	See Ref. 41, Section 7.0. Tricon TCM serial communication ports tested for Class 1E to Non-1E isolation capability at 250 Vac (vs. 600 Vac required by TR) and 250 Vdc. Test level is based on maximum credible voltage (see Ref. 41).

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.4.4.F	Communication Port Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 39 and 57. Surge withstand capability meets IEC 61000-4-5 (Ring Wave) and IEC 61000-4-12 (Combination Wave) basic immunity levels.
4.3.4.5	Coprocessor Module Requirements. Detailed requirements for coprocessors that may be installed in I/O slots but contain local processing capability independent of the main processor.	N/A	See Ref. 20. Section 3.0. Operation of Tricon coprocessors is invoked automatically during application program execution. Coprocessor performance is evaluated during all qualification tests.
4.3.4.6	Chassis Requirements. Chassis must be suitable for mounting in a standard 19 inch rack, and must have adequate strength and provide positive hold down of modules sufficient to meet seismic withstand requirements.	Comply	See Ref. 45, Chapter 3, Page 169. See Ref. 13, Drawing No. 9600164-102 for seismic mounting details. See Ref. 36, Section 7.0 for summary of seismic test results.
4.3.4.7	Backup Devices/Redundancy Requirements. Descriptive information.	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.4.7.A	Redundant Device Requirements. Transfer to a redundant device shall occur within the larger of the main processor scan cycle or three data conversion cycles of the failed module.	N/A	See Ref. 20, Section 7, Subsection 1.0. Because redundant components are always online, component faults do not result in transfers to a redundant component.
4.3.4.7.B	Redundant Device Requirements. Undetected failures in redundant components shall be detectable during periodic surveillance.	N/A	See Ref. 20, Section 7, Subsection 1.0. Because redundant components are always online, failures can be immediately indicated through redundant alarm circuits.
4.3.4.7.C	Redundant Device Requirements. Diagnostics shall not result in indeterminate failure states and repetitive switching between redundant components.	N/A	See Ref. 20, Section 7, Subsection 1.0. Because redundant components are always online, switching between failed components does not occur.
4.3.4.7.D	Redundant Device Requirements. Requirements for affect of transfer mechanism operation on input/output module operation.	N/A	See Ref. 20, Section 7, Subsection 4.0. Because redundant components are always online, "transfers" to redundant components are bumpless.
4.3.5	Programming Terminal Requirements. Special programming terminal hardware or software shall meet the requirements of Sections 4.4.4, 7.7.2 and 7.5.2.	Comply	See Table Sections 4.4.4, 7.7.2, and 7.5.2. No special programming terminal hardware is required.
4.3.6	Environmental Requirements. (section heading)	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.6.1	Normal Environmental Basic Requirements. The normal PLC operating environment is: Temperature Range: 16 to 40°C (60 to 104°F). Humidity Range: 40 to 95% (non-condensing)	Comply	See Ref. 49. Tricon is rated for 0 to 60°C (32 to 140°F), 5% to 95% humidity (non-condensing).
	Power Source Range: As given in Section 4.6.1.1	Exception	See Table Section 4.6.1.1 for exceptions to power source range.
	Radiation Exposure: Up to 1000 Rads	Comply	See Ref. 34. Tricon has been tested to a 1000 Rad dose of Co60 gamma radiation.
4.3.6.2	Abnormal Environmental Basic Requirements. The abnormal PLC operating environment is: Temperature Range: 4 to 50°C (40 to 120°F). Humidity Range: 10 to 95% (non-condensing)	Comply	See Ref. 49. Tricon is rated for 0 to 60°C (32 to 140°F), 5% to 95% humidity (non-condensing).
	Power Source Range: As given in Section 4.6.1.1	Exception	See Table Section 4.6.1.1 for exceptions to power source range.
	Radiation Exposure: Up to 1000 Rads	Comply	See Ref. 34. Tricon has been tested to a 1000 Rad dose of Co60 gamma radiation.

TRICON TOPICAL REPORT

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.6.3	Environmental Withstand Specific Requirements. PLC shall operate for the temperature/humidity profile given in TR Figure 4-4 with operability as given in Section 5.3. Evaluations may be used to establish radiation withstand capability.	Comply	See Ref. 35, Section 7.0 & Ref. 34 for tested radiation capability.
4.3.7	EMI/RFI Withstand Requirements. The PLC shall withstand EMI/RFI levels given in EPRI TR-102323. When exposed to the radiated and conducted test levels, the PLC processors shall continue to function, I/O data transfer shall not be interrupted, discrete I/O shall not change state, analog I/O shall not vary more than 3%.	Exception	Tricon showed some susceptibilities to NRC RG 1.1.80 Rev. 1 (CE101). See Ref. 37 for results.
4.3.8	Electrostatic Discharge (ESD) Withstand Requirements. The PLC shall withstand ESD levels given in EPRI TR-102323.	Comply	See Ref. 40.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.9	Seismic Withstand Requirements. PLC shall be suitable for qualification as a Category 1 Seismic device. The PLC shall meet performance requirements during and after exposure to OBE and SSE levels shown in TR Figure 4-5.Relay contacts of relay output modules shall not chatter.	Comply	See Ref. 36. Seismic testing demonstrates that the TRICON is qualified as a Category I seismic device within the test limits shown in Figure 4-5. Due to limitations of the seismic test table, the five OBE tests and the SSE test of the TRICON were performed using a test response spectrum (TRS) that did not envelope the required response spectrum (RRS) below 4.5 Hz for the OBE and 6.3 Hz for the SSE
4.4	Software/Firmware. (section heading)	- - -	No requirements.
4.4.1	Executive. (section heading)	- - -	No requirements.
4.4.1.1	Background. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.1.2	Main Processor Executive Capability Requirements. The main processor executive shall: A. Acquire inputs from the modules. B. Implement the application program in a continuous loop. C. Load outputs to the modules. D. Perform power-up and run time diagnostics. E. Manage communications. F. Upload application programs. G. Support on-line diagnostics, maint. and troubleshooting. H. Implement the application program functions. I. Perform power-up initialize functions. J. Implement redundancy functions.	Comply	See Ref. 42.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.1.3	Program Flow Control Requirements. Requirements for PLCs where scanning of the inputs and application program execution are performed in parallel.	Comply	See Ref. 42. Tricon is a scan based system execution of each application program scan is preceded by an input module data request. While program is being executed for a given scan, the input modules continue to collect inputs from the field devices for the next scan.
	The use of application program interrupts shall be restricted. The use of interrupts that result in non-deterministic application program execution should not be permitted.	Comply	See above.
	Requirements for PLCs that implement interrupts that could result in non-deterministic application program execution.	N/A	Tricon is a scanned based system. See Ref. 42
4.4.1.4	Unintended/Unused Function Isolation Requirements. Descriptive information.	- - -	No requirements.
4.4.1.5	Coprocessor Executive Capability. (section heading)	- - -	No requirements.
4.4.1.5.1	Coprocessor Executive Capability Background. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.1.5.2	Coprocessor Executive Capability Requirements. Requirements for coprocessor resident executives or invoked utilities.	N/A	Tricon coprocessors are not user programmable. Tricon executive software includes coding for control and operation of embedded coprocessors.
4.4.2	Media Requirements. Software media provided by the manufacturer shall be high quality and new. CD-ROMS or 3-1/2 inch floppy disks are acceptable. Packaging shall preclude damage during shipping. Media shall be clearly labeled including revision and serial number. Media shall include electronic identification.	Comply	See Ref. 46, Project Administration section. See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.4.3	Ladder Logic Requirements. Descriptive information.	- - -	No requirements.
4.4.3.A	Standard Functions. Simple normally inactive and normally active paths.	Comply	See Ref. 46, Table 39.
4.4.3.B	Standard Functions. Transition ON/OFF (one-shot) paths.	Comply	See Ref. 46, Table 39.
4.4.3.C	Standard Functions. Simulate break before make and make before break contact actions.	Comply	See Ref. 46, Table 39. Requires two program scans.
4.4.3.D	Standard Functions. Coils that change paths from normal to alternate states when energized.	Comply	See Ref. 46, Table 37.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.3.E	Standard Functions. Coils that change paths from normal to alternate states when energized and remain there until the coils are de-energized and a reset signal is applied.	Comply	See Ref. 46, Table 37.
4.4.3.F	Standard Functions. Timing functions that can be set from 0.1 seconds to 2 hours.	Comply	See Ref. 47, TMR function. Must be set to multiples of the application program scan time.
4.4.3.G	Standard Functions. Counters that perform up or down counting from at least 1 to 9999.	Comply	See Ref. 47, CTD and CTU functions.
4.4.3.H	Standard Functions. Methods to perform less than, equal to and greater than numeric comparisons.	Comply	See Ref. 47, LT, GT and EQ conditional statements.
4.4.3.I	Standard Functions. Addition, subtraction, multiplication, and division functions for integer and floating point numbers. Out of range and error on division by zero.	Comply	See Ref. 47, ADD, SUB, MUL and DIV operators, DINT and REAL point types. CHK_ERR function block.
4.4.3.J	Standard Functions. Square root, exponentiation and logarithm functions. Out of range indications.	Comply	See Ref. 47, SQRT, EXPT and LOG functions. CHK_ERR function block.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.3.K	Standard Functions. A PID algorithm with 5 to 500% proportional band, 1% resolution, 0 to 100 repeats per minute integral action, 1 repeat per second resolution, anti-reset windup, 0 to 100 minutes rate action, 1 second resolution, output limiting, out of range indication, bumpless transfer to external switch activated manual control, cascade control.	Comply	See Ref. 47, PID and CHK_ERR function blocks. See Ref. 15.
4.4.3.L	Standard Functions. A dynamic compensation function. Lead/lag ratio of 0 to 10, minimum resolution of 0.05, 0.01 to 100 minute lag time, minimum 1 second resolution, lead action filter.	Comply	See Ref. 47, LEADLAG and EXPFLTR function blocks. See Ref. 15.
4.4.3.M	Standard Functions. Capability to put limits on values.	Comply	See Ref. 47, LIMIT function.
4.4.3.N	Standard Functions. Implement a function generator with at least five slopes.	Comply	See Ref. 15.
4.4.3.O	Standard Functions. Support Section 4.9.1 communications requirements.	Comply	See Table Section 4.9.1.
4.4.3.P	Standard Functions. Functions to capture results of self-tests.	Comply	See Ref. 47.
4.4.3.Q	Standard Functions. Functions to implement sequence of events requirements in Section 4.4.9.	Comply	See Ref. 59.

TRICON TOPICAL REPORT

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.3.R	Standard Functions. AND, OR and XOR bit manipulation functions.	Comply	See 47, AND, OR and XOR library functions.
4.4.3.S	Standard Functions. Functions to store results in buffer type memory, 10 instances of 50 values. Facilities to transmit this data over a serial port.	Comply	See Ref. 15.
4.4.3.T	Standard Functions. Functions to implement requirements of Section 4.4.7.2.	Comply	See Table Section 4.4.7.2.
4.4.3.U	Standard Functions. Capability to attach comments to ladder logic rungs.	Comply	See Ref. 47.
4.4.4	Software Tools Requirements. A tool shall be provided for programming, debugging and documentation.	Comply	See Ref. 46 and 47. The tool is Tristation 1131.
4.4.4.A	Software Tools Requirements. Ability to use a host device to enter a program in the PLC.	Comply	See Ref. 46, Introduction.
4.4.4.A.1	Software Tools Requirements. Ability to attach explanatory comments to program steps.	Comply	See Ref. 47.
4.4.4.A.2	Software Tools Requirements. Ability to store programs on removable magnetic media.	Comply	See Ref. 46 and 47Appendix A.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.4.A.3	Software Tools Requirements. Ability to perform bit by bit comparison of program contained in PLC and program contained in programming device.	Comply	See Ref. 46Appendix A.
4.4.4.A.4	Software Tools Requirements. Ability to print the program contained in the PLC or programming device in a fashion similar in appearance to programming device display. Include supplemental prints of programming values.	Comply	See Ref. 46 and 47, .
4.4.4.A.5	Software Tools Requirements. Features to aid in I/O mapping and memory management of the PLC.	Comply	See Ref. 47 and 49
4.4.4.A.6	Software Tools Requirements. System security requirements similar to Section 4.9.2.	Comply	See Table Section 4.9.2.
4.4.4.B	Debugging Aids. Descriptive information.	- - -	No requirements.
4.4.4.B.1	Debugging Aids. Ability to highlight all discrete elements not in their normal state.	Comply	See Ref. 46.
4.4.4.B.2	Debugging Aids. Ability to display input, output and intermediate program values.	Comply	See Ref. 46.
4.4.4.B.3	Debugging Aids. Ability to set constants and variables to arbitrary values, including values outside normal range.	Comply	See Ref. 46.
4.4.4.B.4	Debugging Aids. Ability to force outputs.	Comply	See Ref. 46.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.4.B.5	Debugging Aids. Ability to single step through a program.	Comply	See Ref. 46.
4.4.4.B.6	Debugging Aids. Ability to view the status of memory where error codes and other status information is stored.	Comply	See Ref. 60.
4.4.4.C	Software Tools Requirements. Apply Configuration management requirements per Section 7.7.3.	Comply	See Table Section 7.7.3.
4.4.4.D	Software Tools Requirements. Meet requirements of Sections 4.4.5.2 and 4.4.7.2.	Comply	See Table Sections 4.4.5.2 and 4.4.7.2.
4.4.4.E	Software Tools Requirements. Software Verification and Validation requirements of Section 7.4 shall be applied to the software tools.	Comply	See Ref. 52.
4.4.4.F	Software Tools Requirements. Provide features to aid in detecting faults in redundant components which are not detectable by self-diagnostics.	N/A	All faults in redundant components are detectable through self-diagnostics.
4.4.5	Configuration Identification. (section heading)	- - -	No requirements.
4.4.5.1	Configuration Identification Background. Descriptive information.	- - -	No requirements.
4.4.5.2	Configuration Management Aids Requirements. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.5.2.A	Configuration Management. The PLC executive shall include a retrievable, embedded electronic revision level.	Comply	See Ref. 60.
4.4.5.2.B	Configuration Management. Configuration information of configurable modules shall be retrievable in the field.	Comply	See Ref. 47.
4.4.5.2.C	Configuration Management. Software tools for modifying device configurations shall provide measures to prevent unauthorized access.	Comply	See Ref. 47.
4.4.5.2.D	Configuration Management. PLC and support tools shall provide capability to extract and record database information, including program constants.	Comply	See Ref. 47.
4.4.5.2.E	Configuration Management. All PLC devices that include firmware shall be marked with an identifier that includes revision level.	Comply	See Ref. 45, Appendix A.
4.4.5.2.F	Configuration Management. For PLCs with redundancy, tools shall provide capability to confirm that configurations are consistent.	Comply	See items 4.4.5.2.A and 4.4.5.2.B above.
4.4.6	Diagnostics Requirements. (section heading)	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1	General Diagnostic Requirements. PLC must have sufficient diagnostics and test capability to detect all failures that could prevent the PLC from performing its intended safety function.	Comply	See Table Sections 4.4.6.1.1 through 4.4.6.1.14.
	Items 4.4.6.1.1 through 4.4.6.1.6 must be covered by on-line self test.	Comply	See Table Section 4.4.6.2.
	Items 4.4.6.1.7 and 4.4.6.1.8 must be covered in power-up tests.	Comply	See Table Section 4.4.6.3.
	Short term diagnostics changes in module outputs shall be 2 msec or less for DC outputs and 1/2 cycle or less for AC outputs. Capability to disable these diagnostics shall be provided.	Comply	See Ref. 45, Chapter 2 Page 83.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.1	Processor Stall. For PLCs with redundant processors, the PLC shall detect processor stall and halt operation of the failed processor.	Comply	Failure Detect: See Ref. 42, Section 8.13. Failure Alarm: See Ref. 45, Tables 74 and 75, MP Active LED. Application Program Interface: See Ref. 47, TR-MP-STATUS function.
4.4.6.1.2	Executive Program Error. Check of executive firmware integrity using a checksum or similar test.	Comply	Failure Detect: See Ref. 42, Section 8.13. Failure Alarm: See Ref. 45, Chapter 4, Table 75, MP Fault LED. Application Program Interface: See Ref. 47, TR-MP-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.3	Application Program Error. Check of application program integrity using a checksum or similar test.	Comply	Failure Detect: See Ref. 42, Section 8.13. Failure Alarm: See Ref. 45, Chapter 4, Table 74, MP Active LED. Application Program Interface: See Ref. 47, TR-MP-STATUS function.
4.4.6.1.4	Variable Memory Error. Read/Write memory test by writing and reading back bit patterns that test both states of all bits, or similar test.	Comply	Failure Detect: See Ref. 42, Section 8.13. Failure Alarm: See Ref. 45 Chapter 4, Table 75, MP Fault LED. Application Program Interface: See Ref. 47, TR-MP-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.5	Module Communication Error. Check of communication data integrity.	Comply	Failure Detect: See Ref. 42, Section 8.13. Failure Alarm: See Ref. 45, Chapter 4, Table 76, MP COM RX and TX LEDs. Application Program Interface: See Ref. 47, TR-MP-STATUS and TR-PORT-STATUS functions.
4.4.6.1.6	Memory Battery Low. Check of memory battery capacity.	Comply	Failure Detect: See Ref. 45, Chapter 4, Table 75, Bat Low. Failure Alarm: See Ref. 45, Chapter 4, Table 75, Bat Low LED.
4.4.6.1.7	Module Loss of Configuration. For software configurable modules, validate configuration.	Comply	Failure Detect and Alarm: See Ref. 45, Chapter 4, Table 77, Main Chassis Power Module. Application Program Interface: See Ref. 47, TR-CHASSIS-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.8	Failure of Watchdog Timer. Check of operation of watchdog timer.	Comply	Failure Detect: See Ref. 43, Section 8.13. Failure Alarm: See Ref. 45, Chapter 4, Table 75, MP Fault LED. Application Program Interface: See Ref. 47, TR-MP-STATUS function.
4.4.6.1.9	Application not Executing. Failure to complete application program scan.	Comply	Failure Detect: See Ref. 42, Section 8.13. Failure Alarm: See Ref. 45, Chapter 4, Table 75, MP Active LED. Application Program Interface: See Ref. 47, TR-MP-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.10	Analog Output not Following. Failure of analog output to following commanded value.	Comply	Failure Detect: See Ref. 45, Chapter 4, Table 80. Failure Alarm: See Ref. 45, Chapter 4, Table 80, Analog Output Module Fault LED. Application Program Interface: See Ref. 47, TR-SLOT-STATUS function.
4.4.6.1.11	Analog Input not Responding. Failure of analog input to respond to input signal.	Comply	Failure Detect: See Ref. 45, Chapter 4, Table 80 and Table 81. Failure Alarm: See Ref. 45, Chapter 4, Table 80 and Table 81, Module Fault LEDs. Application Program Interface: See Ref. 47, TR-SLOT-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.12	Discrete Input/Ouput not Responding. Failure of discrete input/output to operate correctly.	Comply	Failure Detect: See Ref. 45, Chapter 4, Table 79 & Table 80. Failure Alarm: See Ref. 45, Chapter 4, Table 79 & Table 80, Module Fault LEDs. Application Program Interface: See Ref. 47, TR-SLOT-STATUS, TR-POINT-STATUS and TR-MP-STATUS functions.
4.4.6.1.13	Analog I/O out of Calibration. Analog input or output point out of calibration.	Comply	Failure Detect: See Ref. 45, Chapter 4, Table 80 and Table 81. Failure Alarm: See Ref. 45, Chapter 4, Table 80 and Table 81, Module Fault LEDs. Application Program Interface: See Ref. 47, TR-SLOT-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.14	Power Supply out of Tolerance. Power supply to PLC is interrupted or a chassis power supply module fails.	Comply	Failure Detect: See Ref. 45, Chapter 4, Table 77 & Table 78. Failure Alarm: See Ref. 45, Chapter 4, Table 77 & Table 78, Module Fault LEDs. Application Program Interface: See Ref. 47, TR-CHASSIS-STATUS function.
4.4.6.2	On-Line Self-Test Requirements. On-line self-tests shall cover at least items 4.4.6.1.1 through 4.4.6.1.6 above. Results shall be made available to the application program.	Comply	See Ref. 42, Section 8.1.3. See Table sections 4.4.6.1.1 through 4.4.6.1.6 above.
4.4.6.3	Power Up Diagnostics Requirements. Power up diagnostics shall include all on-line self tests, configuration verification, and test of failure to complete a scan. Application program execution shall be inhibited if power up diagnostics detect a failure.	Comply	See Ref. 42, Sections 8.1.3. The Power Up diagnostics and initializations are followed by execution of the background runtime diagnostics and fault analysis functions, which include the on-line self tests identified in Table Section 4.4.6.2.
4.4.7	Data and Data Base. (section heading)	- - -	No requirements.
4.4.7.1	Data and Data Base Overview. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.7.2	Data and Data Base Requirements. Descriptive information.	- - -	No requirements.
4.4.7.2.A	Data and Data Base Requirements. PLC shall support use of user-defined program constants that are contained in non-volatile memory. Features shall confirm that constants in redundant processors are the same.	Comply	See Ref. 46, Application Development. See Ref. 45, Table 8, memory is battery backed. See Ref. 42, Section 8.1.3, constants in memory are continuously verified.
4.4.7.2.B	Data and Data Base Requirements. PLC shall provide functions to read and modify data base constants. Features shall confirm that modified constants are consistent between redundant processors.	Comply	See Ref. 46, Application Development. See Ref. 42, Section 8.1.3, constants in memory are continuously verified.
4.4.7.2.C	Data and Data Base Requirements. PLC shall provide features to prevent modifications to data base constants over connected communication paths.	Comply	See Ref. 46, Project Administration.
4.4.7.2.D	Data and Data Base Requirements. PLC shall provide features to permit transmitting input, outputs and calculated values to other devices over a serial port.	Comply	See Ref. 15.
4.4.8	Other Non-Ladder Logic Programming Languages. (section heading)	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.8.1	Requirements for Sequential Logic Languages. Sequential logic language other than ladder logic may be used. Language shall provide capabilities given in Section 4.4.3. Language must support tools with features given in Section 4.4.4.	Comply	See Ref. 46, Application Development. Tristation 1131 also provides Function Block Diagram and Structured Text languages for application development. All discussions in Table Sections 4.4.3 and 4.4.4 apply to these languages as well.
4.4.8.2	Standard High Level Languages. (section heading)	- - -	No requirements.
4.4.8.2.1	Overview of Standard High Level Languages. Descriptive information.	- - -	No requirements.
4.4.8.2.2	Requirements for Standard High Level Languages. Required capabilities of supported standard high level programming languages.	N/A	Tricon does not support use of standard high level programming languages.
4.4.9	Sequence of Events Processing Requirements. Descriptive information.	- - -	No requirements.
4.4.9.A	Sequence of Events. Shall permit application program to capture, store and time tag up to 20 transitions of up to 50 different discrete events of inputs or application objects.	Comply	See Ref. 48, Chapter 3. A single SOE block (or list of discrete variables) will support recording of 100,000 events.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.9.B	Sequence of Events. Shall permit starting and stopping the event recording.	Comply	See Ref. 48, Chapter 2,. SOESTRT and SOESTOP commands.
4.4.9.C	Sequence of Events. Shall permit transmitting the data to an external device using a PLC communication port.	Comply	See Ref. 46, Introduction. Supports transmission of data through TCM.
4.4.9.D	Sequence of Events. Relative accuracy of time tags shall be one scan cycle ± 50 msecs.	Comply	See Ref. 46, , Using Time Synchronization. Accuracy of time tags is one scan cycle ± 25 msecs
4.4.10	System Integration Requirements. An appropriate level of system integration and integration testing shall be applied to the test specimen and TSAP.	Comply	See Table Section 5.2.C.
4.5	Human/Machine Interface (HMI). (section heading)	---	No requirements.
4.5.1	Human/Machine Interface (HMI) Background. Descriptive information.	---	No requirements.
4.5.2	Requirements for Human/Machine Interface Functions. Descriptive information.	---	No requirements.
4.5.2.A	HMI Functions. PLC shall support switching a loop controller between manual and automatic via switch inputs. For control loops with integral action, auto/manual tracking shall be provided.	Comply	See Ref. 47, LEADLAG and PID function descriptions. See Ref. 15.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.5.2.B	HMI Functions. PLC shall support setpoint adjustments via switch inputs. Adjustments shall include increase, decrease, and rate of change of setpoint.	Comply	See Ref. 15.
4.5.2.C	HMI Functions. PLC shall support manual initiation of equipment via switch inputs. PLC shall support detection of manually initiated equipment.	Comply	See Ref. 15.
4.5.2.D	HMI Functions. PLC shall support display of status of discrete and continuous value parameters via connected devices.	Comply	See Ref. 15.
4.5.2.E	HMI Functions. PLC shall support sending information to a serial port device. Information sent shall include input, output and internal variable values, on-line diagnostics, sequence of events (SOE) data, and results of calculations, comparisons and bit manipulations.	Comply	See Ref. 15.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.5.3	Requirements for Interactive Features. The PLC shall provide mechanisms to prevent unauthorized access to or inadvertent use of on-line functions.	Comply	See Ref. 13, Chassis Options.
	Interactive features shall be available through a programming, maintenance and debugging port. PLC shall operate with no connection to this port.	Comply	See Ref. 46.
	PLC shall mask interactive commands during run mode.	Comply	See Ref. 13, Chassis Options.
4.5.4	Requirements for Operator Action System Response Times. For any operator action that requires PLC confirmation, the PLC shall include features to enable confirmation within 0.5 seconds.	Comply	See Ref. 47. As an example, a discrete input to discrete output sequence with intervening internal timer function would meet this requirement.
4.5.5	Display Requirements. LEDs are acceptable for any status displays.	Comply	See Ref. 45, Chapter 4.
4.5.6	Alarm Processing Requirements. Descriptive information.	- - -	No requirements.
4.5.6.A	Alarm Processing. PLC shall have ability to compare inputs or derived parameters to setpoints.	Comply	See Ref. 15.
4.5.6.B	Alarm Processing. PLC shall have ability to latch an alarm condition and reset based on alarm reset condition.	Comply	See Ref. 15.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.5.6.C	Alarm Processing. PLC shall have ability to blink an output indicator.	Comply	See Ref. 47, BLINK function. As an example, a discrete output driven by a BLINK coil would meet this requirement.
4.5.6.D	Alarm Processing. PLC shall have ability to acknowledge an alarm.	Comply	See Ref. 46, LATCH coil function. As an example, a discrete input connected to a LATCH coil would meet this requirement.
4.5.6.E	Alarm Processing. Application program shall have ability to capture results of self-diagnostics.	Comply	See Ref. 46. As an example, TR_xxx_STATUS functions return diagnostic status of system hardware to application program.
4.5.6.F	Alarm Processing. Application program shall have ability to store results of items A through E in a buffer and transmit the data via a communication port.	Comply	See Ref. 45, Chapter 2, Page 38, As an example, Sequence of Events utility can store and transmit alarm information.
4.5.7	Hard Manual Backup. Descriptive information.	---	No requirements.
4.6	Electrical. (section header)	---	No requirements.
4.6.1	Power Supply Requirements. (section heading)	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.1.1	PLC Power Sources and Power Supply Requirements. Descriptive information.	- - -	No requirements.
4.6.1.1.A	Power Sources. AC sources shall operate from at least 90 Vac to 150 Vac and 57 to 63 Hz.	Exception	See Ref. 45 and 49. Model 8310 AC power supply modules are rated for 85 to 140 Vac input.
	AC sources shall operate at the temperature and humidity range given in Section 4.3.6.	Comply	See Ref. 35. Model 8310 AC power supply modules were tested as per required temperature and humidity range (see Table Section 4.3.6.3).

