invensys™

TRICONEX®

TRICONEX PRODUCTS – INVENSYS PROCESS SYSTEMS

Project:	TRICON v10 NUCLEAR QUALIFICATION PROJECT

Non -Proprietary copy per 10CFR2.390
- Areas of proprietary information have been redacted.
- Designation letter corresponds to Triconex proprietary policy categories (Ref. transmittal number NRC-V10-09-001, Affidavit, Section 4.)

EQUIPMENT QUALIFICATION SUMMARY REPORT

Document No: 9600164-545

Revision 3

August 03, 2009

	Name	Signature	Title
Author:	Frank Kloer		Qualification Engineer
Reviewers:	Alan Sands		Project QA Engineer
Approval:	Naresh Desai		Project Manager

Revision History

Revision	Date	Description	Author
0	07/26/07	Initial Issue.	Hariprasad Parthasarathy
1	05/10/08	Revised section 4.5 of Summary Report. Added sections 3.4 and 3.6, and revised section 4.5 of Appendix B- Application Guide.	Hariprasad Parthasarathy
2	10/03/08	Revised to incorporate comments from NUPIC audit items (Reference ARR 597) into Sections 4.0 and 4.5, and Appendix B, Section 4.5. Corrected miscellaneous typographical errors. Revised Section 4.5 of Appendix B- Application Guide to include as-tested analog/digital field power supply configuration requirements.	Frank Kloer
3	08/03/09	Revised various sections of Summary Report to make typographical corrections and add reference designators (Reference ARR 711).	Frank Kloer

Table of Contents

1.0 INTRODUCTION

This summary report documents the basis for generic qualification of the Tricon v10 Programmable Logic Controller (PLC) system for safety-related applications in nuclear power plants. The basis for qualification is compliance with EPRI TR-107330, Reference 7.6, 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 Traceability Matrix (CTM) included as Appendix A, documents the compliance of the Tricon v10 PLC with each of the requirements specified in EPRI TR-107330.

The Tricon is a mature commercial PLC with more than twenty 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 of the Tricon. The TMR design enables the Tricon system to be highly fault tolerant, to identify and annunciate faults that inevitably occur, and to allow replacement of modules 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 v10 PLC. Note that the Tricon v10 Programmable Logic Controller (PLC) system is a successor to the Tricon v9 system, which was nuclear qualified and approved for safety related use by the Nuclear Regulatory Commission (NRC) in year 2001. The Tricon v10 system includes enhanced Main Processor (model 3008), the next generation differential Analog Input (NGAID) module, the next generation differential Digital Output (NGDO) module, SMT versions of previously qualified I/O modules, and the Tricon Communication Module (TCM).

The Tricon v10 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 v10 system meets the acceptance criteria. In applying the Tricon v10 system to a specific safety-related application, the user must confirm that the qualification envelope bounds the plant-specific requirements. Additional guidance in the form of qualification limitations on the use of the Tricon v10 system in safety-related applications is provided in Appendix B - Application Guide. A comparison of the Tricon V10 Qualification to the EPRI TR-107330 requirements is documented in Appendix A - EPRI TR-107330 Requirements Compliance and Traceability Matrix. Exceptions and clarifications to the requirements and/or test methodology have been summarized in Table 6-1.

The generic qualification of the Tricon v10 PLC encompasses both the hardware and the software used in the system. The hardware includes termination assemblies, signal conditioners, chassis, power supplies, main processor modules, communication modules, input/output modules, termination assemblies, signal conditioners and interconnecting cables. The specific Tricon modules selected for qualification are defined in the Master Configuration

List, Reference 7.34. 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 v10 system involved technical evaluations and qualification tests. This report summarizes the results of these evaluations and tests and provides references to the applicable documents for more detailed information.

2.0 PROJECT OVERVIEW

This section provides an overview of the Tricon v10 Nuclear Qualification Project. EPRI TR-107330 provides generic requirements for qualifying commercial PLCs for use in safety-related applications in nuclear 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 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 EPRI 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 v10 Nuclear Qualification Project was initiated by Triconex to qualify the Tricon v10 system in accordance with the EPRI TR-107330 requirements. Quality Assurance requirements and special procedures that were unique to the Tricon v10 Nuclear Qualification Project are documented in the Nuclear Qualification Quality Plan, Reference 7.32. The major activities completed as part of this project include the following:

- Identifying the specific PLC modules and supporting devices to be qualified. The Tricon hardware included in the qualification envelope are listed in the Master Configuration List, Reference 7.34. This hardware was integrated in a complete test system intended to demonstrate capabilities typical of various nuclear safety systems. The design of the test system is documented in the Tricon System Description, 7.36, and associated System Drawings, 7.37 through 7.39.
- Developing an application program to support the required testing. The Test Specimen Application Program (TSAP) was developed to simulate operation of the Tricon for various qualification tests. Development, including verification and validation (V&V) of the TSAP was done in accordance with the Triconex QA program and a project-specific Software Quality Assurance Plan, Reference 7.35. The TSAP program and associated V&V activities are documented in References 7.67 through 7.71.
- Specifying the set of qualification tests to be performed on the test system, including defining a set of Operability and Prudency tests to be performed at suitable times in the qualification process. Operability and Prudency 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 7.33. Test procedures are provided in References 7.40 through 7.50.

- Performing the qualification tests and documenting the results. Results of these tests, documented in References 7.51 through 7.62, define the qualification envelope and form the basis for the application guidance contained in this report.
- Performing other technical evaluations as needed to demonstrate compliance with regulatory requirements and other technical requirements in EPRI TR-107330. Evaluation of the embedded operating system and programming software is documented in the Software Qualification Report, Reference 7.66. Evaluation of new hardware modules (MP 3008, NGAID 3721, NGDO 3625, and Tricon Communication Module (TCM)) is documented in Critical Digital review (CDR), Reference **7.74**. A failure modes and effects analysis evaluating the effects of component failures on Tricon operation is provided in Reference 7.64. Reference 7.63 documents an analysis of Tricon system reliability/availability. Reference 7.65 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 Technical Product Guide, Reference 7.30, and the Tricon Planning and Installation Guide, Reference 7.31. The specific hardware and software that has been qualified is identified in the Master Configuration List, Reference 7.34. For convenience, Table 3-1 at the end of this section lists the Tricon modules that have been qualified for nuclear safety-related applications.

The Tricon system was designed as a safety-critical system, and all aspects of its design are based on a 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.

3.1 Tricon System Hardware

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

3.1.1 Main Chassis

A Tricon system consists of one main chassis and up to fourteen additional expansion chassis. The Tricon main chassis supports the following modules:

- Three main processors
- Two redundant power supply modules
- Communications modules
- Input/Output modules

The main chassis has a key switch which sets the Tricon 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.

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.

3.1.2 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 buses. 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

3.1.3 Remote Extender Modules

The Remote Extender Modules (RXM) are multi-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 extenders of the Tricon I/O bus, which 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 non safety-related expansion chassis.

3.1.4 External Termination Assemblies

The External Termination Assemblies (ETAs) are printed circuit board assemblies used for landing field wiring. The assemblies contain terminal blocks, resistors, fuses, and blown fuse indicators. The standard assemblies are configured for specific applications (e.g. digital input, analog input, etc.). The thermocouple input termination assembly provides cold-junction temperature compensation sensors and can be ordered with upscale, downscale, or programmable burnout detection. The resistance temperature device (RTD) termination assemblies include signal conditioning modules. Each termination assembly includes an interface cable that connects the termination assembly to the Tricon chassis backplane.

3.1.5 Power Supply Modules

All power supply modules are rated for 175 watts, which is sufficient to supply the power requirements of a fully populated chassis. Two different power supply modules can be used in a single chassis. Three qualified models are available to support different power sources: 120 VAC/VDC, 230 VAC and 24 VDC.

The power supply modules possess built in diagnostic circuitry to check for out-of-range voltages and/or over temperature conditions. The power supply modules also contain the system alarm contacts. The chassis backplane provides terminal strip interfaces for power and alarm connections. The alarm feature operates independently for each power module. On the main chassis, the alarm contacts on both power supply modules actuate on the following states:

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

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

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

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

3.1.6 Main Processor Modules

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

The second 32-bit primary processor manages execution of the control program and all system diagnostics at the main processor module level. Between the 32-bit processors 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 flash memory on each module. The main processors communicate with one another through a proprietary, high speed, voting, bi-directional serial channel called TriBUS. Each main processor has an I/O channel for communicating with one of the three legs of each I/O and communication module. Each main processor has an independent clock circuit and selection mechanism that enables all three main processors to synchronize their operations each scan to allow voting of data and exchange of diagnostic information.

The IOCCOM processors constantly poll respective legs for all the input and output modules in the system. They continually update an input data table in 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 TriTime. 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 (2-o-o-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. If an analog input value on one leg has a significant deviation from the other leg inputs, the point will be alarmed and the main processors will use the average value of the two analog inputs on the other two legs.

The primary processors on the main processor modules 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 IOCCOM processors generate smaller output tables, each corresponding to an individual output module in the system. Each small table is transmitted to the appropriate leg of the corresponding output module over the I/O data bus.

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

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

- Verification of fixed program memory.
- Verification of the static portion of RAM.
- Verification of the 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 TriTime interface.
- Verification of the TriBUS interface.

When a fault is detected on a main processor module, it is annunciated and voted out, and processing continues through the remaining two main processors. When the faulty main processor is replaced, it runs a self-diagnostic to determine its basic health. When the self-diagnostic is successfully completed, the main processor then begins the process of "re-education," where the control program is transferred from one 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.

3.1.7 Input/Output Modules

The 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 Tricon Planning and Installation Guide, Reference 7.31.

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-o-o-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 Tricon Planning and Installation Guide, Reference 7.31.

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 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.

3.1.8 Communication Module

Like the I/O modules, the Tricon Communication Module (TCM) has three separate communication buses 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 CRC checks, handshaking, and other protocol-based features. These features are supported in hardware and firmware. Firmware provides core functionality common to all the TCMs with additional coding to support the specific communication protocol.

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

3.2 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 EPRI TR-107330, Section 4.4. Compliance of the Tricon software with these requirements is summarized in the Compliance Traceability Matrix, Appendix A. A brief description is provided below.

