TRICONEX

Triconex Corporation

15091 Bake Parkway
Irvine, California 92618
United States of America

Telephone +1 949 699 2100
Facsimile +1 949 768 6601
http://www.triconex.com

October 2, 2000

Document Control Desk
United States Nuclear Regulatory Commission
Washington, DC 20555

Subject: Nuclear Safety Related Qualification of the TRICON TMR Programmable Logic Controller (PLC) – Final Qualification Summary Report Submittal

References: 1. Letter, T. Martel (Triconex) to NRC, September 29, 2000, subject; Nuclear 1E Qualification of the TRICON TMR PLC – Additional Project Qualification Document Submittals

2. Project Number 709

Gentlemen:

For the last 36 months, the Triconex Corporation has been involved in an effort to qualify the Tricon Triple Module Redundant (TMR) Programmable Logic Controller hardware and software product line for nuclear safety related applications. This effort has included an extensive program of hardware and software testing, analyses, and evaluation. The purpose of this letter is to submit the final TRICON Qualification Summary Report, Triconex Document No. 7286-545, for your review. The TRICON Qualification Summary Report provides a detailed summary of the results of the nuclear safety related qualification testing program carried out in accordance with the requirements of EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants. The NRC approved the qualification approach outlined in EPRI TR-107330 in a Safety Evaluation Report (SER) issued on July 30, 1998. The TRICON Qualification Summary Report documents compliance with the EPRI document.

Per your request and in order to expedite the review process, Triconex has previously submitted the supporting program, test, evaluation and analysis documents referenced in the TRICON Qualification Summary Report. The most recent reference document submittal was provided by Reference 1. A consolidated listing of all the reference documents submitted to date is provided in Attachment 1.

The final TRICON Qualification Summary report, along with the previously submitted supporting reference documents, provide the basis of our request for NRC issuance of an SER approving the use of Triconex Corporation's TRICON PLC in safety-related applications in nuclear power plants.

D062

We look forward to meeting with you at your convenience to discuss the final Qualification Summary Report and any previously submitted material. In addition to the documents submitted, other associated project records and data are available in the Triconex offices for your review.

If you have any questions regarding the enclosed report, please contact me at (281) 360-6401 or Mr. Michael Phillips at (949) 699-2111.

Sincerely,

Michael Phillips / FOR J.T.M

J. Troy Martel, P. E.
Triconex Nuclear Qualification Project Director

Enclosure
cc: L. Raynard Wharton, NRC (w/o enclosure)
P. Loeser, NRC (w/enclosure)

Attachment 1 to Triconex letter dated October 2, 2000

Listing of Documents Transmitted to the NRC in Support of the
Nuclear Safety Related Qualification of the TRICON TMR Programmable Logic Controller (PLC)

Submittal Date	Document Description	Document Number	Rev
PROGRAM DOCUMENTS			
03/21/00	Quality Plan (Nuclear Qualification Project)	QPL-01	Rev 3
03/21/00	Master Test Plan	7286-500	Rev 2
07/17/00	Master Test Plan	7286-500	Rev 3
03/21/00	Master Configuration List	7286-540	Rev 19
07/17/00	Master Configuration List	7286-540	Rev 20
09/29/00	Master Configuration List	7286-540	Rev 22
03/21/00	Software Quality Assurance Plan	7286-537	Rev 2
TEST SPECIMEN			
09/29/00	Tricon Test Specimen Description	7286-541	Rev 0
09/29/00	Certificate of Conformance	7286-542	Rev 0
04/03/00	Test System Arrangement/Wiring Drawings	7286-001-329	(various)
04/03/00	Test System Functional Diagrams	7286-430-444	(various)
04/03/00	Test System Loop Diagrams	7286-531-543	(various)
TEST PROCEDURES			
03/21/00	Set-up & Check-out Test Procedure	7286-502	Rev 2
03/21/00	Operability Test Procedure	7286-503	Rev 2
03/21/00	Prudency Test Procedure	7286-504	Rev 2
03/21/00	Environmental Test Procedure	7286-506	Rev 0
03/21/00	Seismic Test Procedure	7286-507	Rev 0
03/21/00	EMI/RFI Test Procedure	7286-510	Rev 1
03/21/00	Surge Withstand Test Procedure	7286-508	Rev 1
03/21/00	1E/Non 1E Isolation Test Procedure	7286-509	Rev 0
TEST REPORTS			
07/17/00	Pre-Qualification Test Report	7286-524	Rev 0
07/17/00	Environmental Test Report	7286-525	Rev 0
07/17/00	Seismic Test Report	7286-526	Rev 0
07/17/00	EMI/RFI Test Report	7286-527	Rev 0
07/17/00	Surge Test Report	7286-528	Rev 0
07/17/00	1E/Non 1E Isolation Test Report	7286-529	Rev 0
07/17/00	Performance Proof Test Report	7286-530	Rev 0
TEST SPECIMEN APPLICATION SOFTWARE			
04/03/00	TSAP Functional Specification	7286-517	Rev 1
04/03/00	TSAP Design Specification	7286-518	Rev 1
04/03/00	TSAP Program Listing	7286-519	Rev 4
03/21/00	TSAP Validation Test Procedure	7286-513	Rev 0
07/17/00	TSAP V&V Report	7286-536	Rev 0

Attachment 1 to Triconex letter dated October 2, 2000

Listing of Documents Transmitted to the NRC in Support of the
Nuclear Safety Related Qualification of the TRICON TMR Programmable Logic Controller (PLC)
(continued)

TECHNICAL REPORTS/EVALUATIONS

07/17/00	Software Qualification Report	7286-535	Rev 1
09/29/00	Reliability/Availability Study	7286-531	Rev 0
07/17/00	Failure Modes & Effects Analysis	7286-532	Rev 0
09/29/00	Radiation Hardness Evaluation	7286-533	Rev 1
09/29/00	Tricon System Accuracy Specification	7286-534	Rev 1
10/02/00	**Qualification Summary Report**	7286-545	Rev 1

MANUFACTURER'S DOCUMENTATION

03/21/00	TRICON Hardware User Manuals (binder)		
03/21/00	a) Planning & Installation Guide	9720051-006	Rel. 6
03/21/00	b) User's Manual for Field Terminations	9720052-006	Rel. 6
03/21/00	Manuals for Communication Product (binder)		
03/21/00	a) Network Planning & Installation	9720045-003	Rel. 3
03/21/00	b) Intelligent Communication Modules	9720047-003	Rel. 3
03/21/00	c) Sequence of Events User's Manual	9720042-001	Rel. 1
03/21/00	d) System Aliases Manual	9720054-002	Rel. 2
03/21/00	TS 1131 Programmer Manuals plus CD		
03/21/00	a) Getting Started Guide	9720068-001	Ver. 2.0
03/21/00	b) Users Guide	9720069-001	Ver. 2.0
03/21/00	c) TRICON Libraries	9720066-001	Ver. 2.0
03/21/00	Triconex Training Manual	5600-0020/99	1999
03/21/00	Technical Product Guide, V 9.4	9791007-005	7/99
03/21/00	Technical Product Guide, V 8	9791007-002	2/95

TRICONEX

Project:	NUCLEAR QUALIFICATION OF TRICON PLC SYSTEM
Purchase Order No.:	ST - 401734
Project Sales Order:	7286

QUALIFICATION SUMMARY REPORT

Document No.: 7286-545

Revision 1

September 18, 2000

	Name	Signature	Title
Author:	Eric Claude	[signature]	Engineer
Approvals:	Mitchell Albers	[signature]	Project Manager
	Troy Martel	[signature] /TM	Triconex Project Director
	Jerry McCann	[signature]	VP, Research & Development

TRICONEX

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	Page 1A	Date:	09/18/00

QUALIFICATION SUMMARY REPORT

Document No.: 7286-545

Revision 1

September 18, 2000

QUALITY ASSURANCE DOCUMENT

This document has been prepared, reviewed, and approved in accordance with the Quality Assurance requirements of 10CFR50, Appendix B, as specified in the MPR Quality Assurance Manual.

	Name	Signature
Prepared by:	Eric Claude	[signature]
Reviewed by:	David Herrell	[signature]
Approved by:	Mitchell Albers	[signature]

Document Change History			
Revision	**Date**	**Change**	**Author**
0	6/27/2000	Initial Issue	E. Claude
1	9/18/2000	Incorporate Triconex and STP comments	E. Claude

TABLE OF CONTENTS

SECTION **PAGE**

APPENDICES

1.0 INTRODUCTION

This report documents the basis for generic qualification of the TRICON Version 9.3.1 programmable logic controller (PLC) system for safety-related applications in nuclear power plants. The basis for qualification is compliance with EPRI TR-107330, Reference 7.4, which has been approved by the U.S. Nuclear Regulatory Commission (NRC) as an acceptable approach for qualifying commercial PLCs for safety-related applications. A detailed compliance matrix, included as Appendix A, documents how the TRICON system complies with each of the requirements specified in EPRI TR-107330.

The TRICON is a mature commercial PLC that has been shown by more than ten years of experience to provide safe and reliable operation in safety critical applications. High reliability and system availability is achieved through the triple modular redundant (TMR) architecture. This design enables the TRICON system to be highly fault tolerant, to identify and annunciate faults that inevitably occur, and to allow replacement of modules with the system on-line so that faults are repaired before they become failures. These features are desirable characteristics for nuclear safety systems, and hence there has been substantial interest in the industry in generic qualification of the TRICON platform.

The TRICON system 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. Where appropriate, compliance with the applicable requirements is defined in terms of a "qualification envelope." This envelope defines the range of conditions within which the TRICON system meets the acceptance criteria. In applying the TRICON to a specific safety-related application, the user must confirm that the qualification envelope bounds the plant-specific requirements. Additional guidance on use of the TRICON system in safety-related applications is provided in the Application Guide, Appendix B.

The generic qualification of the TRICON Version 9.3.1 system encompasses both the hardware and the software used in the system. The hardware includes termination panels, chassis, power supplies, main processor modules, communication modules, input/output modules, and interconnecting cabling. The specific TRICON modules selected for qualification are defined in the Master Configuration List, Reference 7.23. These modules provide the functionality that is typically required for safety-related control and protection systems in nuclear power plants. 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 system has involved technical evaluations and qualification tests (i.e., "type" tests). This report summarizes the results of these evaluations and tests and provides references to the applicable documents for more detailed information.

This report is organized as follows:

- Section 2 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 is an overview description of the TRICON system and its major components.
- Section 4 describes the basis for qualification of the TRICON system hardware, including results of environmental, seismic, electromagnetic compatibility, surge withstand, and Class 1E isolation testing.
- Section 5 describes the basis for qualification of the TRICON system software.
- Section 6 provides reference to the detailed system application guidance that is included in Appendix B of this report.

2.0 TRICON NUCLEAR QUALIFICATION PROJECT

Obsolescence of original instrumentation and control equipment in nuclear safety systems is becoming an increasing problem for competitive operation of nuclear power plants. The industry has recognized the need to develop cost-effective replacement systems based on new digital-based technologies that offer improved functionality, reliability, and performance as well as reduced operations and maintenance (O&M) costs and enhanced safety. The industry has also recognized that use of high quality commercial-off-the-shelf (COTS) systems with a large installation base can further reduce O&M costs through more readily available spare parts and long term vendor technical support.

Programmable logic controllers (PLCs) have been widely used in other industries and provide technology that is being used to retrofit current nuclear plant systems. In nuclear safety-related systems, PLCs have already been qualified on a plant-specific basis primarily through dedication of commercial products. However, widespread application of PLCs in nuclear power plants has been hampered by the lack of a generally accepted method for qualifying commercially available PLCs on a generic basis for safety-related service.

An EPRI and utility sponsored working group, using regulatory requirements, standards, and guidelines, developed EPRI TR-107330 to address this issue. The NRC issued a Safety Evaluation Report (SER) in July 1998 endorsing the EPRI approach.

The objective of EPRI TR-107330 is to provide generic requirements for qualifying commercial PLCs for use in safety-related applications in nuclear power plants. 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 plant 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 TR-107330 requirements are intended for qualifying a PLC as a replacement for specific segments of safety systems at existing plants (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 of existing safety actuation systems to perform control actions that are currently performed using electro-mechanical devices 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, EPRI, and the South Texas Project Nuclear Operating Company (STPNOC) to qualify the TRICON system in accordance with the EPRI TR-107330 requirements. Quality assurance requirements and special procedures that were unique to the TRICON qualification project are documented in the Project Quality Plan, Reference 7.21. The major activities completed as part of this project include the following:

- Evaluating the quality assurance (QA) program established by Triconex. Triconex has had a QA program in place since 1985 modeled on the requirements of ASME NQA-1. This program was revised in 1997 to be fully compliant with 10CFR50, Appendix B and 10CFR21. STPNOC conducted an audit of Triconex's QA program and in January 1998 judged that the program complied with 10CFR50, Appendix B and 10CFR21.

- 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 7.23. 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 7.25, and associated drawings, References 7.26 through 7.28.

- 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 plant 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 7.24. The TSAP program and associated V&V activities are documented in References 7.51 through 7.55.

- 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 7.22. Test procedures are provided in References 7.29 through 7.37.

- Performing the qualification tests and documenting the results. Results of these tests, documented in References 7.38 through 7.44, 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 TRICON operating system and programming software is documented in the Software Qualification Report, Reference 7.49. A failure modes and effects analysis evaluating the effects of component failures on TRICON operation is provided in Reference 7.46. Reference 7.45 documents an analysis of TRICON system reliability. An analysis of the effect of radiation exposure on system operation is provided in Reference 7.47. Reference 7.48 provides a summary of the accuracy specifications for the TRICON system for use in calculating instrument measurement uncertainties and establishing critical control setpoints.

3.0 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 7.19, and the Planning and Installation Guide, Reference 7.20. The specific hardware and software that has been qualified is identified in the Master Configuration List, Reference 7.23. 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 is a mature commercial product and substantial operating experience exists, particularly in the hydrocarbon processing, paper products, and marine industries. In fact, the TRICON is the most widely used digital platform for plant safety-critical systems. The first TRICON system, Version 5, was shipped in 1985 and, until the recent retirement of the last installed Version 5 system, had continued to operate with full technical support by Triconex. Since the introduction of the TRICON PLC, more than 3,500 systems have been installed, accumulating more than 100 million hours of operating time. Triconex maintains detailed records of the operating experience with all systems that have been shipped, and this experience has demonstrated that no system has ever failed to take protective action when required.

The TRICON system was designed from the outset 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 downward 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 10CFR50, Appendix B and 10CFR21. 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.

3.1 TRICON System Overview

A typical TRICON system (for example, one channel 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 plants. Each TRICON system includes a main chassis, illustrated in Figure 1, and may also include additional expansion chassis.

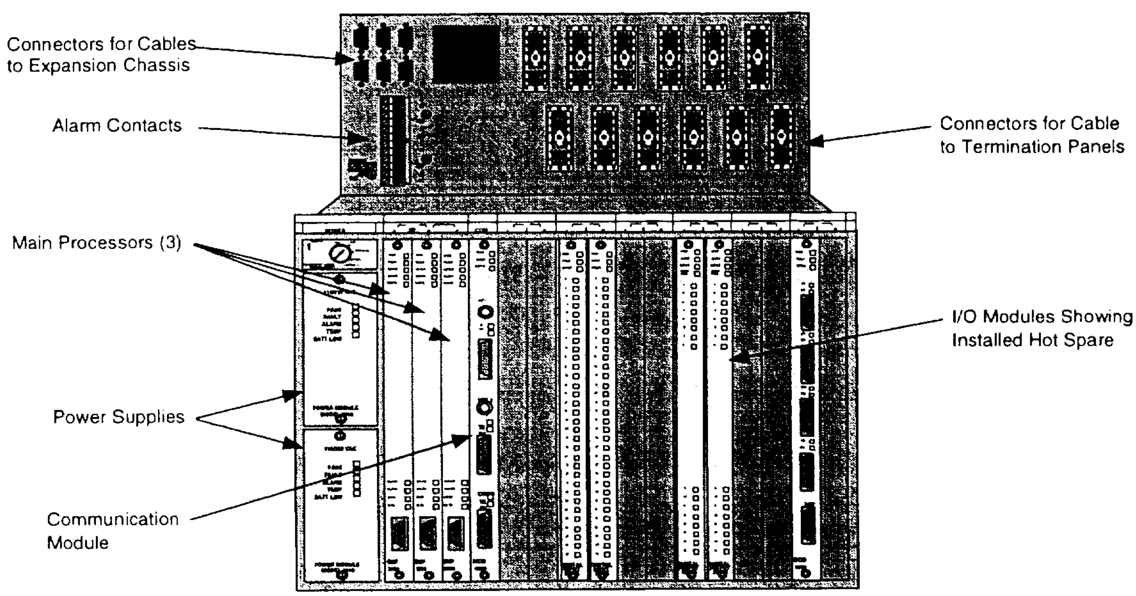


Figure 1. TRICON Main Chassis

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. 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.

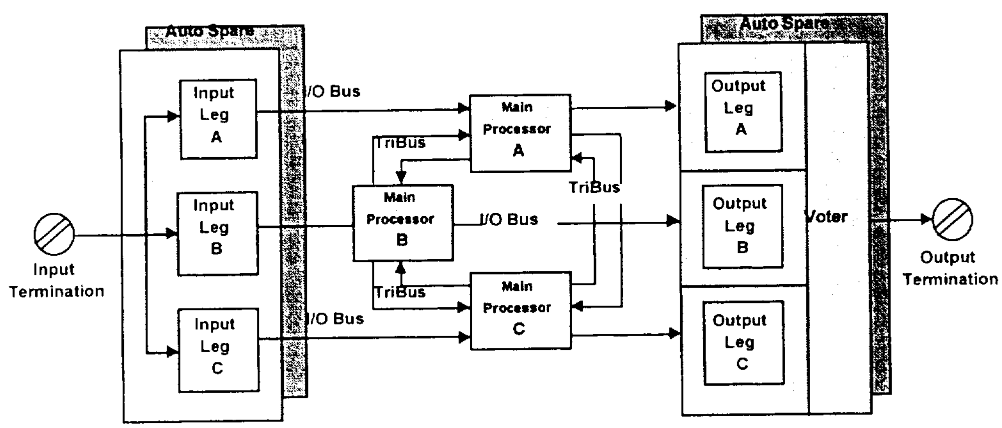


Figure 2. Triple Modular Redundant Architecture.

Figure 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).

3.2 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.

3.2.1 Main Chassis

A TRICON system consists of one main chassis (shown in Figure 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 which 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 via 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 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.

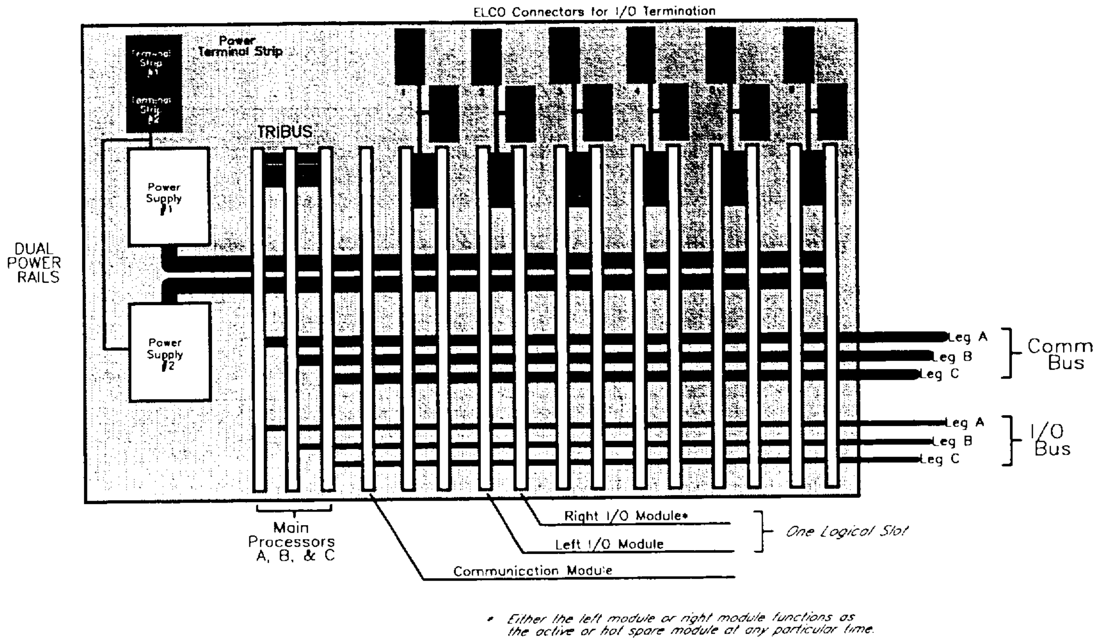


Figure 3. TRICON Chassis Backplane Configuration

3.2.2 Expansion Chassis

Expansion chassis are interconnected via three separate RS-485 communication links, one for each of the three I/O legs. If communication modules are installed, three separate RS-485 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

3.2.3 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.

3.2.4 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 can be ordered with 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.