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.1.1.B	Power Sources. DC sources shall operate from at least 20.4 to 27.6 Vdc.	Exception	See Ref. 45 and 49. Model 8311 DC power supply modules are rated for 22 to 31 Vdc input.
	DC sources shall operate at the temperature and humidity range given in Section 4.3.6.	Comply	See Ref. 35. Model 8311 DC power supply modules were tested as per required temperature and humidity range (see Table Section 4.3.6.3).
4.6.1.1.C	Power Sources. DC sources shall operate for seven days from a 30 VDC source.	Comply	See Ref. 19 Section 10.18.
4.6.1.1.D	Power Sources. Sources shall be capable of supplying 1.2 times bus loading for a fully loaded main chassis.	Comply	See Ref. 49, Page 24.
4.6.1.1.E	Power Sources. Sources shall be capable of supplying 1.2 times bus loading for a fully loaded expansion chassis.	Comply	See Ref. 49 Page 24.
4.6.1.1.F	Power Sources. Hold up time for AC supplied power sources shall be 40 msec.	Comply	Ref. 53, Section 7.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.1.1.G	Power Sources. Sources shall meet the EMI/RFI, surge withstand and ESD requirements of Sections 4.3.7, 4.6.2 and 4.3.8.	Comply	See Ref. 37, Ref. 39 and Ref. 40.
	Sources shall meet the grounding requirements of Section 4.6.8.	Comply	See Table Section 4.6.8.
4.6.1.1.H	Power Sources. Requirements for fan cooled power sources.	N/A	See Ref. 45, Chapter 3, Page 170. Tricon power supplies are convection cooled.
4.6.1.1.I	Power Sources. Faults in redundant power sources shall not prevent operation of the alternate supply.	Comply	See Ref. 45, Page 32. Redundant power sources are independently fused.
4.6.1.2	Loop Power Supply Requirements. Power supply modules shall be provided for external devices. Modules shall provide at least 500 mA at 24 VDC. The modules shall meet requirements A, B, C, F. G and H above.	N/A	No third party power supplies were included in the qualification program.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.2	Surge Withstand Capability Requirements. PLC platform shall withstand IEEE Standard C62.41 ring wave and combination wave, 3000 volt peak surges.	Comply	See Ref. 39 and 57. Power sources meet surge withstand criteria- Circuits were tested to IEC 61000-4-5 and IEC 61000-4-12 using 1 kV Ring wave, and combination waves at 1kV open circuit/0.5kA short circuit per R.G. 1.180, Rev. 1, Level 2. All circuits met TR Section 4.6.2 acceptance criteria.
	Withstand capability applies to power sources, analog and discrete I/O interfaces, and communication port interfaces. Per Section 6.3.5, surge testing shall be conducted per IEEE Standard C62.45.	Partial Exception	Power Sources were tested per Reg Guide 1.180 Rev. 1 for category B low exposure installations to 2KV. IEEE Standards 62.41 and 62.45 do not address testing of I/O and communication circuits; these circuits were tested per Reg. Guide 1.180 Rev. 1 for low exposure level 2 installations at 1KV. Tests were performed to IEC61000-4-5 for Combination Wave and 61000-4-12 for Ring Wave.
4.6.3	Separation. Descriptive information.	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.4	Class 1E/Non-1E Isolation Requirements. The PLC modules shall provide isolation of at least 600 Vac and 250 Vdc applied for 30 seconds. Isolation features shall conform to IEEE 384. Isolation testing shall be performed on the modules.	Exception	See Ref. 41. Only relay output modules, communication ports, and fiber optic chassis inter- connections are intended to provide Class 1E to Non-1E isolation. Isolation tests were performed on relay output module and communication ports. Relay output module meets TR Section 4.6.4 isolation requirements. Communication ports provide isolation to 250 Vac and 250 Vdc for 30 seconds. Fiber optic chassis connections inherently provide isolation through non-conducting fiber optic cables.
4.6.5	Cable/Wiring Requirements. Manufacturer shall supply all PLC hardware interconnecting cabling. All cabling shall be suitable for UL Class 2 service. Specifically, withstand rating shall be larger of 3 times the signal level voltage or 150 volts. Temperature rating shall be 60°C or greater. Vendor shall identify the quantities of PVC type wire and cable used in the system.	Comply	See Ref. 49 and 61 Chassis-to-chassis and chassis-to-termination panel interconnect cables are rated for 300 VAC and a minimum of 80°C. Cable jackets are made of PVC or XLPE.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.6	Termination Requirements. Modules shall be able to be removed without disconnecting field wiring.	Comply	See Ref. 48..
	Features shall be provided to substitute test signals or monitoring instruments for field connections. Connectors to the PLC shall have positive hold down mechanisms.	Comply	See Ref. 45 and 48
	Connectors and terminations to the PLC shall be qualified with the generic PLC.	Comply	See Ref. 3. Field termination panels were included in the qualification test specimen.
4.6.7	Backup Power. Descriptive information.	- - -	No requirements.
4.6.8	Grounding/Shielding Requirements. The PLC equipment shall meet IEEE 1050 and EPRI TR-102323 grounding requirements. This includes supporting connection to single point, multi-point and floating ground systems, and providing separate ground connection points on each chassis for AC ground, DC ground, and signal ground.	Comply	See Ref. 45, Chapter 3.
	The PLC equipment shall meet IEEE 1050 and EPRI TR-102323 shielding requirements. This includes providing shielding connection points for the I/O module field terminations.	Comply	See Ref. 45, Chapter 3.
4.7	Maintenance. (section heading)	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.7.1	Maintenance Background. Descriptive information.	- - -	No requirements.
4.7.2	Diagnosis/Built-in Testability Requirements. Descriptive information.	- - -	No requirements.
4.7.3	Module Replacement Requirements. The PLC shall contain features to aid in module replacement.	Comply	See Ref. 45, Chapter 3.
	The maintenance manual shall contain a description of any hardware configuration item for each module.	Comply	See Ref. 45, Chapter 3.
	The module hold downs shall be easily accessible and provide ease of removal and reinstallation.	Comply	See Ref. 45, Chapter 3.
4.7.4	Preventive Maintenance Requirements. Equipment manuals shall contain preventive maintenance information. Preventive maintenance shall also include components identified in Section 4.7.8.2.	Comply	See Ref. 45, Chapter 3. See Table Section 4.7.8.2.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.7.5	Surveillance Testing Requirements. The PLC shall support IEEE 338 surveillance testing through: - Ability to read input, intermediate and output values. - Ability to force output values. - Ability to make connections to all I/O signals. - Ability to program I/O operations.	Comply	See Ref. 49, Page 59. Tristation 1131 connection permits required access to application program variables. Also, screw terminals used on field termination panels can be loosened for connection to all I/O signals.
	Features and procedures shall be provided that permit detection of failures of all redundant components if those failures are not detectable by self-diagnostics or are masked by redundant channel behavior.	N/A	See Ref. 45, Chapter 4. All failures of redundant devices are indicated by module fault LEDs.
4.7.6	Output Bypass/Control Devices. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.7.7	Hot Repair Capability. The PLC shall support installing I/O modules with backplane power applied.	Comply	See Ref. 45, Chapter 3
	Low power modules shall support removal with field power applied.	Comply	See Ref. 45, Chapter 3. Modules can be "hot-swapped" with field power applied. Active modules shall not be removed from a chassis. An active module can be replaced on-line through insertion of a similar module in the adjoining spare slot and after bumpless transfer of control to the spare module.
	When output modules are removed from the backplane, the state of the outputs should be known.	N/A	Removal of an output module from the chassis results in disconnection of all field wiring from the module.
4.7.8	Manufacturer System Life Cycle Maintenance. (section heading)	---	No requirement.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.7.8.1	Parts Replacement Life Cycle Requirements. The baseline configuration of the qualified PLC shall be established.	Comply	See Ref. 3.
	Records shall be maintained for revision history and changes.	Comply	See Ref. 62, QAM 4.0, Design Control.
	Records shall be maintained for tracking failures.	Comply	See Table Section 7.8.
	Testing shall be performed as necessary to maintain a qualified platform based on future revisions or replacements.	Comply	See Ref. 63.
4.7.8.2	Component Aging Analysis Requirements. A periodic surveillance and maintenance interval shall be determined per IEEE 323 to account for any significant aging mechanisms.	Comply	See this report, Section 4.15.
4.7.9	Maintenance Human Factors. Descriptive information.	---	No requirements.
4.7.9.A	Special PLC Manufacturer Equipment. The manufacturer shall provide documentation for PLC support equipment.	N/A	See Ref. 45, Chapter 3. No special tools required for routine maintenance.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.7.9.B	Test Equipment Connections. Test equipment connections shall be supported by documentation and hardware, including interconnection devices. The manufacturer shall provide any special instruction for use of test equipment connections.	Comply	See Ref. 45, Chapter 3. This section provides instruction and precautions for connection and use of Tristation 1131 to perform recommended routine maintenance activities.
4.7.9.C	Job Aids. Aids for operating the PLC equipment shall be provided.	Comply	See various sections of Ref. 45 for equipment pictures, and operational recommendations and warnings. See Ref. 45, Chapter 3 for description of module installation keying.
4.7.9.D	Help Screens. Help screens for software used to support maintenance shall be provided.	Comply	See Ref. 45. Tristation 1131 software may be used during maintenance.
4.8	Requirements for Third Party/Sub-Vendor Items. All items provided by sub-vendors or third parties shall be subjected to all applicable requirements and tests. Compatibility of operation with the PLC shall be demonstrated through tests.	Comply	See Ref. 56. Third party signal conditioners were included in the qualification program.
4.9	Other. (section heading)	- - -	No requirements.
4.9.1	Data Handling and Communication Interface Overview. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.9.1.1	Peripheral Communication Requirements. The PLC executive and/or application software tools shall provide features to prevent loss of serial communication from degrading the application program.	Comply	See Ref. 53. Communication port failure tests performed throughout qualification testing showed no effect on application program or PLC scan cycle.
	Communication overhead time shall be deterministic.	Comply	See Ref. 7.
	Peripheral communications shall support at least 1000 character communication buffers. (Note: 1 character = 1 byte. A real variable uses 8 bytes or eight characters).	Comply	See Ref. 46, Aliases for Tricon Points. Aliased variables (points) are automatically buffered each scan for use by external hosts. Over 2000 real memory variables can be aliased (= 16000 characters).
	Serial communications shall support checksum (or equivalent) data quality checks.	Comply	Tricon serial communications implement Cyclic Redundancy Checks (CRC) for compatibility with standard industry communication protocols.
	Requirements for redundant communication hardware.	N/A	No redundant communication hardware.
4.9.1.1.1	Software Isolation Requirements. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.9.1.1.1.A	Software Isolation. Features shall be provided to permit sending serial port data with no hardware or software handshaking.	Comply	See Ref. 46, Configurable Modules (TCM), and Peer-to-Peer Communication.
4.9.1.1.1.B	Software Isolation. Features shall be provided to permit the application program to ignore communication port incoming data.	Comply	See Ref. 46, Configurable Modules (TCM), and Peer-to-Peer Communication.
4.9.1.1.1.C	Software Isolation. Software shall permit use of the send data functions with the receive data functions disabled.	Comply	See Ref. 46, Configurable Modules (TCM), and Peer-to-Peer Communication.
4.9.1.1.1.D	Software Isolation. Features shall be provided to disable interrupts caused by full serial port receive buffers.	Comply	See Ref. 58. No interrupts to main processors are generated based on communication buffer full interrupts.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.9.1.	PLC Peer-to-Peer Communication Requirements. Peer-to-peer link shall meet requirements of Section 4.3.4.4, except item B.	Comply	See Ref. 45, Section 3.8, TCM Module, Net 1 port. Tricon Peer-to-Peer protocol is proprietary. See Ref. 8. Net 1 port surge withstand capability meets IEC 801-5 "basic immunity" levels.
	Communication time shall be deterministic.	Comply	See Ref. 46, Peer-to-Peer Communication Data Transfer Time.
	Communication errors shall not affect other portions of the application program or inhibit the PLC scan cycle. Queues for communicated data shall be supported and queue status shall be available to the communication program. Loss of communication shall be detected and made available to the application program.	Comply	See Ref. 64. TCM Module Net 1 port failure tests showed no effect on application program or PLC scan cycle. See Ref. 46, Peer-to-Peer Communication.
	Use of the peer-to-peer communication link shall support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 20, Section 3 and Table Section 4.2.1.A. Peer-to-Peer communication link was implemented during all qualification testing.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.9.2	Overall System Security Requirements. Switching the main processor from RUN mode to other modes shall be by keylock switch.	Comply	See Ref. 45, Chapter 2.
	Features shall ensure that redundant components operate in the same mode, and that program changes are loaded into all redundant processors.	Comply	See Ref. 45, Chapter 2, Main Processor Modules. See Ref. 46, Chapter 5.
	Provisions shall prevent modification of the application program and operating system while the PLC in on-line.	Comply	See Ref. 45, Chapter 2, Page 28 and Ref. 46, System Administration, Elements of a Security System.
4.9.3	Heartbeat Requirements. The PLC shall provide capability to activate a "heartbeat" external to the PLC.	Comply	See Ref. 15.
4.9.4	Hazardous Materials Requirements. Material data sheets shall be provided for all hazardous materials associated with the PLC.	N/A	No hazardous materials associated with the Tricon PLC.
4.10	Shipping and Handling Requirements. Packaging and shipping shall be in accordance with ANSI N45.2.2.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1	Packaging Requirements. Descriptive information.	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.10.1.A	Items Shipped. Shall be packaged to avoid damage or degradation due to various environmental and handling factors which may be encountered during shipping and storage.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1.B	Items Shipped. Packaging shall include desiccant materials as required.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1.C	Items Shipped. Items shall be inspected for cleanliness prior to packaging. Items not immediately packaged shall be protected from contamination.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery. See Ref. 54, Section QAM 10.0, Inspection and Testing.
4.10.1.D	Items Shipped. Cushioning shall be provided to protect against shock and vibration.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1.E	Items Shipped. Items and containers shall be marked with appropriate identification.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery. See Ref. 54, Section QAM 8.0, Product, Parts, and Material Identification and Traceability.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.10.1.F	Items Shipped. Copies of packing lists shall be included with each carton shipped.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1.G	Items Shipped. ESD sensitive items shall be appropriately packaged, handled and marked.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1.H	Items Shipped. Packaging shall be suitable for movement using hand trucks.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1.I	Items Shipped. Special handling or storage requirements shall be marked on the containers.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1.J	Items Shipped. See Section 4.4.2 for requirements for software storage media.	Comply	See Table Section 4.4.2.
4.10.2	Shipping Requirements. Requirements for mode of shipping, use of fully enclosed vehicles, special handling and stacking instructions as necessary, and container markings and protective covers.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.10.3	Storage Requirements. Storage and shelf life requirements shall be provided for all PLC items.	Comply	See Ref. 54, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
5	Acceptance/Operability Testing. Descriptive information.	- - -	No requirements.
5.1	Acceptance/Operability Testing Overview. The development, design and performance of acceptance testing shall use the documentation requirements of Section 8.14.	Comply	See Table Section 8.14.
5.2	Pre-Qualification Acceptance Test Requirements. Descriptive information.	- - -	No requirements.
5.2.A	Application Objects Testing. Testing of the software objects in the PLC library shall be performed. This testing shall be in addition to any testing performed by the manufacturer.	Exception	See Ref. 2, Section 5. Triconex and TUV Rheinland have performed extensive testing of the Tricon PLC application software. Results of this testing are documented in Ref. 58. Accordingly, this testing was not performed.
5.2.B	Initial PLC Calibration. The generic qualification sample PLC shall be calibrated to NIST traceable sources.	Comply	See Ref. 19, Section 9.0.
5.2.C	System Integration. System integration testing portion of TSAP V&V shall be performed during acceptance testing.	Comply	See Ref. 65.

TRICON TOPICAL REPORT

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
5.2.D	Operability Tests. The Operability Test shall be performed during acceptance testing.	Comply	See Ref. 53.
5.2.E	Prudency Tests. The Prudency Test shall be performed during acceptance testing.	Comply	See Ref. 66.
5.2.F	Burn-In Test. A minimum 352 hour burn-in test shall be performed during acceptance testing.	Exception	See Ref. 2, Appendix 3. Triconex routinely conducts burn-in tests on all Tricon hardware as part of manufacturing process. This testing meets TR requirements for burn-in testing. Accordingly, this testing was not performed.
5.3	Operability Test Requirements. Descriptive information.	- - -	No requirements.
5.3.A	Accuracy. Accuracy checks shall be performed on the analog input/output modules.	Comply	See Ref. 20, Section 2.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
5.3.B	Response Time. Response time of analog input to digital output and digital input to digital output sequences shall be measured. For baseline (acceptance) testing, the acceptance criteria is that the measured response time shall not vary more than 20% from the value calculated from manufacturer's data. For all subsequent testing, the measured value shall not vary more than 10% from the baseline.	Exception	See Ref. 20, Section 3. Based on Tricon design, it is not practicable to perform a test that provides consistent (within ±20%) measured response times. Instead, manufacturer's data is used to calculate maximum expected AI to DO and DI to DO response times. The acceptance criteria for all tests is that the calculated response times are not exceeded.
5.3.C	Discrete Input Operability. Discrete inputs shall be tested for capability to detect changes in the inputs.	Comply	See Ref. 20, Section 4.
5.3.D	Discrete Output Operability. Discrete outputs shall be tested for ability to operate within rated voltages and currents.	Comply	See Ref. 20, Section 5.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
5.3.E	Communication Operability. If any communication functions are included in the qualification envelope, then operability of the ports shall be tested. Tests shall look for degradation in bit rates, signal levels and pulse shapes of communication protocol.	Partial Exception	See Ref. 20, Section 1. The TCM Module NET1 and NET2 ports are included in the qualification envelope. Test equipment to measure degradation of bit rates, pulse shapes, and signal levels was not available at the time testing was performed. The port protocol is proprietary and not amenable to TR specified tests-. Port operation is monitored for correct performance throughout all qualification tests.
5.3.F	Coprocessor Operability. If any coprocessors are included in the qualification envelope, then tests shall be performed specifically on these coprocessors.	Comply	See Ref. 20. Section 1. Operation of Tricon coprocessors is invoked automatically during application program execution. Separate coprocessor tests are not required.
5.3.G	Timer Tests. Accuracy of timer functions shall be tested.	Comply	See Ref. 20, Section 6.
5.3.H	Test of Failure to Complete Scan Detection. The function of the mechanism to detect failure to complete a scan shall be tested. The power up testing of this feature may be used to establish its operability.	Comply	See Ref. 20, Section 8.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
5.3.I	Failover Operability Tests. If redundancy with automatic transfer to a redundant device is used, tests shall be performed to establish operability of the failover hardware.	Comply	See Ref. 20, Section 7.
5.3.J	Loss of Power Test. The AC and DC power sources shall be shut off for at least 30 seconds and reapplied.	Comply	See Ref. 20, Section 8.
5.3.K	Power Interrupt Test. The AC power sources shall be interrupted for a 40 millisecond hold-up time.	Comply	See Ref. 20, Section 9.
5.4	Prudency Testing Requirements. The Prudency tests shall be performed with the power supply sources at the minimum values specified in Section 4.6.1.1.	Partial Exception	See Ref. 21, Section 2, Subsection 3.1. To accommodate power frequency changes, external power to the 230Vac chassis power supplies was provided through a step-up transformer which was fed by the same external power supply for the 115Vac chassis power supplies. This limited the voltage to the 115Vac chassis power supplies to 97Vac.
5.4.A	Burst of Events Test. Tests shall be performed to verify operation of the PLC under highly dynamic input/output variation conditions.	Comply	See Ref. 21, Section 2.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
5.4.B	Failure of Serial Port Receiver Test. The receiving device connected to the main processor serial communication port shall be simulated to fail in various modes. PLC response time shall be verified to not degrade unacceptably.	Comply	See Ref. 21, Section 3.
5.4.C	Serial Port Noise Test. The transmit line to the main processor serial communication port shall be subjected to white noise. PLC response time shall be verified to not degrade unacceptably.	Comply	See Ref. 21, Section 3.
5.4.D	Fault Simulation. For PLC's that include redundancy, failures in redundant elements shall be simulated.	Comply	See Ref. 20, Section 1, Subsection 3.0, and Ref. 6, Section 7. Fault simulation in redundant elements is performed during the Failover portion of Operability testing, in lieu of during Prudency Testing..