3.2.1 TRICON OPERATING SYSTEM

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

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

Upon power up (when the MP is inserted in the MP slot of the main chassis), the EMP goes through the power up initialization and diagnostics. Power up sequence includes a series of Power up diagnostics – Microprocessor tests, RAM tests, Flash memory tests, Watchdog test, Clock Calendar test, etc. Power up sequence is also initiated by hardware and software reset of the EMP. Upon successful completion of Power up sequence, the EMP enters the Scan task. Figure 8 shows the ETSX tasks and priorities.

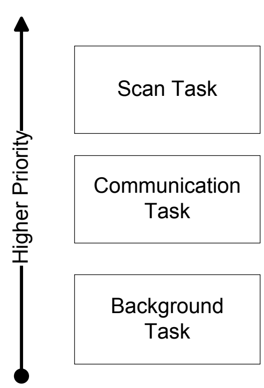


Figure 8 - ETSX tasks and priorities

The Scan task performs the following steps:

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

The **Communication task** runs every 10 milliseconds or when a communication port interrupt occurs. The communication task does the following:

1. Process Messages from IOC/COM.
2. Process Messages from COMMUNICATION MODULES.
3. Fill Tribus communication buffers.
4. Check Event Buffers.
5. Send Diagnostic Messages across secondary channel.
6. Perform Transport task.
7. Do any loader background work (TriStation messages for download)
8. Handle any Tribus Messages from other MPs.

The **Background task** is responsible to run diagnostics, handle debug port commands, and write information to flash memory.

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. The application program shall be designed to provide appropriate error recovery and annunciation of such faults. Use of several of the diagnostic data inputs are mandated in the Application Guide, Appendix B.

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

3.2.2 TRISTATION 1131 PROGRAMMING SOFTWARE

Application programming is generated using the TriStation 1131 Developer's Workbench, which runs in a Windows XP 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**, Reference 7.3**. 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, Ladder 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 TCM module. Programs and translated code are protected by 32-bit 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.

3.2.3 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 management, 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 Application Guide, 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 un-restricted 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.

3.3 Qualified Tricon Modules

The specific Tricon modules being 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 7.34

Table 3-1: Qualified Tricon Modules

Module Type	Model Number	Description
Main Processor	3008	Enhanced Main Processor III, V10, 16 Mb
High Density (HD) Main Chassis	8110	Main Chassis # 1
HD Expansion Chassis	8111	I/O expansion chassis
HD Remote Expansion Chassis	8112	Remote I/O expansion chassis

Module Type	Model Number	Description
Power Supply	8310	120 VAC/VDC Power Supply
	8311	24 VDC Power Supply
	8312	230 VAC Power Supply
Remote Extender	4200	Remote Extender Module (Primary)
	4201	Remote Extender Module (Remote)
Communication	4352A	Tricon Communication Module, Fiber
Analog Input	3701	AI Module, 0-10 VDC
	3703E	EAI Module, Isolated, 0-5/0-10 VDC
	3721	NGAI, -5-5 VDC
Analog Output	3805E	Analog Output Module, 4-20 mA
Digital Input	3501T	EDI Module, 115V AC/DC
	3502E	EDI Module, 48V AC/DC
	3503E	EDI Module, 24V AC/DC
Digital Output	3601T	EDO Module, 115 VAC
	3603T	EDO Module, 120 VDC
	3607E	EDO Module, 48 VDC
	3623T	SDO Module, 120 VDC
	3625	NGDO Module, 24 VDC
Pulse Input	3511	Pulse Input Module
Thermocouple Input	3708E	ITC Thermocouple Input Module
Relay Output	3636T	ERO Module, N.O., Simplex
Blank I/O slot Panel	8105	Blank I/O slot Panel
Seismic balance Module	8107	Seismic balance Module

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 7.6. 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 and requirements for qualification tests are specified in Section 6 of the EPRI TR-107330 respectively. Compliance of the Tricon hardware and the Tricon v10 qualification program with the detailed EPRI test requirements is summarized in the Compliance Traceability Matrix, Appendix A.

Tricon hardware qualification was demonstrated primarily by conducting a series of qualification tests in accordance with EPRI TR-107330 in order to comply with the applicable regulatory requirements and industry standards. The required tests and their sequence were defined in the Master Test Plan, Reference 7.33. A test sequence was chosen in which irradiation exposure was prior to environmental exposure. Sequencing of testing implies the existence of a significant aging mechanism. Per IEEE 627-1980, significant aging mechanisms must satisfy a number of criteria including. "In the normal service environment, the aging mechanism causes degradation during the design life of the equipment that is appreciable compared to degradation caused by the design basis events." Radiation exposure to the TR-107330 levels does not meet this criterion. Results of the qualification testing on the TRICON test specimen demonstrate this.

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

Pre-Qualification testing included the following:

- System setup and checkout test, described in Reference 7.40, 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 7.41, 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, 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 7.42, to establish baseline performance and to demonstrate the ability of the Tricon to operate within specifications under dynamic

conditions. The prudency test included a burst of events test, a serial port receiver failure test, and a serial port noise test.

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

Qualification testing included the following:

- Radiation Exposure testing, Reference 7.43, to demonstrate the ability of the Tricon v10 PLC to operate properly after being exposed to radiation. The operability tests and prudency tests were performed immediately after to demonstrate proper operation of the system.
- Environmental testing, Reference 7.44, to demonstrate the ability of the Tricon v10 PLC to operate properly under the extremes of temperature and humidity. The operability test was performed at the high and low temperature and humidity conditions and also immediately after the environmental test (at ambient conditions) to demonstrate proper system operation. The prudency test was also performed at the high temperature conditions.
- Seismic testing, Reference 7.45, to demonstrate the ability of the Tricon v10 PLC 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 tests were performed immediately after the seismic test to demonstrate continued proper operation of the system.
- Electromagnetic interference (EMI) and radio frequency interference (RFI) testing, Reference 7.46, to demonstrate the suitability of the Tricon v10 PLC for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility
- Electrical Fast Transient (EFT) testing, Reference 7.47, to demonstrate the suitability of the Tricon v10 PLC for qualification as a safety-related device with respect to susceptibility to repetitive electrical fast transients on the power and signal input/output leads.
- Surge Withstand testing, Reference 7.48, to demonstrate the suitability of the Tricon for qualification as a safety-related device with respect to AC power and signal line electrical surge withstand capability.
- Electrostatic Discharge (ESD) testing, Reference 7.49, to demonstrate the suitability of the Tricon v10 PLC for qualification as a safety-related device with respect to immunity to electrostatic discharge exposure
- Class 1E-to-non 1E electrical isolation testing, Reference 7.50, to demonstrate the suitability of the Tricon v10 PLC for qualification as a safety-related, Class 1E device with respect to providing electrical isolation at Non-1E field connections..

After the qualification tests, the following performance proof 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. A failure mode and effects analysis, Reference 7.64, and a reliability and availability analysis, Reference 7.63, were performed.

4.1 Test System Configuration

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

Triconex Drawing 9600164-100 (Reference 7.39) shows the general arrangement and interconnection of the test system chassis. The Tricon System Description, Reference 7.36, provides an overview and description of the TUT and test system. A detailed identification of the tested equipment is provided in the project Master Configuration List, Reference 7.34.

During testing, the TUT was executing an application program (TSAP) developed specifically for the qualification project and designed to exercise the TUT in a manner that supported data collection requirements during testing. The TSAP is described in Reference 7.68. The Master Configuration List identifies the revision level of all test system software and firmware.

a, b

Two PCs running the TriStation software were used to communicate with and monitor the status of the TUT and the Simulator Tricons. The TriStation software used for this purpose was the TS1131, which is Windows-based application software.

During each of the qualification tests, operation of the TUT was monitored and recorded by the DAS. The recorded data was evaluated in detail before, during, and after the test period. The data evaluation considered operation (per the TSAP) of at least one input or output point on each I/O module installed in the TUT, and operation of all peripheral communication interfaces including the Simulator Tricons Peer-to-Peer and MODBUS interfaces. The data was monitored for deviations or trends from normal performance.

4.2 Radiation Qualification

Radiation qualification testing of the TUT was performed as described in the Radiation Test Procedure, Reference 7.43. This testing was performed in accordance with the requirements of EPRI TR-107330, Reference 7.6 and IEEE Standard 381-1977, Reference 7.21. The objective of radiation testing was to demonstrate that the Tricon does not experience failures upon exposure to Co60 gamma radiation. Requirements for radiation withstand capability are specified in EPRI TR-107330, Section 4.3.6, which requires that the PLC be able to withstand a radiation exposure of up to 1000 rads.

Compliance of the Tricon radiation qualification testing with these requirements is described in the Radiation Test Procedure, Reference 7.43.

The radiation test acceptance criteria are as given below based on Appendix 4 of the Master Test Plan, Reference 7.33, and EPRI TR-107330, Section 4.3.6, Reference 7.6:

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

Radiation exposure testing of the TUT was performed on December 13th and 14th, 2006 at the University of Massachusetts, - Lowell, Massachusetts. The testing complied with the specific requirements of EPRI TR-107330, Sections 4.3.6 as described above, and the general requirements of IEEE 381-1977, Reference 7.21. Results of the testing are described in the Radiation Test Report, Reference 7.53. Review of the post-radiation operability and prudency test results shows that exposure to the radiation test conditions had no adverse effect on the TUT.

Conclusions from this test are as follows:

1. Radiation Exposure Testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977. All of the tested TUT

components were exposed to Co60 gamma radiation doses of 1000 rads, plus margin. a, b

2. The TUT met all applicable acceptance requirements of the post-radiation exposure visual inspections performed as part of Radiation Exposure Testing.
3. Results of the post-radiation operability and prudency Tests demonstrate that the applied Radiation Exposure Test conditions had no adverse effect on the TUT performance.
4. The Radiation Exposure Test results demonstrate that the Tricon v10 PLC will not experience failures due to normal and abnormal service conditions of gamma radiation exposure. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.

4.3 Environmental Qualification

Environmental qualification testing of the TUT was performed as described in the Environmental Test Procedure, Reference 7.44. This testing was performed in accordance with the requirements of IEEE 381-1977, Reference 7.21. The objective of environmental testing was to demonstrate that the Tricon does 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 test PLC 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-107330).
- Environmental testing shall be performed with the power supply sources set to values that maximize heat dissipation in the test PLC.
- Power supplies shall be loaded such that nominal current draws at nominal power supply output voltages are equal to the power supply rating.
- The test PLC shall be powered with its TSAP operating during environmental testing, with 1/2 of the discrete and relay outputs ON and loaded to their rated current. In addition, all analog outputs shall be set to between 1/2 and 2/3 of full scale.