3.2.5 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. Two qualified models are available to support different power sources: 120 V ac or V dc and 24 V dc. The 230 VAC power supply was successfully tested for environmental and seismic qualification, but was not tested for EMC and surge withstand. Testing of the 230 VAC power will be continued if justified based on utility demand.

The power supply modules possess built in diagnostic circuitry to check for out-of-range voltages and/or over temperature conditions. Indicator 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
- A configured module is missing somewhere in the system
- A module is inserted in an unconfigured slot
- A fault is detected on a Main Processor or I/O module in the main chassis
- A fault is detected on an I/O module in an expansion chassis
- A main processor detects a system fault
- The inter-chassis I/O bus cables are incorrectly installed (i.e. cross connected)

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

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

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

3.2.6 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 8-bit processors and one 32-bit processor. One of the 8-bit processors is a dedicated, leg-specific I/O communication (IOC) microprocessor that processes all communication with the system I/O modules. The second 8-bit dedicated, leg-specific processor manages interfaces with all communication modules in the system.

The 32-bit primary processor manages execution of the control program and all system diagnostics at the main processor module level. Between each 8-bit processor and the 32-bit primary processor is a dedicated dual port 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 read-only memory (ROM) 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 IOC processors constantly poll respective legs for all the input and output modules in the system. They continually update an input data table in shared memory 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 shared memory, 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 shared memory. 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 IOC 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.
- Testing of all basic floating-point processor instructions.
- Verification of the shared memory interface with each I/O communication processor and communication channel.
- Verification of handshake signals and interrupt signals between the CPU, each I/O communication processor and communication channel.
- Checking of each I/O communication processor and communication channel microprocessor, ROM, shared memory access and loopback of RS-485 transceivers.
- Verification of the TriClock 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.

3.2.7 Input/Output Modules

As shown in Figure 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 7.20.

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 7.20.

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.

3.2.8 Communication Modules

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 three types of qualified communication modules are as follows:

- The Enhanced Intelligent Communications Module (EICM) allows the TRICON to communicate with Modbus masters and slaves. Each EICM contains four serial ports and one parallel port that can operate concurrently. Each serial port is uniquely addressed and supports either the Modbus or TriStation interface. The parallel port provides a Centronics interface to a printer.

- The Advanced Communications Module (ACM) acts as an interface between a TRICON and the Foxboro Intelligent Automation (I/A) Series distributed control system. The TRICON system appears to the Foxboro system as a "Control Processor" node on the I/A communication network (the "Nodebus"). The ACM communicates process information at full network data rates for use anywhere on the I/A Series system, transmitting all TRICON aliased data and diagnostic information to operator workstations in display formats. This module can be configured for one-way transmittal of information.

- The Network Communications Module (NCM) allows the TRICON to communicate with other TRICONs and with external hosts over IEEE 802.3 networks. This includes PCs running the TriStation programming software that is used to develop and download application programs to the TRICON controller. The NCM provides two BNC port connectors: Net 1 supports Peer-to-Peer and time synchronization protocols, and Net 2 supports open networking to external systems using Triconex applications.

3.3 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.

3.3.1 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. Three sets of dedicated function microprocessor firmware exist on the main processor. The main 32-bit microprocessor has the operating environment firmware. The two additional microprocessors (the I/O and communication interfaces) each have their own firmware. The main microprocessor firmware includes all the built-in self-diagnostics and triple redundancy functions; no additional diagnostic functions must be developed by the user in the application program.

The operating system executes a sequence of steps in four main blocks: Power Up, Background, Scan Level, and Loader. A detailed description of the system is provided in the Software Qualification Report, Reference 7.49. Briefly, the key functions included in each of the four main blocks include the following:

- Power Up – performs memory, clock, and TriBus communication tests on a reset of the main processor.
- Background – contains runtime diagnostic and fault analysis functions, including microprocessor checks, verification of variables stored in RAM, checks of the I/O and communication bus interfaces, checks on the application program (checksum), and TriBus fault analysis test.
- Scan Level – obtains and votes on input data, executes the application program, and generates outputs at the scan cycle interval set by the application program. The input data validation checks described above are completed during this step.
- Loader – Processes any TriStation messages.

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 HICB-17, "Guidance on Self-Test and Surveillance Test Provisions." The diagnostics are integrated into the base TRICON and require no special 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 BTP HICB-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.

3.3.2 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 can then be 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 via the NCM 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 CRC does not match 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.

3.3.3 Application Program

The application program implements the desired protection, monitoring, and control functions defined by the design basis documents for the plant-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.

3.4 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 7.23. Section 4 of this report summarizes the qualification testing of these modules and the specific qualification envelope applicable to each one.

Table 3-1. Qualified TRICON Modules

MODULE TYPE	MODEL NO.	MODULE TYPE/DESCRIPTION
Main Processor	3006	Enhanced Main Processor II, V9, 2 Mb
Remote Extender	4210	Remote Extender Module (Primary)
	4211	Remote Extender Module (Remote)
Communication	4119A	EICM, V9, Isolated
	4329	Network Communication Module, V9
	4609	Advanced Communication Module
Analog Input	3700A	AI Module, 0-5 VDC, 6% Overrange
	3701	AI Module, 0-10 VDC
	3703E	EAI Module, Isolated
	3704E	HDAI Module, 0-5/0-10 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
	3504E	HDDI Module, 24/48 VDC (24V)
	3505E	EDI Module, 24 VDC, Low Threshold
Digital Output	3601E	EDO Module, 115 VAC
	3603T	EDO Module, 120 VDC
	3604E	EDO Module, 24 VDC
	3607E	EDO Module, 48 VDC
	3623	SDO Module, 120 VDC
	3624	SDO Module, 24 VDC
Pulse Input	3510	Pulse Input Module
Thermocouple Input	3706A	NITC Input Module
	3708E	ITC Thermocouple Input Module
Relay Output	3636R	ERO Module, N.O., Simplex
Power Supply	8310	120 VAC/VDC Power Supply
	8311	24 VDC 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 8.21.

3.5 Qualification of Newer Versions of the TRICON System

Hardware qualification tests were performed on Version 9.3.1 of the TRICON system. Subsequent to this testing, Triconex has released Version 9.4 of the TRICON system. The software qualification effort evaluated Version 2.0 of the TriStation 1131 Developer's Workbench software. This version of the software was released for use with Version 9.4.

Triconex will extend all qualification results to the current TRICON product offering through established quality assurance program procedures.

4.0 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 7.4. 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 7.22. 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, described in Reference 7.29, which documented proper configuration and operation of the test system. This test was performed after manufacturing and assembly of the system, and as required, throughout the qualification process. This test includes verification of hardware, software, and cabling including interconnections to all equipment.

- Operability tests, defined in Reference 7.30, 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, described in Reference 7.31, 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.

A burn-in test, Reference 7.32, was also defined in the Master Test Plan to check for early component failures. However it was concluded that the normal elevated temperature burn-in process that is performed by Triconex as part of the manufacturing process is sufficient to detect early component failures. Consequently, the additional burn-in test was not conducted.

Qualification testing included the following:

- Environmental testing, Reference 7.33, to demonstrate the ability of the TRICON to operate properly under the extremes of temperature and humidity. Proper operation of the system under high radiation levels is also an environmental concern; however this was demonstrated by analysis instead of testing, Reference 7.47. 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 7.34, 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.

- Surge testing, Reference 7.35, to demonstrate the suitability of the TRICON for qualification as a safety-related device with respect to AC power line electrical surge withstand capability.

- Class 1E-to-non 1E electrical isolation testing, Reference 7.36, to demonstrate the suitability of the TRICON for qualification as a safety-related, Class 1E device with respect to providing electrical isolation at Non-1E field connections.

- Electromagnetic compatibility (EMC) testing, described in Reference 7.37, to demonstrate the suitability of the TRICON for qualification as a safety-related device with respect to electromagnetic emissions and susceptibility.

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 the EPRI report. In addition to the radiation withstand analysis noted above, a failure modes and effects analysis, Reference 7.46, and a reliability and availability analysis, Reference 7.45, were performed.

4.1 TRICON Test Specimen Configuration

The tested equipment consisted of four TRICON chassis populated with selected input, output, communication, and power supply modules as shown in Figure 4. The TRICON test specimen also included external termination panels provided for connection of field wiring to the TRICON input and output modules. In addition to the TRICON test specimen, a third-party (Lambda) field power supply was included in selected qualification tests.

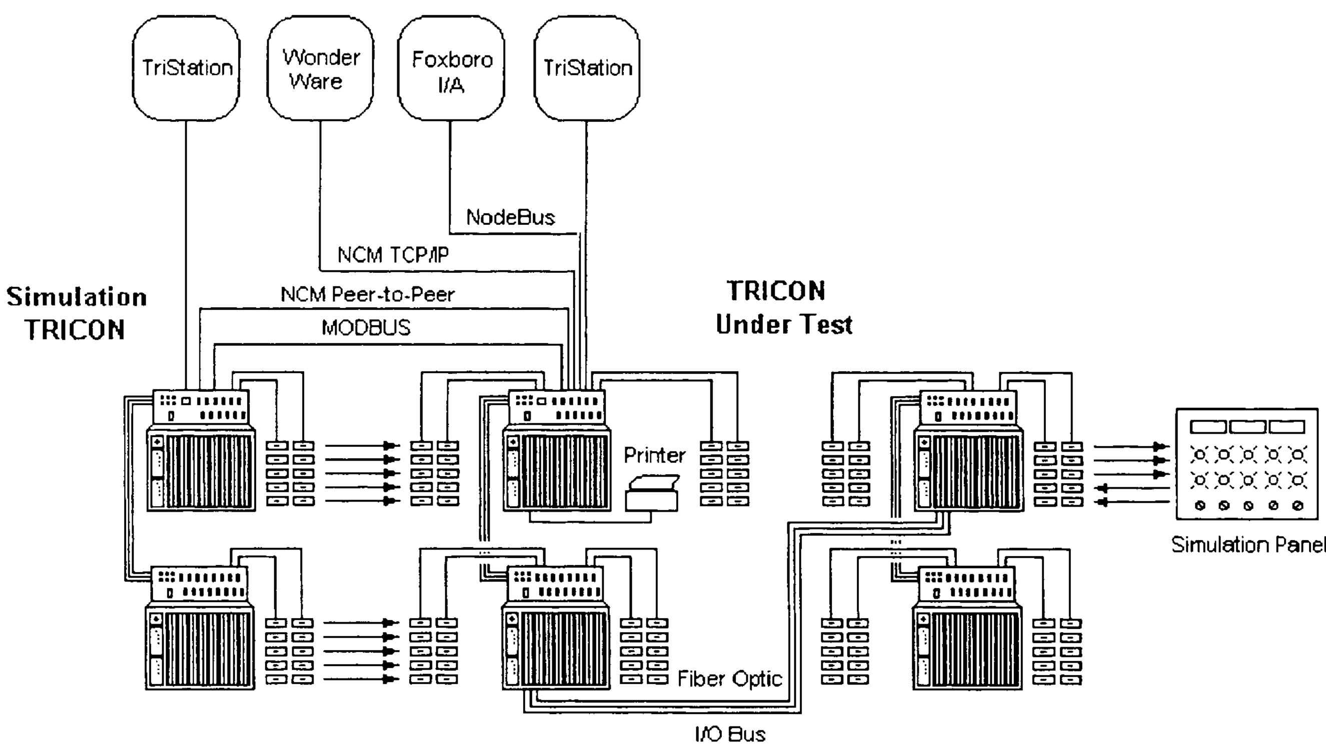


Figure 4. TRICON Test System

Triconex Drawing 7286-102 (Reference 7.28) shows the general arrangement and interconnection of the TRICON Test Specimen chassis. The System Description, Reference 7.25, 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 7.23.

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 7.51. 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 TRICON system. This system was configured with a simulator application program which was used to create a variety of static and dynamic input signals as described in Reference 7.50. Thermocouple and RTD simulators, 4 to 20mA calibrators, and a pulse generator were used to provide additional analog inputs to the TRICON test system.

Analog and digital outputs from the TRICON test specimen were monitored with indicator lights and a data logger system. The data logger system also monitored analog and digital inputs to the TRICON test specimen. This data logger consisted of a PC-based data acquisition system with 29 analog channels and 107 digital channels. Data was recorded with this system during the various tests, and then analyzed 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 TRICON test specimen and the simulator TRICON. The TriStation software used for this purpose was the MSW version, which is a DOS-based program that is superseded by the TriStation 1131 software. The version of the TriStation software used to support the qualification testing has no effect on the results of this testing.

Two additional workstations were installed to demonstrate the ability of the TRICON test system to communicate to external systems throughout the qualification test program. A Foxboro Intelligent Automation (I/A) workstation was installed and configured to monitor the TRICON test system through the ACM module. A Wonderware workstation was installed to monitor the TRICON test system through the NCM module. These two workstations were configured to record system status and diagnostic data from the TRICON and also to monitor the status of internal test specimen variables.

During each of the qualification tests, operation of the TRICON test system was monitored and recorded by the test system data logger and the Wonderware and Foxboro I/A workstations. The recorded data was evaluated in detail before, in some cases 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 TRICON test system, and operation of all peripheral communication interfaces including the Simulator TRICON Peer-to-Peer and MODBUS interfaces, the Wonderware and Foxboro I/A interfaces, and the test system printer interface. The data was monitored for deviations or trends from normal performance.

4.2 Environmental Qualification

Environmental qualification testing of the TRICON test system was performed as described in the Environmental Test Procedure, Reference 7.33. This testing was performed in accordance with the requirements of IEEE 381-1977, Reference 7.9. The objective of environmental testing was to demonstrate the TRICON and the third-party field power supply do not experience failures due to abnormal service conditions of temperature and humidity.

Requirements for environmental testing are specified in EPRI TR-107330, Section 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 the EPRI TR).

- Environmental testing shall be performed with the power supply sources set to values that maximize heat dissipation in the test PLC.

- Power supplies shall be loaded such that nominal current draws at nominal power supply output voltages are equal to the power supply rating.

- The test PLC shall be powered with its TSAP operating during environmental testing, with 1/2 of the discrete and relay outputs ON and loaded to their rated current. In addition, all analog outputs shall be set to between 1/2 and 2/3 of full scale.

Compliance of the TRICON environmental qualification testing with these requirements is described in the Environmental Test Procedure, Reference 7.33.

In addition to the modules which 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 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 7.22, and EPRI TR-107330, Section 4.3.6, Reference 7.4.

- The TRICON Test Specimen 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 TRICON Test Specimen 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 TRICON Test Specimen shall pass the Prudency Test following at least 48 hours of operation at high temperature and humidity.

Environmental testing of the TRICON Test Specimen and Lambda field power supply was performed on October 24 through 30, 1999 at Wyle Laboratories in Huntsville, Alabama. 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 381-1977, Reference 7.9. Results of the testing are described in the Environmental Test Report, Reference 7.39.

As described in the Test Report, the actual sequence of testing was as follows:

- Installation in the Wyle Laboratories environmental test chamber, and stabilization at ambient temperature and relative humidity conditions.
- Ramp-up to 140°F and 95% relative humidity over an 8 hour period.
- Hold at 140°F and 95% RH for a 48 hour period.
- High temperature Operability Test performed over a 39 hour period.
- High temperature Prudency Test performed over a 4 hour period.
- Ramp-down to 35°F and low humidity over a 7 hour period.
- Hold at 35°F and low humidity for an 8 hour period.
- Low temperature Operability Test performed over a 12 hour period
- Ramp-up to ambient temperature and humidity over a 10 hour period.
- Hold at ambient temperature and humidity for a 2 hour period.
- Ambient temperature Operability Test performed over a 9 hour period

The value of relative humidity at the low temperature condition was not established due to measuring equipment malfunction. Nevertheless, as described in the test report, the actual moisture content in the test chamber environment at the low temperature condition was substantially lower then that at the high temperature condition. Accordingly, the test achieved the objective of exposing the tested equipment to a wide range of humidity conditions.

Review of the data collected during the test shows that the TRICON Test Specimen operated as intended. A number of module diagnostic messages were indicated at the TriStation Console during testing. These messages included two indications of Test Specimen 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 7.39. It is important to note that the diagnostic messages did not indicate failures of the system, only faults. The system met its safety function throughout testing.

For example, thermocouple modules produced "bad cold junction" messages when the ambient temperature was not within the 32 to 140°F design range of the module. The data collected, however, shows that the thermocouple modules produced accurate temperature readings at all times. Other messages were generated because of a loose wire and off-normal conditions created by manipulating the connected test system circuits. As expected, all of the diagnostic messages cleared when the initiating condition was removed.

The two hardware faults that occurred did not affect the expected operation of the TRICON, which is consistent with the fault tolerant design of the system. These two faults are described in the Test Report, and include the following:

- The Model 3603E 120 VDC digital output module developed a voter fault diagnostic during the high temperature Operability test period. The spare 3603E module was installed, operated correctly throughout the remainder of the environmental test, and did not experience any faults.

- The Model 3611E 115 VAC digital output module developed a diagnostic fault message during the high temperature Operability test period. The fault remained into the ambient temperature hold period. The spare 3611E module was installed, operated correctly throughout the remainder of the environmental test, and did not experience any faults. However, the root cause of the module fault could not be determined, and it was therefore concluded that the module did not demonstrate acceptable operation during environmental testing.

Two other modules, a Model 3703E 4-20 mA input module and a Model 3708E thermocouple input module were also replaced with spare modules during the environmental testing. These modules did not experience any hardware failures, but were replaced simply to clear diagnostic messages so that operation of the modules could be monitored more easily. The Test Report provides additional details on these modules.

All module replacements were performed in a manner consistent with Section 5.9.8 of IEEE 381-1977 which describes acceptable methods for replacing components during qualification testing. In all cases, the replacement modules had been in the environmental chamber since the start of the test, and thus were exposed to the same temperature and humidity profile.

Review of the post-test operability and prudency test results shows that exposure to the environmental test conditions had no adverse effect on the TRICON Test Specimen and Lambda field power supply performance.

Conclusions from this test are as follows:

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

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

3. Two digital output module faults occurred during environmental testing which were the result of component failures. Because of the fault tolerant design of the TRICON PLC, the digital output points of the two modules (Model 3603E and Model 3611E) continued to perform as expected. However, based on post-test inspection results, the Model 3611E module is not recommended for nuclear safety related application. The Model 3601E module provides functionality comparable to the Model 3611E and demonstrated acceptable performance during environmental testing.

4. The environmental test results demonstrate that the TRICON PLC and the Lambda field power supply will not experience failures due to abnormal service conditions of temperature and humidity.

4.3 Seismic Qualification

Seismic qualification of the TRICON was accomplished by performing the seismic test as described in Reference 7.34. The objective of seismic testing is to demonstrate the suitability of the TRICON and the Lambda field power supply for qualification as a Category 1 seismic devices.

EPRI TR-107330, Sections 4.3.9 and 6.3.4, requires that the test PLC be seismically tested in accordance with IEEE 344, Reference 7.8. 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.

Compliance of the TRICON seismic qualification testing with these requirements is described in the Seismic Test Procedure, Reference 7.34.

The TRICON Test Specimen and Lambda field power supply were mounted to the seismic test table in accordance with mounting details provided on Triconex Drawing No. 7286-101. The seismic test mounting simulated a typical 19" rack mount configuration using standard TRICON front and rear chassis mounting brackets and fastener hardware, standard TRICON external termination panel mounting plates, and manufacturer supplied field power supply mounting plates. All fastener torque values indicated on Triconex Drawing 7286-101 were verified. Additional details on the equipment arrangement for seismic testing are provided in the Seismic Test Report, Reference 7.40.

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 TRICON Test Specimen 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 TRICON Test Specimen shall remain intact, all modules installed in the TRICON Test Specimen shall remain fully inserted, and no functional or non-functional parts of the TRICON Test Specimen shall fall off.

- The Model 3636R electromechanical 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.

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

Seismic testing of the TRICON Test Specimen was performed on November 1 through 4, 1999 at Wyle Laboratories in Huntsville, Alabama. Tests were performed in accordance with the Triconex Seismic Test Procedure, Reference 7.34. The following tests were performed in the order given:

- Resonance search testing was performed as described in IEEE-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 50 Hz test frequency range, the accelerations experienced at the response accelerometer attachment points equaled or slightly 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 same test response spectrum (TRS) which is shown in Figure 5. The acceleration capability of the Wyle Triaxial Seismic Simulator Table was limited to a maximum of 10 g's based on 5% damping with the equipment tested. Therefore, OBE and SSE tests were performed using a maximum acceleration level of 10 g's.