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
5.5	Operability/Prudency Testing Applicability Requirements. As a minimum, Operability and Prudency tests shall be performed: - During acceptance testing: Operability – All, Prudency – All - During environmental testing: Operability – All, Prudency – All - During seismic testing: Operability – All, Prudency – All - After seismic testing: Operability – All, Prudency – None - During EMI/RFI testing: Operability – All except analog I/O checks, Prudency – Only burst of events test - After ESD testing: Operability – All, Prudency - None	Partial Exception	Due to short duration of seismic SSE tests, and special set-up required for EMI/RFI tests, it is not practicable to perform Operability and Prudency tests at those times. The testing complied with the other requirements of Section 5.5. See Ref. 2 for detailed qualification test plan.
5.6	Application Software Objects Acceptance (ASOA) Testing. Requirements for ASOA testing.	Exception	See Ref. 2, Section 5, and Table Section 5.2.A
6	Qualification Testing and Analysis. Descriptive information.	- - -	No requirements.
6.1	Qualification Process Overview. Descriptive information.	- - -	No requirements.
6.1.1	PLC System Qualification Overview. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.2	PLC System Test Configuration Requirements. Descriptive information.	- - -	No requirements.
6.2.1	Test Specimen Hardware Configuration Requirements. Hardware configuration shall be developed and documented consistent with the requirements of Sections 6.5 and 8.2.	Comply	See Table Sections 6.5 and 8.2
6.2.1.A	Module Types. The test specimen shall include at least one type of module needed to encompass the requirements of Section 4.3. Multiple samples of configurable modules shall be included to cover the different configurations. For T/C modules, only one T/C type needs to be tested unless different types use different signal conditioning.	Comply	See Ref. 3 for identification of module types included in test specimen. One of each available module type was included. Configurable modules (analog inputs, T/C inputs, pulse inputs) use only software to invoke different configurations and therefore do not require multiple installed samples.
6.2.1.B	Module Types. The test specimen shall include modules needed to support Operability testing.	Comply	See Ref. 20 for identification of module tests performed during Operability testing.
6.2.1.C	Ancillary Devices. The test specimen shall include at least one of each type of ancillary device needed to meet the TR requirements.	Comply	No ancillary devices used in test specimen.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.2.1.D	Chassis Types. The test specimen shall include at least one of each type of chassis needed to meet the TR requirements. Connections between chassis shall use maximum permissible cable lengths.	Comply	See Ref. 3 for identification of chassis types and interconnecting cable lengths used in test specimen.
6.2.1.E	Power Supplies. The test specimen shall include the power supplies needed to meet the TR requirements. Additional resistive loads shall be placed on each power supply output so that the power supply operates at rated conditions.	Exception	See Ref. 3 for identification of power supplies included in test specimen. The Tricon design does not allow for adding resistive load on the power supplies without altering design and operation. To demonstrate significant power supply loading, one chassis of the test specimen was fully populated with one module in each slot.
6.2.1.F	Dummy Modules. Dummy modules shall be used to fill all remaining slots in the main chassis and at least one expansion chassis. The dummy modules shall provide a power supply and weight load approximately equal to an eight point discrete input module.	Exception	See Ref. 24. Seismic Balance Modules (SBMs) were installed in two test specimen chassis to increase the weight loading to that representative of a fully module populated chassis. Dummy modules did not provide a load on the power supplies.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.2.1.G	Termination Devices. The test specimen shall include at least one of each type of termination device and associated cabling used to provide field connections.	Comply	See Ref. 3 for identification of external termination panels and interconnecting cables used in the test specimen.
6.2.1.H	Redundant Devices. The test specimen shall include any devices needed to implement any redundancy included in the qualification envelope.	Comply	See Ref. 3 for identification of redundant devices used in test specimen. These devices include redundant main processor modules, chassis power supplies, chassis interconnect cabling, and chassis fiber optic interconnect modules and cables.
6.2.1.I	Additional Modules. The test specimen shall include any additional modules needed to support Operability and Prudency testing and to support module arrangement variations.	Comply	See Ref. 20 and 21 for identification of module tests performed during Operability and Prudency testing. No module arrangement variations required in test specimen.
6.2.1.1	Test Specimen Hardware Arrangement Requirements. Descriptive information.	- - -	No requirements.
6.2.1.1.A	Seismic Testing. Hardware shall be arranged to maximize stress on the chassis and mountings.	Comply	See Ref. 24, Section 3.3.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.2.1.1.B	Environmental Testing. Modules shall be arranged to simulate maximum expected temperature rise across the chassis.	Comply	See Ref. 22, Section 3.4
6.2.2.	Test Specimen Application Program (TSAP) Configuration Requirements. Descriptive information.	- - -	No requirements.
6.2.2.A	TSAP Communication Commands. TSAP shall include a serial communication output sequence.	Comply	See Ref. 17, Section 34.
6.2.2.B	TSAP Programming. TSAP shall include program sequences to support Operability and Prudency testing.	Comply	See Ref. 20, 21 and 17.
6.2.2.C	TSAP Programming. TSAP shall include a program sequence to change the state of an output once each cycle.	Comply	See Ref. 17.
6.2.2.D	TSAP Programming. TSAP shall include any functions needed to support redundancy, and fault detection and failover.	Comply	No special TSAP functions required.
6.2.2.1	Coprocessor TSAP Requirements. If a coprocessor uses a high-level language, then it shall have its own TSAP which implements the given functions.	N/A	See Ref. 20. Section 1. Operation of Tricon coprocessors is invoked automatically during application program execution.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.2.3	Test Support Equipment Requirements. Test equipment to support Acceptance and Operability testing shall be provided.	Comply	See Ref. 14 and 42.
6.2.3.A	Test Support Equipment. Equipment shall include panels for connecting and simulating inputs and outputs.	Comply	See Ref. 14 and 42.
6.2.3.B	Test Support Equipment. Equipment shall include test and measurement equipment with required accuracy.	Comply	See Ref. 14 and 42.
6.2.3.C	Test Support Equipment. Equipment shall include special tools and devices needed to support testing.	Comply	See Ref. 14 and 42.
6.2.3.D	Test Support Equipment. All test equipment shall be controlled per IEEE 498.	Comply	Intent of IEEE 498 requirements for test equipment calibration control was met by following the requirements of QAM 11.0. Ref. 4 includes requirements for identification and control of calibrated test equipment during qualification testing.
6.3	Qualification Tests and Analysis Requirements. All PLC testing shall be performed on a calibrated system with all user setpoint values adjusted to default values.	Comply	See Ref. 19, Section 9.0. No user setpoints.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.3.1	Aging Requirements. Testing shall include environmental, electrostatic discharge (ESD), seismic, EMI/RFI and surge withstand testing. Environmental testing shall be performed first.	Comply	See Ref. 2, Section 5.
6.3.2	EMI/RFI Test Requirements. EMI/RFI testing to be performed as described in Section 4.3.7. Susceptibility tests to be performed at 25%, 50% and 75% of specified levels in addition to the specified levels.	Exception	See Ref. 25, Section 3.2 and Ref. 57. EMI/RFI testing performed per R.G. 1.180, R1. Testing performed at levels lower than specified levels only as needed to establish susceptibility threshold.
6.3.2.1	EMI/RFI Mounting Requirements. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	See Ref. 25, Section 3.3. Due to space limitations of NTS Labs EMI/RFI chamber, the test specimen was mounted less than six feet above the floor. The test specimen was mounted in a Rittal cabinet with sides and doors removed. Cabinets provided no significant shielding.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.3.3	Environmental Testing Requirements. Testing shall be performed using the temperature and relative humidity profile given in TR Figure 4-4. Margin shall be applied to maximum and minimum specified temperatures and humidities. Power sources shall be set to maximize heat dissipation. PLC shall be energized with TSAP operating. One-half of all discrete and relay outputs shall be on and energized to rated current. All analog outputs shall be set to one-half to two-thirds full scale output.	Comply	See Ref. 22, Sections 3.2, 3.4 and 3.5.
6.3.3.1	Environmental Test Mounting Requirements. PLC shall be mounted on a simple structure. Air temperature at bottom of chassis shall be monitored. No additional cooling fans shall be included.	Comply	See Ref. 22, Sections 3.3, 3.4 and 3.6.
6.3.4	Seismic Test Requirements. PLC shall be vibration aged using five OBEs with the RRS as shown in TR Figure 4-5 followed by an SSE with the RRS shown in TR Figure 4-5. Testing shall conform to IEEE 344. Tri-axial, random, multi-frequency tests shall be used. Repairs during testing shall conform to IEEE 344.	Comply	See Ref. 24, Sections 3.1, 3.2 and Step 10.2.10.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.3.4.1	Seismic Test Mounting Requirements. Test specimen shall be mounted per manufacturer's recommendations. Mounting structure shall have no resonances below 100 Hz. Most susceptible mounting configuration shall be tested. All mounting screws shall be torqued to known values.	Comply	See Ref. 24, Section 3.3.
6.3.4.2	Seismic Test Measurement Requirements. Relay contacts shall be monitored for chatter. One half of the relays shall be energized and on half de-energized. One quarter of the relays shall transition from ON to OFF and one quarter from OFF to ON during the tests. The PLC shall be powered with the TSAP operating. One half of the digital outputs shall be ON and loaded to their rated current. Power sources shall be at lower voltage and frequency limits. One or more response accelerometers shall be mounted on each chassis.	Clarification	See Ref. 24, Sections 3.4, 3.5, 3.6 and 3.7.
6.3.4.3	Seismic Test Performance Requirements. Seismic test shall include a resonance search, five OBE's, one SSE and an Operability test.	Comply	See Ref. 24, Sections 3.1, 3.3 and 4.4.
6.3.4.4	Seismic Test Spectrum Analysis Requirements. The test response spectrum from the control and specimen response accelerometers shall be reported at 1/2, 1, 2, 3 and 5% damping.	Comply	See Ref. 32.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.3.5	Surge Withstand Capability Testing. Surge testing shall be conducted per Section 4.6.2 and IEEE C62.45.	Comply	See Table Section 4.6.2.
6.3.5.1	Surge Withstand Test Mounting Requirements. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	See Ref. 27. Due to space limitations of NTS Labs EMI/RFI chamber, the test test specimen was mounted less than six feet above floor. Test specimen was mounted in a Rittal cabinet with the sides and doors removed.
6.3.6	Class 1E to Non-1E Isolation Testing. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	See Ref. 29. Due to space limitations of NTS Labs EMI/RFI chamber, the test specimen was mounted less than six feet above floor. Test specimen was mounted in a Rittal cabinet with the sides and doors removed.
6.4	Other Tests and Analysis. (section heading)	- - -	No requirements.
6.4.1	FMEA. An FMEA analysis of the PLC shall be performed.	Comply	See Ref. 10.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.4.2	Electrostatic Discharge (ESD) Testing Requirements. ESD testing of the PLC shall be performed per EPRI TR-102323.	Comply	See Ref 40, Section 7.0.
6.4.3	Power Quality Tolerance Requirements. Power quality tolerance testing shall be performed during acceptance testing, at the end of the elevated temperature test while still at high temperature and following seismic tests. The same AC source shall be connected to redundant power supplies during testing.	Comply	See Ref. 20, Section 10.
6.4.4	Requirements for Compliance to Specifications. Test instrumentation measurement accuracy shall be considered. Compliance to specifications shall be considered for each module or grouping of modules.	Comply	Where required, data analyses have been performed to provide for correction of the measured test data prior to comparison to acceptance criteria to account for the accuracies of the instruments used during testing. See Ref. 53
6.4.4.A	Environmental Test Compliance. Environmental Operability test results shall be evaluated for compliance to specifications.	Comply	See Ref. 35 and 52.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.4.4.B	Seismic Test Compliance. The seismic levels achieved during testing shall be used as the seismic withstand response spectrum.	Comply	See Ref. 36 and 52
6.4.4.C	Class 1E to Non-1E Test Compliance. Test levels shall be checked for compliance to Section 4.6.4 specifications.	Comply	See Ref. 41 and 52
6.4.4.D	Surge Withstand Test Compliance. Test levels shall be checked for compliance to Section 4.6.2 specifications.	Comply	See Ref. 39 and 52
6.4.4.E	EMI/RFI Test Compliance. PLC performance shall be checked for compliance to Section 4.3.7 specifications.	Comply	See Ref. 37 and 52
6.4.4.F	Power Quality Test Compliance. Results shall be evaluated for compliance to Sections 4.6.1 and 4.2.3.7 specifications.	Comply	See Ref. 52.
6.4.4.G	ASOA Test Compliance. Results shall be evaluated for compliance to Section 5.6 requirements.	Exception	See Ref. 2, Section 5. ASOA testing not performed.
6.4.4.H	Quality Assurance Program Compliance. Results of audits of manufacturer's QA Program shall be checked for compliance to Section 7 requirements.	Comply	Triconex is a 10CFR50, Appendix B supplier. The manufacturing and qualification processes are owned and controlled by Triconex. MPR was contracted by Triconex to perform some of the qualification tests. An audit of MPR was performed by Triconex. See Audit Report V0510.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.4.5	Human Factors. Descriptive Information.	- - -	No requirements.
6.5	Quality Assurance Measures Applied to Qualification Testing. Test program TSAP development, hardware procurement, test specimen chain of custody, and tests and data analysis shall meet the requirements of 10CFR50, Appendix B.	Comply	See Ref. 2, 4 and 5.
7	Quality Assurance. Descriptive information.	- - -	No requirements.
7.1	QA Overview. Descriptive information.	- - -	No requirements.
7.2	10CFR50 Appendix B Requirements for Safety-Related Systems. Descriptive information.	- - -	No requirements.
7.2.A	10CFR50 Applicability. Regulations apply to all qualification activities.	Comply	See Ref. 4, Section 3.
7.2.B	10CFR50 Applicability. Regulations apply to application specific activities.	N/A	Requirement applies to safety-related application of a PLC.

TRICON TOPICAL REPORT

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
7.2.C	10CFR50 Applicability. Regulations apply to PLC dedication activities.	N/A	Tricon PLC is manufactured under a 10CFR50 Appendix B program. Requirement applies to dedication of a commercial PLC.
7.2.D	10CFR50 Compliance. Quality processes other than 10CFR50 shall be shown to be commensurate with 10CFR50.	N/A	Tricon PLC is manufactured under a 10CFR50 Appendix B program.
7.2.E	10CFR50 Compliance. Qualifier shall perform audits to confirm that manufacturer's quality process has been applied to the PLC product.	Comply	Triconex is a 10CFR50, Appendix B supplier. The manufacturing and qualification processes are owned and controlled by Triconex. MPR was contracted by Triconex to perform some of the qualification tests. An audit of MPR was performed by Triconex. See Audit Report V0510.
7.2.F	10CFR50 Compliance. Audits performed against programs other than 10CFR50 shall demonstrate that the program process is commensurate with 10CFR50.	N/A	Tricon PLC is manufactured under a 10CFR50 program.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
7.2.G	V&V Program Evaluation. Qualifier shall evaluate the manufacturer's V&V program to the criteria in Section 7.4.	Comply	Triconex is a 10CFR50, Appendix B supplier. The manufacturing and qualification processes are owned and controlled by Triconex. V&V activities are performed by Triconex Engineering.
7.2.H	Qualification Test Witnessing. The qualifier shall have the right to witness qualification tests.	Comply	See Ref. 4 and 2. A Triconex Project Quality Assurance Engineer was permanently assigned to the qualification project. See the NQQP and Master Test Plan for PQAE responsibilities.
7.3	10CFR21 Compliance Requirements. Section lists 10CFR21 compliance requirements of a utility which applies the PLC in a safety-related application.	N/A	Requirement applies to safety-related application of a PLC.
	PLC manufacturer shall support problem reporting and tracking.	Comply	See Table Section 7.8.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
7.4	Verification and Validation Requirements. Qualifier shall evaluate the manufacturer's V&V process for software, firmware and software tools against IEEE 7-4.3.2 and IEEE 1012.	Comply	Triconex is a 10CFR50, Appendix B supplier. Triconex procedures ensure compliance with the applicable portions of IEEE 7-4.3.2 and IEEE 1012. See Ref. 4, 5 and 44
	If the manufacturer V&V processes do not meet requirements applicable to Nuclear Power Plants, then compensatory measures shall be implemented.	N/A	See above. Manufacturer V&V processes meet requirements applicable to Nuclear Power Plants.
7.5	Manufacturer Qualification Maintenance Throughout Product Life Cycle. (section heading)	- - -	No requirements.
7.5.1	Overview of Manufacturer Qualification Maintenance Throughout Product Life Cycle. Descriptive information.	- - -	No requirements.
7.5.2	Requirements for Manufacturer Qualification Maintenance Throughout Product Life Cycle. The qualifier shall obtain documentation confirming that the PLC manufacturer will ensure upward compatibility, maintain rigor of processes, commit to at least five year support for the qualified PLC configuration, and commit to six months notice before withdrawing product support.	Comply	Triconex is a 10CFR50, Appendix B supplier. The manufacturing and qualification processes are owned and controlled by Triconex.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
7.5.3	Life Cycle Support for Tools Requirement. PLC manufacturer shall ensure continued access to the same versions of application software development tools, or capability to reconstruct functionality with using revised tools.	Comply	See Ref. 5.
7.6	Compensatory Quality Activities for Legacy Software. (section heading)	- - -	No requirements.
7.6.1	Overview of Compensatory Quality Activities for Legacy Software. Descriptive information.	- - -	No requirements.
7.6.2	Requirements for Compensatory Quality Activities for Legacy Software. The qualifier may compensate for shortcomings in legacy software by evaluating documented operating experience in applications similar to nuclear safety related applications, and by performing tests of legacy software to confirm conformance to requirements. The manufacturer shall place legacy software under configuration control once baselined.	N/A	See Ref. 58. No legacy software is included in the qualification project scope.
7.7	Configuration Management. (section heading)	- - -	No requirements.
7.7.1	Configuration Management Overview. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
7.7.2	Hardware Configuration Management Requirements. The scope shall include revisions to module design, module component configuration, compatibility of revised modules with existing hardware, and manufacturer documentation.	Comply	See Ref. 5.
7.7.2.A	Hardware Configuration Management Review. Utility (and Qualifier) shall evaluate the manufacturer configuration management process for design revisions to NQA-1.	Comply	See Ref. 58. Configuration management reviews considered both hardware and software.
7.7.2.B	Hardware Configuration Management Review. Utility (and Qualifier) shall evaluate the manufacturer configuration management process for methods of identification of each constituent component within the PLC modules to NQA-1.	Comply	See Ref. 58. Configuration management reviews considered both hardware and software.
7.7.2.C	Hardware Configuration Management Review. Utility (and Qualifier) shall evaluate the manufacturer configuration management process for methods of document control to NQA-1.	Comply	See Ref. 58. Configuration management reviews considered both hardware and software.
7.7.3	Software Configuration Management Requirements. The scope of software configuration management includes creation and revision of firmware, runtime software libraries, software engineering tools, and documentation.	Comply	See Ref. 5.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
7.7.3.A	Software Configuration Management Review. Utility (and Qualifier) shall evaluate the manufacturer software configuration management process for definition of organization and responsibilities to Reg. Guide 1.169, Section C.	Comply	See Ref. 58.
7.7.3.B	Software Configuration Management Review. Utility (and Qualifier) shall evaluate the manufacturer software configuration management process for methods of configuration identification, control, status and audits to Reg. Guide 1.169, Section C.	Comply	See Ref. 52.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
7.7.3.C	Software Configuration Management Review. Utility (and Qualifier) shall evaluate the manufacturer configuration management process to ensure sub-tier suppliers maintain comparable levels of configuration management per Reg. Guide 1.169, Section C.	Comply	See Ref. 58.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
7.8	Problem Reporting/Tracking Requirements. PLC manufacturer shall maintain a problem reporting and tracking system that includes classification of problems, description of problems, identification of affected hardware, type of application, description of configuration, name of reporting site and means to contact site, type of site, and cumulative operating time of PLC when problem occurred. Manufacturer shall provide a mechanism for making this information available to all nuclear utility users.	Comply	Key Procedures: - QAM 14.0: Corrective Action - QAM 19.0: Servicing - QAM 13.3: 10CFR21 Reporting - QPM 14.0: QA Review Board - QPM 14.1: Customer Contacts - QPM 13.2: Product Discrepancies. - QPM 19.1 to 6: RMA Process Key Documents: - Product Discrepancy Reports - Customer Service Database - Customer System Config. Files - Product Alert Notices
8	Documentation. Descriptive information.	- - -	No requirements.
8.1	Equipment General Overview Document Requirements. Descriptive information.	- - -	No requirements.
8.1.A	Manufacturer Documentation. Documentation shall include a description of the PLC.	Comply	See Ref. 45, Chapter 1, 2, 3 and 4, Ref. 48, 49, and 50.
8.1.B	Manufacturer Documentation. Documentation shall include a description of the chassis interconnections.	Comply	See Ref. 45, Chapter 3.
8.1.C	Manufacturer Documentation. Documentation shall include a module overview and selection guide.	Comply	See Ref. 45, Chapter 2.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.1.D	Manufacturer Documentation. Documentation shall include a description of the overall I/O capacity and processing speeds.	Comply	See Ref. 45, Chapter 2.
8.1.E	Manufacturer Documentation. Documentation shall include installation information.	Comply	See Ref. 45, Chapter 3, Ref. 48 and 14.
8.1.F	Manufacturer Documentation. Documentation shall include handling and storage requirements.	Comply	See Ref. 45, Chapter 3.
8.1.G	Manufacturer Documentation. Documentation shall include a description of the self-diagnostics and redundancy features.	Comply	See Ref. 45, Chapter 2.
8.2	Equipment General Specifications Requirements. Manufacturer documentation shall provide general specifications for the PLC.	Comply	See Ref. 45 and 49.
8.3	Operator's Manual Requirements. Manufacturer documentation shall include information on operation of the PLC.	Comply	See Ref. 45 and 49.
8.4	Programmer's Manual Requirements. Manufacturer shall provide detailed information on the use of the functions available in the PLC processors.	Comply	See Ref. 46 and 47.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.4.A	Programmer's Manual Requirements. Manual shall include a summary and brief description of available functions.	Comply	See Ref. 46 and 47
8.4.B	Programmer's Manual Requirements. Manual shall include a detailed description of each function.	Comply	See Ref. 46 and 47
8.4.C	Programmer's Manual Requirements. Manual shall include examples of complex functions.	Comply	See Ref. 46, Section 2.
8.4.D	Programmer's Manual Requirements. Manual shall include limitations on use of functions.	Comply	See Ref. 46 and 47
8.4.E	Programmer's Manual Requirements. Manual shall include methods for resource management.	Comply	See Ref. 46 and 47
8.4.F	Programmer's Manual Requirements. Manual shall include a user manual for programming and debugging tools, and for any programming terminal.	Comply	See Ref. 46 and 47
8.4.G	Programmer's Manual Requirements. Manual shall include detailed information for creating user defined functions.	Comply	See Ref. 46 and 47
8.4.H	Programmer's Manual Requirements. Manual shall include a detailed description of operation of conditional statements.	Comply	See Ref. 46 and 47

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.4.I	Programmer's Manual Requirements. Manual shall include a description of limitations of PID and lead/lag functions.	Comply	See Ref. 46 and 47
8.4.J	Programmer's Manual Requirements. Manual shall include a description of interaction between main processor and I/O modules.	Comply	See Ref. 46 and 47
8.4.K	Programmer's Manual Requirements. Manual shall include a detailed description of interaction between the application program and redundancy features.	Comply	See Ref. 47.
8.4.L	Programmer's Manual Requirements. Manual shall include any software build procedures and software tools.	Comply	See Ref. 46 and 47
8.4.M	Programmer's Manual Requirements. Manual shall include a description of the operation of the executive.	Comply	See Ref. 46 and 47
8.4.N	Programmer's Manual Requirements. Manual shall include a description of data, data base and configuration management.	Comply	See Ref. 46 and 47
8.4.O	Programmer's Manual Requirements. Manual shall include a description of operation and use of self-diagnostics.	Comply	See Ref. 47.
8.4.P	Programmer's Manual Requirements. Manual shall include a manual for coprocessor programming.	N/A	Coprocessor operation is invoked automatically.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.5	Equipment Maintenance Manual Requirements. Manufacturer documentation shall contain information for calibration, trouble shooting, maintenance, required special tools or software, and communication protocols.	Comply	See Ref. 45, Chapter 4, and Ref. 50
	Manufacturer documentation shall include results of component aging analysis.	Comply	See this report, Section 4.12.
8.6	Qualification Documentation Requirements. Qualifier shall provide and submit all qualification documentation to customer utility for review and approval.	Comply	See Ref. 3.
8.6.1	Programmatic Documentation Requirements. Descriptive information.	- - -	No requirements.
8.6.1.A	Programmatic Documentation. A test plan shall be prepared which includes test plans for environmental, seismic, surge, Class 1E to Non-1E, EMI/RFI, availability/reliability, FMEA and ASOA qualification activities.	Comply	See Ref. 1 and 2.