Section 4.3.6.2 of EPRI TR-107330 (Reference 9.3) requires that the generic PLC meet its performance requirements over abnormal environmental conditions of 40°F to 120°F and 10% to 95% relative humidity (non-condensing). Section 4.3.6.3 of EPRI TR-107330 (Reference 9.3) requires that the test PLC operate for the environmental (temperature and humidity) withstand profile given in Figure 4-4 of the TR. The profile includes a beginning ramp-up period (unspecified in duration) from ambient to 140°F and 90% relative humidity (non-condensing). These conditions are held for 48 hours minimum, after which the Operability and Prudency tests are run. Conditions are then ramped down over a four hour minimum period to 40°F and 5% relative humidity. These conditions are held for 8 hours minimum, after which a second Operability test is run. Conditions are then ramped up over a four hour minimum period to ambient temperature and relative humidity. The equipment is stabilized at ambient conditions, after which a final Operability test is run. Section 6.3.3 of EPRI TR-107330 (Reference 9.3) requires that Environmental Testing be performed with margins of 5°F and 5% applied to the temperature and humidity values given above.

a, b

Figure 6-1 of this report shows the actual Environmental Test profile which was achieved in the NTS Laboratories environmental test chamber. This profile bounds the test profile given in Figure 4-4 of EPRI TR-107330 (Reference 7.**6**).

Compliance of the Tricon environmental qualification testing with these requirements is described in the Environmental Test Procedure, Reference 7.44.

In addition to the modules which were installed and operating in the TUT 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 5 of the Master Test Plan, Reference 7.33, and EPRI TR-107330, Section 4.3.6, Reference 7.6:

- The TUT shall operate as intended during and after exposure to the environmental test conditions. Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) collected during testing shall demonstrate operation as intended.

- The TUT shall pass the Operability Test following at least 48 hours of operation at high temperature and humidity, following at least 8 hours of operation at low temperature and humidity and upon completion of the test.
- The TUT shall pass the Prudency Test following at least 48 hours of operation at high temperature and humidity.

Environmental testing of the TUT was performed on December 13th, 2006 through January 15th, 2007 at National Technical Systems in Boxborough, Massachusetts. The testing complied with the specific requirements of EPRI TR-107330, Sections 4.3.6 and 6.3.3, as described above, and the general requirements of IEEE 381-1977, Reference 7.21. Results of the testing are described in the Environmental Test Report, Reference 7.54.

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

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

a, b

a, b

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

Conclusions from this test are as follows:

5. Environmental testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977.
6. The TUT met all applicable performance requirements during and after application of the environmental test conditions.

7. One digital output module fault occurred during Environmental Testing. The fault indication was cleared through the Enhanced Diagnostic Monitor (EnDM) and did not return for the remainder of the Environmental Test. Because of the fault tolerant design of the Tricon v10 PLC, the monitored digital output point of the module (Model 3623T) continued to perform as expected during the fault condition.
8. Results of the operability and prudency tests performed during and after Environmental Testing show that exposure to the Environmental Test conditions had no adverse effect on the TUT performance
9. The environmental test results demonstrate that the Tricon v10 PLC will not experience failures due to abnormal service conditions of temperature and humidity. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.

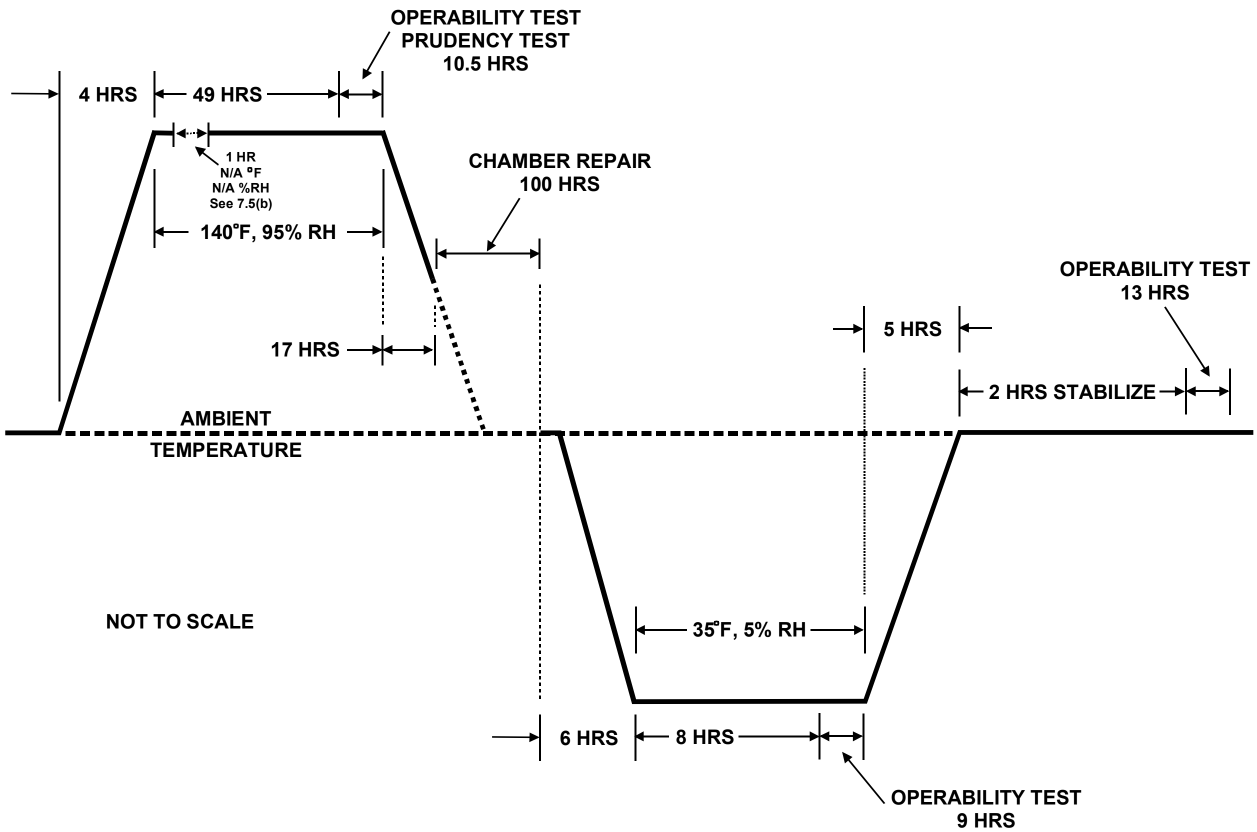


Figure 6-1: Environmental Test Applied Temperature and Humidity Profile

4.4 Seismic Qualification

Seismic qualification testing of the TUT was performed as described in the Seismic Test Procedure, Reference 7.45. The objective of seismic testing was to demonstrate the suitability of the Tricon for qualification as a Category 1 seismic device.

EPRI TR-107330, Sections 4.3.9 and 6.3.4, requires that the test PLC be seismically tested in accordance with IEEE 344-1987, Reference 7.20. The testing shall 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 tri-axially (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 7.45.

a, b

a, b

Also, in full accordance with the requirements of Section 6.3.4.2 of EPRI TR 107330 (Reference 9.3), during each OBE and SSE test run, 1/4 of the relay outputs were shown to transition from OFF to ON at least once, and 1/4 were shown to transition from ON to OFF at least once. The field circuits for the relay output points described above were configured with resistive loads which resulted in the approximate rated current through the output points at the nominal rated output point voltage. This loading configuration met the requirements of Section 6.3.4.2 of EPRI TR 107330 (Reference 9.3).

a, b

The seismic test acceptance criteria are as given below based on Appendix 6 of the Master Test Plan, Reference 7.33 and EPRI TR-107330, Section 4.3.9, Reference 7.6:

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

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

- Resonance search testing was performed as described in IEEE-344-1987, Section 7.1.4. The tests were performed to provide information on the dynamic response of the equipment mounted on the seismic test table.

- Each TUT chassis was exposed to five OBE tests and one SSE test were performed using the same test response spectrum (TRS) which is shown in Figure 1 and Figure 2 respectively.

Figure 1: OBE Test Acceleration

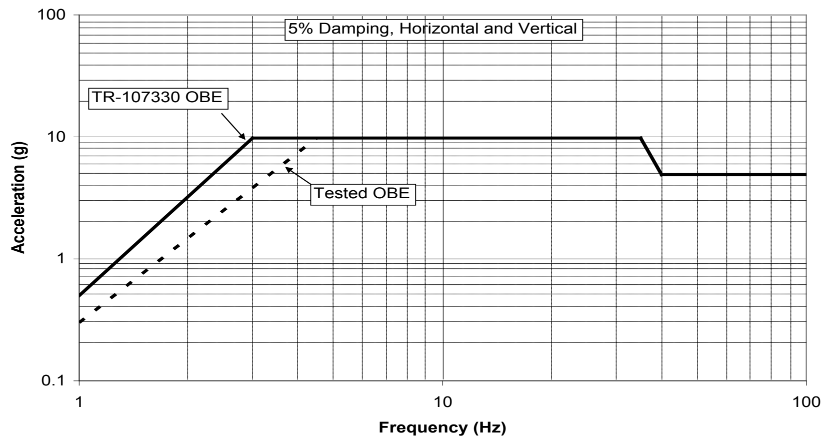
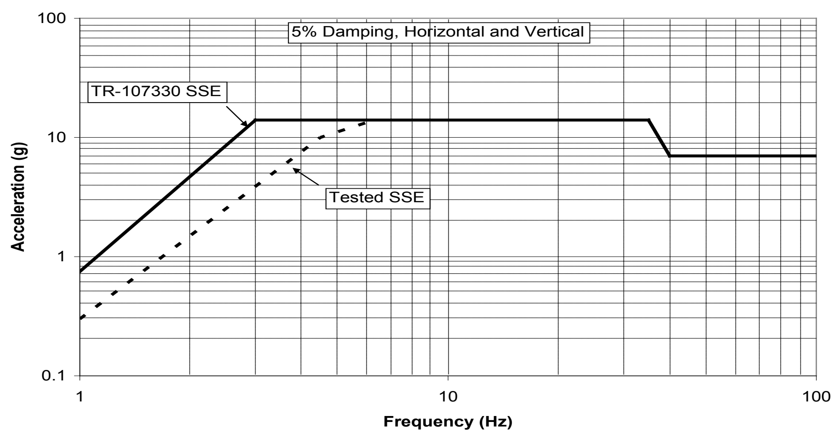


Figure 2: SSE Test Acceleration



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

Results of the testing are described in the Seismic Test Report, Reference 7.55. Data collected during and after each OBE and SSE test demonstrate that the TUT operated as intended throughout the testing. The TUT was visually inspected for damage or degradation following each OBE and SSE test. Results of these inspections showed no physical damage or degradation of the test specimen.