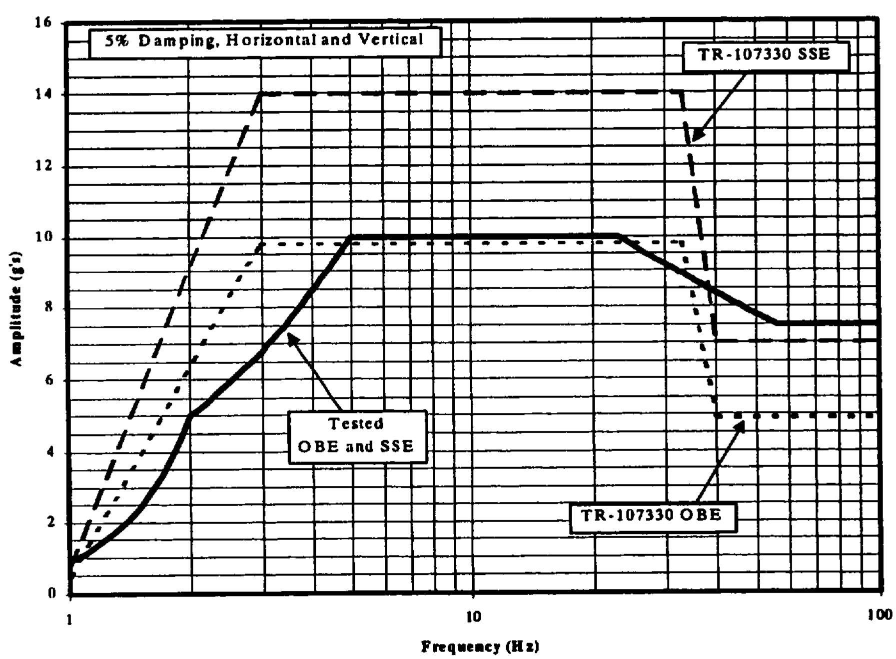


Figure 5. Seismic Test Accelerations

The TRICON Test Specimen and field power supply performance were monitored at the start of, during and for a short period following each OBE and SSE test. During testing, the TRICON Test Specimen was operating in accordance with execution of the Test Specimen

Application Program (TSAP). The field power supply was powered and supplying 90% rated current to resistive load banks.

Results of the testing are described in the Seismic Test Report, Reference 7.40. Data collected during and after each OBE and SSE test demonstrate that the TRICON Test Specimen operated as intended throughout the testing. The monitored output voltage of the Lambda field power supply shows that it varied no more than 1% throughout all of the seismic testing, demonstrating acceptable operation.

The TRICON Test Specimen 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 TRICON Test Specimen was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 344-1987.

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

3. The seismic test results demonstrate that the TRICON PLC platform and the Lambda field power supply are suitable for qualification as Category 1 seismic equipment.

4. The horizontal and vertical seismic withstand response spectrum of the TRICON PLC and Lambda field power supply as determined by testing is shown in Figure 5. The figure is based on a damping value of 5% used in the data analysis.

5. The seismic test results demonstrate that the equipment mounting configurations shown in Triconex Drawing No. 7286-101 are adequate to support seismic qualification of the TRICON PLC and the Lambda field power supply.

4.4 Radiation Qualification

EPRI TR-107330, Section 4.3.6, requires that the test PLC be able to withstand a radiation exposure of up to 1000 rads. The TR further states that evaluations are adequate to demonstrate radiation withstand capability. The Triconex Radiation Analysis Report, Reference 7.47, provides an evaluation of the withstand capability of the TRICON to a cumulative radiation exposure of 1000 rads over a 40 year operating period. The evaluation concludes that this exposure will not prevent the TRICON from performing its safety-related function.

4.5 Electromagnetic Compatibility Qualification

Electromagnetic interference (EMI) and radio frequency interference (RFI) testing was performed to demonstrate the suitability of the Triconex TRICON PLC for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility.

All of the TRICON Test Specimen components were subjected to EMI/RFI testing as required except for the 230 VAC power supply module and the third party Lambda field power supply. Due to time constraints on testing encountered while at Wyle Laboratories, EMI/RFI testing of these components was not performed. Future testing to establish EMI/RFI performance of these components will be performed if justified by utility demand for the components.

EMI/RFI testing of the TRICON Test Specimen was performed inside a shielded enclosure at Wyle Laboratories in Huntsville, Alabama. The testing was performed in accordance with the EMI/RFI Test Procedure, Reference 7.37, and in accordance with the EPRI TR-107330 and TR-102323 test method requirements. The specific tests conducted include the following MIL-STD-462D and IEC test methods:

Test Type	Test Method	Frequency Range
Conducted Emissions	CE101	30 Hz to 50 kHz
Conducted Emissions	CE102	50 kHz to 400 MHz
Radiated Emissions, Magnetic Field	RE101	30 Hz to 100 kHz
Radiated Emissions, Electric Field	RE102	10 kHz to 1 GHz
Conducted Susceptibility, Audio Frequency	CS101	30 Hz to 50 kHz
Conducted Susceptibility , High Frequency	CS114	50 kHz to 400 MHz
Radiated Susceptibility, Magnetic Field	RS101	30 Hz to 100 kHz
Radiated Susceptibility, Electric Field	RS103	10 kHz to 1 GHz
Conducted Susceptibility, EFT/Burst	IEC 801-4	2.5 to 5 kHz, 3 Hz Burst Repetition Rate

Where necessary, testing was also performed at levels lower than the EPRI TR specified levels to establish the envelope of acceptable performance.

The TRICON Test Specimen was installed in the EMI/RFI chamber in open-frame racks as required by the EPRI TR. 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 a revised TSAP operating. 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 TRICON Test Specimen is described in the EMI/RFI Test Procedure, Reference 7.37.

During EMI/RFI testing, operation of the TRICON test system was monitored by the test system data logger and the Wonderware and Foxboro I/A workstations. The status of the TRICON diagnostic indicating LED's was also recorded to demonstrate continued correct operation.

The EPRI TR 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, Surge Withstand, 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 7.22, and EPRI TR-107330, Section 4.3.7, Reference 7.4:

- The TRICON Test Specimen shall meet allowable equipment emission limits as specified in EPRI TR-102323 for conducted and radiated emissions.
- The TRICON Test Specimen shall operate as intended during and after application of the EMI/RFI test levels specified in EPRI TR-102323 for conducted and radiated susceptibility.

In addition, evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance 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%.

EMI/RFI testing of the TRICON Test Specimen was performed from November 9 through December 9, 1999 at Wyle Laboratories in Huntsville, Alabama. Results of the susceptibility testing showed that the TRICON main processors and coprocessors continued to function correctly throughout all test exposure levels. 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. However, some susceptibilities were identified in the TRICON input, output and communication modules during the following susceptibility tests:

- Radiated Electric Field Susceptibility from 10 kHz to 1 GHz (RS103)
- Low Frequency Conducted Susceptibility from 30 Hz to 50 kHz (CS101)
- High Frequency Conducted Susceptibility from 50 kHz to 400 MHz (CS114)
- IEC 801-4 Electrical Fast Transient (EFT) Susceptibility

For the emissions tests, the TRICON Test Specimen was found to comply with the allowable equipment emissions levels for radiated magnetic field emissions from 30 Hz to 100 kHz (RE101). However, specific exceedances were found for the following tests:

- Radiated Electric Field Emissions from 10 kHz to 1 GHz (RE102)
- Low Frequency Conducted Emissions from 30 Hz to 50 kHz (CE101)
- High Frequency Conducted Emissions from 50 kHz to 400 MHz (CE102)

Detailed results of all the EMI/RFI tests are described in the EMI/RFI Test Report, Reference 7.41. For convenience, these results are summarized in the following table.

Summary of EMI/RFI Test Results

Test	Frequencies	Test Level	Test Results
CE101	30 Hz – 50 kHz	EPRI TR-102323, Figure 7-1	Exceeded limit on 120 VAC power supply leads by 3.1 to 5.6 dB
CE102	50 kHz – 400 MHz	EPRI TR-102323, Figure 7-2	Power supplies passed. Exceeded limit on I/O and communication cables at specific frequencies
RE101	30 Hz – 100 kHz	EPRI TR-102323, Figure 7-3	Passed
RE102	10 kHz – 1 GHz	EPRI TR-102323, Figure 7-4	Exceeded limit at specific locations and frequencies by 0.1 to 21.8 dB
CS101	30 Hz – 50 kHz	6.3 V rms	System passed. Data for five I/O and communication modules was inconclusive as shown in Table 6-1 of the EMI/RFI Test Report.

Test	Frequencies	Test Level	Test Results
CS114	50 kHz – 400 Mhz	89 dB μA (See Note 1)	System passed. Six I/O and communication modules show susceptibility, and four modules were inconclusive as shown in Table 6-1 of the EMI/RFI Test Report.
RS101	30 Hz – 100 kHz	EMI/RFI Test Report, Figure 2-1 (See Note 2)	System and all modules passed.
RS103	10 kHz – 1 GHz	10 V/m	System passed. Data for four I/O modules show susceptibility as shown in Table 6-1 of the EMI/RFI Test Report.
IEC 801-4	2.5 – 5 kHz	+/- 3 kV	System passed. Data for one communication module shows susceptibility as shown in Table 6-1 of the EMI/RFI Test Report.

Notes:

1) EPRI TR-102323-R1 requires CS114 tests be performed at a test level of 103 dB μA, which corresponds with CS114 Curve 4 from MIL-STD-461D. The TRICON was tested at a CS114 test level of 95 dB μA, which corresponds with CS114 Curve 3 from MIL-STD-461D.

2) EPRI TR-102323-R1 requires RS101 tests be performed using the MIL-STD-461D, Army Only test level. The TRICON was tested at levels closer to the RS101 Navy Only test levels. Figure 4-2 in the Application Guide (Appendix B of this report) provides a comparison of the as-required and as-tested levels.

4.6 Surge Withstand

Surge withstand testing was performed to demonstrate the suitability of the TRICON PLC for qualification as a safety-related device with respect to AC power line electrical surge withstand capability. As described above in Section 4.5, time constraints prevented surge testing of the 230 VAC power supply and the third-party Lambda field power supply.

EPRI TR-107330, Section 6.3.5, requires that surge withstand testing of the PLC be conducted in accordance with IEEE Guide C62.45, Reference 7.12, which covers AC power supply connections to the PLC. Since C62.45 does not address surge testing of signal and data communication lines, IEC 801-5, Reference 7.13, was used instead. IEC-801-5 implements surge testing using wave forms described in IEEE C62.41, Reference 7.11.

As described in the Surge Withstand Test Procedure, Reference 7.35, the TRICON Test Specimen chassis power supplies were subjected to the following surge tests:

- 3.0 kV peak, 0.5 μs, 100 kHz ring wave pulses at a repetition rate of approximately one pulse per minute.
- 3.0 kV peak combination wave pulses with an open-circuit voltage waveform of 1.2 μs rise time and 50 μs duration and a short-circuit current waveform of 8 μs rise time and 20 μs duration at a repetition rate of approximately one pulse per minute.

The TRICON I/O and data communication lines were subjected to combination wave pulses with the following amplitudes:

- 500 V peak across one point of each AC rated digital input, digital output and relay output module.
- 1000 V peak between ground and the common connection of one point on each digital input and digital output module.
- 1000 V peak between ground and the shield connection (or the common connection if there is no shield connection) of one point on each analog input and analog output module.
- 1000 V peak between ground and the signal ground pin on selected EICM, ACM and NCM module communication ports.

For I/O modules, one point on each module was tested. Each of the discrete output points included was tested twice, once in the ON state and once in the OFF state.

EPRI TR-107330, Section 4.3.4.3, requires surge withstand testing of any devices required for connecting the main PLC chassis to other types of chassis. The TRICON Test Specimen uses two types of connections between chassis. RS-485 cables are used to directly link the backplane communication bus of connected chassis. No interposing devices are required and therefore surge withstand testing of this connection is not required. RXM modules are used to fiber-optically link the backplane communication bus of connected chassis. Because electrical transients can not be transmitted through the fiber optic cables, surge withstand testing of this connection is not required.

The surge withstand testing was performed at Wyle Laboratories in Huntsville, Alabama. Prior to the start of testing, all of the TRICON Test Specimen modules (power, communication, chassis interface 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 TRICON Test Specimen was powered with the TSAP operating. The AC and DC power sources to the TRICON Test Specimen 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 the TRICON test system was monitored by the test system data logger and the Wonderware and Foxboro I/A workstations. 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 7.42.

The surge withstand test acceptance criteria are as follows, based on Appendix 6 of the Master Test Plan, Reference 7.22, and EPRI TR-107330, Section 4.6.2, Reference 7.4:

- Applying the surge test voltages to the specified test points shall not damage any other module or device in the Test Specimen, or cause disruption of the operation of the Test Specimen 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 7.42, show that:

1. Surge withstand testing of the TRICON Test Specimen was performed in accordance with the applicable requirements of EPRI TR-107330, IEEE Standards C62.41-1991 and C62.45-1987, and IEC Standard 801-5.

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.

3. Six of the eight digital output modules included in the TRICON Test Specimen exhibited vulnerability (permanent damage) to the applied surge test levels. These modules included:

    - Model 3611E, 115 VAC digital output
    - Model 3604E, 24 VDC digital output
    - Model 3624, 24 VDC digital output
    - Model 3607E, 48 VDC digital output
    - Model 3603E, 120 VDC digital output
    - Model 3623, 120 VDC digital output

    In all cases the damaged points were detected by system diagnostics and indicated by status LED's and alarm lamps. In no case did a valid test result in damage to a module other than the module to which the surge test voltage was applied. In all but one case (digital output module 3603E) the damaged points were found to have failed in the OPEN (or Loss of Power) state. Based on this performance, the TRICON system meets the TR-107330 acceptance criteria for surge withstand. Because the digital output modules listed above exhibited surge voltage vulnerability, the modules are acceptable for use in safety-related applications as long as one (or more) of the following conditions is satisfied:

- Qualified surge suppression devices are used on the safety-related discrete output lines,
- The safety-related application can be demonstrated not susceptible to surge voltages on the discrete output lines. These would likely include most applications powered from plant vital power supplies, which are typically located indoors and are segregated or isolated from the high voltage power distribution systems in the plant.
- The safety-related function can be demonstrated not susceptible to a common mode surge which might disable the same safety function in all redundant trains, or
- The discrete output modules are not controlling a safety-related function.

4. The Model 3603E digital output module and associated Model 9661-910 termination panel exhibited vulnerability (permanent damage) to applied surge voltages. The Model 3603T digital output module and associated Model 9661-910 (revised) termination panel are revised versions of the Model 3603E module and ETA. These revised components were tested and demonstrated to have acceptable surge withstand capability (i.e., no demonstrated vulnerability). By evaluation (Reference 7.58) it is determined that the design modifications incorporated in the Model 3603T module do not affect the environmental, seismic and EMI/RFI test results obtained for the Model 3603E module. Therefore, the Model 3603T digital output module and its associated termination panel are considered equivalent replacements for the Model 3603E module.

4.7 1E to Non-1E Isolation

Class 1E to Non-1E isolation testing was performed to demonstrate the suitability of the Triconex TRICON 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 PLC is based on a system design which 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 following communication modules were tested for Class 1E isolation capability:

- EICM Module, RS-232 (MODBUS) interface
- ACM Module, Dual Nodebus (DNB) and RS-423 interface to Foxboro I/A Console
- NCM Module, IEEE 802.3 (TCP/IP) interface

In addition, the TRICON Model 3636R 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 384-1981, Reference 7.10. In particular, IEEE 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 7.31, 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 7.44.

The Class 1E to Non-1E Isolation Test Procedure, Reference 7.36, 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 Wyle Laboratories in Huntsville, Alabama. During testing, the TRICON Test Specimen was powered with the TSAP operating. The AC and DC power sources to the TRICON Test Specimen 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 TRICON test system was monitored by the test system data logger and the Wonderware and Foxboro I/A workstations. 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 7.43.

Isolation test acceptance criteria are as follows based on Appendix 6 of the Master Test Plan, Reference 7.22, and EPRI TR-107330, Section 4.6.4, Reference 7.4:

- Applying the isolation test voltages for the required time to the specified TRICON Test Specimen test points shall not disrupt the operation of any other module in the Test Specimen, or cause disruption of the Test Specimen backplane signals.

- Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate satisfactory operation of the TRICON Test Specimen 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 TRICON Test Specimen to operate as intended.

Test results described in the Isolation Test Report, Reference 7.43, show that:

1. Class 1E to Non-1E isolation testing of the TRICON Test Specimen was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 384-1981.

2. The TRICON Test Specimen met all applicable performance requirements during and after application of the Class 1E to Non-1E isolation test voltages.

3. The isolation test results (together with the Prudency Test communication port fault tests) demonstrate that the following TRICON PLC communication module ports provide adequate electrical isolation per IEEE 384-1981 between the safety related portions of the TRICON and connected non-safety related communication circuits:

    - Enhanced Intelligent Communication Module (EICM) Model 4119A, Serial Port Modbus Interfaces

    - Advanced Communication Module (ACM) Model 4609, Dual Nodebus (DNBI) and RS-423 Serial Port Interfaces to a Foxboro I/A Console

    - Network Communication Module (NCM) Model 4329, IEEE 802.3 (TCP/IP) Net 2 Interface to a Wonderware Console

    The testing demonstrated electrical isolation capability of the communication ports to applied voltages of 250 VAC (at 10 amps maximum) and 250 VDC (at 5 amps maximum) for 30 seconds.

4. The Class 1E to Non-1E isolation test results demonstrate that the TRICON PLC relay output module Model 3636R provides adequate electrical isolation per IEEE 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 23.4 amps maximum) and 250 VDC (at 10 amps maximum).

5. The Model 4211 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 384-1981 electrical isolation requirements.

4.8 Electrostatic Discharge

EPRI TR-107330 includes requirements for electrostatic discharge (ESD) testing of the PLC being qualified in accordance with IEC 801-2. Test points for ESD testing are selected on the basis of accessibility of the equipment during operation. The TRICON is intended for installation in a fully surrounding cabinet which will prevent access to the equipment during normal operation. Administrative controls (e.g., procedures requiring use of static discharge control devices such as grounding straps) will be required to prevent or reduce exposure to electrostatic discharges. Consequently, as discussed in the Master Test Plan, Reference 7.22, ESD testing was not performed as part of the qualification program. Triconex has, however, tested the TRICON for electrostatic discharge against the requirements of IEC 801-2 for Level 3 air discharges (8 kV) and Level 2 contact discharges (4 kV).

4.9 Performance Proof Testing

Performance proof testing was conducted at the completion of all qualification testing to demonstrate the continued acceptable performance of the TRICON Test Specimen after exposure to the various qualification test conditions. The proof testing involved performing the Operability Test, Reference 7.30, and the Prudency Test, Reference 7.31. 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 Test Report, Reference 7.44. This test report serves 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 report, including a summary of the specific manufacturer's performance specifications which 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 and analog input to digital output sequences were measured during all runs of the Operability Test procedure. Triconex provides a method for calculating the maximum expected digital input to digital output and analog input to digital output 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 $\pm 1\%$ 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 TRICON Test Specimen.

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 TRICON PLC on loss and restoration of power to the chassis power supplies. The test results demonstrated predictable and consistent response of the TRICON Test Specimen to a loss of power. The test results also demonstrated predictable and consistent response of the TRICON Test Specimen on recovery of power. In addition, successful restart of the

TRICON Test Specimen 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 VAC and 230 VAC 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 VDC 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.

   Each run of the Operability Test procedure also included tests to demonstrate power hold-up time performance of the Lambda field power supply on an interruption of source power for approximately 47 milliseconds. The test results showed the hold-up time for the Lambda power supply was less than 8 milliseconds, which is lower than the TR-107330 acceptance criteria of at least 40 milliseconds.

9. Power Quality Tolerance – Tests to demonstrate tolerance of the TRICON PLC and Lambda field power supply to changes in the quality (voltage and frequency) of AC and DC source power was 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 TRICON Test Specimen. 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 TRICON operating application program.

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 EICM, ACM, NCM, and Chassis I/O expansion RS-485 ports.

4.10 Failure Modes and Effects Analysis

As part of the TRICON qualification effort, a failure modes and effects analysis (FMEA) was performed as documented in Reference 7.46. The FMEA was performed in accordance with the guidelines of Section 6.4.1 of EPRI TR-107330, Reference 7.4.

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 7.46. 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 7.19 and 7.20 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 plant safety-related applications incorporate the manufacturer's recommended methods and frequencies to maximize system reliability and operability.

4.11 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 7.45. 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 plant refueling outage cycle), the reliability is 99.9984% and the availability is 99.9853%.

4.12 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 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 and the backup batteries.

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.

5.0 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 7.49.

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 HICB-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems";
- Branch Technical Position HICB-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 7.49. Key results are summarized in the following sections.

5.1 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 HICB-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 the Triconex company. Consequently, the required software documentation listed above is embodied in several sets of Triconex documents:

- Triconex company 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 9.3.1 of the TRICON software was extensively reviewed as part of the qualification effort. As described in the Software Qualification Report, Reference 7.49, the Triconex quality and engineering procedures provide the equivalent controls and definition of the development process as would be expected in the software planning documents defined in BTP-14. The software development, V&V, and test documentation was found to be in compliance both with Triconex procedural requirements as well as the intent of the current industry standards. This provides high confidence that the software was developed and tested in a controlled and structured manner, which will tend to produce high quality software products.

5.2 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 Part 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 15 years ago, 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 first revision of the Triconex QA Manual in 1986 was developed based on the requirements of NQA-1, and specified controls that essentially comply with the requirements of 10 CFR 50, Appendix B. The software development procedures have become more formalized since 1986, although the basic processes have not been significantly changed. The current processes and procedures have been audited and shown to be in compliance with ISO-9001 and 10 CFR 50, Appendix B, and 10 CFR 21.