TRICON TOPICAL REPORT

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.6.1.B	Programmatic Documentation. Test specifications shall be prepared which include equipment identifications, interfaces and service conditions.	Comply	See Ref. 2 and 3.
8.6.1.C	Programmatic Documentation. Procedures shall be prepared for qualification testing.	Comply	See Ref. 2, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 29, and 65.
8.6.1.D	Programmatic Documentation. Test reports shall be prepared for each qualification test performed.	Comply	See Ref., 34, 35, 36, 37, 38, 39, 40 41, 53, 64, 66, 67 and 68.
8.6.1.E	Programmatic Documentation. Reports on audits performed on the manufacturer shall be prepared.	Comply	Triconex is a 10CFR50, Appendix B supplier. The manufacturing and qualification processes are owned and controlled by Triconex. MPR was contracted by Triconex to perform some of the qualification tests. An audit of MPR was performed by Triconex. See Audit Report V0510.
8.6.1.F	Programmatic Documentation. Reports on design evaluations shall be prepared.	Comply	See Ref. 8. Design evaluations include interface cable similarity analysis.
8.6.2	Technical Items and Acceptance Criteria Documentation Requirements. Descriptive information.	---	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.6.2.A	Technical Items Documentation. Documentation shall include test specimen requirements.	Comply	See Ref. 1.
8.6.2.B	Technical Items Documentation. Documentation shall include test specimen purchasing records.	N/A	See Ref. 3 .
8.6.2.C	Technical Items Documentation. Documentation shall include TSAP development documentation.	Comply	See Ref., 17, 18, 4344, 64, 66, 67, and 68.
8.6.2.D	Technical Items Documentation. See Sections 8.8, 8.9, 8.10, 8.12 and 8.13.	- - -	No requirements.
8.6.2.E	Technical Items Documentation. See Section 8.14.	- - -	No requirements.
8.6.3	Application Guide Documentation Requirements. A qualification summary document shall be provided.	Comply	See Appendix B of this report.
8.6.3.A	Application Guide. Guide shall include results of environmental Operability testing to support each specific safety related application.	Comply	See Ref. 35, 52, and 53, and Appendix B of this report.
8.6.3.B	Application Guide. Guide shall include results of seismic testing including seismic withstand capability for all damping values used in test data analysis.	Comply	See Ref. 36 and Appendix B of this report.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.6.3.C	Application Guide. Guide shall include results of Class 1E to Non-1E isolation testing.	Comply	See Ref. 41 and Appendix B of this report.
8.6.3.D	Application Guide. Guide shall include results of surge withstand testing.	Comply	See Ref. 39 and 57, and Appendix B of this report.
8.6.3.E	Application Guide. Guide shall include results of EMI/RFI testing.	Comply	See Ref. 37 and 57, and Appendix B of this report.
8.6.3.F	Application Guide. Guide shall include results of power quality testing.	Comply	See Ref. 52 and Appendix B of this report.
8.6.3.G	Application Guide. Guide shall describe any combination of software objects or special purpose objects created to support testing.	N/A	No software objects or special purpose objects were used in testing.
8.6.3.H	Application Guide. Guide shall include a description of the as-tested PLC configuration.	Comply	Appendix B of this report.
8.6.3.I	Application Guide. Guide shall include a description of the executive software and software tools revision levels included in qualification.	Comply	See Ref. 3 and Appendix B of this report.
8.6.3.J	Application Guide. Guide shall include a description of the as-tested PLC configuration.	Comply	See Ref. 42 and Appendix B of this report.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.6.3.K	Application Guide. Guide shall include a summary of the FMEA and availability analysis.	Comply	See Ref. 9, 10 and Appendix B of this report.
8.6.3.L	Application Guide. Guide shall include the setpoint analysis support document.	Comply	See Ref. 9 and Appendix B of this report.
8.6.3.M	Application Guide. Guide shall include information from manufacturer audits and surveys applicable to future purchasing.	Comply	See Appendix B of this report.
8.6.3.N	Application Guide. Guide shall include a description of the redundancy features include in qualification.	Comply	See Appendix B of this report.
8.6.3.O	Application Guide. Guide shall include a description of external devices included in qualification.	Comply	See Appendix B of this report.
8.6.3.P	Application Guide. Guide shall include a description of the PLC configuration management methods.	Comply	See Appendix B of this report.
8.6.3.Q	Application Guide. Guide shall include a summary of the component aging analysis.	Comply	See Appendix B of this report.
8.6.3.R	Application Guide. Guide shall include a description of seismic mounting methods.	Comply	See Ref. 14 and Appendix B of this report.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.6.3.S	Application Guide. Guide shall include a description of qualification envelopes for specific modules if different from the overall envelope.	Comply	Appendix B of this report.
8.6.3.T	Application Guide. Guide shall include a description of any application hardware or software features that are assumed in order to meet qualification requirements.	Comply	See Appendix B of this report.
8.6.4	Supporting Analyses Documentation Requirements. Documentation shall be provided of the FMEA and Availability/Reliability Analyses.	Comply	See Ref. 10 and 11.
8.6.5	Class 1E to Non-1E Isolation Test Plan. A Class 1E to Non-1E Isolation test plan and report shall be provided. The test plan shall be reviewed and approved by the utility.	Comply	See Ref. 2, 29 and 41.
8.7	V&V Documentation Requirements. Descriptive information.	---	No requirements.
8.7.A	V&V Documentation. Documentation shall include a software quality assurance plan.	Comply	See Ref. 5.
8.7.B	V&V Documentation. Documentation shall include a software requirements specification.	Comply	See Ref. 17.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.7.C	V&V Documentation. Documentation shall include a software design description.	Comply	See Ref. 18.
8.7.D	V&V Documentation. Documentation shall include a software V&V plan.	Comply	See Ref. 5.
8.7.E	V&V Documentation. Documentation shall include a software V&V report.	Comply	See Ref. 44.
8.7.F	V&V Documentation. Documentation shall include software user documentation.	Comply	See Ref. 46.
8.7.G	V&V Documentation. Documentation shall include a software configuration management plan.	Comply	See Ref. 5.
8.8	System Description Requirements. A test specimen hardware and software description document shall be provided.	Comply	See Ref. 42.
8.9	Critical Characteristics Listing Requirement. A critical characteristics listing document shall be provided.	N/A	Triconex is a 10CFR50, Appendix B supplier. Commercial dedication of Tricon PLC is not required.
8.10	System Drawing Requirements. A set of test specimen hardware, software and configuration drawings shall be provided.	Comply	See Ref. 14.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.10.A	System Drawing Requirements. Drawings shall include a functional description of the test specimen.	Comply	See Ref. 15, Functional Drawings.
8.10.B	System Drawing Requirements. Drawings shall include a schematic of the test specimen.	Comply	See Ref. 12 and 14, Wiring Schedule and System Drawings.
8.10.C	System Drawing Requirements. Drawings shall include diagrams that define the TSAP.	Comply	See Ref. 15, Functional Diagrams.
8.10.D	System Drawing Requirements. Drawings shall show test specimen wiring, power distribution and grounding.	Comply	See Ref. 12 and 14, Wiring Schedule and System Drawings.
8.10.E	System Drawing Requirements. Drawings shall show layout of test specimen chassis, modules and qualification test fixtures.	Comply	See Ref. 12 and 14, Wiring Schedule and System Drawings.
8.10.F	System Drawing Requirements. Drawings shall show test specimen mounting and mounting fixtures, including special installation requirements.	Comply	See Ref. 12 and 14, Wiring Schedule and System Drawings.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.11	System Software/Hardware Configuration Document Requirements. Software and hardware configuration used for qualification testing shall be documented, including identification and revision of executive software, module firmware, software tools, downloadable PLC executive packages, and the TSAP (including printout). The identification, revision level and serial number of hardware shall be documented.	Comply	See Ref. 3.
8.12	System Database Documentation Requirements. The TSAP database used for qualification testing shall be documented.	Comply	See Ref. 15, and 18.
8.13	System Setup/Calibration/Checkout Procedure Requirements. All setup, calibration and checkout procedures used during qualification shall be documented.	Comply	See Ref. 19.
8.14	System Test Documentation Requirements. A test plan and test report shall be provided covering qualification Operability testing. The documents shall include test requirements, acceptance criteria, sequence of testing, data recording methods, test equipment requirements and a test data summary.	Comply	See Ref. 2, 20 and 53.
8.15	Manufacturer's Quality Documentation Requirements. The manufacturer shall provide its Quality Assurance Plan.	Comply	See Ref. 4 and 5.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.16	Manufacturer's Certifications Requirements. Manufacturer shall provide certificates of conformance for all test specimen hardware.	Comply	See Ref. 56.

Table Notes:

1. The requirement summaries are intended to paraphrase the basic hardware, software or programmatic requirements, and may not include all of the detailed requirement text given in the corresponding section of TR-107330. The statement of compliance for each requirement given in the table pertains to the detailed requirements as given in the corresponding section of EPRI TR-107330.

2. Definition of Compliance Terms:

---	The referenced TR-107330 section does not include any specific PLC requirements. No statement of compliance is necessary.
N/A	The TR-107330 requirement is not applicable to the specific design of the Tricon PLC. No statement of compliance is necessary. The Comments column provides a basis for the requirement being not applicable.
Comply	The Tricon PLC design fully complies with the corresponding requirement as given in the applicable section of EPRI TR-107330.
Exception	The Tricon PLC design does not fully comply with the corresponding requirement as given in the applicable section of EPRI TR-107330. The Comments column provides a disposition of the compliance exception.

3. Comments provide traceability of compliance to requirements through identified references. See the List of References following these Table Notes.

List of References:

Note: Unless indicated, applicable revision levels of all Triconex documents, reports, procedures and drawings were per the current revision of Triconex Document No. 9600164-540, Master Configuration List upon completion of the Nuclear Qualification Project. Subsequent revisions are maintained in the Triconex R&D Engineering database (Agile).

1. EPRI Technical Report TR-107330, Final Report dated December, 1996, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants.

2. Triconex Document No. 9600164-500, Tricon Nuclear Qualification Program Master Test Plan (MTP).

3. Triconex Document No. 9600164-540, Tricon Nuclear Qualification Program Master Configuration List (MCL).

4. Triconex Document No. 9600164-002, Tricon Nuclear Qualification Quality Plan (NQQP)

5. Triconex Document No. 9600164-537, Tricon Nuclear Qualification Program Software Quality Assurance Plan (SQAP).

6. Triconex Document No. 9600164-730, Analog Input/Output Machine Count Calculations.

7. Triconex Document No. 9600164-731, Maximum Response Time Calculations.

8. Triconex Document No. 9600164-538, External Termination Panel Interface Cable Similarity Analysis.

9. Triconex Document No. 9600164-534, Tricon System Accuracy Specifications.

10. Triconex Document No. 9600164-531, Failure Modes and Effects Analysis.

11. Triconex Document No. 9600164-532, Reliability/Availability Study.

12. Triconex Document No. 9600164-700, Wiring Schedule.

13. Triconex Drawing No. 9600164-100 to 103 & 9600164-105, System Drawings.

14. Triconex Drawing No. 9600164-200 to 207, System Drawings.

15. Triconex Drawing No. 9600164-600 to 614, Function Diagrams.

16. Triconex Document No. 9600121-001, Tricon System Test Requirements Specification.

17. Triconex Document No. 9600164-517, TSAP Software Requirements Specification.

18. Triconex Document No. 9600164-518, TSAP Software Design Description.

19. Triconex Document No. 9600164-502, System Setup & Checkout Procedure.

20. Triconex Document No. 9600164-503, Operability Test Procedure.

21. Triconex Document No. 9600164-504, Prudency Test Procedure.

22. Triconex Document No. 9600164-506, Environmental Test Procedure.

23. Triconex Document No. 9600164-511, Radiation Exposure Test Procedure.

24. Triconex Document No. 9600164-507, Seismic Test Procedure.

25. Triconex Document No. 9600164-510, EMI/RFI Test Procedure.

26. Triconex Document No. 9600164-514, EFT Test Procedure.

27. Triconex Document No. 9600164-508, Surge Withstand Test Procedure.

28. Triconex Document No. 9600164-512, ESD Test Procedure.

29. Triconex Document No. 9600164-509, Class 1E Isolation Test Procedure.

30. NTS Document No. TP62987-07N-ENV, Procedure for Environmental Qualification.

31. NTS Document No. TP62987-07N-RAD, Procedure for Radiation Testing.

32. NTS Document No. TP62987-07N-SEI, Procedure for Seismic Qualification.

33. NTS Document No. TP62987-07N-EMI, Procedure for EMI Qualification.

34. Triconex Document No. 9600164-512, Tricon Nuclear Qualification Program Radiation Exposure Test Report.

35. Triconex Document No. 9600164-525, Tricon Nuclear Qualification Program Environmental Test Report.

36. Triconex Document No. 9600164-526, Tricon Nuclear Qualification Program Seismic Test Report.

37. Triconex Document No. 9600164-527, Tricon Nuclear Qualification Program EMI/RFI Test Report.

38. Triconex Document No. 9600164-521, Tricon Nuclear Qualification Program EFT Test Report.

39. Triconex Document No. 9600164-528, Tricon Nuclear Qualification Program Surge Withstand Test Report.

40. Triconex Document No. 9600164-522, Tricon Nuclear Qualification Program ESD Test Report.

41. Triconex Document No. 9600164-529, Tricon Nuclear Qualification Program Class 1E to Non 1E Isolation Test Report.

42. Triconex Document No. 9600164-541, Tricon Nuclear Qualification Program System Description.

43. Triconex Document No. 9600164-513, TSAP Software Verification and Validation Plan.

44. Triconex Document No. 9600164-536, TSAP Final V&V Report.

45. Planning and Installation Guide for Tricon v9-v10 Systems, Part No. 9700077-002.

46. Tristation 1131 Developer's Workbench, Document No. 9700100-003.

47. Tristation 1131 Developer's Workbench Libraries Reference, TS 1131 Version 4.1, Document No. 9700098-003.

48. Tricon Version 9-10 Systems Field Termination Guide, Part No. 9700052-012.

49. Tricon Version 9-10 System Technical Product Guide, Part No. 9791007-013.

50. Tricon Version 9-10 System Communication Guide, Part No. 9700088-001.

51. Tricon V9-10 System, Safety Consideration Guide, Part No. 9700097-001.

52. Triconex Document No. 9600164-545, Equipment Qualification Summary Report.

53. Triconex Document No. 9600164-566, Performance Proof Operability Test Report.

54. Triconex Corporation, Quality Assurance Manual Date 06/07/2007.

55. . Triconex Part No. 1600083-200 document attachment, 7B34_analog.pdf.

56. Triconex Document No. 9600164-540, Master Configuration List.

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

58. Triconex Document No. 9600164-535, Software Qualification Report.

59. SOE Recorder User's Guide, v4.0, Document Number 9720081-003.

60. Enhanced Diagnostics Monitor v2.0 User's Guide, Document Number 9720107-002.

61. Triconex Document Number 9600164-538, External Termination Panel Interface Cable Assembly Similarity Analysis.

62. Triconex Corporation Quality Assurance Manual.

63. Triconex Engineering Procedure EDM 75.00, Nuclear Product Qualification.

64. Triconex Document No. 9600164-573, Performance Proof Prudency Test Report.

65. Triconex Document No. 9600164-716, TSAP Software Validation Test Procedure.

66. Triconex Document No. 9600164-570, Pre-Qualification Prudency Test Report.

67. Triconex Document No. 9600164-713, V&V Test Phase Summary Report.

68. Triconex Document No. 9600164-717, Software Validation Test Report.

invensys
Operations Management

TRICONEX TOPICAL REPORT

APPLICATION GUIDE

Document No.: 7286-545-1

Revision 2

Appendix B

TRICON TOPICAL REPORT

TABLE OF CONTENTS

SECTION **PAGE**

1.0 INTRODUCTION 4

2.0 SYSTEM CAPABILITIES 5
2.1 The Tricon Programmable Logic Controller 5
2.2 Key System Features 5

3.0 SYSTEM DESIGN GUIDANCE 7
3.1 Power 7
3.2 Connection to Plant Instrumentation and Controls 8
3.3 Tricon Chassis Configuration 9
3.4 Tricon Communications Interfaces 11
3.5 Failure Analysis and SAR Chapter 15 12
3.6 Diversity and Defense-in-Depth 14
3.6.1 Licensing Criteria 15
3.6.2 Defense-In-Depth and Diversity Requirements 16
3.6.3 Diversity Implementation 18
3.7 Setpoint Accuracy Calculations 21
3.8 Bypass and Indication 25
3.9 Self-Test Capabilities 26
3.10 Surveillance Capabilities 28
3.11 Operational Constraints 31
3.12 Error Reporting and Tracking 32

4.0 ENVIRONMENT AND LOCATION 33
4.1 Mounting 33
4.2 Temperature and Humidity 33
4.3 Heat Loads in Cabinets and Rooms 34
4.4 Seismic Acceleration Limits 34
4.5 Radiation Fields 37
4.6 EMI/RFI Compatibility 37
4.7 Electrical Fast Transient Testing 44
4.8 Surge Withstand Testing 44
4.9 Electrostatic Discharge (ESD) Testing 45
4.10 Isolation Testing 45
4.11 Operability Testing 46

5.0 PROGRAMMING GUIDANCE 48
5.1 Cycle time 48
5.2 Software Quality Assurance Processes 49
5.3 Guidance for Application Programming 50
5.4 Loss of Power Fault Indication 53
5.5 Communication with External Systems 54
5.6 Peer-to-Peer Communication 55
5.7 Communication Application Safety Layer 56

6.0 INSTALLATION, COMMISSIONING, AND MAINTENANCE 58
6.1 Required testing 58
6.2 Operations Procedures 58
6.3 Maintenance Procedures 59
6.4 Application Program Maintenance Procedures 60
6.5 Maintenance and Bypass Capabilities 61

7.0 REFERENCES 64

TRICON TOPICAL REPORT

1.0 INTRODUCTION

This report provides guidelines and qualification limitations for applying the Triconex Tricon Programmable Logic Controller (PLC) in nuclear power plant systems classified as Safety Related and Important to Safety. The guidance provided in this document is intended to simplify use and application of the Tricon by consolidating design requirements, operational limitations, and other important data derived from the generic qualification program. Additional requirements and limitations may apply to a plant-specific application.

Some of the guidance provided in this document is not necessarily specific to the Tricon PLC or TriStation 1131 Developer's Workstation. In these cases, the guidance provided is generic and should be applied to any installation involving digital equipment. Installation practices can create long term problems, which are often ascribed to software. Correct initial system installation will enhance reliable system operation. In that respect, the generic guidance provided should be considered appropriate for use with any PLC in a safety critical application.

Guidelines are provided for design, licensing, installation, operation, and maintenance of the system. Many of the guidelines in this document are interrelated. As an example, consider generation of fault alarms. The fault alarm has implications in design, operating and maintenance procedures, plant interface, main control room impacts, and several other seemingly unrelated topics, including system power supply. Therefore, the guidelines should be considered as a whole, rather than in separated, individual pieces.

In addition to the guidelines presented in this document, the standard manufacturer's recommendations provided by Triconex for application of the Tricon should be followed. These are documented in the Triconex Planning and Installation Guide (Reference 7.13).

2.0 SYSTEM CAPABILITIES

2.1 The Tricon Programmable Logic Controller

The Tricon Programmable Logic Controller (PLC) with the TriStation 1131 Development Workstation provides a suitable platform for implementation of safety-critical digital Instrumentation and Control systems. The Triple Modular Redundant design of the Tricon PLC has been shown to provide a high degree of reliability in addition to high availability. These characteristics make the Tricon platform particularly suited to nuclear safety-related applications. The TriStation 1131 Development Workstation, when used as described in this guide, provides a suitable means for developing and maintaining application software and configuring the Tricon system.

A detailed description of the Tricon PLC and TriStation 1131 is provided in Section 4.1 of the Qualification Summary Report (Reference 7.18).

Hardware type tests were performed with Version 10.2.1 of the Tricon system. However, the specific version of the Tricon system supplied for nuclear plant applications may be a later version. If versions later than Version 10.2.1 are supplied for nuclear safety-related applications, the qualification basis described in this report will be augmented with technical evaluations or additional testing based on the requirements established in Section 6.8 of IEEE Standard 323-1974.

2.2 Key System Features

This section provides an overview of the key features of the Tricon PLC.

The Tricon PLC is constructed of individual modules, installed in rack mount chassis. There are certain modules that are required, such as power supplies and Main Processors. The remaining modules, number of chassis required, and locations of the modules are configurable.

The Tricon PLC is designed as a Triple Modular Redundant (TMR) system and has been demonstrated to be resistant to single, active failure mechanisms. The power supplies are dual redundant, with each supply capable of providing all power requirements to the chassis in which it is installed. The backplane communication paths are triple redundant. The input and output modules are triple redundant internal to the module. Three separate Main Processor modules are required. Communication modules to external systems may be single train or dual redundant.

TRICON TOPICAL REPORT

The Tricon PLC was designed as a single division Emergency Shutdown System or Safety Instrumentation System. Industries other than nuclear make use of only a single division safety system. The Tricon will be used in the nuclear industry in a mode retaining the existing redundancy provided in separated channels, divisions, and trains.

The Tricon PLC provides conservative alarming of internal faults. Rather than fail to identify internal faults, the Tricon identifies possible faults for resolution by maintenance. The Tricon does not attempt a program-based determination of the safety consequences of a given fault condition.

Faults on a Tricon PLC are not indicators of system failure. Rather, the system continues to operate through faults, based on the TMR design. Faults are indicators that maintenance action is required to restore complete redundancy. There are no known, identified, active single points of failure within a Tricon PLC except Software Common Cause Failure. While the Tricon PLC can tolerate a single fault on every module and continue to implement the application program correctly, prompt repair decreases the already remote possibility of multiple faults combining into a failure. From review of the system, there is a large class of faults where multiple faults may exist on a single module with no adverse effect on system operability.

The Tricon PLC uses triplicated, isolated analog and digital inputs, sampled from a single input point. Each input is voted prior to use in the application software. The median analog value is selected for use. Faults on any single portion of the input circuit will be alarmed and that faulted input will not be used by the application software.

The Tricon PLC qualified digital outputs provide quad voting circuits on each output. Each output is voted from the three separate output channels. The supervised digital outputs check for current flow and appropriate voltage levels. Output voter diagnostics are performed to detect failures in the voter circuit and to detect shorts or opens on the expected field load to be driven by the output. Faults will be alarmed.

The Tricon PLC analog outputs provide three separate digital to analog conversion channels on each point. The current flow from each analog output is measured. Faults in a given digital to analog converter channel will be alarmed and the output module then copes with the fault.

A list of qualified Tricon hardware is provided in the main body of this Summary Report.

The Tricon PLC requires an installation design that separates and isolates the 24 V dc field power supplies to the discrete input/output (I/O) and analog I/O module circuits.

3.0 SYSTEM DESIGN GUIDANCE

The Triconex technical manuals, including the planning and installation guides, provide technical information on the application of the Tricon PLC; use of the TriStation 1131 Programmer's Development Workstation; and the operation and maintenance of the resulting system. This Application Guide supplements the requirement in those documents as appropriate for nuclear safety systems. In addition, certain TÜV Rheinland Restrictions and Requirements for all safety, Emergency Shutdown (ESD), and Fire and Gas systems have been modified to fit the expected applications in the nuclear power industry and are incorporated in this guidance document.

For applications in industries other than nuclear power, only one Tricon PLC is used to provide the safety system functionality. In the nuclear power industry, the Tricon PLC will be used as a replacement for the existing channels, divisions, and trains of safety systems, with one or more PLCs being used to replace a single channel, division, or train. Thus, each protection channel, division, or train will retain the high degree of independence required by IEEE Standard 603. This degree of redundancy results in lessened restrictions from those necessary in a single channel, division, or train safety system.