Conclusions from this test are as follows:

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

2. The TUT met all applicable performance requirements during and after application of the seismic test vibration levels.
3. Results of the Operability Test performed after Seismic Testing show that exposure to the Seismic Test conditions had no adverse effect on the TUT performance.
4. The seismic test results demonstrate that the Tricon v10 PLC platform is suitable for qualification as Category 1 seismic equipment. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.
5. The horizontal and vertical seismic withstand response spectrum of the Tricon PLC determined by testing is shown in Figures 1 and 2. The figure is based on a damping value of 5% used in the data analysis.
6. The seismic test results demonstrate that the equipment mounting configurations shown in System Drawings are adequate to support seismic qualification of the Tricon v10 PLC.
7. The TUT chassis alarm relay contacts were not monitored for contact chatter during Seismic Testing. Therefore, the TUT chassis alarm relays were not seismically qualified as part of Seismic Testing.

4.5 Electromagnetic and Radio Frequency Interference Qualification

Electromagnetic interference (EMI) and radio frequency interference (RFI) testing was performed to demonstrate the suitability of the Tricon v10 PLC for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility.

All of the TUT components were subjected to EMI/RFI testing as required. EMI/RFI testing of the TUT was performed inside a shielded enclosure. The testing was performed in accordance with the EMI/RFI Test Procedure, Reference 7.46, and in accordance with the EPRI TR-107330, Reference 7.6 and NRC RG 1.180, Reference7.4 test method requirements. The specific tests conducted include the following MIL-STD-461E and IEC test methods:

The following EMI/RFI emissions tests were performed:

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

The following EMI/RFI susceptibility tests were performed:

- IEC 61000-4-3, Radiated Susceptibility, 26 MHz to 1 GHz
- IEC 61000-4-6, Conducted Susceptibility, 150 kHz to 80 MHz
- IEC 61000-4-8, Radiated Susceptibility, Power Line Frequency Magnetic Field
- IEC 61000-4-9, Radiated Susceptibility, Pulsed Magnetic Field
- IEC 61000-4-10, Radiated Susceptibility, Damped Oscillatory Magnetic Field

- IEC 61000-4-13, Conducted Susceptibility, Harmonics and Interharmonics
- IEC 61000-4-16, Conducted Susceptibility, Common-Mode Disturbances

Where necessary, testing was also performed at levels lower than the EPRI TR-107330 specified levels to establish the envelope of acceptable performance. Compliance of the Tricon EMI/RFI qualification testing with these requirements is described in the EMI/RFI Test Procedure, Reference 7.46.

The EPRI TR-107330 requires that a portion of the Operability and Prudency tests be performed during the EMI/RFI testing. However, the TUT as configured for EMI/RFI testing did not support Operability or Prudency testing. Instead, the Operability and Prudency tests were run at the completion of all qualification testing to demonstrate acceptable system performance following EMI/RFI, EFT, ESD, 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 7.33, and EPRI TR-107330, Section 4.3.7, Reference 7.6:

- The TUT shall meet allowable equipment emission limits as specified in NRC RG 1.180, Rev 1 for conducted and radiated emissions.
- The TUT shall operate as intended during and after application of the EMI/RFI test levels specified in NRC RG 1.180 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 TUT was performed from February 17th through April 16th, 2007 at National Technical Systems in Boxboro, Massachusetts. The TUT was installed in the EMI/RFI chamber in open-frame racks as required by the EPRI TR-107330. Wiring connections and grounding were in accordance with the manufacturer's recommendations. Additional EMI/RFI protective and mitigating devices such as power or I/O line filters, enclosed cabinets, and extra cable shielding were not used so that the specific emissions and susceptibilities of the equipment could be determined.

During EMI/RFI testing, the TUT was powered with TSAP operating. The AC and DC power sources to the TUT chassis power supplies were set at nominal source voltage and frequency conditions. In order to minimize transmission of outside EMI/RFI sources into the EMI/RFI test chamber, all power, signal, and communications cables entering the EMI/RFI test chamber were passed through filters located in the chamber walls.

a, b

The specific configuration of the TUT is described in the EMI/RFI Test Procedure, Reference 7.46.

During EMI/RFI testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during and after each test to verify normal operation of the system and all peripheral communication interfaces. The status of the TUT diagnostic indicating LED's was also recorded to demonstrate continued correct operation. Results of the EMI/RFI testing are described in the EMI/RFI Test Report, Reference 7.56. In addition, the conclusions from additional tests to determine the impact of the Tricon v10 PLC input and output module EMI/RFI susceptibilities are detailed in the EMI/RFI Test Report.

Conclusions of this test are as follows:

1. EMI/RFI tests were performed in accordance with the requirements and methodologies of NRC RG 1.180, Rev. 1. The following EMI/RFI tests were performed:
   - Radiated Magnetic Field Emissions from 30 Hz to 100 kHz (MIL-STD-461E, RE101)
   - Radiated Electric Field Emissions from 2 MHz to 1 GHz (MIL-STD-461E, RE102)
   - Low Frequency Cond. Emissions from 30 Hz to 10 kHz (MIL-STD-461E, CE101)
   - High Frequency Cond. Emissions from 10 kHz to 2 MHz (MIL-STD-461E, CE102)
   - High Frequency Radiated Susceptibility from 26 MHz to 1 GHz (IEC 61000-4-3)
   - Radio Frequency Conducted Susceptibility from150 kHz to 80 MHz (IEC 61000-4-6)
   - Magnetic Field Radiated Susceptibility at 60 Hz (IEC 61000-4-8)
   - Pulsed Magnetic Field Radiated Susceptibility (IEC 61000-4-9)
   - Damped Magnetic Field Radiated Suscept., at 100 kHz and 1 MHz (IEC 61000-4-10)
   - Harmonics and Interharmonics Conducted Susceptibility (IEC 61000-4-13)
   - Common Mode Disturb. Conducted Suscept., 15 Hz to 150 kHz (IEC 61000-4-16)
2. The TUT successfully passed all of the EMI/RFI susceptibility tests. The main processors continued to function correctly throughout testing. The transfer of input and output data was not interrupted. There were no interruptions or inconsistencies in the operation of the system or the software.
3. The TUT fully complies with the allowable equipment emissions levels defined in NRC RG 1.180, Rev. 1 for MIL-STD-461E, RE101 and RE102 testing.
4. The TUT does not fully comply with the allowable equipment emissions levels defined in NRC RG 1.180, Rev. 1 for MIL-STD-461E, CE101 and CE102 testing.

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

- 20 VAC Chassis Power Supply Line Lead. Conducted emission exceeded at:
  179.7 Hz by 11.2 dBµA   538.8 Hz by 8.9 dBµA

299.8 Hz by 13.8 dBμA 659.7 Hz by 2.1 dBμA
419.7 Hz by 13.0 dBμA 899.6 Hz by 1.5 dBμA

- 120 VAC Chassis Power Supply Neutral Lead. Conducted emission exceeded at:
  179.9 Hz by 11.0 dBμA 539.7 Hz by 9.6 dBμA
  299.8 Hz by 14.9 dBμA 659.9 Hz by 2.8 dBμA
  419.3 Hz by 13.1 dBμA
- 230 VAC Chassis Power Supply Line Lead. Conducted emission exceeded at:
  179.9 Hz by 4.0 dBμA 539.7 Hz by 7.6 dBμA
  299.8 Hz by 8.3 dBμA 659.7 Hz by 6.0 dBμA
  419.7 Hz by 8.7 dBμA 779.6 Hz by 1.7 dBμA
- 230 VAC Chassis Power Supply Neutral Lead. Conducted emission exceeded at:
  179.9 Hz by 3.8 dBμA 539.7 Hz by 7.5 dBμA
  299.8 Hz by 8.2 dBμA 659.7 Hz by 5.9 dBμA
  419.7 Hz by 8.6 dBμA 779.6 Hz by 1.6 dBμA

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

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

5. The TUT main processor, chassis power supply, remote extender, and communication modules fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for all of the EMI/RFI susceptibility tests.
6. The TUT discrete and analog input/output hardware, which does not fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for the EMI/RFI susceptibility tests as listed below:

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

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

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

   - RTD Signal Conditioning Module 1600081-001
   - Digital Output Module 3601T (115 VAC) with ETA 9663-610N
7. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.

4.6 Electrical Fast Transient

Electrical fast transient (EFT) testing of the TUT was performed as described in the EFT Test Procedure, Reference 7.47, to demonstrate the suitability of the Tricon v10 PLC for qualification as a safety-related device with respect to susceptibility to repetitive electrical fast transients on the power and signal input/output leads.

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

As described in the EFT Test Procedure, Reference 7.47, the TUT was subjected to the following EFT tests:

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

The EFT test acceptance criteria are as follows, based on Appendix 8 of the Master Test Plan, Reference 7.33, and EPRI TR-107330, Section 4.3.7, Reference **7.6**:

- Applying the EFT Test voltages to the specified TUT interfaces will not damage any other module or device in the TUT, or cause disruption of the operation of the backplane signals or any other data acquisition signals.
- The TUT shall operate as intended during and after application of the IEC 61000-4-4 EFT test levels specified in Sections 4.2 and 5.3 of NRC RG 1.180, Rev. 1 for low exposure applications. Specifically:

  IEC 61000-4-4: Power Leads, Level 3 Test Voltage Level: 2 kV max.
  IEC 61000-4-4: Signal Leads, Level 3 Test Voltage Level: 1 kV max.
- Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance from Section 4.3.7 of EPRI TR-107330:
  - The main processors shall continue to function.
  - The transfer of I/O data shall not be interrupted.
  - The applied EFT disturbances shall not cause the discrete I/O to change state.
  - Analog I/O levels shall not vary more than 3% (of full scale).