All 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.

There are three sets of processes and procedures that describe the various aspects of software life cycle process planning:

- Triconex Quality Assurance Manual (QAM), Reference 7.16.
- Triconex Quality Procedures Manual (QPM), Reference 7.17.
- Triconex Engineering Department Manual (EDM), Reference 7.18.

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.

The first release of the Quality Procedures Manual was in November of 1992. The first set of procedures released were specific to manufacturing activities. The first major revision to the QPM occurred in 1994 when procedures specific to product development first appeared.

The first release of the Engineering Department Manual was in 1986. The first procedures concentrated on configuration and change control issues. While the QAM and QPM do provide some software specific requirements, the EDM provides the specific procedures that relate to development and maintenance of the TRICON software. These engineering procedures define a product life cycle which 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 1999. The evolution of the various Engineering Procedures described in the Software Qualification Report, Reference 7.49, demonstrates the continual refinement and improvement of the procedures from an initial set of eight to the current set of 36.

The initial 1986 procedures, with some expansion and revision, were used to develop Version 6.2.3 of the TRICON. The release of Version 6.2.3 was a significant milestone. Triconex made a commitment to achieve TÜV-Rheinland certification with the release of Version 6.2.3 on February 11, 1990. This certification process required significant effort by the design team, included independent verifications, and marks the beginning of continuous TÜV-Rheinland oversight. Additional discussion of the independent TÜV-Rheinland verification and validation is provided in the following section.

The procedures in place in December of 1986 were effective for the development, release and maintenance of the first TRICON release. Major improvement since that time, some driven by the TÜV-Rheinland certification process, have been effective for control of the TRICON development process.

5.3 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 Std 1012-1986 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 1012-1986 as an acceptable methodology for implementing the verification and validation of safety system software, subject to certain exceptions listed in that Regulatory Guide.

Triconex's verification and validation activities do not strictly follow the ANSI/IEEE 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 7.49.

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 to validate the diagnostic capability and software associated with diagnostics. 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 7.56).

Each new version has been tested by TÜV-Rheinland, with Version 9.3 being certified in February of 1998 to class 5 and class 6 of the DIN standard (Test report 945/EZ 102/98). 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 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 that 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 involves checking the translation of the graphical or text user program to the final code. TÜV testing of the TRICON software consists of the following:

- Internal Fault Routines – Procedures such as the watchdog routines, CPU test, etc. were checked by either monitoring execution of the routines or by forcing the routines by means of fault insertion.

- Noise on the Processor – A software module was developed to simulate noise on the processor by putting the CPU address pointer to arbitrary positions and verifying proper detection.

- Functional Verification – Portions of the Triconex functional verification procedures were performed to verify the software module's performance and validity of the test procedure.

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.

5.4 Safety Analysis

The Safety Analysis as described in BTP-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.

That said, 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 capabilities, 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.

5.5 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, and 9.0, 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 five PANs have been issued against the TRICON since the release of the system over 15 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.

6.0 SYSTEM APPLICATION

This summary report describes tests, evaluations and analyses which were performed to demonstrate generic qualification of the TRICON system for use in safety-related nuclear power plant applications. In any actual nuclear plant application, plant-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 plant 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.

To assist the user with plant-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.

7.0 REFERENCES

7.1 NUREG-800; Standard Review Plan, Section 7.0, "Instrumentation and Controls – Overview of Review Process," Rev. 4 – June 1997

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

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

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

7.5 EPRI Report, TR-106339, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications"

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

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

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

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

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

7.11 IEEE C62.41-1991, "Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits"

7.12 IEEE C62.45-1987, "Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits"

7.13 IEC 801-5, January 1990, "Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment, Part 5 – Surge Immunity Requirements"

7.14 IEEE Std. 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

7.15 IEEE Std. 1012-1986, "IEEE Standard for Software Verification and Validation Plans"

TRICONEX DOCUMENTS

7.16 Triconex Quality Assurance Manual (QAM)

7.17 Triconex Quality Procedures Manual (QPM)

7.18 Triconex Engineering Department Manual (EDM)

7.19 TRICON Product Guide, Triconex Document No. 9791007-004

7.20 TRICON Planning and Installation Guide, Triconex Document No. 9720051-005

TRICONEX NUCLEAR QUALIFICATION PROJECT DOCUMENTS

7.21 Triconex Quality Plan, Triconex Document No. QPL-01.

7.22 Master Test Plan, Triconex Document No. 7286-500

7.23 Master Configuration List, Triconex Document No. 7286-540

7.24 Software QA Plan, Triconex Document No. 7286-537

7.25 Tricon Test Specimen Description, Triconex Document No. 7286-541

7.26 Function Diagrams, Triconex Drawing Nos. 7286-430 to 444

7.27 Test System Loop Diagrams, Triconex Drawing Nos. 7286-531 to 543

7.28 Test System Wiring Drawings, Triconex Drawing Nos. 7286-001 to 329

7.29 Setup and Checkout Test Procedure, Triconex Document No. 7286-502

7.30 Operability Test Procedure, Triconex Document No. 7286-503

7.31 Prudency Test Procedure, Triconex Document No. 7286-504

7.32 Burn-In Test Procedure, Triconex Document No. 7286-505

7.33 Environmental Test Procedure, Triconex Document No. 7286-506

7.34 Seismic Test Procedure, Triconex Document No. 7286-507

7.35 Surge Withstand Test Procedure, Triconex Document No. 7286-508

7.36 Class 1E to Non-1E Isolation Test Procedure, Triconex Document No. 7286-509

7.37 EMI/RFI Test Procedure, Triconex Document No. 7286-510

7.38 Pre-qualification Test Report, Triconex Document No. 7286-524

7.39 Environmental Test Report, Triconex Document No. 7286-525

7.40 Seismic Test Report, Triconex Document No. 7286-526

7.41 EMI/RFI Test Report, Triconex Document No. 7286-527

7.42 Surge Test Report, Triconex Document No. 7286-528

7.43 Class 1E to Non-1E Isolation Test Report, Triconex Document No. 7286-529

7.44 Performance Proof Test Report, Triconex Document No. 7286-530

7.45 Reliability/Availability Study for TRICON PLC Controller, Triconex Document No. 7286-531

7.46 Failure Modes and Effects Analysis (FEMA) for TRICON Version 9 PLC, Triconex Document No. 7286-532

7.47 Radiation Hardness Evaluation, Triconex Document No. 7286-533

7.48 TRICON System Accuracy Specifications, Triconex Document No. 7286-534

7.49 Software Qualification Report, Triconex Document No. 7286-535

7.50 Simulator Application Program (SAP) Functional Requirements and Program Listing, Triconex Document No. 7286-520

7.51 TSAP Functional Requirements Specification, Triconex Document No. 7286-517

7.52 TSAP Design Specification, Triconex Document No. 7286-518

7.53 TSAP Program Listing, Triconex Document No. 7286-519

7.54 TSAP Validation Test Procedure, Triconex Document No. 7286-513

7.55 TSAP V&V Report, Triconex Document No. 7286-536

7.56 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

7.57 TÜV-Rheinland Microelectronic and Process Automation, "Type Approval of TRICON Version 9.3," Report-No. 945/EZ 102/98, February 18, 1998

7.58 E-Mail from Triconex (G. Hufton) to MPR Associates (M. Albers) dated March 22, 2000, "Revised Module Evaluation"

TRICONEX

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	Appendix A, Page 1 of 116	Date:	09/18/00

EPRI TR-107330 REQUIREMENTS COMPLIANCE AND TRACEABLITY MATRIX

Appendix A to

Document No. 7286-545

Revision 1

September 18, 2000

	Name	Signature	Title
Author:	Mitchell Albers	[signature]	Project Manager
Approvals:	Troy Martel	[signature]	Triconex Project Director
	Jerry McCann	[signature]	VP, Research and Development

EPRI TR-107330 REQUIREMENTS COMPLIANCE AND TRACEABLITY MATRIX

Appendix A to

Document No. 7286-545

Revision 1

September 18, 2000

QUALITY ASSURANCE DOCUMENT

This document has been prepared, reviewed, and approved in accordance with the Quality Assurance requirements of 10CFR50, Appendix B, as specified in the MPR Quality Assurance Manual.

	Name	Signature
Prepared By:	Mitchell Albers	[signature]
Reviewed By:	Eric Claude	[signature]
Approved By:	Dave Herrell	[signature]

PURPOSE

The purpose of this appendix is to provide a summary of compliance to each of the EPRI TR-107330 identified requirements as applied to nuclear safety related qualification of the Triconex Tricon Programmable Logic Controller (PLC). This appendix also provides a cross-reference to the Triconex documentation (test procedures, test reports, product manuals, etc.) which provides evidence of the stated compliance.

The information provided in this appendix is presented in table form. Each identified requirement of EPRI TR-107330 is addressed as a row entry in the table. The first column of each row identifies the corresponding section of TR-107330 in which the requirement is given. The second column paraphrases the identified requirement. The third column identifies compliance with the requirement. The fourth column provides reference to the supporting compliance documentation, and provides additional explanation or comment as necessary.

Table Notes and a List of References as identified in the table are included at the end of this appendix.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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.
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.	Exception	See Ref. 6, Section 3.2. Tricon response time varies with system configuration and application program size. The Tricon test specimen (4 chassis, 21 I/O modules, and 3 communication modules) maximum response times were 177 msec (DI to DO) and 264 msec (AI to DO). The test specimen application program included ≈ 800 simple and complex logic elements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Section 4.1.7.
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. 1, Section 4.1.7.
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. 1, Section 4.1.7.
4.2.2	Control Function Requirements. The PLC shall provide a high-level language designed for control algorithms.	Comply	See Refs. 2 and 4.
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. 3.
4.2.3.3	Availability/Reliability Calculation Requirements. An availability calculation shall be prepared which conforms to IEEE 352.	Comply	See Ref. 3.
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. 3.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 3 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. 5.
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. 1, Section 1.3.10 and Ref. 5. The Tricon does not require ringback 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. 6, Sections 8.2 and 10.2.
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 setpoint analysis per ISA RP 67.04.	Comply	See Ref. 7.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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.
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 I/O 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. 1, Section 1.3.5. See Ref. 9 for list of Tricon analog input modules included in the qualification program.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.A	Monotonicity. The analog inputs shall be monotonic to ±1/2 LSB.	Comply	Unpublished specification, verified based on discussion with Triconex engineers.
4.3.2.1.B	Number of Channels. Each analog input module shall provide a minimum of four input channels.	Comply	See Ref. 1, Section 3.3.
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. 1, Section 3.3. Analog input module A/D converters do not wrap on over range.
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. 1, Section 3.3. Analog input module A/D converters do not wrap on under range.
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. 1, Section 3.3.
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.	Exception	See Ref. 1, Section 3.3. 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. 1, Section 3.3, and Ref. 7.

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. 1, Section 3.3.
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.	Exception	See Ref. 1, Section 3.3. Common mode rejection rating of Modules 3700A and 3701 is 80 dB.
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. 6, Section 3.3 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. 1, Section 3.3. 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. 8. Surge withstand capability meets IEC 801-5 "basic immunity" levels.
4.3.2.1.1.I	Analog Voltage Input Module Input Impedance. The input impedance shall be at least 1 megohm.	Comply	See Ref. 1, Section 3.3.
4.3.2.1.2	Current Input Requirements. (section heading)	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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.	Exception	See Ref. 1, Section 3.3. 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 ≤ ± 0.35% of the specified range.	Comply	See Ref. 1, Section 3.3, and Ref. 7.
4.3.2.1.1.C	Analog Current Input Module Resolution. The minimum resolution shall be 12 bits.	Comply	See Ref. 1, Section 3.3.
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. 1, Section 3.3.
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.	Exception	See Ref. 1, Section 3.3. Common mode rejection rating of Modules 3700A and 3701 is 80 dB.
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. 6, Section 3.3 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. 1, Section 3.3. Tricon analog current input module points are not grouped.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 8. Surge withstand capability meets IEC 801-5 "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. 1, Section 3.3. 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.
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.	Exception	See Ref. 10, Section 4.5. 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. 10, Section 4.5. Tricon RTD input signal conditioners span -100°C to 600°C (32 to 1112°F) range.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.2.1.3.C	RTD Input Module Accuracies. Overall accuracies shall be ≤ ± 2°C.	Comply	See Ref. 1, Section 3.3, and Ref. 7. 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. 1, Section 3.3, and Ref. 7. 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. Resulting minimum resolution is 0.33°F (0.19°C).
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. 10, Section 4.5.
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. 10, Section 4.5.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 6, Section 3.3 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. 10, Section 4.5. 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.
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. 8. Surge withstand capability meets IEC 801-5 "basic immunity" levels.
4.3.2.1.3.K	RTD Input Module Input Impedance. The input impedance shall be 1 megohm minimum.	N/A	See Ref. 46. Input impedance of RTD signal conditioning modules is not relevant. Modules are compatible with specific RTD types.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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	Unpublished specification, verified based on discussion with Triconex engineers.
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.	Exception	See Ref. 1, Section 3.5. 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. 1, Section 3.5.
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. 1, Section 3.5, 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. 1, Section 3.3, 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. 1, Section 3.5.

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.	Exception	See Ref. 1, Section 3.5. T/C input module Model 3706A common mode rejection ratio is 85 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. 1, Section 3.5.
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.	Comply	See Ref. 6, Section 3.3 and Table Section 4.2.1.A.
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. 1, Section 3.5. 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.
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. 8. Surge withstand capability meets IEC 801-5 "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. 1, Section 3.5.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Section 3.1. See Ref. 9 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. 1, Section 3.1.
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. 1, Section 3.1.
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. 1, Section 3.1.
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. 1, Section 3.1.
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. 6, Section 3.3 and Table Section 4.2.1.A.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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	See Ref. 46.
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.
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. 8. Surge withstand capability meets IEC 801-5 “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 VDC, 24 VDC, 15 VDC and 12 VDC.	Exception	See Ref. 1, Section 3.1. Tricon discrete DC input modules are for nominal inputs of 115 VDC, 48 VDC 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. 1, Section 3.1.
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. 1, Section 3.1.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Section 3.1.
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. 6, Section 3.3 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	See Ref. 46.
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. 8. Surge withstand capability meets IEC 801-5 "basic immunity" levels.
4.3.2.2.3	TTL Input Requirements. Requirements for TTL level input modules. Based on exception to this requirement, Sections 4.3.2.2.3.A through 4.3.2.2.3.G are not included in this table.	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. 1, Section 3.6. 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. 1, Section 3.6.
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. 1, Section 3.6.
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	See Ref. 46.
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. 1, Section 3.6. 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%.	Exception	See Ref. 1, Section 3.6. Accuracy is ± 1.0% of reading from 20 to 99 Hz. Accuracy is ≤ ± 0.1% of reading from 100 to 20,000 Hz
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. 6, Section 3.3 and Table Section 4.2.1.A.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Section 3.6. 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. 8. Surge withstand capability meets IEC 801-5 "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. 1, Section 1.3.6. See Ref. 9 for identification of Tricon analog output module included in the qualification program.
4.3.3.1.A	Monotonicity. The analog outputs shall be monotonic to ±1/2 LSB.	Comply	Unpublished specification, verified based on discussion with Triconex engineers.
4.3.3.1.B	Number of Channels. Each analog output module shall provide a minimum of four output channels.	Comply	See Ref. 1, Section 3.4.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.1.1	Analog Voltage Output Requirements. Requirements for analog voltage output modules. Based on exception to this requirement, Sections 4.3.3.1.1.A through 4.3.3.1.1.G are not included in this table.	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.	Exception	See Ref. 1, Section 3.4. 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. 1, Section 3.4, and Ref. 7.
4.3.3.1.2.C	Analog Current Output Module Resolution. The minimum resolution shall be 12 bits.	Comply	See Ref. 1, Section 3.4.
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. 1, Section 3.4.
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.	TR Discrepancy	Section 4.2.1.A bases response time on AI to DO or DI to DO configurations. Analog outputs are not addressed.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 8. Surge withstand capability meets IEC 801-5 "basic immunity" levels.
4.3.3.2	Discrete Output Requirements. The PLC shall include modules that provide discrete outputs.	Comply	See Ref. 1, Section 1.3.4. 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. 1, Section 3.2.
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. 1, Sections 3.1 and 3.2. 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.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.3.2.C	Output Circuit Interrupter. Outputs must include a circuit interrupter.	Comply	See Ref. 10, Chapter 2 and Ref. 11, Chapter 6.
4.3.3.2.D	Status Indication. Modules must include indicators that show the ON/OFF status of each point.	Comply	See Ref. 1, Section 3.2.
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 VAC and 24 VAC.	Exception	See Ref. 1, Section 3.2. Tricon discrete AC output modules do not include 24 VAC nominal output.
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. 1, Section 3.2 and Ref. 46.
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.	Exception	See Ref. 1, Section 3.2. Module Model 3601E ON state voltage drop is < 3 V, typical.
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. 1, Section 3.2. Based on load leakage specifications.
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. 1, Section 3.2 and Ref. 46.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 6, Section 3.3 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. 1, Section 3.2. 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. 8. Surge withstand capability was tested to IEC 801-5 "basic immunity" levels. All modules met Section 4.6.2 acceptance criteria. Ref. 8 identifies discrete AC Output modules which demonstrated vulnerability to applied surge test voltages.
4.3.3.2.2	Discrete DC Output Requirements. (section heading)	- - -	No requirements.
4.3.3.2.2.A	Discrete DC Output Module Types. The PLC shall include discrete DC output modules for nominal outputs of 125 VDC, 48 VDC, 24 VDC, 15 VDC and 12 VDC.	Exception	See Ref. 1, Section 3.2. Tricon discrete DC output modules include 120 VDC, 48 VDC and 24 VDC nominal outputs.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Section 3.2 and Ref. 46.
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. 1, Section 3.2. Module Models 3607E and 3604E ON state voltage drops are < 3 V and< 4 V respectively.
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. 1, Section 3.2. Module Models 3623 and 3624 OFF state load leakage is 4 mA max.
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. 1, Section 3.2. Module Model 3607E (48 VDC output) operates from 44 to 80 VDC. Module Model 3604E (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. 6, Section 3.3 and Table Section 4.2.1.A.
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. 1, Section 3.2. Tricon discrete DC output module points are not grouped.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 8. Surge withstand capability was tested to IEC 801-5 "basic immunity" levels. All modules met Section 4.6.2 acceptance criteria. Ref. 8 identifies discrete DC output modules which demonstrated vulnerability to applied surge test voltages.
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.	Exception	See Ref. 1, Section 3.2.4. 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. 1, Section 3.2.4.
4.3.3.2.3.C	Relay Output Module Contact Resistance. The contact resistance shall not exceed 2 ohms.	Comply	See Ref. 46. As delivered contact resistance is less than 2 ohms.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Section 3.2.4.
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. 6, Section 3.3 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. 1, Section 3.2.4. 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. 12. 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. 8. Surge withstand capability was tested to IEC 801-5 "basic immunity" levels.
4.3.3.2.4	TTL Output Requirements. Requirements for TTL level output modules. Based on exception to this requirement, Sections 4.3.3.2.4.A through 4.3.3.2.4.F are not included in this table.	Exception	There is no TTL level output module available for use with the Tricon PLC.
4.3.4	Processor/Other System Component Requirements. (section heading)	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 6, Section 3.3 and Table Section 4.2.1.A. 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.
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. 13, Appendix A. 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. 2, Programs. Number of program elements is supported.
	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. 1, Section 5.1.4.
	Any memory used for field modifiable constants shall be capable of at least 100,000 write cycles.	Comply	See Ref. 46.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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.	Comply	See Ref. 1, Section 1.1.2. See Ref. 6, Section 3.3 and Table Section 4.2.1.A.
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. 14. Remote and expansion chassis interface devices were included in environmental testing. See Ref. 6, 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	Unpublished specification, verified based on discussion with Triconex engineers.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 6, 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.
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.	Exception	See Ref. 12, Section 2.0. Multipin cable connectors 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.	Exception	See Ref. 8, Section 3.2. No interposing devices are used on multipin 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.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Sections 2.2.1 and 6.1. 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.
4.3.4.3.G.1	Redundant Inter-Processor Data Acquisition Backplane Busses. Busses shall be at least dual redundant.	Comply	See Ref. 17, Appendix A.
4.3.4.3.G.2	Redundant Inter-Processor Data Acquisition Backplane Busses. Loss of one bus shall not cause misoperation.	Comply	See Ref. 17, Appendix A.
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. 17, Appendix A.
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. 17, Appendix A.
4.3.4.3.G.5	Redundant Inter-Processor Data Acquisition Backplane Busses. Data acquisition time shall be deterministic.	Comply	See Ref. 17, Appendix A.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 6, Section 3.3. Redundant busses are always operational. Therefore, response time determination and qualification testing performed with redundant busses operational.
4.3.4.4	Communication Port Requirements. The main processor shall provide at least one communication port.	Comply	See Ref. 1, Section 2.4.1, EICM Module.
4.3.4.4.A	Communication Port Data Rate. The port shall support data rates up to 9600 baud.	Comply	See Ref. 1, Section 3.7
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. 1, Section 3.7. EICM supports RS-232, RS-422 or RS-485,
4.3.4.4.C	Communication Port Connector. The port shall provide positive hold down of connectors.	Comply	Screw connectors provided on EICM 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. 46.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 12, Section 7.0. Tricon EICM serial communication ports tested for Class 1E to Non-1E isolation capability at 250 VAC (vs. 600 VAC required by TR) and 250 VDC.
4.3.4.4.F	Communication Port Surge Withstand. Surge withstand shall be as given in Section 4.6.2.	Comply	See Ref. 8. EICM Module serial port surge withstand capability meets IEC 801-5 "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. 6. Section 1. 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. 1, Section 4.1.3.2. See Ref. 26, Drawing No. 7286-101 for seismic mounting details. See Ref. 28, 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. 6, 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	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	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. 6, 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 and 7.5.2. No special programming terminal hardware is required.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.6	Environmental Requirements. (section heading)	- - -	No requirements.
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) Power Source Range: As given in Section 4.6.1.1 Radiation Exposure: Up to 1000 Rads	Exception	See Ref. 13. Tricon is rated for 0 to 60°C (32 to 140°F), 5% to 95% humidity (non-condensing). See Table Section 4.6.1.1 for exceptions to power source range. See Ref. 38. Tricon will perform its safety-related function if subjected to 1000 Rad dose of 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) Power Source Range: As given in Section 4.6.1.1 Radiation Exposure: Up to 1000 Rads	Exception	See Ref. 13. Tricon is rated for 0 to 60°C (32 to 140°F), 5% to 95% humidity (non-condensing). See Table Section 4.6.1.1 for exceptions to power source range. See Ref. 38. Tricon will perform its safety-related function if subjected to 1000 Rad dose of gamma radiation.