3.1 Power

Power supply design considerations that are specific to the Tricon system include the following:

A. Redundant chassis power supplies shall be installed in each chassis. Redundant input power must be provided to the redundant chassis power supplies installed in each chassis. With this configuration, failure of one logic power supply, or the power to that supply, does not affect system operation. The single failure of the power supply will be annunciated.

B. The 120 V ac chassis power supply has been validated to operate successfully over input ranges of 85 V ac to 140 V ac and 47 Hz to 63 Hz. The 230 V ac chassis power supply has been validated to operate successfully over input ranges of 185 V ac to 285 V ac and 47 Hz to 63 Hz. The 24 V dc chassis power supplies have been validated to operate successfully over input ranges of 22 V dc to 31 V dc.

C. The 120 V ac chassis power supplies provide hold-up times on power interrupt of at least 40 milliseconds when installed as the only chassis power supply or when installed in combination with a second chassis power supply. The 24 V dc chassis power supplies provide no hold-up on power interruption. Note that with

redundant power supplies, hold up time is important only for power interruptions with the redundant power source turned off.

D. Modules must be loaded into chassis in a manner that does not overload the chassis logic power supplies. Design methods and tables are provided in the Triconex Planning and Installation Guide for assuring proper, conservative power supply loading.

In addition to these Tricon-specific considerations, the field power supplies that are required to activate critical outputs and source safety-critical inputs must be redundant. These external supplies are separate from the Tricon chassis power supplies. The field power supply redundancy is based on the General Design Criteria requirement for single failure tolerance in nuclear safety related applications. Failure of a single, non-redundant supply would render most safety related applications of a single train inoperable.

3.2 Connection to Plant Instrumentation and Controls

Plant instrumentation and control wiring and interface design considerations that are specific to the Tricon system include the following:

A. The PLC must be wired and grounded according to the procedures defined in the Triconex Planning and Installation manuals, Triconex Part Number 9720077-012.

B. If redundant inputs are provided to a single Tricon, the inputs should not be terminated on a single standard Tricon External Termination Assembly (ETA) and thus read by a single input module. If redundant outputs are provided from a single Tricon, the outputs should not be terminated on a single ETA and thus driven by a single output module. The ETA and cable between the ETA and the Tricon chassis are not single failure tolerant.

C. The qualified module list, provided in the Qualification Summary Report, includes:

- Tricon Communications Module (TCM) providing ModBus and Peer-to-Peer capabilities.
- Digital input modules for 24, 48, and 115 volts ac and dc.
- Digital output modules for 24, 48, and 120 volts dc and 115 volts ac.

- A relay output module for interface to non-safety related systems such as annunciators.
- Analog input modules for 0-5 volt or -5 to +5 volt differential, 0-10 volt, and thermocouple input signals.
- Type J, K, T, and E thermocouples may be directly interfaced to thermocouple input modules, which provide cold junction compensated temperatures in Celsius or Fahrenheit.
- RTD input signals are processed through an external converter, which provides a 0-5 volt signals to a standard 0-5 volt analog input module.
- Thermocouples may be input to standard analog voltage input modules after conditioning through qualified signal conditioning modules.
- Analog output modules for 4-20 ma dc.
- A pulse input module optimized for use with non-amplified magnetic speed sensors common on rotating equipment such as turbines or compressors.

D. Qualified External Termination Assemblies with prefabricated interface cables are available for each module. The qualified version of the ETAs provides screw terminal mounting capabilities for field wiring.

E. Alarm contact outputs are provided on each chassis. These alarms, or a logical and fault tolerant equivalent, shall be wired to appropriate control room annunciation. Faults within the Tricon shall be annunciated to the Operations staff for resolution. The alarm contacts on the power supply modules provide a single summed output for system failure indication.

In addition, to these Tricon-specific considerations, all wiring supplied to the PLC must satisfy the requirements for protective separation according to applicable IEEE standards.

3.3 Tricon Chassis Configuration

A. The Tricon chassis is not explicitly protected against dust, corrosive atmospheres, or falling debris. The user must provide atmospheric and airborne particle protection by mounting the equipment inside an appropriate enclosure.

B. The Tricon must be installed in a mild environment. The Triconex Planning and Installation Guide provides additional installation specifications.

C. The Tricon can support from one to 15 chassis. Module locations and types are defined in the Triconex Planning and Installation Guide.

D. Three types of chassis are provided. Each of the chassis provides logical slots for Tricon modules.

1. Each system must include one Main Chassis for the Main Processors.

2. An Expansion Chassis is available for housing additional modules.

3. A pair of RXM Chassis is required at each end of the fiber optic links to house the triplicated Remote Extender Modules (RXM). The RXM may be used as a means to extend the distance between chassis locations or provide qualified isolation between 1E and non-1E equipment.

E. The Tricon chassis may be interconnected using either standard bus cables or fiber optic cables. In both cases, the connections made are triplicated. General guidelines for the number of chassis and the maximum lengths of standard interconnecting cabling are provided in the Triconex Tricon Planning and Installation Guide (Reference 7.13).

F. In order to minimize the possibility of total loss of communication, the triplicated chassis interconnection cabling should not be run together outside the cabinet. For maximum protection from failure, the chassis interconnection cabling should be run through diverse routes inside the cabinet as well, to the extent possible.

G. If the expansion chassis are connected with standard bus cables, the total length of cable installed to daisy chain up to 15 chassis together may be no longer than 30 meters or 100 feet.

H. If the expansion chassis are connected over fiber optic links, the minimum number of chassis required is three, because the fiber optic links cannot be installed in the Main Chassis. An RXM Chassis must be installed near the Main Chassis for the fiber optic link modules to communicate with the second RXM Chassis. Up to 12 kilometers or 7.5 miles of fiber optic cable may be used between the two RXM chassis. The first RXM Chassis is connected to the Main Chassis using standard bus cables.

I. Triconex provides guidance on the application restrictions that exist for system configuration. These include module configuration to remain within chassis logic power supply limits, and locations where communication modules can be installed. The complete list of standard guidance and restrictions for system

configuration is provided in the Triconex Planning and Installation Guide (Reference 7.13).

3.4 Tricon Communications Interfaces

Communication interface design considerations that are specific to the Tricon system include the following:

A. Communications interfaces can be installed only in the Main Chassis or in the first Expansion Chassis connected to the Main Chassis. If a second chassis is required, the second chassis must be an I/O Expansion Chassis or a Primary RXM Chassis.

B. The communication between the TriStation 1131 PC and the Tricon PLC shall be over a communication link using the IEEE Standard 802.3 protocol, to gain the protection of CRC checks on transmitted messages. In order to provide an 802.3 port, a TCM communication module must be installed.

C. Peer-to-peer communication is allowed between Tricon PLCs, as long as the restrictions provided in Section D, Peer-to-Peer Networking, of this guideline are incorporated in the design.

D. A local non-safety related display panel is recommended, located close to the Tricon. This panel is provided for technician and engineering use during calibration of external devices, diagnostics, and troubleshooting.

E. For communications between a Tricon controller(s) and a safety-related display unit(s), an application layer protocol is required to ensure end -to-end data integrity. The Safety Application Protocol (SAP) is an application layer protocol that allows safety-related communication between a Tricon system and a safety-related display unit. The Tricon controller application and the safety-related display unit use the SAP to exchange safety-critical data. The SAP utilizes a NIST-published cryptographic algorithm, data keys, sequence numbers, etc., for detecting communication errors such as corrupted messages, duplicated messages, out-of-sequence messages, etc.

   Additional guidance is provided in Section 5.7.

In addition, while it might be desirable under certain circumstances to perform all Tricon configuration activities with TriStation 1131 from a single communication network node, the separation and independence requirements established in IEEE Standard 384-1992 discourages cabling across protection channels, train divisions,

cabling, or trains. The interconnections required to provide this functionality with TriStation 1131 would interconnect all Tricon PLCs in all divisions, channels, or trains to a single location, which is not acceptable. For network architectures involving interdivisional communications with non-safety devices (e.g., non-safety video display units), verified conformance to the guidance in Interim Staff Guidance DI&C-ISG-04, Highly Integrated Control Rooms – Communications Issues (Reference7.7), is strongly recommended. Conformance to DI&C-ISG-04 may require supplemental administrative and physical access controls at the installed location or site.

Therefore, to prevent inadvertent configuration changes, communications interfaces should be designed to preclude a TriStation 1131 PC from communicating simultaneously with more than one division, channel, or train of Tricon PLCs. Any network cabling should be implemented in a manner to assure that multiple division, channel, or train connections are not possible. This will help assure that only the desired division, channel, or train is modified. The network cabling for TriStation 1131 should not cross division, channel, or train boundaries.

3.5 Failure Analysis and SAR Chapter 15

A. A Failure Modes and Effects Analysis (FMEA) was performed as part of the qualification effort. Triconex Report 9600164-531 (Reference 7.21) provides the FMEA in tabular format. Results of this FEMA show that only a few vulnerabilities in the Triconex design. Proper system design, installation, and maintenance must address these vulnerabilities. These include the following:

- Loss of redundant power supplied to the Tricon, which is indicated by fail-safe operation of all outputs and of the alarm contacts on each power supply.
- Loss of external power for discrete or analog voltage inputs, which can be detected through system wiring (as a discrete or analog input wired to the required power and alarmed when off or outside user specified tolerances).
- Positioning the Main Chassis Control keyswitch to the STOP position. This will be disabled in the application software configuration.
- Internal shorts or opens on all logic power supply rails, all TriBUS serial links, or all I/O Bus serial communication links inside any of the chassis, or all RXM communication links between chassis, which will result in fail-safe operation of all Tricon outputs in and downstream of the affected chassis. The Main Chassis Power Module Alarm circuits will also be alarmed.

- Faults in all three Main Processor modules, which is indicated by fail-safe operation of all outputs and of the alarm contacts on each power supply.

- Opens or shorts in the cables between any chassis and an External Termination Assembly will result in loss of all signals input from or output to that ETA.

- Destructive loss of an ETA will result in loss of all signals input from or output to that ETA.

- Failures of an input point that are duplicated on more than one leg will result in loss of that input point.

- Multiple failures in an output voter circuit may result in forcing the output point on or off.

- Failure of all three separate, redundant communications processors on a single module will result in various actions, depending on the module type. If the failure occurs in a digital input module, the Main Processor will declare all digital inputs to be off. If the failure occurs on a digital output module, the module microprocessors will force all digital outputs to the fail-safe, de-energized state. If the failure occurs on an analog input module, the Main Processors will declare all inputs downscale. On a pulse input module, the Main Processors will declare all inputs downscale.

B. A reliability and availability analysis was performed as part of the qualification effort. A specific system configuration was subjected to an extensive Markov chain modeling process, using the reliability data provided by Triconex. Triconex Report 9600164-532 provides a Markov model for a given configuration (Reference 7.22). The system models and data provided could be used to estimate the possibility of failure for other Tricon configurations.

- The Tricon offers a field proven reliability, with no failures to implement a required safety action, for over 500 million system operating hours. The likelihood of software common cause failure can thus be shown to be remote.

- From a licensing perspective, the results of the FMEA and Reliability/Availability reports should be incorporated into licensing analyses for each Tricon installation.

- Shorting common power supplies to ground is likely to result in a protective action. The short may result in forcing all inputs to zero, or the short may result in all outputs failing to the de-energized, fail-safe state.

3.6 Diversity and Defense-in-Depth

The main body of the Final Summary Report describes the generic qualification of the Tricon for nuclear safety-related applications based on compliance with hardware and software requirements. In addition to the requirements that relate specifically to the Tricon platform, other important requirements govern the implementation of the Tricon platform in nuclear facilities. This section is provided to address one of the important sets of system-specific requirements (as opposed to platform-specific requirements), namely defense-in-depth and diversity.

The philosophy of defense-in-depth is a multi-layered approach to safe plant operation. For example, in nuclear power plants it includes multiple physical boundaries between the fuel and environment, redundant paths and equipment to provide core cooling, and qualified control and monitoring systems for safe shutdown and long term cooling of the reactor.

When applied to instrumentation and control (I&C) systems, defense-in-depth refers to multiple means to trip the reactor and to initiate safeguards functions for nuclear power plants. It includes provisions for multiple back-up protection actions should the primary protective systems fail to perform. In the original design of nuclear power plants, this is achieved by the use of multiple, independent, and redundant trip channels, independent and redundant safeguards actuation trains, qualification of equipment for the intended service, and diverse means to perform selected protective actions.

Diversity is one aspect of defense-in-depth that is used to avoid equipment common mode failure. Diversity has been applied to nuclear facilities since the earliest designs to account for uncertainties in design and for common mode failure of equipment.

With the use of digital platforms to perform safety functions, the US NRC has placed a special emphasis on evaluation of the common mode failure of software. Though highly unlikely, current regulatory requirements for the design of digital safety-related systems require consideration of a scenario in which all equipment that share a common digital platform are assumed to fail in an unsafe state simultaneously. Alternate plant systems or manual operator actions must therefore be available to provide a means of shutting down the nuclear process to prevent adverse impacts on public health and safety and environmental damage. Due to the extremely low probability of software common mode failure, the alternate shutdown means need not be classified as safety related nor need it meet other safety system criteria such as redundancy, automatic action, etc.

Protection against common mode failure of software is achieved by establishing four "echelons" of defense against equipment failures:

- Control system – The control echelon consists of that non-safety equipment which routinely prevents facility excursions toward unsafe regimes of operation, and is used for normal operation of the facility.

- RTS – The Reactor Trip System (RTS) echelon consists of that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

- ESFAS – The Engineered Safety Features Actuation System (ESFAS) echelon consists of that safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment). The RTS and ESFAS do not have to be diverse, but additional evaluations and equipment are required if they are not diverse.

- Monitoring and indicators – The monitoring and indication echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

Within and between these echelons, a strategy of diversity is employed that includes:

- Diverse signals used to perform the same safety functions;

- Diverse equipment to perform the same safety function;

- Diverse platforms used for safety and non-safety related control and protection systems (i.e., diverse platforms for reactor trip and Anticipated Transient Without Scram mitigating systems);

- Diverse safety or nonsafety equipment installed to provide automatic protective actions when software common cause failure occurs; and

- Diverse indications and controls that allow manual operator action.

The common mode failure of software is considered to be less likely than a single hardware failure, but it is still considered to be a credible event and must be addressed.

3.6.1 Licensing Criteria

NUREG-0800 recognizes that digital I&C upgrades require additional design and qualification approaches than those which were typically employed for analog systems. Analog system performance can typically be predicted by the use of engineering models. Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected

behavior. Current design techniques for digital I&C systems do not have equivalent engineering models that can be used for system validation.

Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. The use of quality processes, including design, peer review, inspections, type testing, and acceptance testing of digital systems and components does not alone accomplish design qualification at high confidence levels. Also, in digital I&C systems, a design using shared data or code has the potential to propagate a common-cause failure. Greater commonality or sharing of hardware among functions within a channel increases the consequences of the failure of a single hardware module and reduces the amount of diversity available within a single safety channel.

The NRC's approach to the review of design qualification of digital systems focuses, to a large extent, upon confirming that the development process incorporated disciplined specification, implementation, verification, and validation of design requirements. Inspection and testing is used to verify correct implementation and to validate desired functionality of the *final product*, but confidence that isolated, discontinuous point failures will not occur derives from the discipline in the *development process*. The NRC's review of digital I&C systems, particularly reactor protection systems, also emphasizes quality, defense-in-depth, and diversity (D3) as protection against propagation of common-mode failure within and between functions. The NRC's position on quality of software for safety system functions is stated in Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." The NRC's position on D3 is stated in BTP 7-19, "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."

3.6.2 Defense-In-Depth and Diversity Requirements

Requirements for establishing appropriate levels of defense-in-depth and diversity (D3) for control and instrumentation systems are described in BTP 7-19 for new designs of or changes to existing RTS and ESFAS systems. In particular, the following activities are required:

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

2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods.

The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.

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

4. A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

As required by BTP 7-19, each licensing basis event must be evaluated to determine if a postulated common-mode failure could disable a safety function that is required to respond to the design basis event being analyzed. If so, then a diverse means of effective response is necessary. The diverse means may be a non-safety system, using either automatic or manual control, if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time. For this evaluation, "best-estimate" methods and assumptions are allowed rather than the more conservative assumptions defined in 10 CFR 50, Appendix K for design basis accident analyses. The evaluation assumes that only the software common mode failure occurs in conjunction with an initiating event, thus not requiring operation of the diverse elements through a seismic event.

For existing nuclear facilities, it is expected that this evaluation would consider whether existing manual controls and indications and/or diverse automatic controls are sufficient to provide the necessary backup to the digital engineered safeguards actuation systems. It is expected that existing plant Emergency Operating Procedures or Emergency Response Guidelines could be used in this evaluation as appropriate. The manual controls and indications and/or diverse automatic controls required for backup would be required to be separate and isolated from the digital engineered safeguards actuation systems. In many existing plants, manual controls are already provided for manual actuation of safety-related equipment at the component level. Additional manual system level actuation may be required, based on the evaluation results.

3.6.3 Diversity Implementation

When the Tricon platform is used to perform RTS, ESFAS, or other protective functions in nuclear facilities, either in new facilities or to upgrade existing systems, the defense-in-depth and diversity analysis described above will need to be performed based on facility-specific accident conditions. The analysis will also need to consider facility-specific diverse indications and controls. One approach to implementing RTS and/or ESFAS functions in nuclear power plants using the Tricon platform is illustrated in Figure 3-1 and is discussed below.

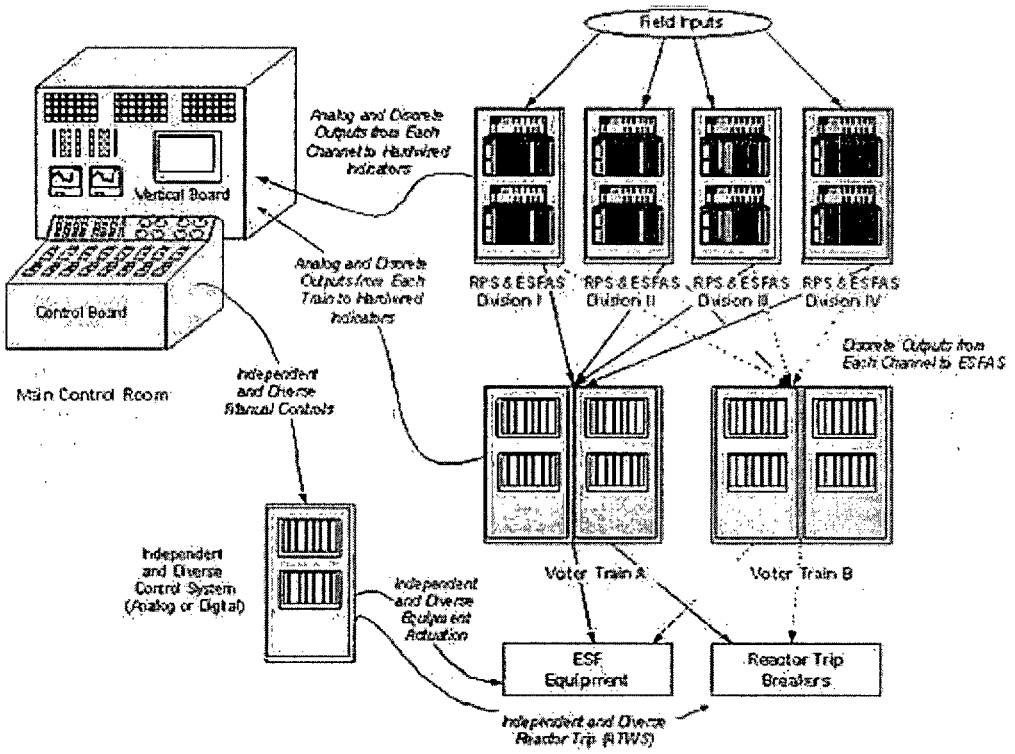


Figure 3-1 Tricon Reactor Protection System with Diversity

The figure illustrates use of the Tricon platform to implement reactor protection system functions using most of the traditional channel, division, and train approach. Such a system could be implemented as an upgrade to an existing plant. With this approach, four Tricon systems are installed to acquire data, perform bistable trip comparisons, and generate discrete outputs to the two trains of the RTS and ESFAS systems. Each of the four systems operates independently. Each of the four Tricon systems may also provide

discrete or analog outputs to drive annunciator points or indicators in the main control room. The final reactor trip voting and ESFAS automatic equipment actuation is performed by the two independent trains.

The hypothetical configuration would combine RPS and ESFAS functions on a single platform, i.e., the V10 Tricon PLC. The Tricon, with its TMR architecture, is resilient against single failures and operating experience has shown it is highly reliable (more than 9,000 units in operation and over 500,000,000 hours without failure to perform on demand). Invensys understands there remains the very rare possibility of a software common cause failure (CCF). Since digital system CCFs are not classified as single failures, postulated digital CCFs are not assumed to be a single random failure in design basis evaluations. The two design attributes sufficient to eliminate consideration of common cause failure – diversity and testability – would not be satisfied by the proposed architecture. Therefore, a diverse actuation system (DAS) would be required with the proposed combined RPS/ESFAS architecture, and is shown in the figure. Invensys recommends full design analysis following BTP 7-19 for partial or complete RPS/ESFAS upgrades or installations including best-estimate techniques to evaluate the effects of digital system CCFs coincident with design basis events. Upon support and approval by the licensee, Invensys will conduct D3 analysis of new and replacement RPS/ESFAS applications in conformance with NUREG/CR-6303, IEEE Std. 279-1971 or IEEE Standard 603-1991, Reg. Guide 1.152 Rev. 2 and BTP 7-19.

Because a CCF is not a design basis event, the alternate shutdown means need only be adequately robust consistent with 10 CFR 50.62. A specifically designed DAS to actuate RPS/ESFAS equipment must independently monitor plant process parameters, automatically initiate protective actions, and must be designed and manufactured in accordance with Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related". When included in the design, the DAS, composed of diverse hardware and software, would independently monitor plant process parameters and automatically initiate protective actions, as shown in the figure. DAS designated components will be configured and programmed to automatically initiate reactor shutdown and activate cooling equipment when accident conditions are sensed.

The DAS will also provide independent and diverse plant information displays in support of manual initiation. As illustrated in the figure, manual operator action will be supported in all Invensys-designed RPS/ESFAS architectures. The operator will have the capability to view plant process information at independent displays – Safety Parameter Display Console (analog or digital display) and the Plant Process Computer and/or DCS VDUs. Manual safety initiation will be independent of both systems. The specific design and technology of the DAS is beyond the scope of this topical report,

but at a minimum, the following would have to be analyzed as part of the D3 assessment:

- design architectures are diverse (including underlying technology, such as hardware and software)
- diverse power source(s)
- quality of the components in the diverse system
- actuation path for the diverse system (i.e., downstream of the Tricon-based RPS/ESFAS, as shown in the figure), and
- timing analysis for manual operator actions, if credited, as well as quality of the operator displays and switches.

The figure also shows that independent and diverse manual controls are also used to actuate reactor trip equipment. In addition to the manual controls, the Anticipated Transient Without Scram (ATWS) system provides independent and diverse automatic actuation of the reactor trip equipment separately.

As illustrated by Figure 3-1, the Tricon platform could be used in both the reactor protection system channels and the RTS and ESFAS trains. With this approach, four independent Tricon systems perform the reactor protection system functions described above, and two additional independent Tricon systems perform the RTS and ESFAS functions of trip logic and equipment actuation. Again, the interface between the four channels and the two RTS/ESFAS trains would typically be discrete signals. The Tricon peer-to-peer communication link could be used and would simplify wiring for new plants. However, this communication link is not triple redundant and therefore communications from one Tricon to another are vulnerable to a single failure if redundant communication paths were not provided. Use of discrete signals would reduce the risk of losing all inputs from one of the reactor protection system channels to the RTS/ESFAS systems.