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

During EFT testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during and after each test to verify normal operation of the system and all peripheral communication interfaces. Results of the EFT testing are described in the EFT Test Report, Reference 7.57. Data collected during and after each voltage test demonstrate that the TUT operated as intended throughout the testing.

Conclusions from this test are as follows:

1. EFT Testing of the TUT was performed in accordance with the applicable requirements of NRC Regulatory Guide 1.180, Rev. 1 and IEC 41000-4-4. The following EFT tests were performed:
   - 120 VAC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
   - 230 VAC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
   - 24 VDC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
   - Peripheral Communications Cables: ± 0.5 kV and ± 1.0 kV
   - ETA Input Power Wires: ± 0.5 kV and ± 1.0 kV
   - Analog Input/Output Wires: ± 0.5 kV and ± 1.0 kV
   - RTD, /T/C and Pulse Input Wires: ± 0.5 kV and ± 1.0 kV
   - Discrete Input/Output Wires: ± 0.5 kV and ± 1.0 kV
2. The TUT met all applicable operational and performance requirements during and after each application of the EFT Tests voltages.
3. The EFT Test results demonstrate that the Tricon v10 PLC will not experience operational failures or susceptibilities due to exposure to repetitive electrical fast transients on the power and signal input/output leads. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.

4.7 Surge Withstand

Surge withstand testing was performed as described in the Surge Withstand Test Procedure, Reference 7.48, to demonstrate the suitability of the Tricon for qualification as a safety-related device with respect to AC power and signal line electrical surge withstand capability.

EPRI TR-107330, Section 4.6.2, requires that surge withstand testing of the PLC be conducted in accordance the requirements of EPRI TR-102323, Reference 7.7. NRC RG

1.180, Rev. 1, Reference 7.4 provides an NRC approved alternative to the Surge Withstand Testing specified in EPRI TR-102323. Surge Withstand Testing of the TUT AC power supplies was performed in accordance with IEC 61000-4-5 and IEC 61000-4-12 requirements.

As described in the Surge Withstand Test Procedure, Reference 7.48, the TUT chassis power supplies and signal lines were subjected to the following surge tests:

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

- 120 VAC and 230 VAC Chassis Power Supplies
- 24 VDC Chassis Power Supplies,

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

- 120 VAC and 230 VAC Chassis Power Supplies,
- 24 VDC Chassis Power Supplies,

<u>IEC 61000-4-12 Ring Wave</u>: ± 1.0 kV (common mode), ± 0.5 kV (differential)

- AC and DC Rated Discrete Input Modules
- AC and DC Rated Discrete Output Modules
- Analog Input and Output Modules (RTD, T/C, Pulse, mV and mA)
- TCM Modules, MODBUS Serial Ports

<u>IEC 61000-4-5 Combination Wave:</u> ± 1.0 kV (common mode), ± 0.5 kV (differential)

- AC and DC Rated Discrete Input Modules
- AC and DC Rated Discrete Output Modules
- Analog Input and Output Modules (RTD, T/C, Pulse, mV and mA)
- TCM Modules, MODBUS Serial Ports

The surge withstand test acceptance criteria are as follows, based on Appendix 8 of the Master Test Plan, Reference 7.33, and EPRI TR-107330, Section 4.6.2, Reference **7.6**:

- Applying the surge test voltages specified in Tables 15 and 22 of NRC RG 1.180, Rev. 1 to the specified TUT test points shall not damage any other module or device in the TUT, or cause disruption of the operation of the TUT backplane signals or any other data acquisition signals that could result in a loss of the ability to generate a trip.
- Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate satisfactory operation of the TUT during and after application of the surge test voltage. The data evaluations shall demonstrate that modules other than the one tested are not damaged and do not experience disruption of their operation.
- Per Section 6.3.5 of TR-107330, failures of one or more redundant devices are acceptable so long as the failures do not result in the inability of the TUT to operate as intended. No faults or failures of redundant devices occurred during Surge Withstand Testing.

The surge withstand testing was performed from March 28th through April 13th, 2007 at National Technical Systems in Boxborough, Massachusetts.

a, b

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

a, b

Results of the surge withstand testing are described in the Surge Withstand Test Report, Reference 7.58. Data collected during and after each voltage tests demonstrate that the TUT operated as intended throughout the testing.

Conclusions from this test are as follows:

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

   IEC 61000-4-5 Combination Wave: ± 2.0 kV

   - 120 VAC and 230 VAC Chassis Power Supplies,
     - Line to Neutral
     - Line to AC Ground
     - Neutral to AC Ground
     - Line and Neutral to AC Ground
   - 24 VDC Chassis Power Supplies,
     - High Side (+) to Low Side (-)
     - Low Side (-) to AC Ground

   IEC 61000-4-12 Ring Wave: ± 2.0 kV

   - 120 VAC and 230 VAC Chassis Power Supplies,
     - Line to AC Ground
     - Neutral to AC Ground

- Line and Neutral to AC Ground

- 24 VDC Chassis Power Supplies,
  - Low Side (-) to AC Ground

IEC 61000-4-12 Ring Wave: ± 1.0 kV

- 120 VAC and 230 VAC Chassis Power Supplies,
  - Line to Neutral
- 24 VDC Chassis Power Supplies,
  - High Side (+) to Low Side (-)

IEC 61000-4-12 Ring Wave, IEC 61000-4-5 Combination Wave: ± 0.5 kV

- AC Rated Discrete Input Modules
  - One Point per Module
  - Line to Neutral
  - Point ON and OFF
- AC Rated Discrete Output Modules
  - One Point per Module
  - Line to Neutral
  - Point ON and OFF

IEC 61000-4-12 Ring Wave, IEC 61000-4-5 Combination Wave: ± 1.0 kV

- AC Rated Discrete Input and Output Modules
  - One Point per Module
  - Neutral to AC Ground
  - Point ON and OFF
- DC Rated Discrete Input and Output Modules
  - One Point per Module
  - Low Side (-) to AC Ground
  - Point ON and OFF
- Analog Input and Output Modules (RTD, T/C, Pulse, mV and mA)
  - One Point per Module
  - Shield to AC Ground
- TRICON Communication Modules (TCMs), MODBUS Serial Ports
  - One Port
  - Connector Shield to AC Ground

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

3. The Surge Withstand Test results demonstrate that the Tricon v10 PLC will not experience operational failures or susceptibilities that could result in a loss of the ability to generate a trip due to exposure to Ring Wave and Combination Wave electrical surges to the components listed above. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.

4.8 Electrostatic Discharge

Electrostatic Discharge (ESD) testing was performed as described in the ESD Test Procedure, Reference 7.49 to demonstrate the suitability of the Tricon v10 PLC for qualification as a safety-related device with respect to immunity to electrostatic discharge exposure.

EPRI TR-107330, Section 4.3.8, requires that the PLC under qualification be tested for immunity to the ESD test levels specified in EPRI TR-102323-R1, Reference 7.7. ESD Testing of the TUT was performed in accordance with IEC 61000-4-2**, Reference 7.8**, using the test levels defined in EPRI TR-102323-R1, Appendix B, Section 3.5.

As described in the Electrostatic Discharge Test Procedure, Reference 7.49, the TUT was subjected to the following EFT tests:

<u>ESD Direct Contact Discharges</u>: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV

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

<u>ESD Direct Air Discharges</u>: ± 2 kV, ± 4 kV, ± 8 kV and ± 15 kV

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

<u>ESD Indirect Contact Discharges</u>: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV

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

The ESD test acceptance criteria are as follows, based on Appendix 8 of the Master Test Plan, Reference 7.33, and EPRI TR-107330, Section 4.3.7 and 4.3.8, Reference **7.6**:

- Applying the ESD Test voltages to the specified TUT interfaces will not damage any other module or device in the TUT, or cause disruption of the operation of the backplane signals or any other data acquisition signals.
- The TUT shall operate as intended during and after application of the IEC 61000-4-2 Level 4 ESD test levels specified in Appendix B, Section 3.5 of EPRI TR-102323-R1 and Section 5 of IEC 61000-4-2. Specifically:

  IEC 61000-4-2: Air Discharges Test Voltage Level: ± 15 kV max.

  IEC 61000-4-2: Contact Discharges Test Voltage Level: ± 8 kV max.
- Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate operation as intended, including the following specific operational performance from Section 4.3.7 of EPRI TR-107330:
  - The main processors shall continue to function.
  - The transfer of I/O data shall not be interrupted.
  - The applied EFT disturbances shall not cause the discrete I/O to change state.
  - Analog I/O levels shall not vary more than 3% (of full scale).
- Per Section 4.3.8 of EPRI TR-107330, failures of one or more redundant devices due to application of ESD test voltages are acceptable so long as the failures do not result in the inability of the TUT to operate as intended.

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

a, b

Results of the ESD testing are described in the ESD Test Report, Reference 7.59. Data collected during and after each voltage tests demonstrate that the TUT operated as intended throughout the testing.

Conclusions from this test are as follows:

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

   <u>ESD Direct Contact Discharges</u>: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV
   - Chassis 1 Battery Cover (4 points)
   - Chassis 1 Control Keyswitch (1 point)
   - All ETA Cable Chassis Connectors, Top Thumbscrews (25 points)
   - All Chassis, Front Horizontal and Vertical Edges (32 points)

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

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

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

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

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

5. The TUT met all applicable operational and performance requirements during and after each application of the ESD Tests voltages.
6. The ESD Test results demonstrate that the Tricon v10 PLC will not experience operational failures or susceptibilities due to exposure to electrostatic discharges to the components listed above. The main processors continued to function. The transfer of I/O was not interrupted. The TCM Peer-to-Peer and MODBUS communication links continued to operate correctly. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.

4.9 Class 1E to Non-1E Isolation

Class 1E to Non-1E isolation testing was performed as described in the Class 1E to Non-1E Isolation Test Procedure, Reference 7.50 to demonstrate the suitability of the Tricon v10 PLC for qualification as a safety-related, Class 1E device with respect to providing electrical isolation at Non-1E field connections.

The qualification of the Tricon v10 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 TCM Module, RS-232 (MODBUS) was tested for Class 1E isolation capability.