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.	Exception	See Ref. 14, Section 7.0. Tricon demonstrated operability at 35 to 140°F, 95% humidity as shown in TR Figure 4-1. Low range humidity during test was not controlled. See Ref. 14, Section 6.5 for disposition of this exception. See Ref. 38 for evaluation of radiation withstand 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	See Ref. 33. Tricon showed some susceptibilities to TR-102323 radiated and conducted test levels (discrete I/O changed state, analog I/O varied more than 3%). Also, Tricon demonstrated some radiated and conducted emissions in excess of TR-1023232 levels. See Ref. 33 for disposition of these exceptions.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.3.8	Electrostatic Discharge (ESD) Withstand Requirements. The PLC shall withstand ESD levels given in EPRI TR-102323.	Exception	See Ref. 16, Section 5. ESD testing not performed. System installation and operation per manufacturer's direction will preclude ESD exposure.
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.	Exception	See Ref. 28. All requirements met except SSE level given in TR Figure 4-5. SSE test level was limited by Wyle Labs seismic table capability. See Ref. 28, Section 7 for SSE test levels used.
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	<u>Main Processor Executive Capability Requirements</u>. 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. 17, App. A, Section 4.2, Software Architecture. - Items A, B, C, E, F, H, and J Subsection 4.2.4, Scan Level - Items D and I Subsection 4.2.2, Power Up - Items D and G Subsection 4.2.3, Background

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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.	N/A	See Ref. 17, Appendix A, Subsection 4.2.4, Scan Level. Execution of each application program scan is preceded by an input module data request.
	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 Ref. 17, Appendix A, Subsection 4.1.2, Main Processor and 4.2.4, Scan Level. Figure 3 shows that only the system timer will normally produce a scan interrupt. The purpose of this interrupt is to begin execution of the scan level block based on the scan cycle interval set by the application configuration.
	Requirements for PLCs that implement interrupts that could result in non-deterministic application program execution.	N/A	See above.
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.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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 coprorocessors.
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. 47, Introduction and Installation sections. See Ref. 45, 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. 2, Normally Open and Normally Closed Contacts.
4.4.3.B	Standard Functions. Transition ON/OFF (one-shot) paths.	Comply	See Ref. 2, Positive and Negative Transition Contacts.
4.4.3.C	Standard Functions. Simulate break before make and make before break contact actions.	Comply	See Ref. 2, Normally Open and Normally Closed Contacts. Requires two program scans.
4.4.3.D	Standard Functions. Coils that change paths from normal to alternate states when energized.	Comply	See Ref. 2, Normal and Negated Momentary Coil Types.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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. 2, Set (Latch) and Reset (Unlatch) Coil Types.
4.4.3.F	Standard Functions. Timing functions that can be set from 0.1 seconds to 2 hours.	Comply	See Ref. 4, 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. 2, 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. 2, 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. 2, 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. 2, SQRT, EXPT and LOG functions. CHK_ERR function block.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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. 4, PID and CHK_ERR function blocks. See Ref. 26, Drawing No. 7286-437, TSAP implementation of PID function.
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. 4, LEADLAG and EXPFLTR function blocks. See Ref. 26, Drawing No. 7286-439, TSAP implementation of LEADLAG function.
4.4.3.M	Standard Functions. Capability to put limits on values.	Comply	See Ref. 2, LIMIT function.
4.4.3.N	Standard Functions. Implement a function generator with at least five slopes.	Comply	See Ref. 26, Drawing No. 7286-442, TSAP implementation of 9 segment function generator.
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. 4, TR_XX_STATUS functions.
4.4.3.Q	Standard Functions. Functions to implement sequence of events requirements in Section 4.4.9.	Comply	See Ref. 4, SOE_XX functions.

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 2, 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. 26, Drawing No. 7286-444, TSAP implementation of two variable, twenty instance first-in/first-out buffers, with buffer contents transmitted over MODBUS and Peer-to-Peer communication ports.
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. 2, Comments, Variable Annotation and Macros.
4.4.4	Software Tools Requirements. A tool shall be provided for programming, debugging and documentation.	Comply	See Ref. 2, Introduction. 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. 2, Introduction.
4.4.4.A.1	Software Tools Requirements. Ability to attach explanatory comments to program steps.	Comply	See Ref. 2, Comments, Variable Annotations and Macros.
4.4.4.A.2	Software Tools Requirements. Ability to store programs on removable magnetic media.	Comply	See Ref. 2, Save Project command.

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. 2, Downloading a Project, Compare to Last Download function.
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. 2, Standard Reports function.
4.4.4.A.5	Software Tools Requirements. Features to aid in I/O mapping and memory management of the PLC.	Comply	See Ref. 2, Configuration Editor or Connections Wizard functions.
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. 2, Operating a Control Panel, Instance View command. Red: Power On, Green: Power Off.
4.4.4.B.2	Debugging Aids. Ability to display input, output and intermediate program values.	Comply	See Ref. 2, Operating a Control Panel, Instance View command.
4.4.4.B.3	Debugging Aids. Ability to set constants and variables to arbitrary values, including values outside normal range.	Comply	See Ref. 2, Operating a Control Panel, Set Value command.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.4.B.4	Debugging Aids. Ability to force outputs.	Comply	See Ref. 2, Operating a Control Panel, Set Value command.
4.4.4.B.5	Debugging Aids. Ability to single step through a program.	Comply	See Ref. 2, Operating a Control Panel, Single Step command.
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. 2, Tricon Diagnostics Panel.
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. 17.
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.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.5.2	Configuration Management Aids Requirements. Descriptive information.	- - -	No requirements.
4.4.5.2.A	Configuration Management. The PLC executive shall include a retrievable, embedded electronic revision level.	Comply	See Ref. 2, Tricon Diagnostic Panel Firmware Version Numbers.
4.4.5.2.B	Configuration Management. Configuration information of configurable modules shall be retrievable in the field.	Comply	See Ref. 2, Configuration Editor, Hardware Allocation command.
4.4.5.2.C	Configuration Management. Software tools for modifying device configurations shall provide measures to prevent unauthorized access.	Comply	See Ref. 2, System Administration, Privileges command.
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. 2, Printing, Standard Reports.
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. 1, 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 A and 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. Items 4.4.6.1.1 through 4.4.6.1.6 must be covered by on-line self test. Items 4.4.6.1.7 and 4.4.6.1.8 must be covered in power-up tests. 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 Comply Comply Comply	See Table Sections 4.4.6.1.1 through 4.4.6.1.14. See Table Section 4.4.6.2. See Table Section 4.4.6.3. See Ref. 1, Sections 4.1.12.1 and 4.1.12.2.
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. 17, Appendix A, Section 4.1.2, Main Processor, Watchdog Timer. Failure Alarm: See Ref. 1, Table 5-2, MP Active LED. Application Program Interface: See Ref. 4, TR-MP-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.2	Executive Program Error. Check of executive firmware integrity using a checksum or similar test.	Comply	Failure Detect: See Ref. 17, Appendix A, Section 4.2.3, Background. Failure Alarm: See Ref. 1, Table 5-2, MP Fault LED. Application Program Interface: See Ref. 4, TR-MP-STATUS function.
4.4.6.1.3	Application Program Error. Check of application program integrity using a checksum or similar test.	Comply	Failure Detect: See Ref. 17, Appendix A, Section 4.2.3, Background. Failure Alarm: See Ref. 1, Table 5-2, MP Active LED. Application Program Interface: See Ref. 4, TR-MP-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 17, Appendix A, Section 4.2.3, Background. Failure Alarm: See Ref. 1, Table 5-2, MP Fault LED. Application Program Interface: See Ref. 4, TR-MP-STATUS function.
4.4.6.1.5	Module Communication Error. Check of communication data integrity.	Comply	Failure Detect: See Ref. 17, Appendix A, Section 4.2.3, Background. Failure Alarm: See Ref. 1, Table 5-2, MP COM RX and TX LEDs. Application Program Interface: See Ref. 4, TR-MP-STATUS and TR-PORT-STATUS functions.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.6	Memory Battery Low. Check of memory battery capacity.	Comply	Failure Detect: See Ref. 1, Table 5-2, Bat Low. Failure Alarm: See Ref. 1, Table 5-2, 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. 1, Section 2.3.3.1, Main Chassis Power Module. Application Program Interface: See Ref. 4, TR-CHASSIS-STATUS function.
4.4.6.1.8	Failure of Watchdog Timer. Check of operation of watchdog timer.	Comply	Failure Detect: See Ref. 17, Appendix A, Section 4.2.3, Background. Failure Alarm: See Ref. 1, Table 5-2, MP Fault LED. Application Program Interface: See Ref. 4, TR-MP-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.9	Application not Executing. Failure to complete application program scan.	Comply	Failure Detect: See Ref. 17, Appendix A, Section 4.1.2, Main Processor, Watchdog Timer. Failure Alarm: See Ref. 1, Table 5-2, MP Active LED. Application Program Interface: See Ref. 4, TR-MP-STATUS function.
4.4.6.1.10	Analog Output not Following. Failure of analog output to following commanded value.	Comply	Failure Detect: See Ref. 1, Section 3.4. Failure Alarm: See Ref. 1, Table 5-18, Analog Output Module Fault LED. Application Program Interface: See Ref. 4, TR-SLOT-STATUS function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.11	Analog Input not Responding. Failure of analog input to respond to input signal.	Comply	Failure Detect: See Ref. 1, Sections 3.3, 3.5 and 3.6. Failure Alarm: See Ref. 1, Tables 5-6, 5-7 and 5-9, Module Fault LEDs. Application Program Interface: See Ref. 4, TR-SLOT-STATUS function.
4.4.6.1.12	Discrete Input/Ouput not Responding. Failure of discrete input/output to operate correctly.	Comply	Failure Detect: See Ref. 1, Sections 3.1 and 3.2. Failure Alarm: See Ref. 1, Tables 5-4, 5-11, 5-14 and 5-16, Module Fault LEDs. Application Program Interface: See Ref. 4, TR-SLOT-STATUS, TR-POINT-STATUS and TR-MP-STATUS functions.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.4.6.1.13	Analog I/O out of Calibration. Analog input or output point out of calibration.	Comply	Failure Detect: See Ref. 1, Sections 3.3, 3.4, 3.5 and 3.6. Failure Alarm: See Ref. 1, Tables 5-6, 5-7, 5-9 and 5-16, Module Fault LEDs. Application Program Interface: See Ref. 4, TR-SLOT-STATUS function.
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. 1,, Section 2.3.2. Failure Alarm: See Ref. 1, Section 2.3.1.3, Power Supply Module Fault LED. Application Program Interface: See Ref. 4, 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. 17, Appendix A, Section 4.2.3, Background. See Table sections 4.4.6.1.1 through 4.4.6.1.6 above.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 17, Appendix A, Sections 4.2.2, Power Up, and 4.2.3, Background. 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.
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. 2, Declaring Constants. See Ref. 1, Section 1.3.1, memory is battery backed. See Ref. 17, Appendix A, Section 4.2.3, Background, constants in memory are continuously verified.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 2, Declaring Constants, Value field. See Ref. 17, Appendix A, Section 4.2.3, Background, 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. 2, System Administration, Privileges or Element Attributes.
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. 26, Drawing No. 7286-444, TSAP implementation of data transmission over MODBUS and Peer-to-Peer communication ports.
4.4.8	Other Non-Ladder Logic Programming Languages. (section heading)	---	No requirements.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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. 2, Programming Languages. 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, Section 2.1.2. A single SOE block (or list of discrete variables) will support recording of 20,000 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, Section 2.2. 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. 48, Introduction. Supports transmission of data through NCM, EICM or ACM (DCM) communication modules.
4.4.9.D	Sequence of Events. Relative accuracy of time tags shall be one scan cycle ± 50 msecs.	Comply	See Ref. 48, Section 1.1.4, Comparing Events Between Tricons.
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.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 4, LEADLAG and PID function descriptions. See Ref. 26, Drawing No. 7286-437 for TSAP implementation of PID function external auto/manual control switch.
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. 26, Drawing No. 7286-437 for TSAP implementation of setpoint adjustment through raise and lower switches with variable rate control.
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. 26, Drawing No. 7286-433 for TSAP implementation of a manual initiation (trip bypass) input switch. Digital inputs can be programmed to detect manual equipment actuations.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.5.2.D	<u>HMI Functions</u>. PLC shall support display of status of discrete and continuous value parameters via connected devices.	Comply	See Ref. 26, Drawing No. 7286-431 for TSAP implementation of an analog recorder output signal to mimic an analog input, and implementation of discrete output signals to operate alarm lamps indicating status of a trip bistable.
4.5.2.E	<u>HMI Functions</u>. 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. 26, Drawing No. 7286-102. Test specimen implemented communication links to Foxboro, Wonderware and Tristation consoles, a second Tricon, and a test system printer. See Ref. 1, Section 2.4.3 for SOE implementation.

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. 1, Section 4.1.9, main chassis keyswitch.
	Interactive features shall be available through a programming, maintenance and debugging port. PLC shall operate with no connection to this port.	Comply	See Ref. 2, Sections 7 and 8, Tristation 1131 connection to EICM module.
	PLC shall mask interactive commands during run mode.	Comply	See Ref. 1, Section 4.1.9, main chassis keyswitch in run position.
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. 4. 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. 1, Section 1.3.10.
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. 26, Drawing No. 7286-431. TSAP implemented bistable trip function.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 26, Drawing No. 7286-431. TSAP implemented bistable setpoint/reset trip function.
4.5.6.C	Alarm Processing. PLC shall have ability to blink an output indicator.	Comply	See Ref. 4, 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. 2, 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. 2. 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. 1, Section 2.4.3, 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.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.1	Power Supply Requirements. (section heading)	---	No requirements.
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. 13. Model 8310 AC power supply modules are rated for 85 VAC to 140 VAC input.
	AC sources shall operate at the temperature and humidity range given in Section 4.3.6.	Exception	See Ref. 6, Section 10. Model 8310 AC power supply modules were tested over required temperature and modified humidity range (see Table Section 4.3.6.3).
4.6.1.1.B	Power Sources. DC sources shall operate from at least 20.4 VDC to 27.6 VDC.	Exception	See Ref. 13. Model 8311 DC power supply modules are rated for 22 VDC to 31 VDC input.
	DC sources shall operate at the temperature and humidity range given in Section 4.3.6.	Exception	See Ref. 6, Section 10. Model 8311 DC power supply modules were tested over required temperature and modified humidity range (see Table Section 4.3.6.3).

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.1.1.C	Power Sources. DC sources shall operate for seven days from a 30 VDC source.	Comply	See Ref. 20.
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. 13, Page 16. Fully loaded main chassis per 4.6.1.1.D includes 3 main processors, 1 EICM communication module, 1 AO module, 1 DO module, 1 DI module and 3 AI modules. Load = 145 W x 1.2 = 174 W. Power source rating is 175 W.
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. 13, Page 16. Fully loaded expansion chassis per 4.6.1.1.D includes 1 AO module, 1 DO module, 1 DI module and 5 AI modules. Load = 115 W x 1.2 = 138 W. Power source rating is 175 W.
4.6.1.1.F	Power Sources. Hold up time for AC supplied power sources shall be 40 msec.	Comply	See Ref. 32, Section 7.0.(h).

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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.	Exception	See Ref. 33. Power sources demonstrated some radiated and conducted emissions in excess of TR-102323 levels. See Ref. 8. Power sources meet TR 102323 surge withstand criteria. See Ref. 16, Section 5. ESD testing not performed. System installation and operation per manufacturer's direction will preclude ESD exposure.
	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. 1, Section 4.1.3.3. 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. 1, Section 2.3. Redundant power sources are independently fused.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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.	Exception	See Ref. 16, Section 3. Third party field power supply was included in environmental and seismic qualification testing. Data for EMI/RFI and surge withstand performance will be obtained as necessary. Power supply source ratings are 105 to 127 VAC, 57 to 63 Hz. Power supply output rating is 6.7 A at 24 VDC, 60°F. Power supply hold up time does not meet TR criteria.
4.6.2	Surge Withstand Capability Requirements. PLC platform shall withstand IEEE C62.41 ring wave and combination wave, 3000 volt peak surges. 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 C62.45.	TR Discrepancy	See Ref. 8. Power sources meet surge withstand criteria. IEEE C62.45 does not address surge testing of I/O and communication circuits. These circuits were tested to IEC 801-5 using combination waves at 500 or 1000 volts peak. All circuits met TR Section 4.6.2 acceptance criteria. Ref. 8 identifies discrete output modules which demonstrated vulnerability to applied surge test voltages.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.6.3	Separation. Descriptive information.	- - -	No requirements.
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. 12. Only relay output modules, communication ports, and fiber optic chassis interconnections 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 Refs. 13 and 50. Chassis-to-chassis and chassis-to-termination panel interconnect cables are rated for > 1000 VAC/DC and up to 60°C. All cables jackets are made of PVC.