Again, independent and diverse automatic and manual controls are used to actuate ESFAS equipment by a diverse control system, which would be likely be more extensive with RTS and ESFAS implemented on a common platform. The defense-in-depth and diversity analysis described above would be used to identify the specific equipment requiring diverse actuation capability. This analysis would also be used to establish whether sufficient time is available for manual operator actuation or if automatic actuation is required. The timing for manual actions would likely be verified by tests in a facility simulator. In addition, the analysis would establish whether

component level actuation is sufficient, or whether certain diverse system-level actuations are necessary.

The diverse equipment actuation circuits would use priority logic modules to combine the credited safety system and the diverse automatic and manual actions into control outputs for the actuated equipment. Priority logic modules are not included in this topical report.

Additional protection from software common mode failures can also be obtained if the Tricon safety systems are installed in a plant with digital non-safety related control and information systems. For example, Invensys has developed a plant design in which TCM modules in each of the independent Tricon safety systems are interfaced to a Foxboro I/A distributed control system (DCS). As previously described, the TCM module can provide one-way communication to the Foxboro I/A system and is qualified as a 1E-to-non 1E isolator. The TCM module provides the DCS with the value of each parameter and the status of the Tricon system diagnostics. This allows the operator to monitor the status of the safety system using the advanced human system interface features available through the DCS. In addition, the DCS can be configured to emulate the safety system trip logic. If the DCS detects that the protection system has failed to respond to an upset condition, it will immediately provide this information to the operator so that he can take appropriate manual action or could provide an automatic trip function or automatic ESF functions, if the DCS is based upon an acceptable quality based design approach. With this approach, the DCS should also be configured to perform automatic and routine cross-comparisons of the data between each channel, division, and train of the Tricon protection system to identify possible field sensor failures.

3.7 Setpoint Accuracy Calculations

An analysis was performed to provide a single concise listing of the accuracy specifications of the Triconex Tricon control system. The specifications documented are those typically used by nuclear industry users for calculating instrument measurement uncertainties and establishing critical control setpoints.

The Triple-Modular Redundant architecture of the Tricon along with its continuous diagnostics and self-calibration features eliminates many of the typical error sources found in standard instrumentation. Component or module failure;, channel, division, or train failures;, or communication failures at the Input, Output, or Main Processor Module level will be corrected and/or compensated for by the Tricon system's ability to detect transient and steady state errors, and to take appropriate corrective actions online through the system's hardware and software voting mechanisms.

Tables 3-1 through 3-3 document the Reference Accuracy specifications for each of the analog I/O modules included in the Triconex Tricon PLC qualification program.

Table 3-1 - I/O Module Accuracy Specifications

I/O Module Type	Model Number	Reference Accuracy (Note 1)
0-10V Analog Input	3701	< 0.15% of FSR (Volts) 0° to 60° C (Note 2 & 3)
0-5V or 0-10V Analog Input (16 Inputs)	3703E	< 0.15% of FSR (Volts) 0° to 60° C (Note 2 & 3)
4-20 mA Analog Output	3805E	< 0.25% (in range of 4-20 mA) of FSR (0-22mA) 0° to 60° C
Thermocouple Input J, K, T, E	3708E	See Table 2
Pulse Input	3511	@ 1,000 Hz to 20,000 Hz – ±0.01% @ 100 Hz to 999 Hz – ±0.1% @ 20 Hz to 99 Hz – ±1.0%
0-5V Analog Input or -5 to +5V Differential	3721	< 0.15% of FSR 0° to 60° C (Notes 2 & 3)

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis, non--linearity, and dead band). Triconex guarantees that the performance of the module meets specifications. This performance has been verified by testing performed on all modules during production. Typically, field application of the modules with respect to calibration accuracies is more stringent than the specified accuracy. Therefore, Reference Accuracy values are considered to be a 95% or better probability value with a 95% or better confidence level.

2. On current loop inputs, a 0.01% precision resistor is used on the input termination to convert the current signal to a voltage reading (250 ohm for 0 -5 VDC or 500 ohm for 0-10 VDC). The resistor accuracy This is not included in the specified module accuracy.

3. FSR = Full Scale Range

Table 3-2 - Reference Accuracy of Model #3708E Thermocouple Input Module

TC Type	Temperature Range	Reference Accuracy (Notes 1 and 2) @0-60°C (32-140°F)	
		T_a=25°C (77°F)	T_a=0-60°C (32-140°F)
		Typical	Maximum
J	-150 to 0°C (-238 to 32°F) 0 to 760°C (>32 to 1400°F)	±1.7°C (±3.0°F))	±5.0°C (±9.0°F) ±3.1°C (±5.5°F)
K	-150 to 0°C (-238 to 32°F) 0 to 1251.1°C (>32 to 2284°F)	±2.3°C (±4.0°F)	±4.5°C (±8.0°F) ±3.9°C (±7.0°F)
T	-161 to 0°C (-250 to 32°F) 0 to 400°C (>32 to 752°F)	±1.7°C (±3.0°F)	±4.8°C (±8.5°F) ±2.5°C (±4.5°F)
E	-200 to 0°C (-328 to 32°F) 0 to 999°C (>32 to 1830°F)	±1.7°C (±3.0°F)	±4.5°C (±8.0°F) ±2.8°C (±5.0°F)

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis, non-linearity, and dead band). Triconex guarantees that the performance of the module meets specifications. This performance has been verified by testing performed on all modules during production Typically, field application of the modules with respect to calibration accuracies is more stringent than the specified accuracy. Therefore, Reference Accuracy values are considered to be a 95% or better probability value with a 95% or better confidence level.

2. Accuracy specifications account for errors related to reference-junction compensation but do not account for errors caused by temperature gradients between the temperature transducers and thermocouple terminations. The user is responsible for maintaining a uniform temperature across the thermocouple termination module.

Table 3-3 - Reference Accuracy of Analog Devices Signal Conditioners

Signal Conditioner Type	Model Number	Reference Accuracy (Note 1)
AD7B34CUSTOM, RTD Signal Converter, 200 ohm Pt., 0 – 600°C	1600083-600	+/- 0.11% span
AD7B34CUSTOM, RTD Signal Converter, 200 ohm Pt., 0 - 200°C	1600083-200	+/- 0.2% span
AD7B340401, RTD Signal Converter, 100 ohm Pt., 0 - 600°C	1600024-040	+/- 0.1% span
AD7B340301, RTD Signal Converter, 100 ohm Pt., 0 - 200°C	1600024-030	+/- 0.15% span
AD7B340201, RTD Signal Converter, 100 ohm Pt., 0 - 100°C	1600024-020	+/- 0.2% span
AD7B340101, RTD Signal Converter, 100 ohm Pt., -100 to +100°C	1600024-010	+/- 0.15% span
AD7B300201, RTD Signal Converter, 0 – 100 mV	1600082-001	+/- 0.1% span

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis, and non-linearity).

3.8 Bypass and Indication

A. Any interface to the existing bypass and inoperable indication system should be incorporated into the new design, with any necessary outputs driven by the Tricon.

B. If the Tricon communicates with a Distributed Control System, Plant Computer, or other Historian, additional software and historian capabilities should be

evaluated for diverse indication and alarming as well as retention of historical data for the control room.

3.9 Self-Test Capabilities

BTP 7-17 and other applicable IEEE standards describe requirements for self-test capabilities for digital systems. The design of the Tricon incorporates most of these features. Specific capabilities provided by the Tricon and considerations for application design are discussed below.

A. As required in BTP 7-17, the Tricon includes self-test features to confirm computer system operation upon system initialization. Additional tests and diagnostics are provided in the Tricon PLC beyond the minimal set identified in BTP HICB-17 and the referenced guidance documents. The Tricon PLC 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.

B. Digital computer-based instrumentation and control systems are prone to different kinds of failures than traditional analog systems. Properly designed self-test, diagnostic, and watchdog timers reduce the time to detect and identify failures, but are not a guarantee of hardware or software error detection. Computer self-testing is most effective at detecting random hardware failures. The Tricon TMR PLC has been designed and validated by the vendor and by TÜV Rheinland to detect and identify failures. The system design goal was 100% detection of failures. Random hardware failures have been demonstrated by Triconex automated testing and by analysis at TÜV Rheinland to be unlikely to defeat the Tricon PLC triple redundancy. Therefore, the TMR design is likely to detect and annunciate these failures if the application software includes detection features and external equipment to annunciate the fault in the control room is provided.

C. The internal self-test functions are transparent to the application programmer and are an integral part of the base platform software. The application is provided self-test results through a simple, pre-designed, verified and validated interface. The platform software is pre-developed, standard, modular, and well structured. The improved ability to detect failures provided by the self-test features reduces the probability of failure associated with the self-test feature and has been demonstrated in certification as a safety critical system and by field experience in similar safety critical applications. Faults and failures detected by hardware, software, and surveillance testing are consistent with the failure detection assumptions of the single-failure analysis and the failure modes and effects analysis. The TMR capabilities decrease the probability of system failure, as

demonstrated in the Availability and Reliability Report. In addition, identification and alarming by the application software, as well as use of valid input data, further increases the overall system reliability in detection of previously undetected faults and failures internal to the existing systems.

D. The Tricon PLC system performs self-tests as well as validation of inputs and outputs on each module. The self-test capabilities of the Tricon and appropriate application software could be credited with some of the test and calibration functions for channels and devices currently provided by manual surveillance tests.

E. The Tricon TMR architecture provides continuous self-testing that will detect, tolerate, and alarm on single internal faults and failures. These self-tests include testing the operability of digital output points, which provide two out of four voting on each of the output points. Single failures in the output drive circuits do not cause inadvertent actuation or prevent necessary actuation of controlled field devices. The output drive voter is diagnosed by internal self-tests within the Tricon Any faults in the output drive circuitry will be annunciated in the control room.

F. The Tricon platform also provides inherent capabilities for testing external devices. The output point can be diagnosed for appropriate current and voltage conditions. If the wiring or field device coil is open or shorted, the Tricon will alarm the loss of the field device for each output point.

G. The Tricon platform provides inherent capabilities for internal self-test and calibration that provide detection of faults in the analog input processing. This resolves issues with drift and calibration uncertainty, which are licensed as being required for the existing analog controls. The Tricon platform has the capability of continuously diagnosing the health of and appropriately adjusting the calibration of the analog to digital signal conversion modules. If the analog to digital conversion module has been significantly adjusted or is outside the limited automatic calibration limits, the module will be marked faulted and an alarm will be generated in the control room. The analog bistable calibrations required by the older, obsolete systems are not required for the Tricon platform.

H. Mechanisms for operator notification of detected failures should comply with the system status indication provisions of IEEE Standard 603 and should be consistent with, and support, plant technical specifications, operating procedures, and maintenance procedures. The Tricon system will provide more diagnostic and notification information than is required in IEEE Standard 603. The Tricon system is designed to support Operations, the safety analysis report, the Technical Specifications, and maintenance functions. New procedures and procedure

changes will be incorporated into the design change to support the Tricon system and the staff in plant operation and maintenance.

3.10 Surveillance Capabilities

This section discusses considerations for changes to existing plant surveillance tests based on the design features incorporated in the Tricon system (including the self-test features discussed above). These considerations are provided here to assist plants in identifying areas in which use of the Tricon system will have a beneficial effect on the surveillance program.

A. Modifications to the existing surveillance tests and licensing commitments will be required, as is identified in BTP 7-17. Self tests and automatic analog input calibration could be used to reduce the surveillance testing requirements for the Tricon PLC. The self-test capabilities of the Tricon and appropriate application software could be credited with some of the test and calibration functions for channels and devices currently provided by manual surveillance tests. The application software would provide additional features to support the reduced surveillance testing requirements. The Tricon provides at least as much test coverage as the existing surveillance tests, through the fault tolerance, detection, and repair capabilities inherent in the Tricon PLC design.

B. Because of design and architectural differences between analog and digital systems, traditional surveillance test provisions for analog systems may not be adequate or appropriate for digital computer-based systems. The required surveillance test capabilities to be included in each system design will have to be evaluated to assure adequacy to fulfill the requirements and the intent of the surveillance tests.

C. The replacement system design should provide the ability to conduct periodic testing consistent with the modified technical specifications and plant procedures. The Tricon PLC application can be designed to provide these capabilities, in accordance with the requirements established in the regulatory guidance referenced in BTP 7-17. There is nothing inherent in the Tricon or TriStation designs that do not comply with the requirements of IEEE Standard 603, as required in BTP 7-17. The Tricon has been successfully evaluated against the recommendations made in IEEE Std. 7-4.3.2 in the Critical Digital Reviews, References 7.19 and 7.20. The Tricon PLC provides capabilities in excess of the minimum criteria found in IEC Standard 880.

D. In order to reduce surveillance testing, an analysis of the Tricon PLC self-test features, single-failure analyses, failure mode and effect analyses, and application

software would be required against the requirements established in the Technical Specifications and by the USNRC. The self-test and failure analysis capabilities are documented in the Software Qualification/Critical Digital Review, Availability/Reliability Study, and FMEA Reports from the qualification program. The application software would also require the capability to confirm that the automatic tests are still functional during plant operation.

E. The Tricon has been designed and would be incorporated into the facility design in a mode that should reduce the current manual maintenance and testing activities in existing systems, thus reducing the risks associated with performing these periodic tests. By invoking the self-checking capabilities inherent in the Tricon architecture, the protection systems assure that the lessened amount of maintenance and testing activities reduce the number of losses of protection functions from inadvertent maintenance or surveillance errors.

F. The actuation device testing specified in Reg. Guide 1.22 is still applicable. As a software-based device, the Tricon can be configured to perform any of the testing described in Reg. Guide 1.22, from complete function to judicious choice of components for several tests.

G. The minor software complexity associated with automating required surveillance testing is offset by the reduced risk associated with performance of such testing. Since the number of technician and engineering physical changes inside the protective systems is reduced, the chance for inadvertent modification is also reduced.

H. Reg. Guide 1.118 states in part that test procedures for periodic tests should not require makeshift test setups. For digital computer-based systems, makeshift test setups, including temporary modification of code or data that must be appropriately removed to restore the system to service, should be avoided or at least, designed into the on-line application software. The application software should be configured to incorporate design features to preclude the need for temporary modifications to hardware or software, jumpers, and reconfiguration to perform periodic testing.

I. As required by ANSI/IEEE Standard 279, Section 4.13; IEEE Standard 603, Section 5.8.3; and RG 1.47, if the protective action of some part of a protection system is bypassed or deliberately rendered inoperative for testing, continued indication of that state shall be provided in the control room automatically. Provisions should also be made to allow operations staff to confirm that the system has been properly returned to service. Not only will the traditional bypass indication be provided, the amount of hardware and jumpers associated with testing a traditional analog system will not exist, since the "jumpers" and

"reconfiguration" would be incorporated into the application software. Thus, the possibility of creating errors or faults through inadvertent system modifications is precluded by design. Since the testing is initiated and controlled by the Operations staff and built into the Tricon software, awareness of testing and test progress is maintained and further enhanced in the control room. Anything not restored to service would also be annunciated in the control room.

J. Hardware and software used to perform automatic self-testing are integral to the Tricon and are classified as safety related, having the same quality and reliability as the Tricon PLC. The Tricon PLC can be applied in a manner that maintains existing channel independence, maintains system integrity, and meets the single-failure criterion. The scope and extent of interfaces between software that performs protection functions and software for other functions such as testing has been designed to minimize the complexity of the software logic and data structures. The complexity resulting from TMR is controlled, and integral to the standard, field-proven base platform.

K. The design should have either the automatic or manual capability to take compensatory action upon detection of any failed or inoperable component. The design capability and plant technical specifications, operating procedures, and maintenance procedures should be consistent with each other. The design provides annunciation in the control room on detection of any fault within the Tricon or of any detectable failure in field sensors or actuators. If the Tricon stops operation, the outputs are driven to an OFF state. Faults in any single portion of the TMR Tricon result in that portion being removed from service and annunciated in the control room. Faulted or inoperable field inputs and outputs are detected and alarmed. Other actions could be built into application software as necessary to implement compensatory actions and annunciate the detected failures of external devices.

L. Plant procedures should specify manual compensatory actions and mechanisms for recovery from automatic compensatory actions.

M. Surveillance testing shall be designed to validate correct operation of the Tricon self-tests, to the extent practical. However, many of the self-test functions embedded in the Tricon are not easily tested outside of Triconex facilities and cannot be readily validated in the field.

N. Surveillance testing taken together with automatic self-testing should provide a mechanism for finding and annunciating all detectable failures. The characteristics of digital systems must be considered in the review of technical specification surveillance features. Architectural differences between digital and analog systems warrant careful consideration during the review of surveillance

test provisions. Furthermore, the concepts used to determine test intervals for hardware-based systems do not directly apply to the software used in digital computer-based instrumentation and control systems. Therefore, previous reliability analysis used to establish test intervals may not apply. The reliability and availability analysis and the FMEA report indicate that the TMR controls exceed the availability targets of the analog hardware they replace, but that there is still a reliability enhancement from shortened surveillance testing. The 500 Million operating hours without a failure to implement a required protective action demonstrates the Tricon capabilities. There is thus no risk that the maintenance and calibration will have to be done more frequently than required with the existing system. The field hardware testing requirements remain unchanged. With the enhanced system reliability, data cross-checking, automatic analog input calibration, automatic output diagnostics, and automated support for the tests, the risk of undetected failures should be decreased.

3.11 Operational Constraints

Specific operational constraints that apply to the use of the Tricon system in nuclear safety-related applications include the following:

A. The Tricon keyswitch shall preferably be in the RUN, or alternatively in the REMOTE, position when the Tricon is not bypassed and thus performing safety related functions. If the Tricon is not in a bypassed state, alarms must occur in the control room if the keyswitch is in any position other than RUN or alternatively REMOTE.

B. The STOP position on the keylock switch shall be disabled in the system software configuration to preclude inadvertently stopping the program while performing software maintenance functions.

C. Repairs to the Tricon must be performed in an expeditious manner. Main Processors should not be left in a faulted state for extended periods. Operation in single Main Processor mode should be minimized and should not be longer than one day to minimize risk of masking other faults. The Tricon has limited diagnostic capabilities in dual processor mode. A second Tricon fault might cause the outputs to go to the safe, de-energized state. The length of time allowable for running in dual or single mode may be calculated using Markov modeling by pre-determination of the minimum acceptable probability to fail on demand. Invensys uses Markov models based on Tricon system states and individual Module data for a given Tricon system configuration. The calculations are based on Markov Models developed by the Instrument Society of America's SP84 committee during the development of the ISA's SP84 Technical Report S84.0.02.

Separate sections of this Application Guideline provide specific recommendations for Maintenance Overrides and Communication with External Systems.

3.12 Error Reporting and Tracking

Triconex has always had formal error tracking and recording systems for industrial safety critical issue notification. Errors are classified according to severity, with Product Alert Notices (PAN) being the most significant, and Technical Advisory Bulletins (TAB) and Technical Application Notes (TAN) being of lesser significance. Product Alert Notices document conditions that may affect the safety of the application. It is essential that all current PANs, TABs, and TANs be reviewed before starting application development, and that the system be kept up-to-date with any newly released PANs, TABs, or TANs as appropriate.

4.0 ENVIRONMENT AND LOCATION

Specific requirements pertaining to the environment in which a safety-related Tricon system is located are discussed in this section. These environment and location requirements are based on the manufacturer's recommendations in the Triconex Planning and Installation Guide (Reference 7.13), and the results of the qualification testing.

4.1 Mounting

A. The Tricon chassis is designed for mounting in 19-inch industry-standard racks. Mounting specifications for standard, non-seismic mounting are provided in the Triconex Technical Product Guide and in the Triconex Planning and Installation Guide

B. The seismic qualified Tricon chassis requires use of the standard mounting brackets on the front of the chassis as well as the additional standard mounting brackets at the rear of the chassis.

C. Seismic mounting details for all qualified Tricon hardware is provided on Triconex Drawing No. 9600164-102, "Seismic Test Equipment Configuration Detail." All fastener torque values are indicated on Triconex Drawing 9600164-102. The mounting uses standard Tricon front and rear chassis mounting brackets and fastener hardware, and standard Tricon External Termination Assembly (ETA) mounting plates.

D. At least 5.25 inches of free space should be provided between the top and bottom panels of each Tricon chassis and solid horizontal plates in order to achieve sufficient convection cooling airflow.

E. Any unused module slots shall be covered with module slot covers.

4.2 Temperature and Humidity

A. Environmental testing of the Tricon was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977. The Tricon met all applicable performance requirements during and after application of the environmental test conditions. The environmental test included high temperatures of 140° F and 95% relative humidity (RH) and low temperatures of 32° F and 5% relatively humidity. The temperature and humidity profile applied during environmental qualification testing of the Tricon PLC is shown in Figure 8-1 of the Environmental Test Report, Triconex Report Number 9600164-525 (Reference 7.25).

B. The specific Tricon hardware that was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List (Reference 7.30).

4.3 Heat Loads in Cabinets and Rooms

A. When mounting the Tricon chassis into enclosures, heat management calculations must be made to avoid exceeding the qualified ambient temperature ratings of the Tricon. For purposes of these calculations, all power consumed by the Tricon should be assumed to be dissipated inside the enclosure where the Tricon chassis is mounted.

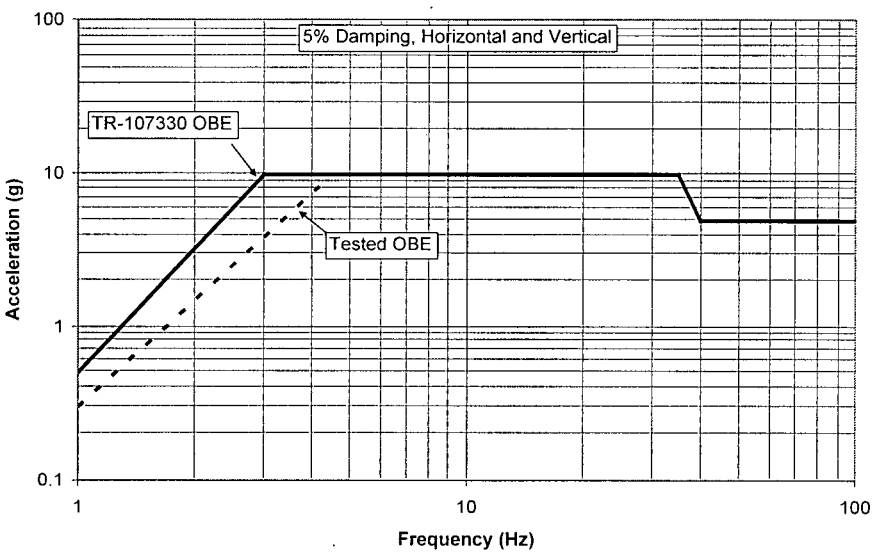
B. If the room temperature plus any heat rise within the cabinet exceeds the Tricon qualification envelope, additional provision must be made for temperature control.

C. The Tricon temperature range must be computed with cabinet doors open and closed.

D. The Triconex Planning and Installation Guide provides guidance on computing the heat load for a loaded chassis.

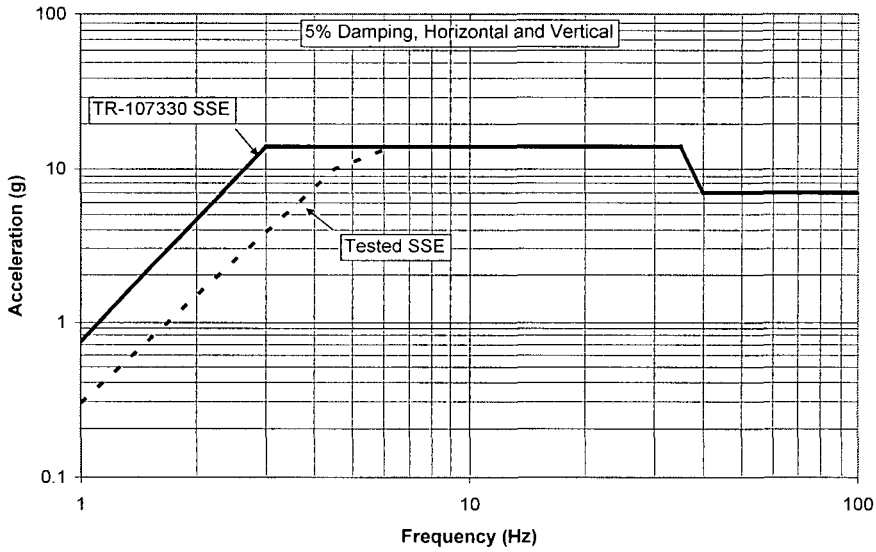
4.4 Seismic Acceleration Limits

Seismic testing was performed in accordance with the requirements of EPRI TR-107330, Section 4.3.9, and IEEE Standard 344.