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

EPRI TR-107330, Section 4.6.4, requires that surge withstand testing of the PLC be conducted in accordance the requirements of IEEE 384-1981, Reference 7.22. 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 7.42, addresses the item (a) isolation requirements for the Tricon communication modules. During prudency testing, the TUT response time was monitored and shown not to degrade. These results are documented in the Performance Proof Prudency Test Report, Reference 7.62. The Class 1E to Non-1E Isolation Test Procedure, Reference 7.60, 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.

As described in the Class 1E to Non-1E Isolation Test Procedure, Reference 7.50, the following TUT components were subjected to the isolation tests:

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

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

<u>Tricon Communication Module (TCM) Model 4352A, MODBUS Serial Port</u>

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

Isolation test acceptance criteria are as follows based on Appendix 8 of the Master Test Plan, Reference 7.33, and EPRI TR-107330, Section 4.6.4, Reference **7.6**:

- Applying the isolation test voltages for the required time to the specified TUT test points shall not disrupt the operation of any other module in the TUT, or cause disruption of the TUT backplane signals or any other data acquisition signals.
- Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate satisfactory operation of the TUT during and after application of the isolation test voltage. The data evaluations shall demonstrate that modules other than the one tested are not damaged and do not experience disruption of their operation.

- Per Section 6.3.6 of EPRI TR-107330, failures of one or more redundant devices are acceptable so long as the failures do not result in the inability of the TUT to operate as intended.

The isolation testing was performed from April 5th through 16th, 2007 at National Technical Systems in Boxboro, Massachusetts. During testing, the TUT was powered with the TSAP operating. The AC and DC power sources to the TUT chassis power supplies were set at nominal source voltage and frequency conditions. The arrangement and grounding of the system during isolation testing was the same as for the EMI/RFI tests.

During isolating testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during and after each isolation test to verify normal operation of the system and all peripheral communication interfaces. The test details are described in the Isolation Test Report, Reference 7.60.

Conclusions from this test are as follows:

1. Class 1E to Non-1E isolation testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 384-1981.
2. The TUT met all applicable performance requirements during and after application of the Class 1E to Non-1E isolation test voltages. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.
3. The isolation test results (together with the Prudency Test communication port fault tests) demonstrate that the Tricon Model 4352A TCM Module MODBUS serial communication ports provide adequate electrical isolation per IEEE 384-1981 between the safety related portions of the TRICON v10 and connected non-safety related communication circuits. In addition, the testing demonstrated electrical isolation capability of the TCM MODBUS serial communication ports to applied voltages of 250 VAC and 250 VDC (at 10 amps maximum) for 30 seconds.
4. The Class 1E to Non-1E Isolation Test results demonstrates that the Tricon v10 PLC relay output module Model 3636T provides adequate electrical isolation per IEEE 384-1981 between the safety related portions of the Tricon v10 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 25 amps maximum) and 250 VDC (at 10 amps maximum).
5. The Tricon v10 Model 4201 Remote RXM fiber optic module is considered an acceptable Class 1E to Non-1E isolation device by design, and was not tested by the procedure. 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.

4.10 Performance Proof Testing

Performance proof testing was conducted at the completion of all qualification testing to demonstrate the continued acceptable performance of the TUT after being exposed to various qualification test conditions. The operability and prudency tests were performed as part of performance proof tests. These procedures were developed in accordance with Sections 5.3 and 5.4 of EPRI TR-107330. Results of these tests are documented in the Performance Proof Operability Test Report, Reference 7.61 and Performance Proof Prudency Test Report, Reference 7.62 . 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. <u>Analog Input/Output Module Accuracy</u> – For all Operability Test runs, the accuracy of each analog input/output module of the TUT was demonstrated to meet the Triconex published specifications. In addition, the test results show no degradation in module accuracy from pre-qualification testing throughout qualification and performance proof testing.
2. <u>Response Time</u> – For all Operability Test runs, the response times for digital input to digital output, analog input to digital output and digital output and "round-robin" sequences of the TUT were measured. Triconex provides a method for calculating the maximum expected digital input to digital output and analog input to digital output and analog output and "round-robin" response time for a specific TUT hardware configuration and TSAP scan time. The test data demonstrates that the maximum response time equation provides a reliable upper bound on the maximum expected response times for a specific hardware configuration and TSAP.
3. <u>Discrete Input Operation</u> – For all Operability Test runs, the OFF to ON and ON to OFF voltage switching levels of each digital input module of the TUT was demonstrated to meet the Triconex published specifications. In addition, the test results show no degradation in discrete input module voltage switching levels from pre-qualification testing throughout qualification and performance proof testing.
4. <u>Discrete Output Operation</u> – For all Operability Test runs, each discrete output module of the TUT was demonstrated to operate ON and OFF at the Triconex published specifications for maximum operating current, and minimum and maximum operating voltage. In addition, the test results show no degradation in operation of the discrete

output modules from pre-qualification testing throughout qualification and performance proof testing.

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

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

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

8. Power Interrupt Performance – For all Operability Test runs, power hold-up time performance of the TUT chassis power supplies were demonstrated on an interruption of source power for approximately 40 milliseconds. The test results demonstrated:
   - The 120 VAC and 230 VAC chassis power supplies meet the EPRI TR-107330 acceptance criteria for hold-up time capability of at least 40 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 EPRI TR-107330 acceptance criteria for hold-up time capability of at least 40 milliseconds. The measured hold-up time capability of the 24 VDC chassis power supplies was less than 3 milliseconds.

9. Power Quality Tolerance – Tests were performed to demonstrate tolerance of the TUT to changes in the quality (voltage and frequency) of AC and DC source power. Tests were performed over Triconex allowable ranges of voltage and frequency for each type of power supply included in the testing. All test results demonstrated acceptable performance of the TUT. In addition, power quality tolerance tests demonstrated acceptable performance of processor memory writes prior to Tricon reset on gradual loss of source power voltage.

10. Burst of Events Performance – Burst of Events testing demonstrated the ability of the TUT to process rapidly changing input and output signals based on the control logic of the TSAP.
11. Communication Port Failure Performance – Communication port failure testing demonstrated no effect on digital input to digital output, analog input to digital output and analog output, and "round-robin" response times during simulated failures of communication lines connected to communication ports on the TCM.

4.11 Failure Mode and Effects Analysis

As part of the Tricon v10 PLC qualification effort, a failure modes and effects analysis (FMEA) was performed as documented in Reference **7.64**. The FMEA was performed in accordance with the guidelines of Section 6.4.1 of EPRI TR-107330, Reference **7.6**.

The system analyzed by the FMEA is identical to the TUT configuration that was used in the Tricon v10 Nuclear Qualification Project. The intent of the FMEA is to identify potential failure states of a typical Tricon v10 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 modular redundant, and no single failure of an individual sub-component would impact the ability of the Tricon 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 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 Assemblies

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 modular 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 **7.64**. 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 7.30 and 7.31 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.

4.12 Reliability and Availability Analysis

Section 4.2.3 of EPRI TR-107330 requires that analyses be performed to determine the *availability* and *reliability* of a PLC in safety-related applications. The *availability* is defined in the EPRI TR-107330 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-107330 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-107330 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 **7.63**. 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-107330, 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-

107330. For a periodic test interval of 18 months (corresponding to the typical nuclear plant refueling outage cycle), the reliability is 99.9987% and the availability is 99.9990%.

4.13 Cable Similarity Analysis

As part of the Tricon v10 PLC qualification effort, a cable similarity analysis was performed as documented in Reference 7.72. The analysis was performed in accordance with the guidelines of IEEE 381-1977, Reference 7.21.

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

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

The analysis concluded that all XLPE and PVC Interface Cable Assemblies in the Tricon v10 Nuclear Qualification Project are qualified.

4.14 System Accuracy Specifications

As part of the Tricon v10 PLC qualification effort, system accuracy specifications for the Tricon v10 system was established as documented in Reference 7.73. The accuracy specifications are documented in accordance with the Section 4.2.4 of EPRI TR-107330, Reference 7.6.

The design of the Tricon enables it to maintain its rated reference accuracy specifications indefinitely. If the rated reference accuracy specifications are not met, the system will generate an alarm and the faulted module will be indicated. Response to the alarm would require replacement of the faulted module and restoration of normal operation. No field adjustments or calibrations of the Tricon are required or possible. The key in the Tricon design is its TMR architecture. By performing continuous cross comparisons between the triplicated values, a true and full verification of actual input and output values is maintained.

The effects of calibrated accuracy including hysteresis and non-linearity and repeatability are applicable to the Tricon system and I/O modules and their error contributions are specified in the System accuracy specifications. The effects of temperature sensitivity, drift over time, power supply variations, arithmetic operations errors, vibration, radiation and relative humidity are not applicable to the Tricon system and I/O modules and their error contribution is zero. The system accuracy specifications cover all the components and modules subjected to qualification testing.

4.15 Component Aging Analysis

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

Per IEEE 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. Application Guide, Appendix B to this report 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," **Reference 7.1** 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 7.66.

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 Revision 2, which endorses IEEE Std 7 4.3.2-2003 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations."
- IEEE Standard 7-4.3.2 provides a digital interpretation of IEEE Standard 603 1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." Title 10 of the Code of Federal Regulations Part 50.55a(h) (10 CFR 50.55a(h)) endorses IEEE Standard 603-1991.

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 7.66. 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**, Reference 7.2**, 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 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. 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 10.2.1 of the Tricon software was extensively reviewed as part of the qualification effort. As described in the Software Qualification Report, Reference 7.66, this review establishes that there are sufficient documents, as well as sufficiently mature product, to accept the Tricon PLC and TriStation 1131 as acceptable for nuclear safety related use. This acceptance is based on certain compensatory actions and evaluations defined in the proprietary appendix to this report.

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

- ISO 9001-1994 in the Version 9.3.1 qualification
- ISO 9001-2000 in the Version 10.2.1 qualification
- 10 CFR 50 Appendix B
- TÜV Certification for DIN V VDE 19250, resp. DIN V VDE 0801 Class 6 in the Version 9.3.1 qualification
- TÜV Certification for IEC 61508, Part 1-7:2000, IEC 61511-1:2004, EN 50156-1:2004, EN 61131-2:2005, EN 61000-6-2:2005, EN 61000-6-4:2001, EN 54-2:1997, NFPA 72:2002, NFPA 85:2001. TÜV concludes that the Tricon Version 10.2.1 system is suitable for safety related applications up to Safety Integrity Level (SIL) 3, based on their test report number 968/EZ 105.06/06, dated 2006-10-31.