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. 1, Section 1.1.2.
	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	Unpublished specifications. Screw or compression terminals used on field termination panels can be loosened for insertion of test signal or monitoring instrument wiring. All cable and wire connectors to the Tricon have screw or latching fastener attachments.
	Connectors and terminations to the PLC shall be qualified with the generic PLC.	Comply	See Ref. 9. Field termination panels were included in the qualification test specimen.
4.6.7	Backup Power. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Section 4.3.
	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. 1, Section 4.3.5.
4.7	Maintenance. (section heading)	- - -	No requirements.
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. 1, Section 1.2.1.
	The maintenance manual shall contain a description of any hardware configuration item for each module.	Comply	See Ref. 1, Section 5.3.
	The module hold downs shall be easily accessible and provide ease of removal and reinstallation.	Comply	See Ref. 1, Section 5.3.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [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. 1, Section 5. See Table Section 4.7.8.2.
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. 13, Page 51. Tristation 1131 connection permits required access to application program variables. Also, screw or compression 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. 1, Section 1.3.10. 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. 1, Sections 1.3 and 5.3.
	Low power modules shall support removal with field power applied.	Comply	See Ref. 1, Section 5.3. 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. 9.
	Records shall be maintained for revision history and changes.	Comply	See Ref. 45, 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. 49.
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 4.12.
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. 1, Section 5. No special tools required for routine maintenance.
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. 1, Section 5. This section provides instruction and precautions for connection and use of Tristation 1131 to perform recommended routine maintenance activities.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.7.9.C	Job Aids. Aids for operating the PLC equipment shall be provided.	Comply	See various sections of Ref. 1 for equipment pictures, and operational recommendations and warnings. See Ref. 1, Section4.1.5.2 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. 2, Help Menus. 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.	Exception	See Ref. 16, Section 3. A third party field power supply was included in environmental and seismic qualification testing. Data for EMI/RFI and surge withstand performance will be obtained as necessary.
4.9	Other. (section heading)	- - -	No requirements.
4.9.1	Data Handling and Communication Interface Overview. Descriptive information.	- - -	No requirements.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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. 32, Attachment 11. 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. 13, Appendix A.
	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. 2, 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. 2, Configurable Modules (EICM), 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. 2, Configurable Modules (EICM), 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. 2, Configurable Modules (EICM), 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. 17, Appendix A. 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]
4.9.1.2	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. 1, Section 3.8, NCM 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. See Ref. 15, Section 7. Net 1 port was tested for isolation capability at 250 VAC and 250 VDC.
	Communication time shall be deterministic.	Comply	See Ref. 2, 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. 32, Attachment 11. NCM Module Net 1 port failure tests showed no effect on application program or PLC scan cycle. See Ref. 2, Peer-to-Peer Communciation.
	Use of the peer-to-peer communication link shall support the response time requirement given in Section 4.2.1.A.	Comply	See Ref. 6, Section 3.3 and Table Section 4.2.1.A. Peer-to-Peer communication link was implemented during all qualification testing.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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. 1, Section 4.1.9.
	Features shall ensure that redundant components operate in the same mode, and that program changes are loaded into all redundant processors.	Comply	See Ref. 1, Section 2.4. See Ref. 2, Downloading a Project.
	Provisions shall prevent modification of the application program and operating system while the PLC in on-line.	Comply	See Ref. 1, Section 4.1.9 and Ref. 2, 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. 26, Drawing No. 7286-438 for TSAP implementation of a heartbeat function.
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. 45, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.1	Packaging Requirements. Descriptive information.	- - -	No requirements.
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. 45, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.10.1.B	Items Shipped. Packaging shall include desiccant materials as required.	Comply	See Ref. 45, 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. 45, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery. See Ref. 45, 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. 45, 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. 45, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery. See Ref. 45, Section QAM 8.0, Product, Parts, and Material Identification and Traceability.
4.10.1.F	Items Shipped. Copies of packing lists shall be included with each carton shipped.	Comply	See Ref. 45, 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. 45, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
4.10.1.H	Items Shipped. Packaging shall be suitable for movement using hand trucks.	Comply	See Ref. 45, 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. 45, 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. 45, Section QAM 15.0, Handling, Storage, Packaging Preservation, and Delivery.
4.10.3	Storage Requirements. Storage and shelf life requirements shall be provided for all PLC items.	Comply	See Ref. 45, 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.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 16, Section 5. Triconex and TUV Rheinland have performed extensive testing of the Tricon PLC application software. Results of this testing are documented in Ref. 17.
5.2.B	Initial PLC Calibration. The generic qualification sample PLC shall be calibrated to NIST traceable sources.	Comply	See Ref. 18, 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. 19, Appendix A.
5.2.D	Operability Tests. The Operability Test shall be performed during acceptance testing.	Comply	See Ref. 20, Appendix B.
5.2.E	Prudency Tests. The Prudency Test shall be performed during acceptance testing.	Comply	See Ref. 20, Appendix C.
5.2.F	Burn-In Test. A minimum 352 hour burn-in test shall be performed during acceptance testing.	Exception	See Ref. 16, 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.
5.3	Operability Test Requirements. Descriptive information.	- - -	No requirements.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
5.3.A	Accuracy. Accuracy checks shall be performed on the analog input/output modules.	Comply	See Ref. 6, Section 2.
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. 6, Section 3. Based on Tricon design, it is not practicable to perform a test which 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. Acceptance criteria for all tests is that the maximum expected 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. 6, 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. 6, Section 5.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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.	Exception	See Ref. 6, Section 1. NCM Module NET1 port is included in qualification envelope. 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. 6. 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. 6, 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. 6, Section 8.
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. 6, Section 7.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 6, 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. 6, 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.	Comply	See Ref. 21, Section 2, Subsection 3.0.
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.
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.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
5.4.D	Fault Simulation. For PLC's that include redundancy, failures in redundant elements shall be simulated.	Exception	See Ref. 6, Section 1, Subsection 3.0, and Ref. 6, Section 7. Fault simulation in redundant elements is performed during Operability testing.
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 environ. 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	TR Discrepancy	Due to short duration of seismic SSE tests, and special set-up required for EMI/RFI tests, Operability and Prudency tests can not be performed at those times. Other requirements of Section 5.5 were complied with. See Ref. 16 for detailed qualification test plan.
5.6	Application Software Objects Acceptance (ASOA) Testing. Requirements for ASOA testing. Based on exception to ASOA testing, Section 5.6 requirements are not included in this table.	Exception	See Ref. 16, 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. 9 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. 6 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. 9 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. 9 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, two chassis of the test specimen were 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 Table Section 6.2.1.E. Dummy power supplies not used in test specimen. See Ref. 22, Section 3.3. Seismic Balance Modules (SBMs) were installed in one test specimen chassis to increase the weight loading to that representative of a fully module populated chassis.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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. 9 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. 9 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 Refs. 6 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 arrangement to maximize stress on the chassis and mountings.	Comply	See Ref. 22, 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. 23, 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. 24, Section 34.
6.2.2.B	TSAP Programming. TSAP shall include program sequences to support Operability and Prudency testing.	Comply	See Refs. 6, 21 and 24.
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. 24, Section 15.
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. 6. Section 1. Operation of Tricon coprocessors is invoked automatically during application program execution.
6.2.3	Test Support Equipment Requirements. Test equipment to support Acceptance and Operability testing shall be provided.	Comply	See Refs. 25 and 26.
6.2.3.A	Test Support Equipment. Equipment shall include panels for connecting and simulating inputs and outputs.	Comply	See Refs. 25 and 26.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.2.3.B	Test Support Equipment. Equipment shall include test and measurement equipment with required accuracy.	Comply	See Refs. 25 and 26.
6.2.3.C	Test Support Equipment. Equipment shall include special tools and devices needed to support testing.	Comply	See Refs. 25 and 26.
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 were met by requiring compliance with ANSI/NCSL Z540-1-1994, "Calibration Laboratories and Measuring and Test Equipment, General Requirements," in all purchase orders with test equipment rental companies. Ref. 36 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. 18, Section 9.0. No user setpoints.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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.	Exception	See Ref. 16, Section 5. Environmental, seismic, EMI/RFI, surge and Class 1E to Non-1E isolation testing performed in order given. ESD testing not performed. System installation and operation per manufacturer's direction will preclude ESD exposure.
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. 27, Section 3.2. EMI/RFI testing performed per Section 4.3.7. 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. 27, Section 3.3. Due to space limitations of Wyle Labs EMI/RFI chamber, test specimen was mounted less than six feet above floor. Test specimen was mounted on open metal mounting racks. Metal racks 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.	Exception	See Ref. 23, Sections 3.2, 3.4 and 3.5. All requirements met except 5% relative humidity during low temperature testing. See Ref. 14, Section 6.0 for disposition of this test exception.
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. 23, 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.	Exception	See Ref. 22, Sections 3.1, 3.2 and Step 10.2.16. All requirements met except SSE level given in TR Figure 4-5. See Ref. 28, Section 7 for SSE test levels used.
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. 22, Section 3.3.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
6.3.4.2	Seismic Test Measurement Requirements. Relay contacts shall be monitored for chatter. One half of the relays shall be enrgized 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.	Exception	See Ref. 22, Sections 3.4, 3.5, 3.6 and 3.7. All requirements met except one of four chassis was not instrumented with a response accelerometer. See Ref. 28, section 6.0 for disposition of this exception.
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. 22, 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. 29.
6.3.5	Surge Withstand Capability Testing. Surge testing shall be conducted per Section 4.6.2 and IEEE C62.45.	Exception	See Table Section 4.6.2.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 30, Section 3.3. Due to space limitations of Wyle Labs EMI/RFI chamber, test specimen was mounted less than six feet above floor. Test specimen was mounted on open metal mounting racks.
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. 31, Section 3.3. Test specimen was mounted less than six feet above floor. Test specimen was mounted on open metal mounting racks.
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. 5.
6.4.2	Electrostatic Discharge (ESD) Testing Requirements. ESD testing of the PLC shall be performed per EPRI TR-102323.	Exception	See Ref. 16, Section 5. ESD testing not performed.
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. 6, Section 10.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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	See Ref. 32.
6.4.4.A	Environmental Test Compliance. Environmental Operability test results shall be evaluated for compliance to specifications.	Comply	See Ref. 32.
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. 28, Section 7.0.
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. 12, Section 7.0.
6.4.4.D	Surge Withstand Test Compliance. Test levels shall be checked for compliance to Section 4.6.2 specifications.	Comply	See Ref. 8, Section 7.0.
6.4.4.E	EMI/RFI Test Compliance. PLC performance shall be checked for compliance to Section 4.3.7 specifications.	Comply	See Ref. 33, Section 7.0.
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. 32.
6.4.4.G	ASOA Test Compliance. Results shall be evaluated for compliance to Section 5.6 requirements.	Exception	See Ref. 16, Section 5. ASOA testing not performed.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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	See Ref. 34.
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 Refs. 16, 35 and 36.
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. 36, Section 3.
7.2.B	10CFR50 Applicability. Regulations apply to application specific activities.	N/A	Requirement applies to safety-related application of a PLC.
7.2.C	10CFR50 Applicability. Regulations apply to PLC dedication activities.	N/A	Tricon PLC is manufactured under a 10CFR50 program. Requirement applies to dedication of a commercial PLC.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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 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	See Ref. 44, Attachment A, Section A. See Ref. 34.
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.
7.2.G	V&V Program Evaluation. Qualifier shall evaluate the manufacturer's V&V program to the criteria in Section 7.4.	Comply	See Table Section 7.4.
7.2.H	Qualification Test Witnessing. The qualifier shall have the right to witness qualification tests.	Comply	See Ref. 43, Section 28.0.
7.3	10CFR21 Compliance Requirements. Section lists 10CFR21 compliance requirements of a utility which applies the PLC in a safety-related application. PLC manufacturer shall support problem reporting and tracking.	N/A Comply	Requirement applies to safety-related application of a PLC. 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	See Ref. 44, Attachment A, Section A. See Ref. 34. See Ref. 35, Section 4. See Ref. 17.
	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	See Ref. 43, Appendix A, Task 6.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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. 35, Section 5.b.
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. 17. 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.
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. 35, Section 5.b.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 17, Appendix A, Section 3.1. 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. 17, Appendix A, Section 3.1. 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. 17, Appendix A, Section 3.1. 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. 35, Section 5.a
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. 17, Appendix A, Section 3.1.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 17, Appendix A, Section 3.1.
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. 17, Appendix A, Section 3.1.
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	See Ref. 44. 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 Discrep. - QPM 19.1 to 6: RMA Process Key Documents: - Product Discrepancy Reports - Customer Service Database - Customer System Config. Files - Product Alert Notices

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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. 1, Sections 1 and 2, and Refs. 10 and 11.
8.1.B	Manufacturer Documentation. Documentation shall include a description of the chassis interconnections.	Comply	See Ref. 1, Section2 and 6 .
8.1.C	Manufacturer Documentation. Documentation shall include a module overview and selection guide.	Comply	See Ref. 1, Section 3.
8.1.D	Manufacturer Documentation. Documentation shall include a description of the overall I/O capacity and processing speeds.	Comply	See Ref. 1, Sections 2 and 4.1.7.
8.1.E	Manufacturer Documentation. Documentation shall include installation information.	Comply	See Refs. 1, 10, 11 and 26.
8.1.F	Manufacturer Documentation. Documentation shall include handling and storage requirements.	Comply	See Ref. 1, Sections 4 and 5.
8.1.G	Manufacturer Documentation. Documentation shall include a description of the self-diagnostics and redundancy features.	Comply	See Ref. 1, Section 1.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.2	Equipment General Specifications Requirements. Manufacturer documentation shall provide general specifications for the PLC.	Comply	See Refs. 1 and 13, and Appendix B of this report.
8.3	Operator's Manual Requirements. Manufacturer documentation shall include information on operation of the PLC.	Comply	See Refs. 1 and 13.
8.4	Programmer's Manual Requirements. Manufacturer shall provide detailed information on the use of the functions available in the PLC processors.	Comply	See Refs. 2 and 4.
8.4.A	Programmer's Manual Requirements. Manual shall include a summary and brief description of available functions.	Comply	See Refs. 2 and 4.
8.4.B	Programmer's Manual Requirements. Manual shall include a detailed description of each function.	Comply	See Refs. 2 and 4.
8.4.C	Programmer's Manual Requirements. Manual shall include examples of complex functions.	Comply	See Ref. 2, Section 4.
8.4.D	Programmer's Manual Requirements. Manual shall include limitations on use of functions.	Comply	See Refs. 2 and 4.
8.4.E	Programmer's Manual Requirements. Manual shall include methods for resource management.	Comply	See Refs. 2 and 4.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
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 Refs. 2 and 4.
8.4.G	Programmer's Manual Requirements. Manual shall include detailed information for creating user defined functions.	Comply	See Refs. 2 and 4.
8.4.H	Programmer's Manual Requirements. Manual shall include a detailed description of operation of conditional statements.	Comply	See Refs. 2 and 4.
8.4.I	Programmer's Manual Requirements. Manual shall include a description of limitations of PID and lead/lag functions.	Comply	See Refs. 2 and 4.
8.4.J	Programmer's Manual Requirements. Manual shall include a description of interaction between main processor and I/O modules.	Comply	See Refs. 2 and 4.
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. 4.
8.4.L	Programmer's Manual Requirements. Manual shall include any software build procedures and software tools.	Comply	See Refs. 2 and 4.
8.4.M	Programmer's Manual Requirements. Manual shall include a description of the operation of the executive.	Comply	See Refs. 2 and 4.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.4.N	Programmer's Manual Requirements. Manual shall include a description of data, data base and configuration management.	Comply	See Refs. 2 and 4.
8.4.O	Programmer's Manual Requirements. Manual shall include a description of operation and use of self-diagnostics.	Comply	See Ref. 4.
8.4.P	Programmer's Manual Requirements. Manual shall include a manual for coprocessor programming.	N/A	Coprocessor operation is invoked automatically.
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. 1, Section 5, and Refs. 15 and 39.
	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. 9.
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 Refs. 16 and 37.

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 Refs. 9 and 16.
8.6.1.C	Programmatic Documentation. Procedures shall be prepared for qualification testing.	Comply	See Refs. 6, 16, 18, 21, 22, 23, 27, 30, and 31.
8.6.1.D	Programmatic Documentation. Test reports shall be prepared for each qualification test performed.	Comply	See Refs. 3, 5, 8, 12, 14, 20, 28, 32, and 33.
8.6.1.E	Programmatic Documentation. Reports on audits performed on the manufacturer shall be prepared.	Comply	See Ref. 34.
8.6.1.F	Programmatic Documentation. Reports on design evaluations shall be prepared.	Comply	See Ref. 38. Design evaluations include radiation withstand analysis.
8.6.2	Technical Items and Acceptance Criteria Documentation Requirements. Descriptive information.	- - -	No requirements.
8.6.2.A	Technical Items Documentation. Documentation shall include test specimen requirements.	Comply	See Ref. 37.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.6.2.B	Technical Items Documentation. Documentation shall include test specimen purchasing records.	N/A	See Refs. 9 and 39. No hardware purchases involved. Test specimen was supplied by manufacturer. Supplied hardware is documented in a Master Configuration List and hardware Certificates of Conformance.
8.6.2.C	Technical Items Documentation. Documentation shall include TSAP development documentation.	Comply	See Refs. 19, 24, 40 and 41.
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 Refs. 14 and 32, 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 Refs. 28 and 29, 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 Refs. 12 and 42, and Appendix B of this report.
8.6.3.D	Application Guide. Guide shall include results of surge withstand testing.	Comply	See Refs. 8 and 42, and Appendix B of this report.
8.6.3.E	Application Guide. Guide shall include results of EMI/RFI testing.	Comply	See Refs. 33 and 42, and Appendix B of this report.
8.6.3.F	Application Guide. Guide shall include results of power quality testing.	Comply	See Ref. 32 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 used in testing.
8.6.3.H	Application Guide. Guide shall include a description of the as-tested PLC configuration.	Comply	See Ref. 25 and 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. 9 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. 25 and Appendix B of this report.
8.6.3.K	Application Guide. Guide shall include a summary of the FMEA and availability analysis.	Comply	See Refs. 3 and 5, and Appendix B of this report.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.6.3.L	Application Guide. Guide shall include the setpoint analysis support document.	Comply	See Ref. 7 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. 26 and Appendix B of this report.
8.6.3.S	Application Guide. Guide shall include a description of qualification envelopes for specific modules if different from the overall envelope.	Comply	See Refs. 12, 30 and 33, and 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.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.6.4	Supporting Analyses Documentation Requirements. Documentation shall be provided of the FMEA and Availability/Reliability Analyses.	Comply	See Refs. 3 and 5.
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 Refs. 12, 16 and 31.
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. 35.
8.7.B	V&V Documentation. Documentation shall include a software requirements specification.	Comply	See Ref. 24.
8.7.C	V&V Documentation. Documentation shall include a software design description.	Comply	See Ref. 40.
8.7.D	V&V Documentation. Documentation shall include a software V&V plan.	Comply	See Ref. 35.
8.7.E	V&V Documentation. Documentation shall include a software V&V report.	Comply	See Ref. 19.
8.7.F	V&V Documentation. Documentation shall include software user documentation.	Comply	See Ref. 2.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.7.G	V&V Documentation. Documentation shall include a software configuration management plan.	Comply	See Ref. 35.
8.8	System Description Requirements. A test specimen hardware and software description document shall be provided.	Comply	See Ref. 25.
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. 26.
8.10.A	System Drawing Requirements. Drawings shall include a functional description of the test specimen.	Comply	See Ref. 26, Functional Drawings.
8.10.B	System Drawing Requirements. Drawings shall include a schematic of the test specimen.	Comply	See Ref. 26, Wiring and Arrangement Drawings.
8.10.C	System Drawing Requirements. Drawings shall include diagrams that define the TSAP.	Comply	See Ref. 26, Functional Drawings.
8.10.D	System Drawing Requirements. Drawings shall show test specimen wiring, power distribution and grounding.	Comply	See Ref. 26, Wiring and Arrangement Drawings.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.10.E	System Drawing Requirements. Drawings shall show layout of test specimen chassis, modules and qualification test fixtures.	Comply	See Ref. 26, Wiring and Arrangement Drawings.
8.10.F	System Drawing Requirements. Drawings shall show test specimen mounting and mounting fixtures, including special installation requirements.	Comply	See Ref. 26, Wiring and Arrangement Drawings.
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 Refs. 9 and 41.
8.12	System Database Documentation Requirements. The TSAP database used for qualification testing shall be documented.	Comply	See Ref. 41.
8.13	System Setup/Calibration/Checkout Procedure Requirements. All setup, calibration and checkout procedures used during qualification shall be documented.	Comply	See Ref. 18.
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 Refs. 6, 16 and 32.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS [1]	COMPLIANCE [2]	COMMENTS [3]
8.15	Manufacturer's Quality Documentation Requirements. The manufacturer shall provide its Quality Assurance Plan.	Comply	See Refs. 35 and 36.
8.16	Manufacturer's Certifications Requirements. Manufacturer shall provide certificates of conformance for all test specimen hardware.	Comply	See Ref. 51.

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

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.
TR Discrepancy	The requirement as given in TR-107330 can not be met. The Comments column provides a discussion and disposition of the identified TR discrepancy.

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

Appendix A - Qualification Summary Report
EPRI TR-107330 Requirements Compliance and Traceability Matrix

<u>List of References</u>:

Note: Unless indicated, applicable revision levels of all Triconex documents, reports, procedures and drawings are per the current revision of Triconex Document No. 7286-540, Master Configuration List.

1. Tricon Version 9 Planning and Installation Guide, Release 5 dated March, 1998, Part No. 9720051-005.
2. Tristation 1131 Developer's Workbench User's Guide, Version 1.1, Copyright 1997, Document No. 9720064-001.
3. Triconex Document No. 7286-531, Reliability/Availability Study for Tricon PLC Controller.
4. Tristation 1131 Developer's Workbench Tricon Library Functions, Version 1.1, Copyright 1997, Document No. 9720065-001.
5. Triconex Document No. 7286-532, Failure Modes and Effects Analysis (FMEA) for Tricon Version 9 PLC.
6. Triconex Procedure No. 7286-503, Tricon Nuclear Qualification Program Operability Test Procedure.
7. Triconex Document No. 7286-534, Tricon System Accuracy Specifications.
8. Triconex Report No. 7286-528, Tricon Nuclear Qualification Program Surge Withstand Test Report.
9. Triconex Document No. 7286-540, Tricon Nuclear Qualification Program Master Configuration List (MCL).
10. Tricon Version 9 User's Manual for Field Terminations, Release 4 dated March 1998, Part No. 9720052-004.
11. Tricon Version 8 User's Manual for Field Terminations, Release 1 dated June 1992, Part No. 9720030-001.
12. Triconex Report No. 7286-529, Tricon Nuclear Qualification Program Class 1E to Non-1E Isolation Test Report.

<u>List of References</u> (continued):

13. Tricon Version 9.2 Technical Product Guide, dated June 1997, Part No. 9791007-004.

14. Triconex Report No. 7286-525, Tricon Nuclear Qualification Program Environmental Test Report.

15. Tricon Version 9 User's Manual for Triconex Intelligent Communication Modules, Release 3 dated March, 1998, Part No. 9720047-003.