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 4-1 Comparison of OBE Test Levels to EPRI TR-107330 OBE Requirements



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 4-2 Comparison of SSE Test Levels to EPRI TR-107330 OBE Requirements

A. Seismic testing demonstrates that the Tricon is qualified as a Category I seismic device within the test limits shown in Figures 4-1 and 4-2. A plant-specific evaluation will be needed to determine whether the as-tested limits bound the plant seismic acceleration requirements. If not, additional evaluation or seismic testing may be required.

B. Monitoring for chatter of the chassis alarm contacts during seismic testing was not done as a result of utilizing an interposing relay installed in the contact monitoring

circuit. Therefore these contacts are not seismically qualified and this contact output is not credited as performing safety functionality for the facility.

4.5 Radiation Fields

Radiation testing of the Tricon was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 323-1974. 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 (Reference7.29)

4.6 EMI/RFI Compatibility

EMI/RFI Testing of the TUT was performed to the requirements of Sections 3 and 4 of NRC Regulatory Guide (RG) 1.180, Rev. 1 (Reference 7.6). Section 3 of NRC RG 1.180 addresses EMI/RFI emissions testing. Section 4 of NRC RG 1.180 addresses EMI/RFI susceptibility testing. Each section endorses both Military Standard MIL STD 461E series and International Electrotechnical Commission (IEC) 61000 series EMI/RFI test methods. Based on the RG, Triconex has the option to use either series of test methods. NRC RG 1.180, Rev. 1 stipulates that for emissions or susceptibility testing, the chosen series of test methods must be applied in its entirety (i.e., there should be no selective application or mixing of the MIL-STD and IEC test methods during susceptibility testing or during emissions testing).) The maximum frequency for emissions and susceptibility test was 1 GHz, since the maximum intentionally generated frequency of the Tricon is 100 MHz (Reference 7.6, Section 6 and Reference 7.26).

A. Test Methods

EMI/RFI emissions testing of the TUT included both radiated and conducted emissions testing done to the following MIL-STD-461E series test methods specified in Section 3 of NRC RG 1.180, Rev. 1:

- MIL-STD-461E, Test Method CE101, Conducted Emissions, Low Frequency (30 Hz to 10 kHz), AC and DC Power Leads
- MIL-STD-461E, Test Method CE102, Conducted Emissions, High Frequency (10 kHz to 2 MHz), AC and DC Power Leads
- MIL-STD-461E, Test Method RE101, Radiated Emissions, Magnetic Field (30 Hz to 100 kHz), TUT Surfaces and Leads

- MIL-STD-461E, Test Method RE102, Radiated Emissions, Electric Field (2 MHz to 1 GHz), Antenna Measurement

EMI/RFI susceptibility testing of the TUT included both radiated and conducted susceptibility testing done to the following IEC 61000 series test methods specified in Section 4 of NRC RG 1.180, Rev. 1:

- IEC 61000-4-3, Radiated Susceptibility, High Frequency (26 MHz to 1 GHz), Antenna Exposure
- IEC 61000-4-6, Conducted Susceptibility, Radio Frequency (150 kHz to 80 MHz), Power and Signal Leads
- IEC 61000-4-8, Radiated Susceptibility, Power Line Frequency (60 Hz) Magnetic Field, Helmholtz Coil Exposure
- IEC 61000-4-9, Radiated Susceptibility, Pulsed Magnetic Field, Helmholtz Coil Exposure
- IEC 61000-4-10, Radiated Susceptibility, Damped Oscillatory Magnetic Field (100 kHz and 1 MHz), Helmholtz Coil Exposure
- IEC 61000-4-13, Conducted Susceptibility, Harmonics and Interharmonics (16 Hz to 2.4 kHz), Power Leads
- IEC 61000-4-16, Conducted Susceptibility, Common-Mode Disturbances (15 Hz to 150 kHz), Power and Signal Leads

All testing was performed with the TUT energized and operating under control of the executing TSAP software.

B. Test Levels

The following lists the EMI/RFI Testing emissions acceptance levels or applied susceptibility test levels from the applicable figures and tables of NRC RG 1.180, Rev. 1.

EMI/RFI Emissions Test Method	NRC RG 1.180, Rev. 1 Acceptance Level
MIL-STD-461E, CE101	Figure 3.1
MIL-STD-461E, CE102	Figure 3.2
MIL-STD-461E, RE101	Figure 3.3
MIL-STD-461E, RE102	Figure 3.4

EMI/RFI Susceptibility Test Method	NRC RG 1.180, Rev. 1 Test Level	
IEC 61000-4-3	Sect. 4.3.3:	10 V/m
IEC 61000-4-6	Sect. 4.1.2:	Power Leads, 140 dBμV
IEC 61000-4-6	Table 15:	Signal Leads, 130 dBμV
IEC 61000-4-8	Table 19:	Continuous, 30 A/m
IEC 61000-4-8	Table 19:	Short Duration, 300 A/m
IEC 61000-4-9	Table 19:	300 A/m
IEC 61000-4-10	Table 19:	30 A/m
IEC 61000-4-13	Table 10:	See Table 10
IEC 61000-4-16	Table 11:	Power Leads, See Table 11
	Table 11:	Signal Leads: 3/10 of Power Leads

C. Emissions Testing

The EMI/RFI emissions test results demonstrate that the Triconex Tricon v10 PLC does fully comply with the allowable emissions levels of NRC RG 1.180, Rev. 1 for MIL-STD-461E in both RE101 and RE102 testing. The Triconex Tricon v10 PLC does not fully comply with the allowable emissions levels of NRC RG 1.180, Rev. 1 for MIL-STD-461E, CE101 and CE102.

D. Susceptibility Testing

The EMI/RFI susceptibility test results show that the Tricon v10 PLC system complies with the minimum susceptibility levels required by NRC RG 1.180, Rev. 1, as presented in Tables 4-1 and 4-2 with regard to the following system level operational criteria. The main processors continued to function correctly throughout testing as noted. The transfer of input and output data was not interrupted. There were no interruptions or inconsistencies in the operation of the system or the software.

The TUT main processor, chassis power supply, remote extender, and communication modules fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for all of the EMI/RFI susceptibility tests listed in Subsection A.

The EMI/RFI susceptibility test results show that the following Tricon v10 PLC input/output hardware does not fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for the listed susceptibility tests:

IEC 61000-4-3 Testing

- RTD Signal Conditioning Module 1600083-600 (threshold levels determined)
- RTD Signal Conditioning Module 1600083-200 (threshold levels determined)
- RTD Signal Conditioning Module 1600024-030 (threshold levels determined)
- RTD Signal Conditioning Module 1600024-020 (threshold levels determined)

IEC 61000-4-6 Testing

- RTD Signal Conditioning Module 1600081-001 (no threshold levels determined)
- Digital Output Module 3601T (115 VAC) w/ ETP 9663-610N (threshold levels determined)

Prior to installing the Tricon v10 PLC in a nuclear safety-related application, an evaluation of the input, output, and communication module susceptibilities should be performed. An evaluation of the module susceptibilities should also be performed for non-safety related applications if there is a potential for the PLC to impact plant reliability and availability. The Tricon v10 PLC EMI/RFI susceptibility testing documented in the EMI/RFI test report (Reference 7.26) provides the data required to perform such an evaluation..

Tables 4-1 and 4-2 included at the end of section 4.65 provide a summary of the EMI/RFI conducted and radiated susceptibility test results for each module installed in the TUT. The purpose of the table is to identify a set of modules that demonstrated acceptable susceptibility performance at the required NRC RG 1.180, Rev. 1 test levels.

The Tricon v10 PLC was tested without the benefit of a secondary enclosure, additional cable and wire shielding, or installed power line filtering. Mitigating actions to address the non-compliances in measured emission levels should incorporate these common in-plant installation features.

The specific Tricon v10 PLC hardware which was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the Triconex Master Configuration List, Document No. 9600164-540 (Reference 7.30).

NOTE: The susceptibility test results given above are contingent on a Tricon v10 PLC installation design that separates and isolates the 24 V dc field power supplies to the discrete I/O and analog I/O module circuits.

TABLE 4-1: SUMMARY OF EMI/RFI CONDUCTED SUSCEPTIBILITY TEST RESULTS

Module Model No.	ETP Model No.	Module Type	IEC 61000-4-6 Radio Frequency 150 kHz - 80 MHz	IEC 61000-4-13 Harmonics and Interharmonics	IEC 61000-4-16 Common-Mode Disturbances
3008	- - -	Main Processor	Pass	Pass	Pass
8310	- - -	Power Supply, 115 VAC	Pass	Pass	Pass
8311	- - -	Power Supply, 230 VAC	Pass	Pass	Pass
8312	- - -	Power Supply, 24 VDC	Pass	Pass	Pass
4200	- - -	Remote Extender	Pass	Pass	Pass
4201	- - -	Remote Extender	Pass	Pass	Pass
4352A	- - -	Communication	Pass	Pass	Pass
3511	9794-110N	Pulse Input	Pass	Pass	Pass
3708E	9782-110N	Thermocouple Input	Pass	Pass	Pass
3501T	9561-810N	Digital Input, 115 VAC	Pass	Pass	Pass
	9561-110N	Digital Input, 115 VAC	Pass	Pass	Pass
3623T	9664-810N	Digital Output, 120 VDC	Pass	Pass	Pass
3603T	9664-810N	Digital Output, 120 VDC	Pass	Pass	Pass
3601T	9663-610N	Digital Output, 115 VAC	**Susceptible**	Pass	Pass
3503E	9563-810N	Digital Input, 24 VDC	Pass	Pass	Pass
3625	9662-810N	Digital Output, 24 VDC	Pass	Pass	Pass
	9662-610N	Digital Output, 24 VDC	Pass	Pass	Pass
3636T	9668-110N	Relay Output	Pass	Pass	Pass
3607E	9667-810N	Digital Output, 48 VDC	Pass	Pass	Pass
3502E	9562-810N	Digital Input, 48 VDC	Pass	Pass	Pass
3701	9795-610N	Analog Input, 0-10 VDC	Pass	Pass	Pass

TABLE 4-1: SUMMARY OF EMI/RFI CONDUCTED SUSCEPTIBILITY TEST RESULTS

Module Model No.	ETP Model No.	Module Type	IEC 61000-4-6 Radio Frequency 150 kHz - 80 MHz	IEC 61000-4-13 Harmonics and Interharmonics	IEC 61000-4-16 Common-Mode Disturbances
	9783-110N	Analog Input, 0-10 VDC	Pass	Pass	Pass
3703E	9790-610N	Analog Input, 0-10 VDC	Pass	Pass	Pass
	9783-110N	Analog Input, 0-10 VDC	Pass	Pass	Pass
3805E	9860-610N	Analog Output, 4-20 mA	Pass	Pass	Pass
3721	9764-310N	RTD, No. 1600083-600	Pass	Pass	Pass
		RTD, No. 1600083-200	Pass	Pass	Pass
		RTD, No. 1600024-040	Pass	Pass	Pass
		RTD, No. 1600024-030	Pass	Pass	Pass
		RTD, No. 1600024-020	Pass	Pass	Pass
		RTD, No. 1600024-010	Pass	Pass	Pass
		mV, No. 1600082-001	Pass	Pass	Pass
		RTD, No. 1600081-001	**Susceptible**	Pass	Pass
3721	9783-110N	Analog Input, 0-5 VDC	Pass	Pass	Pass
	9790-610N	Analog Input, 0-5 VDC	Pass	Pass	Pass
	9783-110N	Analog Input, 0-5 VDC	Pass	Pass	Pass

TABLE 4-2: SUMMARY OF EMI/RFI RADIATED SUSCEPTIBILITY TEST RESULTS

Module Model No.	ETP Model No.	Module Type	IEC 61000-4-3 High Frequency 26 MHz - 1 GHz	IEC 61000-4-8 60 Hz Magnetic Field	IEC 61000-4-9 Pulsed Magnetic Field	IEC 61000-4-10 Oscillatory Magnetic Field
3008	- - -	Main Processor	Pass	Pass	Pass	Pass
8310	- - -	Power Supply, 115 VAC	Pass	Pass	Pass	Pass
8311	- - -	Power Supply, 230 VAC	Pass	Pass	Pass	Pass
8312	- - -	Power Supply, 24 VDC	Pass	Pass	Pass	Pass
4200	- - -	Remote Extender	Pass	Pass	Pass	Pass
4201	- - -	Remote Extender	Pass	Pass	Pass	Pass
4352A	- - -	Communication	Pass	Pass	Pass	Pass
3511	9794-110N	Pulse Input	Pass	Pass	Pass	Pass
3708E	9782-110N	Thermocouple Input	Pass	Pass	Pass	Pass
3501T	9561-810N	Digital Input, 115 VAC	Pass	Pass	Pass	Pass

TABLE 4-2: SUMMARY OF EMI/RFI RADIATED SUSCEPTIBILITY TEST RESULTS

Module Model No.	ETP Model No.	Module Type	IEC 61000-4-3 High Frequency 26 MHz - 1 GHz	IEC 61000-4-8 60 Hz Magnetic Field	IEC 61000-4-9 Pulsed Magnetic Field	IEC 61000-4-10 Oscillatory Magnetic Field
	9561-110N	Digital Input, 115 VAC	Pass	Pass	Pass	Pass
3623T	9664-810N	Digital Output, 120 VDC	Pass	Pass	Pass	Pass
3603T	9664-810N	Digital Output, 120 VDC	Pass	Pass	Pass	Pass
3601T	9663-610N	Digital Output, 115 VAC	Pass	Pass	Pass	Pass
3503E	9563-810N	Digital Input, 24 VDC	Pass	Pass	Pass	Pass
3625	9662-810N	Digital Output, 24 VDC	Pass	Pass	Pass	Pass
3636T	9668-110N	Relay Output	Pass	Pass	Pass	Pass
3607E	9667-810N	Digital Output, 48 VDC	Pass	Pass	Pass	Pass
3502E	9562-810N	Digital Input, 48 VDC	Pass	Pass	Pass	Pass
3701	9795-610N	Analog Input, 0-10 VDC	Pass	Pass	Pass	Pass
	9783-110N	Analog Input, 0-10 VDC	Pass	Pass	Pass	Pass
3703E	9790-610N	Analog Input, 0-10 VDC	Pass	Pass	Pass	Pass
	9783-110N	Analog Input, 0-10 VDC	Pass	Pass	Pass	Pass
3805E	9860-610N	Analog Output, 4-20 mA	Pass	Pass	Pass	Pass
3721	9764-310N	RTD, No. 1600083-600	**Susceptible**	Pass	Pass	Pass
		RTD, No. 1600083-200	**Susceptible**	Pass	Pass	Pass
		RTD, No. 1600024-040	Pass	Pass	Pass	Pass
		RTD, No. 1600024-030	**Susceptible**	Pass	Pass	Pass
		RTD, No. 1600024-020	**Susceptible**	Pass	Pass	Pass
		RTD, No. 1600024-010	Pass	Pass	Pass	Pass
		mV, No. 1600082-001	Pass	Pass	Pass	Pass
		RTD, No. 1600081-001	Pass	Pass	Pass	Pass
3721	9783-110N	Analog Input, 0-5 VDC	Pass	Pass	Pass	Pass
	9790-610N	Analog Input, 0-5 VDC	Pass	Pass	Pass	Pass
	9783-110N	Analog Input, 0-5 VDC	Pass	Pass	Pass	Pass

4.7 Electrical Fast Transient Testing

EFT Testing of the TUT was performed in accordance with the applicable requirements of NRC Regulatory Guide 1.180, Rev. 1 and IEC 41000-4-4. The following EFT tests were performed (Reference 7.31):

- 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
- ETP 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

A. The TUT met all applicable operational and performance requirements during and after each application of the EFT Test voltages.

B. The EFT Test results demonstrate that the Triconex Tricon v10 PLC will not experience operational failures or susceptibilities due to exposure to repetitive electrical fast transients on the power, communication and signal input/output leads.

4.8 Surge Withstand Testing

Surge withstand testing of the Tricon PLC 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 (Reference 7.27):

- IEC 61000-4-5 Combination Wave: ± 2.0 kV (common mode and differential): Chassis Power Supplies
- IEC 61000-4-12 Ring Wave: ± 2.0 kV (common mode): Chassis Power Supplies
- IEC 61000-4-12 Ring Wave: ± 1.0 kV (differential mode): Chassis Power Supplies
- IEC 61000-4-12 Ring Wave, IEC 61000-4-5 Combination Wave: ± 0.5 kV (differential): AC and DC Rated Discrete Input/Output Modules, Analog Input/Output Modules, TCM Communication Modules, MODBUS Serial Ports
- IEC 61000-4-12 Ring Wave, IEC 61000-4-5 Combination Wave: ± 1.0 kV (common mode): AC and DC Rated Discrete Input/Output Modules, Analog Input/Output Modules, TCM Communication Modules, MODBUS Serial Ports

The specific Tricon hardware that was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List (Reference 7.307.29).

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

B. The Surge Withstand Test results demonstrate that the Triconex 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.

4.9 Electrostatic Discharge (ESD) Testing

ESD Testing of the TUT was performed in accordance with the applicable requirements of Appendix B, Section 3.5 of EPRI TR-102323-R1 and IEC 61000-4-2. The following ESD tests were performed:

ESD Direct Contact Discharges: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV
ESD Direct Air Discharges: ± 2 kV, ± 4 kV, ± 8 kV and ± 15 kV
ESD Indirect Contact Discharges: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV

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

The ESD Test results demonstrate that the Triconex Tricon v10 PLC will not experience operational failures or susceptibilities due to exposure to electrostatic discharges. 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.

4.10 Isolation Testing

Class 1E to Non-1E isolation testing of the Tricon was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 384-1981.

A. The testing demonstrated electrical isolation capability of Model 4352A TCM Communication Module and the Model 3636T Relay Output Module. Note that since interposing relays were required to monitor chassis alarm contacts, the chassis alarms are not qualified for electrical isolation and will require interposing relays, especially if these contacts are to be wired to nonsafety annunciator systems.

B. The testing demonstrated electrical isolation capability of the TCM MODBUS serial communication ports to applied voltages of 250 V ac and 250 V dc, 10 amps maximum, for 30 seconds.

C. The testing demonstrated electrical isolation capability of the relay output points to applied voltages of 600 V ac, at 25 amps maximum, and 250 V dc, at 10 amps maximum.

D. The fiber optic cables are incapable of transmitting electrical faults from the remote Non-1E RXM module to the primary RXM module (which would be installed in the safety related Tricon chassis), and therefore meet IEEE Standard 384-1981 electrical isolation requirements.

4.11 Operability Testing

Operability testing involves exposing the TUT to various normal and abnormal conditions of input/output operation and source power. Operability Testing was performed in accordance with the requirements of Sections 5.3 and 6.4.3 of EPRI TR--107330 and the Invensys Triconex published specifications, to ensure that performance data for the TUT were achieved during and after being subjected to the various qualification tests. The following specific tests were performed:

- Analog Input/Output Accuracy Test
- Response Time Test
- Discrete Input Test
- Discrete Output Test
- Timer Test
- Failover Test
- Loss of Power/Failure to Complete Scan Detection Test
- Power Interruption Test
- Power Quality Tolerance Test

The Operability Tests successfully established performance data for the TUT in accordance with the Invensys Triconex published specifications and/or EPRI TR-107330 specifications and all acceptance criteria stated in the procedure were met.

The test results for the Pre-Qualification Operability Test and Performance Proof Operability Test were analyzed to determine for any degradation in the performance of the TUT. The analyses established that the TUT performed in accordance with Invensys Triconex published specifications and/or EPRI TR-107330 specifications before and,

after Qualification Tests and no degradation in the performance of the TUT were identified.

5.0 PROGRAMMING GUIDANCE

This section provides guidance on development of safety-related application programs for the Tricon. Included is guidance on design of application programs, implementation of software quality assurance processes, and operator notification of Tricon system alarms. Some of the guidance provided on application program design and software quality assurance is not specific to the Tricon system, but is included to assist the plant with understanding applicable regulatory requirements.

5.1 Cycle time

A. The Tricon PLC input to output response times are a function of the actual hardware configuration of the PLC and the scan time of the application program loaded in the PLC. Invensys Triconex provides response time formulas for calculating the upper bound on response times for a particular hardware and application program configuration (Reference 7.32). The application specific maximum allowable response time shall be used to design the Tricon hardware and software configuration. The Triconex calculations do not include the time response of external devices, including the RTD to voltage converters.

B. The scan time of the Tricon must be set to meet the required response time of the process and also to provide adequate margin to allow adequate time to run the diagnostics. To do this, set the Tricon scan time below 50% of the required response time. This provides sufficient processing time to perform diagnostics. Less time may result in decreased diagnostic coverage, which is not acceptable. Any scan time significantly greater than the expected 50% of the target scan time shall result in an alarm to the operator, which would generate an annunciation in the control room. Engineering evaluation of the scan time fault should be performed and adjustments or repairs made if the error persists. These requirements are provided in the TÜV Rheinland restrictions for safety critical use of the Tricon. Further guidance on sampling and process response is found in NUREG-1709.

C. Based on the architecture of the Tricon PLC, consistent loop response times within ±20% are not possible. Rather, the system response time should be based on not exceeding the maximum calculated response time. Testing during the qualification has demonstrated that the measured input to output response times were less than the maximum expected values that were calculated based on equations provided by Invensys Triconex. The testing demonstrates that the response time formulas provide a reliable upper bound on maximum expected response times for a particular hardware and application program configuration. In addition, the test results show no degradation in response time from initial pre-qualification testing throughout qualification and performance proof testing.

D. The Tricon PLC timer function accuracy is a function of the scan time of the application program loaded in the PLC. Specifying an absolute baseline timer function accuracy is therefore inconsistent with the architecture of the Tricon PLC. Instead, application timer function accuracy and the maximum scan time computation for the entire application will be considered in development of any actual application programming. Timers should operate in multiples of the Tricon scan interval to maximize accuracy. During qualification testing, timer functions were demonstrated to not expire any earlier than the required timing period and no later than three scan periods after the required timing period. Longer timers will thus provide increased accuracy. For extremely short timing functions where extreme accuracy is required, an external timing relay is recommended. The accuracy of the timers is dependent on the scan time used in the application. For the specific scan time used in baseline testing, a 1-minute timer function provided accuracy of 0.19%, and a 5-minute timer function accuracy provided accuracy of 0.093%.

E. The response time to an RTD input was not measured. However, the time response of the field installed RTD and the thermowell in which it is likely installed, will be known and the time response of the Analog Devices RTD to voltage converter is published. These values add to the time response determined for an analog voltage input for RTD inputs.

5.2 Software Quality Assurance Processes

General considerations relating to software quality assurance processes include the following:

A. The Triconex Product Alert Notices (PAN), Technical Advisory Bulletins (TAB), and Technical Application Notes (TAN) should be reviewed as they are released for applicability to the installed system. This requires the bulletins go to the engineer responsible for the system, rather than solely to licensing, procurement engineering, or maintenance.

B. The application must be created under a nuclear safety-related software quality assurance process. A process acceptable to the USNRC is outlined in the Standard Review Plan in Branch Technical Position 7- 14.

C. After commissioning, any changes to the application itself or the application program must be made under strict change-control procedures, similar to those required in BTP 7-14. All changes must be thoroughly verified and validated, as well as audited and approved by the plant safety change control committee or

group. After an approved change is made, all appropriate software and documentation must be archived.

D. Configuration data shall be retained, including programs, system configuration, module configuration, input/output databases, and other Tricon and TriStation 1131 configuration items.

E. Since the user readable program is available only on the PC, retention of the PC configuration items is critical for long term maintenance. In addition to printed documentation of the application program, at least two electronic copies of the program must be archived in separate locations. This is necessary to comply with requirements for dual storage of safety related quality records.

F. The archival media must be write-protected after storage of the application program to avoid accidental changes. More robust media than diskettes are recommended, to include the longer-lived CD-R, CD-RW, or DVD.