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)
- Triconex Quality Procedures Manual (QPM)
- Triconex Engineering Department Manual (EDM).

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 Department Manual provides the procedures specific to the development, verification, configuration control, maintenance, and enhancement of the Tricon and software. All manuals have been improved, expanded, and enhanced during the period of time in which the Tricon has been produced. These engineering procedures define a product life cycle 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 2006. The evolution of the various Engineering Procedures described in the Software Qualification Report, Reference 7.66, demonstrates the continual refinement and improvement of the procedures.

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 1012-1998 provide an approach that is acceptable to the NRC for meeting the requirements of 10 CFR 50, Appendix B and the guidance given in Regulatory Guide 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.” NRC Regulatory Guide 1.168 endorses IEEE Standard 1012-1998 as an acceptable methodology for implementing the verification and validation of safety system software, subject to certain exceptions listed in that Regulatory Guide.

Triconex verification and validation activities do not strictly follow the ANSI/IEEE 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 7.66.

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 7.72).

Each new version of Tricon was tested by TÜV Rheinland, with Version 10.2.1 being certified in October of 2006 to Safety Integrity Level (SIL) 3, IEC standard (Test Report 968/EZ105.06/06, Reference 7.76). The testing preformed by TÜV Rheinland examines both the hardware and the software. Both the Tricon system software (main processors and associated communication and I/O support modules) and the application development tools software (TriStation 1131) are reviewed and tested with each new version. The TÜV Rheinland driven development, release and maintenance procedures are effective for control of the Tricon development process.

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

The TÜV-Rheinland software analysis consists of examination of the code and support documentation to ensure that specifications are met and those 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.

The TÜV-Rheinland testing of the Tricon and TriStation software consists of the following:

- The Triconex life cycle and life cycle documentation was evaluated, including verification and validation at the unit, module, and system levels. TÜV Rheinland concluded that the development life cycle meets the expectations of IEC 61508.
- TÜV Rheinland performed a Functional Safety Assessment at Triconex facilities. TÜV Rheinland engineers evaluated the application and effectiveness of Triconex measures to avoid failures, as well as the measures taken to detect and control failures within the hardware, and concluded that Triconex complies with expectations. TÜV Rheinland does take credit for Triconex system, module, automated fault insertion, and unit level hardware and software verification and validation tests. TÜV Rheinland engineers evaluated the module level Failure Modes and Effects Analysis (FMEA) and found Triconex FMEA acceptable.
- TÜV Rheinland reviewed the software and hardware life cycle documentation, as well as the configuration management and change control applied to that documentation, and concluded that Triconex documentation and processes are appropriate and meet the software and hardware life cycle expectations established in IEC 61508.
- TÜV Rheinland engineers inspected the average Probability of Failure on Demand (PFDavg) and Mean Time To Spurious Failure (MTTF spurious) spreadsheet prepared by Triconex, and concluded that the spreadsheets used accepted methodologies and reasonably conservative failure data (Bellcore, Issue 6).
- TÜV Rheinland engineers inspected the Triconex upgrades of many of the previously accepted modules. These upgrades included changing through-hole components for surface mount components. The TÜV Rheinland engineers concluded that the surface mount modules are 100% plug-compatible, and are form, fit, and function replacements for the through-hole modules. The firmware was slightly modified to support the new microprocessor model used on the new modules.

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

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

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. a, b

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.

A summary of exceptions to the EPRI TR-107330 requirements and/or test methodology is summarized in Table 6-1. Appendix A contains a compliance traceability matrix of the EPRI requirements versus the Tricon v10 Qualification with appropriate references.

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.

Table 6-1 Summary of Exceptions/Clarifications to EPRI TR-107330 Requirements

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.2.1.1.A	Analog Voltage Input Module Ranges. The PLC shall include analog voltage input modules with ranges of: 0 to 10 VDC, -10 to 10 VDC, and 0 to 5 VDC.	Partial Exception	Tricon analog voltage input modules do not include a –10 to 10 VDC range.
4.3.2.1.1.D	Analog Voltage Input Module Common Mode Voltage. The common mode voltage capability shall be at least 10 volts with a common mode rejection ratio of at least 90 dB.	Partial Exception	Common mode rejection rating of Module 3701 is 80 dB, Module 3721 is 85dB, and Module 3703 is 90dB.
4.3.2.1.1.A	Analog Current Input Module Ranges. The PLC shall include analog current input modules with ranges of: 4 to 20 mA and 10 to 50 mA or 0 to 50 mA.	Partial Exception	Tricon analog current input modules do not include a 10 to 50 mA or 0 to 50 mA range.
4.3.2.1.1.E	Analog Current Input Module Common Mode Rejection Ratio. The common mode rejection ratio shall be at least 90 dB.	Partial Exception	Common mode rejection rating of Module 3701 is 80 dB, Module 3721 is 85dB, and Module 3703 is 90dB..
4.3.2.1.3.A	RTD Input Module Types. The PLC shall include RTD input modules for use with 2, 3 or 4 wire European (DIN 43 760) or US standard 100 ohm RTDs.	Partial Exception	Tricon RTD input signal conditioners are for use with 2 or 3 wire, 100 ohm platinum RTDs.
4.3.2.1.3.B	RTD Input Module Ranges. The PLC shall include RTD input modules with a range of at least 0 to 800°C (32 to 1472°F).	Exception	Tricon RTD input signal conditioners span -100°C to 600°C (32 to 1112°F) range.
4.3.2.1.3.D	RTD Input Module Resolution. The minimum resolution shall be 0.1° or less for both °C or °F scaling.	Exception	Tricon RTD input signal conditioners (32 to 1112°F max. span = 1 to 5 V output) are interfaced with a 12 bit, 0 to 5 V analog input module. Resulting minimum resolution is 0.33°F (0.19°C).

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.2.1.3.G	RTD Input Module Response Time. The overall response time of the RTD input modules must support the response time requirement given in Section 4.2.1.A.	Exception	See Table Section 4.2.1.A. For large step changes (0 to 90% of full scale range), RTD's and input signal conditioners have a relatively long input update rate, and were not considered in qualification response time testing.
4.3.2.1.4.A	T/C Input Module Types. The PLC shall include T/C input modules for use with type B, E, J, K, N, R, S and T thermocouples over the specified temperature ranges.	Partial Exception	Tricon T/C input modules are for use with type E, J, K and T thermocouples. Type J input range is –250 to 2000°F (vs. TR requirement of 32 to 2192°F).
4.3.2.1.4.D	T/C Input Module Resolution. The minimum resolution shall be 0.1° or less for both °C or °F scaling.	Exception	Minimum resolution is 0.125°F (0.07°C).
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.	Partial Exception	Tricon discrete DC input modules are for nominal inputs of 115 VDC, 48 VDC and 24 VDC.
4.3.2.2.3	TTL Input Requirements. Requirements for TTL level input modules.	Exception	There is no TTL level input module available for use with the Tricon PLC.
4.3.2.3.1.D	Pulse Input Module Count Accuracy. The module shall have up and down count modes with a range of at least 9999. The accuracy of the count shall be ≤ 0.1%.	Exception	The Tricon pulse input module provides speed or RPM measurement only.
4.3.2.3.1.E	Pulse Input Module Frequency Accuracy. The module shall have a frequency mode with a range of at least 20 to 5000 Hz. The accuracy of the frequency measurement shall be ≤ 0.1%.	Partial Exception	Accuracy is ± 1.0% of reading from 20 to 99 Hz. Accuracy is ± 0.1% of reading from 100 to 999 Hz. Accuracy is ±0.01% from 1000 to 20,000 Hz

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.3.1.1	Analog Voltage Output Requirements. Requirements for analog voltage output modules.	Exception	There is no analog voltage output module available for use with the Tricon PLC.
4.3.3.1.2.A	Analog Current Output Module Ranges. The PLC shall include analog current output modules with ranges of: 4 to 20 mA or 0 to 20 mA, and 10 to 50 mA or 0 to 50 mA.	Partial Exception	Tricon analog current output module output range is 4 to 20 mA.
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.	Partial Exception	Tricon discrete AC output modules do not include 24 VAC nominal outputs.
4.3.3.2.2.A	Discrete DC Output Module Types. The PLC shall include discrete DC output modules for nominal outputs of 125 VDC, 48 VDC, 24 VDC, 15 VDC and 12 VDC.	Partial Exception	Tricon discrete DC output modules include 120 VDC, 48 VDC and 24 VDC nominal outputs.
4.3.3.2.2.C	Discrete DC Output Module ON State Voltage Drop. The ON state voltage drop shall not exceed 2 VDC at 0.5 amps.	Exception	Module Model 3607E ON state voltage drop is < 3 V.
4.3.3.2.2.D	Discrete DC Output Module OFF State Leakage. The OFF state leakage current shall not exceed 2 mA.	Exception	Module Models 3625 OFF state load leakage is 4 mA 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	Module Model 3607E (48 VDC output) operates from 44 to 80 VDC. Module Model 3625 (24 VDC output) operates from 22 to 45 VDC.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.3.2.3.A	Relay Output Module Types. The PLC shall include relay output modules that provide normally open and normally closed contacts.	Partial Exception	Tricon relay output module contacts are normally open.
4.3.3.2.4	TTL Output Requirements. Requirements for TTL level output modules.	Exception	There is no TTL level output module available for use with the Tricon PLC.
4.3.4.4.E	Communication Port Class 1E to Non-1E Isolation. The Class 1E to Non-1E isolation capability shall meet the requirements of Section 4.6.4.	Exception	Tricon TCM serial communication ports tested for Class 1E to Non-1E isolation capability at 250 VAC (vs. 600 VAC required by TR) and 250 VDC. Test level is based on maximum credible voltage.
4.3.6.1	Normal Environmental Basic Requirements. The normal PLC operating environment is: Temperature Range: 16 to 40ºC (60 to 104ºF). Humidity Range: 40 to 95% (non-condensing)	Comply	Tricon is rated for 0 to 60ºC (32 to 140ºF), 5% to 95% humidity (non-condensing).
	Power Source Range: As given in Section 4.6.1.1	Exception	See Table Section 4.6.1.1 for exceptions to power source range.
	Radiation Exposure: Up to 1000 Rads	Comply	Tricon has been tested to a 1000 Rad dose of Co60 gamma radiation.
4.3.6.2	Abnormal Environmental Basic Requirements. The abnormal PLC operating environment is: Temperature Range: 4 to 50ºC (40 to 120ºF). Humidity Range: 10 to 95% (non-condensing)	Comply	Tricon is rated for 0 to 60ºC (32 to 140ºF), 5% to 95% humidity (non-condensing).
	Power Source Range: As given in Section 4.6.1.1	Exception	See Table Section 4.6.1.1 for exceptions to power source range.
	Radiation Exposure: Up to 1000 Rads	Comply	Tricon has been tested to a 1000 Rad dose of Co60 gamma radiation.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.3.7	EMI/RFI Withstand Requirements. The PLC shall withstand EMI/RFI levels given in EPRI TR-102323. When exposed to the radiated and conducted test levels, the PLC processors shall continue to function, I/O data transfer shall not be interrupted, discrete I/O shall not change state, analog I/O shall not vary more than 3%.	Exception	Tricon showed some susceptibilities to NRC RG 1.1.80 Rev. 1 (CE101).
4.6.1.1.A	Power Sources. AC sources shall operate from at least 90 VAC to 150 VAC and 57 to 63 Hz. AC sources shall operate at the temperature and humidity range given in Section 4.3.6.	Exception Comply	Model 8310 AC power supply modules are rated for 85 VAC to 140 VAC input. Model 8310 AC power supply modules were tested as per required temperature and 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. DC sources shall operate at the temperature and humidity range given in Section 4.3.6.	Exception Comply	Model 8311 DC power supply modules are rated for 22 VDC to 31 VDC input. Model 8311 DC power supply modules were tested as per required temperature and humidity range (see Table Section 4.3.6.3).