16. Triconex Document No. 7286-500, Tricon Nuclear Qualification Program Master Test Plan.

17. Triconex Document No. 7286-535, Tricon Nuclear Qualification Program Software Qualification Report.

18. Triconex Procedure No. 7286-502, Tricon Nuclear Qualification Program System Setup and Check-Out Test Procedure.

19. Triconex Document No. 7286-536, Tricon Nuclear Qualification Program TSAP Verification and Validation Report.

20. Triconex Document No. 7286-524, Tricon Nuclear Qualification Program Pre-Qualification Test Report.

21. Triconex Procedure No. 7286-504, Tricon Nuclear Qualification Program Prudency Test Procedure.

22. Triconex Procedure No. 7286-507, Tricon Nuclear Qualification Program Seismic Test Procedure.

23. Triconex Procedure No. 7286-506, Tricon Nuclear Qualification Program Environmental Test Procedure.

24. Triconex Procedure No. 7286-517, Tricon Nuclear Qualification Program TSAP Functional Requirements Specification.

25. Triconex Document No. 7286-541, Tricon Nuclear Qualification Program Tricon Test Specimen Description.

List of References (continued):

26. Triconex Drawing Nos. 7286-001 through 7286-543, STPNOC Tricon Generic Qualification System.

27. Triconex Procedure No. 7286-510, Tricon Nuclear Qualification Program EMI/RFI Test Procedure.

28. Triconex Report No. 7286-526, Tricon Nuclear Qualification Program Seismic Test Report.

29. Wyle Laboratories Test Report No. 41339-1, Rev. A dated November 11, 1999, Environmental Stress Test and Seismic Simulation Test program on a Four Chassis Industrial Controller.

30. Triconex Procedure No. 7286-508, Tricon Nuclear Qualification Program Surge Withstand Test Procedure.

31. Triconex Procedure No. 7286-509, Tricon Nuclear Qualification Program Class 1E to Non-1E Isolation Test Procedure.

32. Triconex Report No. 7286-530, Tricon Nuclear Qualification Program Performance Proof Test Report.

33. Triconex Report No. 7286-527, Tricon Nuclear Qualification Program EMI/RFI Test Report.

34. South Texas Project Nuclear Operating Company Audit Report of the Triconex Corporation, No. 97-047.

35. Triconex Document No. 7286-537, Tricon Nuclear Qualification Program Software Quality Assurance Plan.

36. Triconex Document No. QPL-01, Tricon Nuclear Qualification Program Quality Plan.

37. 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.

38. Triconex Report No. 7286-533, Tricon Nuclear Qualification Program Radiation Hardness Evaluation.

<u>List of References</u> (continued):

39. Tricon Version 9 802.3 Network Planning and Installation Guide, Release 3 dated March, 1998, Part No. 9720045-003.

40. Triconex Procedure No. 7286-518, Tricon Nuclear Qualification Program TSAP Design Specification.

41. Triconex Procedure No. 7286-519, Tricon Nuclear Qualification Program TSAP Program Listing.

42. Wyle Laboratories Test Report No. 41339-2 dated March 21, 2000, Electromagnetic Interference (EMI) Test Report on a Tricon PLC System.

43. STP Nuclear Operating Company Purchase Order No. ST-401734 dated December 9, 1997, with the Triconex Corporation, Qualification of a Programmable Logic Controller.

44. STP Nuclear Operating Company Purchase Order No. ST-401734, Supplement No. 1 dated December 9, 1997, with the Triconex Corporation, Qualification of a Programmable Logic Controller.

45. Triconex Corporation Quality Assurance Manual, Revision 13 dated April 4, 1999.

46. E-Mail from G. Hufton (Triconex) to M. Albers (MPR Associates) dated April 17, 2000, Responses to Tricon Equipment Specification Questions.

47. Tristation 1131 Developer's Workbench Getting Started Manual Version 1.1, Copyright 1997, Document No. 9720061-001.

48. Tricon Version 9 Sequence of Events User's Manual, Release 1, Update 3 dated January 1997, Part No. 9720042-001.

49. Triconex Engineering Procedure EDM 75.00, Nuclear Product Qualification, Draft.

List of References (continued):

50. E-Mail from R. Popp (Triconex) to M. Albers (MPR Associates) dated April 24, 2000, Responses to Tricon Equipment Specification Questions.

51. Triconex Document No. 7286-542, Tricon Nuclear Qualification Program, Certificate of Conformance, Nuclear Qualification Test Specimen.

TRICONEX

Document:	7286-545	Title:	APPLICATION GUIDE		
Revision:	1	Page:	Appendix B, Page 1 of 54	Date:	9/18/00

APPLICATION GUIDE

Appendix B to

Document No. 7286-545

Revision 1

September 18, 2000

	Name	Signature	Title
Author:	David Herrell	[signature]	Engineer
Approvals:	Mitchell Albers	[signature]	Project Manager
	Troy Martel	[signature] /JTM	Triconex Project Director
	Jerry McCann	[signature]	VP, Research and Development

TRICONEX

Document:	7286-545	Title:	APPLICATION GUIDE		
Revision:	1	Page:	Appendix B, Page 1A	Date:	9/18/00

APPLICATION GUIDE

Appendix B to

Document No. 7286-545

Revision 1

September 18, 2000

QUALITY ASSURANCE DOCUMENT

This document has been prepared, reviewed, and approved in accordance with the Quality Assurance requirements of 10CFR50, Appendix B, as specified in the MPR Quality Assurance Manual.

	Name	Signature
Prepared by:	David Herrell	[signature]
Reviewed by:	Eric Claude	[signature]
Approved by:	Mitchell Albers	[signature]

Document Change History			
Revision	**Date**	**Change**	**Author**
0	6/27/2000	Initial Issue	D. Herrell
1	9/18/2000	Incorporate Triconex and STP Comments	D. Herrell

TABLE OF CONTENTS

1.0 INTRODUCTION

This report provides guidelines 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 Manual (Reference 7.11).

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 7.15).

Hardware type tests were performed with Version 9.3.1 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 9.3.1 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.

A. 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.

B. 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.

C. The TRICON PLC was designed to be used as a single channel Emergency Shutdown System or Safety Instrumentation System. Industries other than nuclear make use of only a single channel 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.

D. 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.

E. 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 correctly implement the application program, 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.

F. 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.

G. 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.

H. 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.

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

J. The TRICON PLC requires an external power supply for powering analog field inputs. A qualified Lambda dc power supply is available from Triconex.

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 trains or channels of safety systems, with one or more PLCs being used to replace a single train. Thus, each protection train or channel 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 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 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.

E. A third party field power supply is available through Triconex. This power supply will be qualified to the same levels as the TRICON PLC.

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 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 9720051.

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:

- Communications modules - Enhanced Intelligent Communication Module (EICM); Network Communication Module (NCM) providing an 802.3 Port; and Advanced Communication Module (ACM), the Foxboro I/A Series Nodebus Interface also providing an 802.3 Port.
- 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, 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 module optimized for use with non-amplified magnetic speed sensors common on rotating equipment such as turbines or compressors.

D. Qualified External Termination Assemblies (ETA) 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 Guideline 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 Guidelines.

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. 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 Manual (Reference 7.11).

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 can not 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 Manual (Reference 7.11).

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 802.3 protocol, to gain the protection of CRC checks on transmitted messages. In order to provide an 802.3 port, at least a NCM or ACM communication module must be installed. The EICM module does not provide CRC protection for messages, and thus should not be used for downloads from the TriStation 1131 PC.

C. Peer-to-peer communication is allowed between TRICON PLCs, as long as the restrictions provided in Section 5.6, 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.

In addition, while it might be desirable under certain circumstances to perform all TRICON configuration activities from a single communication network, the separation and independence requirements established in IEEE Standard 384-1992 discourages cross protection train cabling. The interconnections required to provide this functionality would interconnect all TRICON PLCs in all divisions,.channels, or trains to a single location.

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 was performed as part of the qualification effort. Triconex Report 7286-532 (Reference 7.17) provides the FMEA in tabular format. Results of this FEMA show that there are only a few parts of the Triconex design that are vulnerable. 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 (ETA) 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

7286-531 provides a Markov model for a given configuration (Reference 7.18). The system models and data provided could be used to estimate the possibility of failure for other TRICON configurations.

C. The TRICON offers a field proven reliability, with no failures to implement a required safety action, for over 100 million system operating hours. The likelihood of software common cause failure can thus be shown to be remote.

D. From a licensing perspective, the results of the FMEA and Reliability/Availability reports should be incorporated into licensing analyses for each TRICON installation.

E. 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 plant systems. 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. 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. 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 a protective action.

Diversity is one aspect of defense-in-depth that is used to avoid equipment common mode failure. Diversity has been applied to nuclear plant systems 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 requires consideration of a scenario where all equipment that shares a common digital platform fails in an unsafe state simultaneously. Alternate plant systems or manual operator actions must therefore be available to provide a means of shutting down and cooling the reactor. 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 reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.

- 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).

- 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); 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 (D-in-D&D) 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) HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." The NRC's position on D-in-D&D is stated in BTP HICB-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 (D-in-D&D) for control and instrumentation systems are described in BTP HICB-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-HICB-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, automatic, or manual 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 10CFR50, 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 power plants, 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 and/or ESFAS functions, either in new plants or to upgrade existing systems, the defense-in-depth and diversity analysis described above will need to be performed based on plant-specific accident conditions. The analysis will also need to consider plant-specific diverse indications and controls. One approach to implementing RTS and/or ESFAS functions using the TRICON platform is illustrated in Figure 1 and is discussed below.

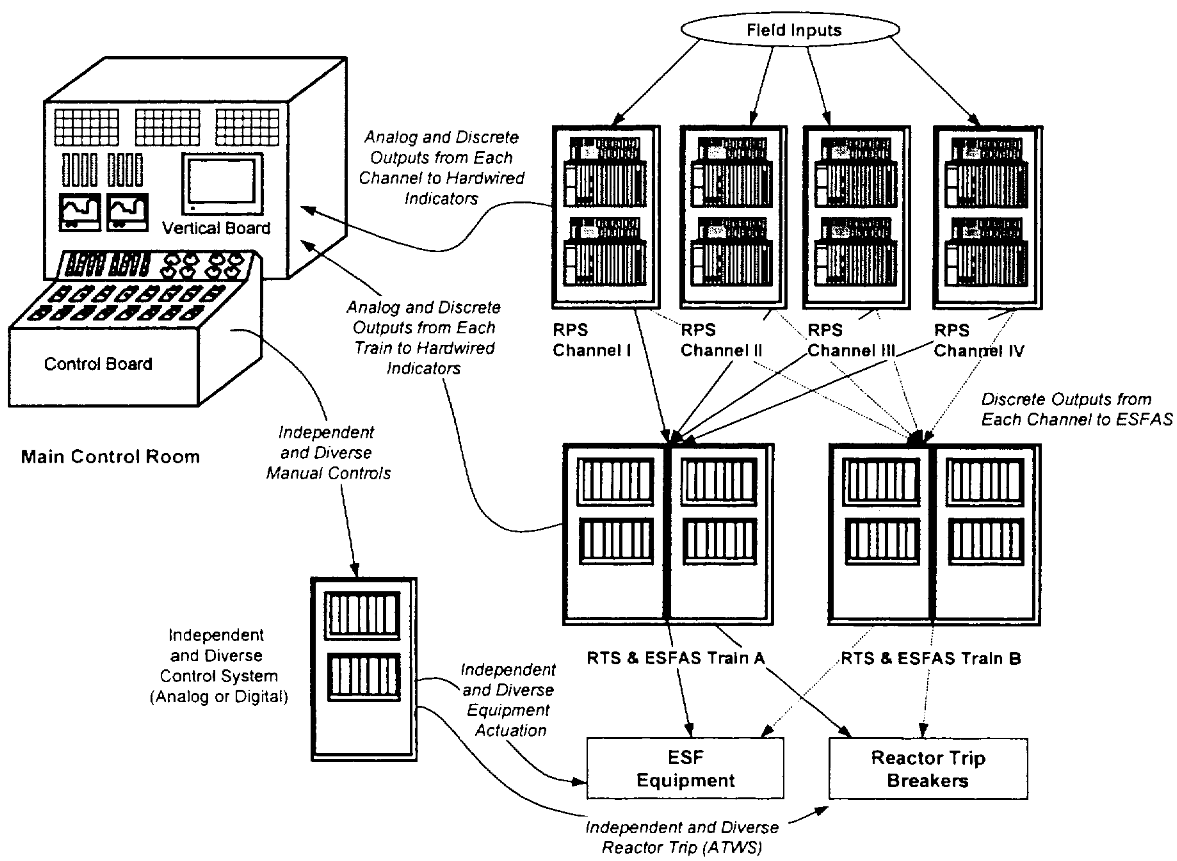


Figure 1. TRICON Reactor Protection System with Diversity

The figure illustrates use of the TRICON platform to implement reactor protection system functions using the traditional divisional 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 logic and automatic equipment actuation is performed by the two independent RTS systems.

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.

While not illustrated by Figure 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. 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 manual controls are used to actuate ESFAS equipment via a diverse control system. 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 whether automatic actuation is required. 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 parallel inputs to the critical equipment. To avoid false actuation, two normally open contacts should be wired in series. These contacts would have to close to actuate the equipment. The two contacts should be actuated by separate modules in the independent and diverse control system. Thus, the failure of a single module or a single contact would not result in false actuation of safety related equipment.

Additional protection from software common mode failures can also be obtained if the TRICON safety systems are installed in a plant with a digital non-safety related control and information systems. For example, Triconex has developed a plant design in which each of the independent TRICON safety systems are interfaced via the ACM module with a Foxboro I/A distributed control system (DCS). As previously described, the

ACM module provides one-way communication to the Foxboro I/A system and is qualified as a 1E-to-non 1E isolator. The ACM 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. With this approach, the DCS can also be configured to perform automatic and routine cross-comparisons of the data between each channel of the TRICON protection system to identify possible field sensor failures.

3.7 Setpoint Analysis and Accuracy

A. The accuracy of each analog input/output module was demonstrated to meet the following Triconex published product specifications, with no degradation in module accuracy throughout qualification testing.

Module	Description	Accuracy
3700A	RTD Input	less than ±1.2°C (over a 0°C to 360°C range)
		±1.2°C (over a >360°C to 600°C range)
3706A	Type J T/C Input	±7.0°F (over a -250°F to 32°F range)
		±5.0°F (over a >32°F to 2000°F range)
3708E	Type J T/C Input	±9.0°F (over a -238°F to 32°F range)
		±5.5°F (over a >32°F to 1400°F range)
3700A	0 to 5 V dc Input	±0.0075 V dc (over a 0 to 5 V dc range)
3701	0 to 10 V dc Input	±0.015 V dc (over a 0 to 10 V dc range)
3510	Pulse Input	±1.0% (over a 20 Hz to 99 Hz range)
		±0.1% (over a 100 Hz to 999 Hz range)
		±0.01% (over a 1,000 Hz to 20,000 Hz range)
3703E	4 to 20 mA Input	±0.030 mA (over a 4 to 20mA range)
3704E	4 to 20 mA Input	±0.050 mA (over a 4 to 20mA range)
3805E	4 to 20 mA Output	±0.055 mA (over a 4 to 20mA range)

B. The OFF to ON and ON to OFF voltage switching levels of each digital input module were demonstrated to meet the following Triconex published product specifications, with no degradation in voltage switching levels throughout testing.

Module	Description	Point Drive Capability Switching Level OFF to ON or ON to OFF
3504E	24 V dc Digital Input	6 V dc ≤ V_{SWITCH} ≤18 V dc
3501E	115 V ac Digital Input	28 V ac ≤ V_{SWITCH} ≤86 V ac
3502E	48 V dc Digital Input	11 V dc ≤ V_{SWITCH} ≤32 V dc
3503E	24 V dc Digital Input	6 V dc ≤ V_{SWITCH} ≤18 V dc
3505E	24 V dc Digital Input	4 V dc ≤ V_{SWITCH} ≤12 V dc

C. Each discrete output module was demonstrated to operate ON and OFF at the following manufacturer's published product specifications for maximum operating current, and minimum and maximum operating voltage.

		Point Drive Capability		
Module	Description	Max. Current	Min. Volts	Max. Volts
3604E	24 V dc Digital Output	2.0 amp	22 V ac	45 V ac
3624	24 V dc Digital Output	0.7 amp	16 V ac	30 V ac
3607E	48 V dc Digital Output	1.0 amp	44 V ac	80 V ac
3603E	120 V dc Digital Output	0.8 amp	90 V ac	150 V ac
3623	120 V dc Digital Output	0.8 amp	90 V ac	150 V ac
3601E	115 V ac Digital Output	2.0 amp	80 V ac	155 V ac
3636R	115 V ac Relay Output	2.0 amp	N/A	155 V ac

D. Accuracy, repeatability, thermal effects, and other necessary data for use in setpoint analyses are provided in the System Accuracy Specification (Reference 7.19).

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 HICB-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 HICB-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 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 HICB-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 this 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 HICB-17. There is nothing inherent in the TRICON or TriStation designs that does not comply with the requirements of IEEE Standard 603, as required in BTP HICB-17. The TRICON has been successfully evaluated against the recommendations made in IEEE Std 7-4.3.2 in the Critical Digital Review, Reference 7.16. 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 in a mode that reduces the current manual maintenance and testing activities, thus reducing the risks associated with performing the 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 are 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. 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 and Reg. Guide 1.47, if the protective action of some part of a protection system is bypassed or deliberately rendered inoperative for testing, that fact should be continuously indicated in the control room. 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 can not be readily validated in the field.

N. Surveillance testing taken together with automatic self-testing should provide a mechanism for 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 100 Million operating hours without a failure to implement a required protective action demonstrates the TRICON's 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 be in the RUN 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.

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.

D. Separate sections of this Application Guideline provide specific recommendations for Maintenance Overrides and Communication with External Systems.

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 Manual (Reference 7.11), and the results of the qualification testing.

4.1 Mounting

A. The TRICON chassis is designed for mounting in 19" 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. 7286-101, "Generic Qualification System Equipment Mounting Details." A copy of this drawing is included as Attachment 1 to the Seismic Test Report, Triconex Report Number 7286-526. All fastener torque values are indicated on Triconex Drawing 7286-101. 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" 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. The temperature and humidity profile applied during environmental qualification testing of the TRICON PLC is shown in Figure 7-1 of the Environmental Test Report, Triconex Report Number 7286-525 (Reference 7.21).

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 7.28).

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

A. Seismic testing was performed in accordance with the requirements of EPRI TR-107330, Section 4.3.9, and IEEE Standard 344.

B. Seismic testing demonstrates that the TRICON is qualified as a Category I seismic device within the test limits shown on Figure 4-1. Due to limitations of the seismic test table, the five OBE tests and the SSE test of the TRICON were performed using the same test response spectrum (TRS), shown in Figure 4-1. 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.

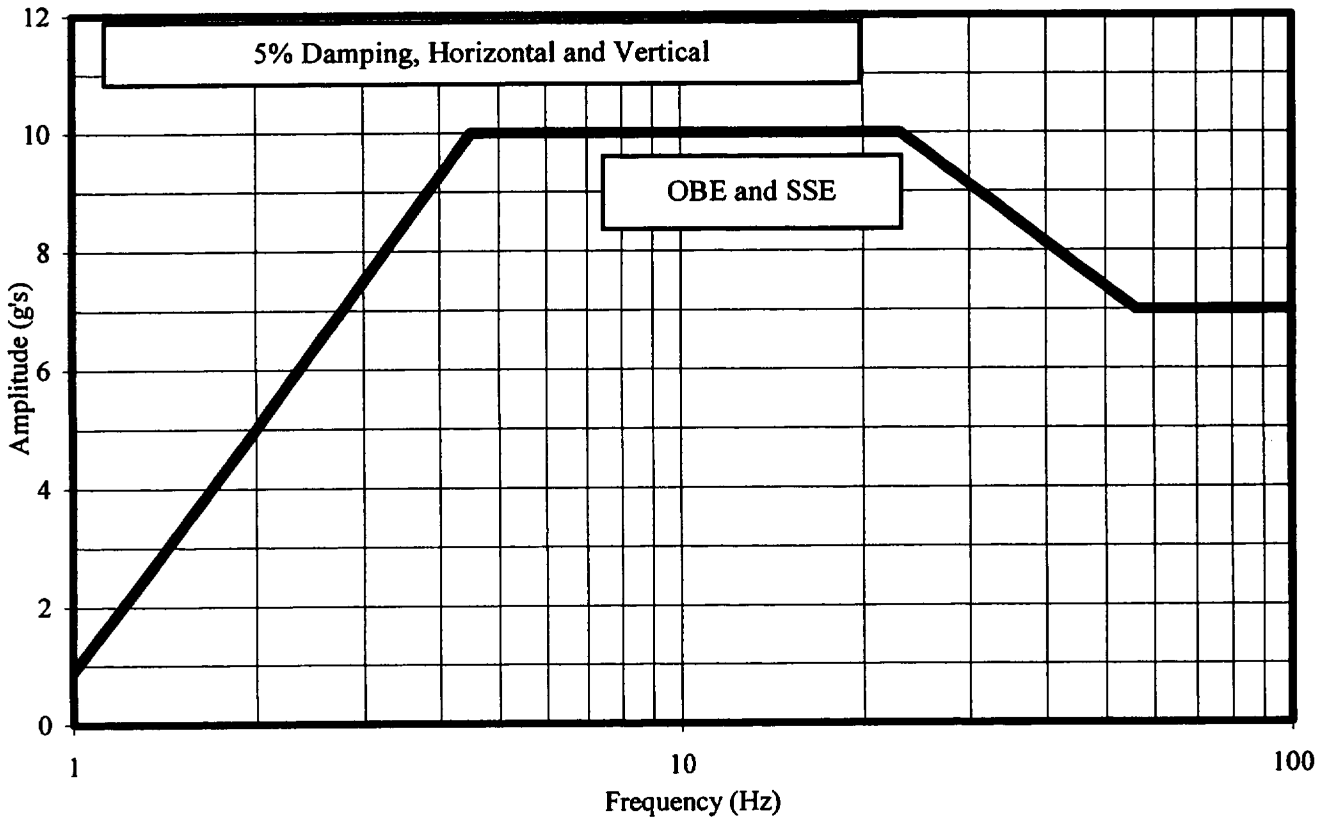


Figure 4-1. Seismic Withstand Response Spectrum

4.5 Radiation Fields

The Triconex Radiation Analysis Report (Reference 7.27) provides an evaluation of the withstand capability of the TRICON to a mild environment radiation exposure of 1000 rads integrated over a 40 year period. The evaluation concludes that this level of exposure will not prevent the TRICON from performing its safety-related function.