5.3 Guidance for Application Programming

Specific guidance for development of application programs using the TriStation 1131 programming tool is discussed below. The guidance provided below is intended to: (1) minimize the chance for design errors built into application programs during the development process, (2) maximize the reliability of the process used to download application programs from the TriStation 1131 PC to the Tricon PLC, and (3) support required software quality assurance processes.

A. The PC used for developing, controlling, interfacing, and downloading to the Tricon shall have enabled Error Correcting Code (ECC) memory and shall be listed, at least when initially put into service, on the applicable Microsoft Windows Hardware Compatibility List. This PC should not be used for any other functions, to avoid uncontrolled and unintentional changes to the Windows environment or computer security risks.

B. The Tricon is programmed in one or more of the supported IEC 61131-3 languages. The functional diagrams shall be generated using the TriStation 1131 Developer's Workbench.

C. The TriStation 1131 Developer's Workbench generates printed output of the application software equivalent to the traditional I&C Logic Drawings. This output shall be used for independent verification and validation and application review. This printed output should be considered the primary reference to the application.

D. Programs shall be developed in accordance with TriStation 1131 User's Manuals, which provide guidelines for the programming of software written in Function Block Diagrams, Ladder Diagrams, Structured Text, and Cause Effect Matrix Programming Language. Modifications to certain TUV restrictions related to application programming are provided in this section.

E. Applications programs should be developed with guidance from various industry sources, including NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems."

F. Application programs shall be a product of a disciplined implementation process, providing the traceability necessary to associate source code with higher level design documents to enhance verification, validation, and other aspects of software quality assurance.

G. The programmer shall use methods to maximize structure and readability, including use of comments.

H. Application programs shall be designed to enhance the capability of the software to handle exception conditions, recover from internal failures, and prevent propagation of errors arising from unusual circumstances.

I. Application programs shall be designed to reduce the likelihood that faults will be introduced during adaptive or corrective software changes made after delivery.

J. Each variable shall be initialized. Variables may be set once in the first scan after startup, or in each scan, as required by the programmed function. Constant values shall be declared.

K. Constants, such as setpoints, that might require modification are to be defined as variables, to allow online changes to these variables without requiring a software download. TriStation 1131 can modify Tricon variables without having to download the complete application.

L. Comments shall be included in the program. Each network purpose shall be commented. Operations or series of operations shall be described in comments, to maximize the ease of reading, understanding, and modifying networks. Comments shall be structured and placed in the network to minimize interface ambiguities and errors.

M. Application program comments should reference the higher-level design documentation, particularly for data type, variable, and constant declarations.

N. For any unusual or complex constructs as well as any deviations from normal programming practices, comment blocks shall be provided explaining the purpose and operation of the construct or the reason for the deviation.

O. Names for variables, procedures, functions, data types, constants, exceptions, objects, methods, labels, and other identifiers shall be descriptive, consistent, and traceable to higher-level (i.e., software design) documents. Naming conventions are an important part of the coding style and practices. Using the same name for multiple variables should be avoided unless obviously advantageous and, when employed, shall be accompanied by clear, consistent, and unambiguous notations in all locations where the variable is used.

P. The Tricon must detect open and short circuits in the wiring between the PLC and the critical field devices, as well as open or short circuits in the field devices. Detected faults shall be alarmed in the control room. An application should not use the OVDDISABLE function, which disables the output module short, open, and load validation self test functions for any supervised outputs.

Q. Existing Triconex-supplied functions and Structured Text can be used to create special purpose function blocks in the User Library for use in program generation.

R. Support for surveillance testing shall be provided in the basic Tricon application program. No program changes shall be necessary to implement any of the required periodic surveillance tests.

S. A Tricon normally does not contain any disabled points unless there is a specific reason for disabling them, such as initial testing. To disable points, the Tricon keyswitch must be in PROGRAM mode rather than RUN or REMOTE mode. If the system does contain one or more disabled variables, then an installed network should annunciate in the control room to indicate that disabled points are present. No disabled points should be present in an operating unit.

T. TÜV requires a safety application to include networks that will initiate a safe shutdown of the process being controlled if the Tricon goes to single processor mode. In a nuclear environment, the expected divisional or channel redundancy in nuclear applications does not require this functionality. However, any of the faults identified below should be annunciated in the control room and should be repaired in an expeditious manner. The following system information variables, accessible

as outputs of the TR_MP_STATUS function block, should be checked:

- **MPMAIN**-At least one Main Processor is out-of-sync or faulted.
- **IOMAIN**-MPMAIN is on, or at least one leg of one I/O module has faulted.
- **MPBAD**-Two Main Processors are out-of-sync or faulted (in single mode).
- **IOBAD**-MPBAD is on, or at least one I/O module is in single mode.

U. One condition that can energize the IOBAD variable is the presence of Bad Board errors on any two legs of an I/O module. Bad Board means that a fatal error has been reported by one of the legs of the I/O module, or communication to one of the legs has been lost. However, the IOBAD variable cannot distinguish between modules that are critical to the process and modules that are not critical. For example, an output module that interfaces to status lamps on a local panel is usually not critical to the process. Logic should be generated which provides a lower level annunciation of the detected fault for those modules that do not perform safety-related functions. This logic should consider whether reflash of the output is necessary as additional faults occur. With this additional logic, repair of the failed module is still required, but at a lower priority than repair of modules implementing safety critical functions.

V. The system mechanisms to detect failure to complete a scan (or watchdog timers) are checked during hardware diagnostics performed on power-up of the Tricon PLC. If a failure of a watchdog timer mechanism is detected, the PLC power-up will stop and the main processor fault indicators will turn on. Therefore, successful restart of the Tricon PLC on restoration of power indicates proper functioning of the watchdog timer mechanisms. Additionally, these watchdog timers are periodically tested during system operation.

5.4 Loss of Power Fault Indication

A. The Tricon PLC exhibits clear indications of power loss on chassis alarm relay outputs, analog outputs, and discrete outputs. All outputs are placed in a fail-safe, de-energized condition during power failure. The Tricon PLC also provides clear indication of power restoration through the same mechanisms.

B. On one occasion during qualification testing for the V9, a Tricon module did not restart on a momentary loss of power. Triconex Design Engineering indicates that, with one power source turned off and momentary glitches on the redundant power source, there is a remote possibility that the power fail/reset circuit on an

individual module may not operate correctly. This fault was clearly indicated on the system and was resolved by recycling the system power supplies. Most electronic equipment cannot tolerate short duration, transient power losses.

C. During qualification testing loss of power tests were performed. The test results demonstrate a predictable and consistent response of the Tricon PLC to loss of power including:

(a) Chassis alarm relay circuits change state to indicate the loss of power condition.

(b) Analog output points go to a zero output value during the loss of power period.

(c) Discrete and relay output points held closed during application program execution open during the loss of power period.

(d) All communication links to peripheral devices are disabled during the loss of power period. The communication links that were monitored during testing include the TCM module connections to the TriStation Console and the Simulator Tricon PLC running the MODBUS protocol and Peer-to-Peer networking.

D. The loss of power test results also demonstrate a predictable and consistent response of the Tricon PLC to restoration of power including:

(a) Chassis alarm relay circuits change state to indicate restoration of power.

(b) Analog output points go to the value commanded by the application program on restoration of power.

(c) Discrete and relay output points held closed during application program execution re-close on restoration of power.

(d) All external communication links are restored on restoration of power.

5.5 Communication with External Systems

A. Communication with external systems must use the approved module.

B. There are no restrictions on incoming communication from external systems when operated in a mode where only date and time adjustments are allowed to the Tricon. Restrictions are provided and must be incorporated when the external

systems are allowed to write data into the Tricon, as defined in Sections 5.5, D, and 6.5 of this report.

C. Under certain conditions, the Tricon may be run in a mode where an external computer or operator station can write to the Tricon PLC variables. This is normally done by means of a communication link. In this mode, serial communication must not be allowed to write directly to input or output variables. Restrictions and guidance for Maintenance and Override functions are provided in a separate section of the application guideline. These restrictions are based on guidance from the "Safety Considerations Guide for Tricon v9—v10 Systems." The communication link and variables shall comply with the Maintenance and Override requirements provided in Section 6.5 of this Application Guide.

D. Nonsafety and safety communication links cannot be mixed on any communications module.

5.6 Peer-to-Peer Communication

A. The Tricon supports redundant physical peer-to-peer communication links and provides embedded support for the redundancy. Application programs can determine whether the peer-to-peer network is operating in single or redundant mode. If the peer-to-peer operation is critical, loss of redundancy should be alarmed in the control room.

B. Any use of the peer-to-peer communication shall be evaluated to determine if the delay between message initiation and message reception is acceptable for the given safety related application. The normal delay is up to 6 scan times.

C. The sending node must set the sendflag in the send call to one so that the sending node sends new data as soon as the acknowledgment for the last data is received from the receiving node.

D. Because safety systems tend to remain in a single state for extended periods, messages containing state values may not change regularly. The sending node must use the TR_USEND function block and include a diagnostic integer variable that gets incremented with each new message. The receiving node must check this variable for change every time it processes new data, because the message itself may not change.

E. The sending node should require no more than five TR_USEND functions in an application. The Tricon only initiates five TR_USEND functions per scan. In order to send data as fast as possible, the TR_USEND function must be initiated

as soon as the acknowledgment for the last data is received from the receiving node. If maximum throughput is not required, more than five TR_USEND functions may be programmed. Evaluations should be performed to verify that the required safety functions occur within the maximum time interval possible for multiple communications failures on all transmitted messages.

F. The sending node must check the status of the TR_URCV and TR_PORT_STATUS functions to see if there is a network problem.

G. The receiving node's application must include logic to see whether new data is received within the specified maximum time-out limit. The maximum time-out limit is equal to half the process-tolerance time. If the receiving node does not get at least one sample of new data from the sending node within the maximum time-out limit, then the receiving node's program must take one or more of the following actions, depending on requirements for the safety functions being implemented:

- Use the last data received for safety-related decisions in the application.
- Use default values for safety-related decisions in the application
- Initiate the appropriate safety functions.

H. If new data is not received within the specified maximum time out limit, the receiving node's application must also check the status of the TR_URCV and TR_PORT_STATUS functions to see if there is a network problem that requires operator intervention.

I. In any case, this failure shall be annunciated in the control room, preferably from both Tricon PLCs, and appropriate maintenance action shall be implemented immediately. The specific actions that an application should take depend on the process safety requirements. The receiving node must check the diagnostic integer variable every time it receives new data to see whether this variable has changed.

5.7 Communication Application Safety Layer

A. The Tricon supports redundant physical safety-related SAP communication links with qualified display units. If the communication is safety-related, loss of redundancy must be alarmed in the control room.

B. In the Tricon System, the communication subsystem cannot be used to provide measures and techniques to insure the integrity of communication. As with Peer

to Peer (section 5.6), the application on each end is responsible for the end-to-end integrity of safety-critical communications.

C. The safety-related application code implementing the SAP must be functionally independent from the transmission code (i.e., the network stack).

D. Even when the messages are arriving in a correct (deterministic) manner the safety data still may be corrupted. As with Peer-to-Peer, the data integrity assurance is a fundamental component of the safety-related application code implementing the SAP to achieve the communication-link integrity requirements.

E. The communication channel (i.e., transmission protocols at the lower layers of the network stack) must not use the same hash function as the SAP.

F. All SAP-defined measures for data integrity assurance must be implemented within the SAP based safety application.

G. SAP communication error handling will be defined and implemented by the application program.

H. Any use of the SAP for communication must be evaluated to determine if the delay between message initiation and message reception is acceptable for the given safety-related application.

I. The application on each end shall implement a diagnostics message to detect loss of communication.

J. Detected communication failures shall be annunciated in the control room, from the Tricon PLC(s). The safety-related display unit shall program and display the alarm for the detected communications errors.

6.0 INSTALLATION, COMMISSIONING, AND MAINTENANCE

This section discusses considerations for installation, commissioning, and long term maintenance of safety-related Tricon systems. This guidance is intended to identify important considerations for these activities particularly for microprocessor-based safety systems. As such, much of the guidance is relatively generic in nature and is not specific only to the Tricon system.

6.1 Required testing

A. Functional testing must be performed to validate the correct design and operation of the user-written application program for commissioning and after any modification is implemented. The amount of validation after a change must be appropriate to the magnitude and safety criticality of the modification.

B. After a safety system is commissioned, no changes to the system software (operating system, I/O drivers, diagnostics, etc.) may be performed without re-commissioning the system. This requirement is provided in the TÜV Rheinland restrictions for safety critical use of the Tricon.

C. Periodic testing shall be performed to the requirements established in the Technical Specifications. Credit for self-tests can be used to reduce the requirement for surveillance testing, based on changes to the Technical Specifications. Guidance for applying the inherent and application program generated capabilities of the Tricon PLC for surveillance is provided in a separate section of this report.

6.2 Operations Procedures

A. Dependent on the level to which faults are displayed in the control room, abnormal operating and alarm response procedures will require modification. If, for example, the operator can query the status of individual Tricon modules, more detailed procedures and training will be required than if a multiple level failure and trouble alarm annunciation scheme is provided with Maintenance personnel providing troubleshooting and Technical Specification impact determination.

B. Operating procedures for the safety system being replaced will have to be modified to accommodate the Tricon. Procedures for new fault alarms will have to be created. Procedures for the unlikely software common cause failure will have to be validated. Procedures for entry, exit, and performance of maintenance and surveillance testing procedures will have to be modified or enhanced for the differences between an older analog and a newer digital protection system.

6.3 Maintenance Procedures

Specific maintenance considerations for the Tricon system include the following:

A. The Tricon PLC Main Chassis requires two batteries for RAM backup of the application programs. These batteries provide backup power to maintain system programming in the unlikely event of total loss of the two independent power sources and chassis power supplies. When powered, the Tricon will alarm when the battery power falls to a point where it can no longer support system operation. Based on the shelf life limitations of lithium batteries, new batteries should be ordered when the battery life alarm occurs or every ten years, whichever comes first.

B. The Tricon PLC power supplies contain electrolytic capacitors for filtering. These power supplies should be replaced on a ten year cycle.

C. Section 5 of the Triconex Planning and Installation Manual contains recommendations for periodic testing of power supplies and toggling field points.

D. The maintenance procedures should be written with the guidance from the Triconex Planning and Installation Guide (Reference 7.13).

E. Logical pairs of locations exist for input and output module locations. For a given location, either of the two logical locations are equivalent. Procedures and documentation should be generated that allow the normal primary card to be installed in either of the logically paired locations in a chassis. Thus, the spare card referred to in this section could be either location in a logical pair of locations and the primary module could be in either location as well.

F. In order to assure timely access to known operable modules, it is recommended that spare modules be installed in the on-line Tricon PLCs. At least one hot spare of every type of I/O module should be installed in each division, channel, or train. This hot spare module should be installed as active, redundant cards. By keeping the modules in operation, any faults on the spare modules will be diagnosed by the Tricon, since the spare modules will be actively used in control. There are no identified life-limited failure mechanisms for these modules. By following this recommendation, the spare modules will be available for instant use by maintenance personnel. When a faulted module is returned to Triconex for repair, additional spare modules exist in other divisions, channels, or trains.

Additional important maintenance considerations for digital systems that are not specific to the Tricon system include the following:

G. Procedures shall be developed to support normal maintenance functions. Since an installed spare is expected to be available in each division or channel, the procedures should be based on used of that spare module or a module from another division or channel, to replace the failed module. The industries currently using the Tricon for safety functions offer several lessons learned. This process is based on those lessons. The procedures for module replacement shall include appropriate instructions to 1) find, verify, and remove only the inactive spare card from the bypassed channel in preparation for replacing the faulted module, 2) insert the spare card at the faulted module logical paired location, 3) wait for the system to transfer control to the newly installed module, 4) remove the faulted module only after the Tricon has been confirmed to have transferred control to the new module, 5) repair the faulted module after diagnosis of the problem, and 6) reinstall the refurbished module as a hot spare somewhere in the channel, division, or train.

H. Modifications resulting from Maintenance procedures must be coordinated with Operations to minimize risk during performance of the Maintenance procedures, including surveillance testing.

6.4 Application Program Maintenance Procedures

Considerations for application program maintenance procedures that relate specifically to the Tricon system include the following:

A. Applications procedures should be created and implemented for configuration management.

B. A procedure shall be written for downloading a configuration to the Tricon. This procedure shall provide compensatory measures to disable the Tricon outputs during the download. A procedure is provided in the Triconex TriStation 1131 Developer's Workstation User's Guide for a Download All into a Tricon PLC, in the section labeled 'Downloading A Project.' Since this procedure requires removal of all three Main Processors to clear all of the application code from memory completely, all Tricon outputs will go to the fail-safe state, with all discrete outputs powered off and analog outputs set to 0 milliamperes. Operations and Engineering should be adequately prepared to avoid unnecessary challenges to other safety systems and the nuclear generating station.

C. Based on TÜV's evaluation and recommendations, when development and testing of the safety application is complete or after any modifications are performed, the Download All and Compare functions should be used to download and verify the success of the download of the final application to the Tricon. When the

download is verified to be correct, the RUN or REMOTE function is used to start running the programs. Any required testing would be performed and the Tricon would be removed from bypass. Taking these steps guarantees that all of the variables in the safety application logic will be initialized properly in the Tricon's memory, and that only a valid downloaded program would be loaded in the Tricon. This also resolves the issues and concerns from multiple downloaded changes, including fragmentation and possible exhaustion of free memory in the Tricon.

D. Connecting a TriStation PC to an online Tricon is possible. With the keyswitch in the RUN position, the TriStation can not affect the program or variables. With the keyswitch in the RUN position, the TriStation cannot pause or halt the application program. There is also password security in the TriStation 1131 to lessen the chance of unauthorized access. For that reason, there are no restrictions to connecting a TriStation PC to a Tricon.

E. While not specific to the Tricon system, any changes to the application itself or the application program after commissioning must be made under strict change-control procedures, such as those required in BTP-14. Modifications to the application software shall be made with at least as rigorous a set of software quality assurance procedures, including independence of verification and validation activities, as were used during the initial program development. All changes must be thoroughly verified and validated, as well as audited and approved by the plant safety change control committee or group. After an approved change is made, it must be archived.

6.5 Maintenance and Bypass Capabilities

Existing safety-related systems in nuclear power plants typically include bypass capabilities for maintenance and testing. Implementation of these capabilities in a digital system requires particular attention to prevent undesired operation of the system. Generic guidance on the implementation of bypass capabilities is provided below.

A. Maintenance bypasses can be initiated either using special switches connected to PLC inputs, or overrides can be programmed into the Tricon to enable a remote device to serially request the override. This allows the user to request bypassing a single sensor or all functions implemented in a Tricon PLC.

B. If special switches are used to initiate the bypass, these discrete inputs will be used to deactivate actuators and sensors under maintenance or to force safety functions to an enabled or disabled state. The maintenance bypass conditions are handled as part of the application program of the PLC. The switches would

conform to the specifications and requirements for class 1E devices and circuits. This is equivalent to the process currently used in most US nuclear plants.

C. If bypasses are programmed into the Tricon, enabling a remote device to request the bypass over appropriate serial communication links to the PLC, the programming must be implemented in accordance with NRC regulatory guidance.

D. Connecting to the PLC over serial lines shall be performed using protocols with protection from garbled or corrupted communication packets. Any communication protocol used should include CRC, address check, and check of the communication time frame.

E. If no bypass functions are active, lost communication should lead to a warning to the operator. If bypass functions are active, lost communication shall be annunciated to the operator and at the Tricon. After loss of communication, the design safety evaluation should determine whether a time delayed automatic removal of the bypass is desirable. If this function is implemented, a warning should be provided to the operator prior to implementing the removal.

F. The external system shall provide individual action requests as integer values. Each action request shall be provided as separate integer values. If the integer were set to zero, the action request would be cancelled after the implement command contact changes state. The action request integer is required to change on no less than a one-second period. If the Tricon detects an unchanged input for an unacceptable period, the lost communication process described in this section shall be implemented. The commanded action request shall be valid as long as the action request integer value changes on a periodic basis.

G. The use of the maintenance bypass function should be documented on the external system and should be visible on the TriStation 1131, when connected. The data retained should include time stamps at the beginning and end of the bypass; the ID of the person who activated the bypass (if the information cannot be easily entered, it should be retained in the work permit); and the tag name of the signal or function being overridden.

H. The maintenance bypass function would not be performed by the TriStation 1131 engineering workstation.

I. If signal bypass is possible, the Tricon shall have a pre-defined table or code in the application program that defines the signals that may be bypassed and, implicitly, those that may not be bypassed. If simultaneous bypasses are possible for multiple signals, the Tricon shall have a pre-defined table or code in the application programs defining which combinations are acceptable.

J. Direct bypasses shall not be installed on inputs or outputs. Bypasses have to be checked and implemented in relation to the application. Multiple bypasses in a Tricon are allowed as long as only one bypass is used in a given safety related group.

K. An alarm shall exist for bypasses in the appropriate control room. It shall not be possible to override or disable the alarm.

L. The PLC shall alert the operator that a bypass condition exists. The warning shall exist until the bypass is removed. This alert may be used to confirm that the bypass condition has been installed or removed.

M. It may be desirable, from decisions made based on licensing and failure analysis, to have a second, backup, method to remove maintenance bypasses. Functions of this nature require extensive testing prior to being placed in service.

N. The external system and Tricon programs as well as programmatic guidance enforce a limited time span for the bypass to be in place. Typically, no more than one shift should be required or allowed. Hardwired indication should be considered in a location where the control room operator is reminded of the loss of that division or channel of protective functions. The number and location of lamps should be based on the plant license requirements.

O. The external system should check regularly that no discrepancies exist between its bypass command list and the Tricon PLC bypass accepted list.

7.0 REFERENCES

7.1 USNRC Standard Review Plan, Chapter 7, Revision 5

7.2 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position 7-14, Revision 5, Guidance on Software Reviews for Digital Computer-Based I&C Systems

7.3 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position 7-18, Revision 5, Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems

7.4 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position 7-17, Revision 5, Guidance on Self-Test and Surveillance Test Provisions

7.5 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position 7-21, Revision 5, Guidance on Digital Computer Real-Time Performance

7.6 USNRC Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," October 2003

7.7 USNRC Interim Staff Guidance DI&C-ISG-04, Highly Integrated Control Rooms – Communications Issues, Revision 0, September 28, 2007

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

7.9 EPRI TR-102323-R1, Guidelines for Electromagnetic Interference Testing in Power Plants

7.10 IEEE Standard 323-1974, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

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

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

TRICONEX DOCUMENTS

7.13 Triconex Planning and Installation Guide, Part Number 9720077-012

7.14 Triconex User's Manual for Field Terminations, Part Number 9700052-018

7.15 Triconex Technical Product Guide, Part Number 9791007-013

7.16 Triconex TriStation 1131 Developer's Workbench User's Guide, Part Number 9700100-003

7.17 Triconex Safety Considerations Guide for Tricon v9-v10 Systems, Part Number 9700097-007

TRICONEX NUCLEAR QUALIFICATION PROJECT DOCUMENTS

7.18 Qualification Summary Report, Triconex Report Number 9600164-545

7.19 Software Qualification Report, including the Critical Digital Review, Triconex Report Number 7286-535

7.20 Critical Digital Review of the Tricon V10.2.1, Triconex Report Number 9600164-539

7.21 Failure Modes and Effects Analysis, Triconex Report Number 9600164-531

7.22 Reliability/Availability Study, Triconex Report Number 9600164-532

7.23 Tricon System Accuracy Specifications, Triconex Report Number 9600164-534

7.24 Seismic Test Report, Triconex Report Number 9600164-526

7.25 Environmental Test Report, Triconex Report Number 9600164-525

7.26 EMI/RFI Test Report, Triconex Report Number 9600164-527

7.27 Surge Withstand Test Report, Triconex Report Number 9600164-528

7.28 Class 1E to non-1E Isolation Test Report, Triconex Report Number 9600164-529

7.29 Exposure Test Report, Triconex Report Number 9600164-533

7.30 Master Configuration List, Triconex Report Number 9600164-540

7.31 Electrical Fast Transient Test Report, Triconex Report Number 9600164-521

7.32 Response Time Calculation, Triconex Document Number 9600164-731