4.6 Electro-Magnetic Compatibility

A. The following EMI/RFI tests were performed on the TRICON PLC:

- Radiated Magnetic Field Emissions from 30 Hz to 100 kHz (RE101)
- Radiated Electric Field Emissions from 10 kHz to 1 GHz (RE102)
- Low Frequency Conducted Emissions from 30 Hz to 50 kHz (CE101)
- High Frequency Conducted Emissions from 50 kHz to 400 MHz (CE102)
- Radiated Magnetic Field Susceptibility from 30 Hz to 100 kHz (RS101)

- Radiated Electric Field Susceptibility from 10 kHz to 1 GHz (RS103)
- Low Frequency Conducted Susceptibility from 30 Hz to 50 kHz (CS101)
- High Frequency Conducted Susceptibility from 50 kHz to 400 MHz (CS114)
- Electrical Fast Transient Susceptibility (IEC 801-4)

These tests were performed in accordance with the requirements and methodologies of EPRI TR-107330 and EPRI TR-102323-R1, with two exceptions described in item D below.

B. The TRICON PLC fully complies with the allowable equipment emissions levels defined in Section 7 of EPRI TR-102323-R1 for radiated magnetic field emissions testing from 30 Hz to 100 kHz (RE101).

C. The TRICON PLC does not fully comply with the allowable equipment emissions levels defined in Section 7 of EPRI TR-102323-R1 for the following emissions tests:

- Radiated Electric Field Emissions from 10 kHz to 1 GHz (RE102)
- Low Frequency Conducted Emissions from 30 Hz to 50 kHz (CE101)
- High Frequency Conducted Emissions from 50 kHz to 400 MHz (CE102)

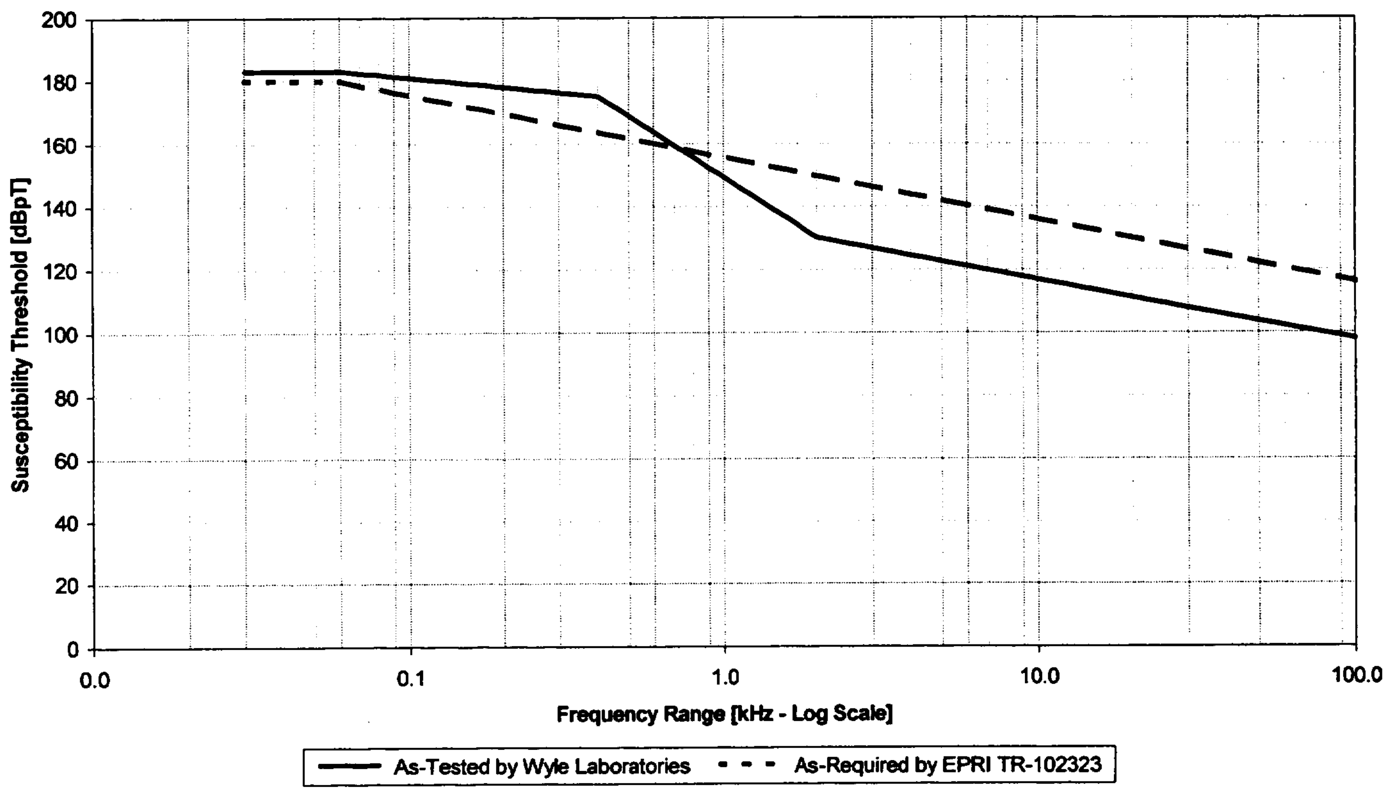
Sections 6.3, 6.4 and 6.5, and Appendix C of the EMI/RFI Test Report, Triconex Report 7286-527 (Reference 7.22) provide a detailed description of the emissions non-compliance that were measured during each of the tests listed above. The TRICON PLC was tested without the benefit of a secondary enclosure, additional cable and wire shielding, or installed power line filtering. Mitigating actions to address the measured emission level non-compliance would likely incorporate these common in-plant installation features.

An understanding of the electromagnetic emissions from a device is necessary to minimize the potential for the device to adversely affect the operation of other equipment that is physically located near the device, shares common electrical connections with it, or has wires or cables routed in close proximity to it. Therefore, prior to installing the TRICON PLC in a nuclear safety-related or non-safety related application, an evaluation of the device emission levels should be made to determine whether the emission levels provided in the EMI/RFI Test Report (Reference 7.22) are acceptable for the planned application, or if mitigating actions would be required.

D. The TRICON PLC system successfully passed all of the EMI/RFI susceptibility tests listed, subject to the following two test level exceptions provided below:

Figure 4-2

RS101 Radiated Magnetic Field Susceptibility Test - 30 Hz to 100 kHz
Comparison of Actual Test Levels to As-Required Test Levels



1) EPRI TR-102323-R1 requires RS101 tests to be performed using the MIL-STD-461D, Army Only, test levels. The TRICON was tested at levels closer to the RS101 Navy Only test levels. Figure 4-2 provides a comparison of the as-required and as-tested levels.

2) EPRI TR-102323-R1 requires CS114 tests to be performed at a test level of 103 dBμA, which corresponds with CS114 Curve 4 from MIL-STD-461D. The TRICON was tested at a CS114 test level of 95 dBμA, which corresponds with CS114 Curve 3 from MIL-STD-461D.

E. The main processors and coprocessors continued to function correctly throughout susceptibility 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.

F. The TRICON PLC input, output, and communication modules fully comply with the as-tested radiated magnetic field (RS101) susceptibility thresholds shown in

Figure 4-2. There were no interruptions in the transfer of input, output, and communication data. There were no spurious changes in state of the discrete inputs and outputs. The analog input and output levels did not vary by more than ±3% of the expected levels.

G. The TRICON PLC input, output and communication modules do not fully comply with the minimum recommended susceptibility thresholds defined in Section 4 and Appendix B of EPRI TR-102323-R1 for the following susceptibility tests:

- Radiated Electric Field Susceptibility from 10 kHz to 1 GHz (RS103)
- Low Frequency Conducted Susceptibility from 30 Hz to 50 kHz (CS101)
- High Frequency Conducted Susceptibility from 50 kHz to 400 MHz (CS114)
- IEC 801-4 Electrical Fast Transient (EFT) Susceptibility

Sections 6.7, 6.8, 6.9 and 6.10, and Appendix C of the EMI/RFI Test Report, Triconex Report Number 7286-527, provide a detailed description of the module susceptibilities which were measured during each of the tests listed above, and the results of threshold testing which was performed. Module susceptibilities included spurious changes in the state of the discrete inputs and outputs, variations in analog input and output levels of greater than ±3% of the expected levels, and momentary loss of communications with peripheral devices. In some cases, the recorded test data provides inconclusive evidence of the susceptibility of particular modules. In these cases, the modules are conservatively assumed susceptible.

An understanding of the electromagnetic susceptibility of a device is necessary to ensure that its operation will not be adversely affected by EMI/RFI levels already present or permitted in the area where the device will be located. Therefore, prior to installing the TRICON 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 PLC EMI/RFI susceptibility testing documented in the EMI/RFI Test Report, Triconex Report Number 7286-527, provides the data required to perform such an evaluation. This evaluation could include one or more of the following:

(a) Demonstrate that the EMI/RFI levels at which the PLC modules are susceptible are not credible threats at the point of installation.

(b) Demonstrate that the type of susceptibility failures that occurred during the EMI/RFI testing will not adversely affect the safety function of the PLC or plant operation. For example, variations in analog input and output levels in excess of ±3% may not impact the safety-related function of the PLC or adversely affect plant operation.

(c) Implement actions to mitigate unacceptable EMI/RFI sources. The TRICON PLC was tested without the benefit of a secondary enclosure, additional cable and wire shielding, or installed power line filtering. Mitigating actions to address module susceptibility levels would likely incorporate these common in-plant installation features. Mitigating actions might also include administrative controls on the EMI/RFI sources.

(d) Perform additional testing to address those cases where the recorded EMI/RFI test data provides inconclusive evidence of the susceptibility of particular modules, and therefore the modules are assumed to be susceptible. Additional testing may demonstrate that some modules are not actually susceptible to the applied EMI/RFI test levels.

H. Table 6-1 in Attachment 6 of the EMI/RFI Test Report, Triconex Report Number 7286-527, provides a summary table of the EMI/RFI susceptibility test results (Pass, Fail or Inconclusive) for each module installed in the TRICON PLC. The purpose of the table is to identify a set of modules that demonstrated acceptable susceptibility performance at similar test levels. The CS114 test level acceptance criteria on which the summary table is based differs significantly from the test level acceptance criteria recommended in EPRI TR-102323-R1. Basing Table 6-1 on lower acceptance criteria for CS114 testing allows the identified set of modules to encompass at least one of each module type that might typically be used in a safety-related application. The impact of the lower CS114 susceptibility threshold criteria will have to be addressed as described above for each specific plant application.

A comparison of the Table 6-1 and EPRI TR-102323-R1 acceptance criteria for each susceptibility test is given below:

Test Method	Table 6-1 Acceptable Results	TR-102323-R1 Acceptance Criteria
RS101	Figure 4-2	Figure 4-2
RS103	10 V/m	10 V/m
CS101	6.3 V rms	6.3 V rms
CS114	89 dBμA	103 dBμA
IEC 801-4	±3 kV	±3 kV

I. Compliance with TR-102323 EMI/RFI limits will be enhanced by the use of power line filtering, instrument grounding techniques, single or double point grounds on shielded cabling and jumpers, twisted pair cabling, and installation inside a shielded, grounded cabinet.

4.7 Surge Withstand Testing

A. Surge withstand testing of the TRICON PLC was performed in accordance with the applicable requirements of EPRI TR-107330, IEEE Standards C62.41-1991 and C62.45-1987, and IEC Standard 801-5. The following types of surge withstand tests were performed:

- IEEE C62.41 Ring Wave Test, 3.0 kV: Chassis Power Supplies
- IEC 801-5 Combination Wave Test, 3.0 kV: Chassis Power Supplies
- IEC 801-5 Combination Wave Test, 0.5 kV and 1.0 kV: Discrete Input Modules
- IEC 801-5 Combination Wave Test, 0.5 kV and 1.0 kV: Discrete Output Modules
- IEC 801-5 Combination Wave Test, 1.0 kV: Analog Input/Output Modules
- IEC 801-5 Combination Wave Test, 1.0 kV: Communication Modules

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 7.28).

B. The Surge Withstand Test Report, Triconex Report Number 7286-528, Attachment 2, provides a summary table of the surge withstand tests performed on the TRICON PLC. The summary results show that in all cases the TRICON PLC continued to operate in accordance with the test acceptance criteria given in EPRI TR-107330, Section 4.6.2 following application of the surge test voltages.

C. Five of the seven digital output modules included in the TRICON PLC exhibited vulnerability (permanent damage) to the applied surge test levels. These modules included:

- Model 3604E, 24 V dc digital output
- Model 3624, 24 V dc digital output
- Model 3607E, 48 V dc digital output
- Model 3603E, 120 V dc digital output
- Model 3623, 120 V dc digital output

In all cases the damaged points were detected by system diagnostics and indicated by status LED's and alarm lamps. In no case did a valid test result in damage to a module other than the module to which the surge test voltage was applied. In all but one case (digital output module 3603E) the damaged points were found to have failed in the OPEN (or Loss of Power) state. Based on this performance, the TRICON system meets the TR-107330 acceptance criteria for surge withstand. However, because the digital output modules listed exhibited surge voltage vulnerability, the modules are not acceptable for use in safety-related applications that are susceptible to surge voltages on discrete output lines, unless qualified surge suppression devices are attached to the discrete output lines.

The digital output modules listed above are acceptable for safety-related applications that can be demonstrated not susceptible to surge voltages on the discrete output lines. These would likely include most applications powered from plant vital power supplies, which are typically located indoors and are segregated from the high voltage power distribution systems in the plant.

D. The Model 3603E digital output module and associated Model 9661-910 ETA exhibited vulnerability (permanent damage) to applied surge voltages. The Model 3603T digital output module and associated Model 9661-910 (revised) ETA are revised versions of the Model 3603E module and ETA. These revised components were demonstrated through testing performed as part of the TRICON Nuclear Qualification effort to have acceptable surge withstand capability (i.e., no demonstrated vulnerability). By evaluation, it is determined that the design modifications incorporated in the Model 3603T module and ETA do not affect the environmental, seismic and EMI/RFI test results obtained for the Model 3603E module and ETA. Therefore, the Model 3603T digital output module and Model 9661-910 (revised) ETA are considered equivalent, preferred replacements for the Model 3603E digital output module and Model 9661-910 ETA, and are qualified for nuclear safety related use.

4.8 Electrostatic Discharge (ESD) Testing

A. Triconex has tested and certified the TRICON for Electrostatic Discharge to the requirements established in IEC 801-2, Level 3 (8KV).

B. ESD events may cause solid state device damage that does not result in an immediate failure, but that results in performance degradation or eventual failure. Testing does not necessarily demonstrate that long term degradation in the module does not exist. Triconex has tested to a lower level than that required in EPRI TR-102323. The levels provided in EPRI TR-102323, 8 kV direct contact discharge and 15 kV for air discharge, can be achieved in nuclear power plants. However, subjecting a safety grade system to such levels would be poor maintenance practice.

C. The TRICON equipment will be installed in cabinets with limited access. Field wiring inputs have been tested for surge withstand and do not offer a means of entry for ESD events. ESD sources are likely to be technicians performing surveillance or maintenance activities. Prevention of ESD events will reduce the risk of inappropriate safety system performance. Therefore, all work should be performed using standard electronics ESD control practices. These practices should be used during incoming inspection, storage, handling, installation, operation, testing, module removal, and maintenance.

4.9 Isolation Testing

A. 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. The TRICON met all applicable performance requirements during and after application of the Class 1E to Non-1E isolation test voltages. The Class 1E to Non-1E isolation test results demonstrate that the following TRICON PLC communication module ports provide adequate electrical isolation per IEEE 384-1981 between the safety related portions of the TRICON and connected non-safety related communication circuits:

- Enhanced Intelligent Communication Module (EICM) Model 4119A, Serial Port Modbus Interfaces
- Advanced Communication Module (ACM) Model 4609, Dual Nodebus (DNBI) and RS-423 Serial Port Interfaces to a Foxboro I/A Console
- Network Communication Module (NCM) Model 4329, IEEE 802.3 (TCP/IP) Net 2 Interface to a Wonderware Console

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.

B. The Class 1E to Non-1E isolation test results demonstrate that the TRICON PLC relay output module Model 3636R provides adequate electrical isolation per IEEE 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 V ac (at 23.4 amps maximum) and 250 V dc (at 10 amps maximum).

C. The Model 4211 Remote RXM fiber optic module is considered an acceptable Class 1E to Non-1E isolation device by design. The fiber optic cables are incapable of transmitting electrical faults between the remote Non-1E RXM module and the primary RXM module (which would be installed in the safety related TRICON chassis), and therefore meet IEEE 384-1981 electrical isolation requirements. No testing was deemed necessary to validate this electrical isolation.

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. Triconex provides an equation for calculating the upper bound on response times for a particular hardware and application program configuration. The application specific maximum allowable response time shall be used to design the TRICON hardware and software configuration. Note that 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 which were calculated based on equations provided by Triconex. The testing demonstrates that the Triconex equations 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 0.14%, and a 5-minute timer function accuracy provided accuracy of 0.07%.

E. The response time to an RTD input was not measured. However, the time response of the field installed RTD itself 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.

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 (BTP) 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-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 or CD-RW.

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 NT environment.

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.

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, 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 can not 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 which were monitored during testing include the EICM module connections to the TriStation Console and the Simulator TRICON PLC running the MODBUS protocol, the ACM module connection to the Foxboro Intelligent Automation (I/A) Console, and the NCM module connections to the Wonderware Console and the Simulator TRICON PLC running 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 one of the approved modules.

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, 5.6, 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 Appendix A, "Maintenance Override" of the "TÜV Rheinland Report No. 945/EL 374/97," and in the "TriStation 1131 Programmer's Development Workbench User's Guide" in Appendix D. The communication link and variables shall comply with the Maintenance and Override requirements provided in Section 6.5 of this Application Guide.

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 800 milliseconds. However, up to 2 seconds may elapse from message initiation to message reception.

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.

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 five 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 Manual (Reference 7.11).

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 or channel. 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 or channels.

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 or division.

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 completely clear all of the application code from memory, 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** 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 can not 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.

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 can not 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

7.2 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position HICB-14, Guidance on Software Reviews for Digital Computer-Based I&C Systems

7.3 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position HICB-18, 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 HICB-17, Guidance on Self-Test and Surveillance Test Provisions

7.5 USNRC Regulatory Guide 1709, Selection of Sample Rate and Computer Wordlength in Digital Instrumentation and Control Systems

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

7.7 EPRI TR-102323-R1, Guidelines for Electromagnetic Interference Testing in Power Plants

7.8 IEEE Standard 323-1974, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

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

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

TRICONEX DOCUMENTS

7.11 Triconex Planning and Installation Guide, Part Number 9720051-005

7.12 Triconex User's Manual for Field Terminations, Part Number 9720052-004

7.13 Triconex Technical Product Guide, Part Number 9791007-004

7.14 Triconex TriStation 1131 Developer's Workbench User's Guide, Part Number 9720069-001

TRICONEX NUCLEAR QUALIFICATION PROJECT DOCUMENTS

7.15 Qualification Summary Report, Triconex Report Number 7286-545

7.16 Software Qualification Report, including the Critical Digital Review, Triconex Report Number 7286-535

7.17 Failure Modes and Effects Analysis, Triconex Report Number 7286-532

7.18 Reliability/Availability Study, Triconex Report Number 7286-531

7.19 Tricon System Accuracy Specifications, Triconex Report Number 7286-534

7.20 Seismic Test Report, Triconex Report Number 7286-526

7.21 Environmental Test Report, Triconex Report Number 7286-525

7.22 EMI/RFI Test Report, Triconex Report Number 7286-527

7.23 Surge Withstand Test Report, Triconex Report Number 7286-528

7.23 Class 1E to non-1E Isolation Test Report, Triconex Report Number 7286-529

7.24 TSAP Functional Requirements Specification, Triconex Report Number 7286-517

7.25 TSAP Design Specification, Triconex Report Number 7286-518

7.26 Performance Proof Test Report, Triconex Report Number 7286-530

7.27 Radiation Analysis Report, Triconex Report Number 7286-533

7.28 Master Configuration List, Triconex Report Number 7286-540