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
4.6.2	Surge Withstand Capability Requirements. PLC platform shall withstand IEEE C62.41 ring wave and combination wave, 3000 volt peak surges.	Comply	Power sources meet surge withstand criteria. Circuits were tested to IEC 61000-4-5 and IEC 61000-4-12 using 1 kV Ring wave, and combination waves at 1kV open circuit/0.5kA short circuit per R.G. 1.180, Rev. 1, Level 2.. All circuits met TR Section 4.6.2 acceptance criteria.
	Withstand capability applies to power sources, analog and discrete I/O interfaces, and communication port interfaces. Per Section 6.3.5, surge testing shall be conducted per IEEE C62.45.	Partial Exception	Power Sources were tested per Reg Guide 1.180 Rev. 1 for category B low exposure installations to 2KV. IEEE 62.41 and 62.45 do not address testing of I/O and communication circuits; these circuits were tested per Reg. Guide 1.180 Rev. 1 for low exposure level 2 installations at 1KV. Tests were performed to IEC61000-4-5 for combination wave and 61000-4-12 for Ring Wave.
4.6.4	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	Only relay output modules, communication ports, and fiber optic chassis inter- connections are intended to provide Class 1E to Non-1E isolation. Isolation tests were performed on relay output module and communication ports. Relay output module meets TR Section 4.6.4 isolation requirements. Communication ports provide isolation to 250 VAC and 250 VDC for 30 seconds. Fiber optic chassis connections inherently provide isolation through non-conducting fiber optic cables.
5.2.A	Application Objects Testing. Testing of the software objects in the PLC library shall be performed. This testing shall be in addition to any testing performed by the manufacturer.	Exception	Triconex and TUV Rheinland have performed extensive testing of the Tricon PLC application software. Results of this testing are documented in Ref. 58.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
5.2.F	Burn-In Test. A minimum 352 hour burn-in test shall be performed during acceptance testing.	Exception	Triconex routinely conducts burn-in tests on all Tricon hardware as part of manufacturing process. This testing meets TR requirements for burn-in testing.
5.3.B	Response Time. Response time of analog input to digital output and digital input to digital output sequences shall be measured. For baseline (acceptance) testing, the acceptance criteria is that the measured response time shall not vary more than 20% from the value calculated from manufacturer's data. For all subsequent testing, the measured value shall not vary more than 10% from the baseline.	Exception	Based on Tricon design, it is not practicable to perform a test 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. The acceptance criterion for all tests is that the calculated response times are not exceeded.
5.3.E	Communication Operability. If any communication functions are included in the qualification envelope, then operability of the ports shall be tested. Tests shall look for degradation in bit rates, signal levels and pulse shapes of communication protocol.	Partial Exception	TCM Module NET1 port is included in qualification envelope. Test equipment to measure degradation of bit rates, pulse shapes, and signal levels was not available at the time testing was performed. Port protocol is proprietary and not amenable to TR specified tests. Port operation is monitored for correct performance throughout all qualification tests.
5.4	Prudency Testing Requirements. The Prudency tests shall be performed with the power supply sources at the minimum values specified in Section 4.6.1.1.	Partial Exception	To accommodate power frequency changes, external power to the 230Vac chassis power supplies was provided through a step-up transformer which was fed by the same external power supply for the 115Vac chassis power supplies. This limited the voltage to the 115Vac chassis power supplies to 97Vac.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
5.5	Operability/Prudency Testing Applicability Requirements. As a minimum, Operability and Prudency tests shall be performed: - During acceptance testing: Operability – All, Prudency – All - During 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	Partial Exception	Due to short duration of seismic SSE tests, and special set-up required for EMI/RFI tests, it is not practicable to perform Operability and Prudency tests at those times. Other requirements of Section 5.5 were complied with.
5.6	Application Software Objects Acceptance (ASOA) Testing. Requirements for ASOA testing.	Exception	See Table Section 5.2.A
6.2.1.E	Power Supplies. The test specimen shall include the power supplies needed to meet the TR requirements. Additional resistive loads shall be placed on each power supply output so that the power supply operates at rated conditions.	Exception	The Tricon design does not allow for adding resistive load on the power supplies without altering design and operation. To demonstrate significant power supply loading, one chassis of the test specimen was fully populated with one module in each slot.
6.2.1.F	Dummy Modules. Dummy modules shall be used to fill all remaining slots in the main chassis and at least one expansion chassis. The dummy modules shall provide a power supply and weight load approximately equal to an eight point discrete input module.	Exception	Seismic Balance Modules (SBMs) were installed in two test specimen chassis to increase the weight loading to that representative of a fully module populated chassis. Dummy modules did not provide a load on the power supplies.

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
6.3.2	EMI/RFI Test Requirements. EMI/RFI testing to be performed as described in Section 4.3.7. Susceptibility tests to be performed at 25%, 50% and 75% of specified levels in addition to the specified levels.	Exception	EMI/RFI testing performed per R.G. 1.180, R1. Testing performed at levels lower than specified levels only as needed to establish susceptibility threshold.
6.3.2.1	EMI/RFI Mounting Requirements. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	Due to space limitations of NTS Labs EMI/RFI chamber, test specimen was mounted less than six feet above floor. Test specimen was mounted in a Rittal cabinet with sides and doors removed. Cabinets provided no significant shielding.
6.3.5.1	Surge Withstand Test Mounting Requirements. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	Due to space limitations of NTS Labs EMI/RFI chamber, test specimen was mounted less than six feet above floor. Test specimen was mounted in a Rittal cabinet with the sides and doors removed.
6.3.6	Class 1E to Non-1E Isolation Testing. Test specimen shall be mounted on a non-metallic surface six feet above floor with no secondary enclosure. PLC shall be grounded per manufacturer's recommendations.	Exception	Test specimen was mounted less than six feet above floor. Test specimen was mounted in a Rittal cabinet with the sides and doors removed.
6.4.4.G	ASOA Test Compliance. Results shall be evaluated for compliance to Section 5.6 requirements.	Exception	ASOA testing not performed.

7.0 REFERENCES

Standards, Guides and Regulatory Documents

7.1 NUREG-0800; 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 U.S. Nuclear Regulatory Commission Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," October 2003

7.5 USNRC Regulatory Guide 1.209, Dated March 2007- Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Triconex Documents

7.26 Triconex Quality Assurance Manual (QAM)

7.27 Triconex Quality Procedures Manual (QPM)

7.28 Triconex Engineering Department Manual (EDM)

7.29 **Not used**

7.30 9791007-014, Tricon Technical Product Guide

7.31 9720077-008, Tricon Planning and Installation Guide

Triconex Nuclear Qualification Project Documents

7.32 9600164-002, Nuclear Qualification Quality Plan

7.33 9600164-500, Master Test Plan

7.34 9600164-540, Master Configuration List

7.35 9600164-537, Software Quality Assurance Plan

7.36 9600164-541, Tricon System Description

7.37 9600164-500-515, Function Diagrams

7.38 9600164-700, Wiring Schedule

7.39 9600164-100-300, Test System Wiring Drawings

7.40 9600164-502, System Setup and Checkout Procedure

7.41 9600164-503, Operability Test Procedure

7.42 9600164-504, Prudency Test Procedure

7.43 9600164-511, Radiation Test Procedure

7.44 9600164-506, Environmental Test Procedure

7.45 9600164-507, Seismic Test Procedure

7.46 9600164-510, EMI/RFI Test Procedure

7.47 9600164-514, EFT Test Procedure

7.48 9600164-508, Surge Withstand Test Procedure

7.49 9600164-512, ESD Test Procedure

7.50 9600164-509, Class 1E to Non-1E Isolation Test Procedure

7.51 9600164-560, Pre-Qualification Operability Test Report

7.52 9600164-570, Pre-Qualification Prudency Test Report

7.53 9600164-533, Radiation Test Report

7.54 9600164-525, Environmental Test Report

7.55 9600164-536, Seismic Test Report

7.56 9600164-527, EMI/RFI Test Report

7.57 9600164-521, EFT Test Report

7.58 9600164-528, Surge Test Report

7.59 9600164.522, ESD Test Report

7.60 9600164-529, Class 1E to Non-1E Isolation Test Report

7.61 9600164-566, Performance Proof Operability Test Report

7.62 9600164-573, Performance Proof Prudency Test Report

7.63 9600164-532, Reliability/Availability Study for Tricon v10 PLC

7.64 9600164-53**1**, Failure Modes and Effects Analysis (FEMA) for Tricon v10 PLC

7.65 9600164-534, Tricon System Accuracy Specifications

7.66 9600164-535, Software Qualification Report

7.67 9600164-517, TSAP Software Requirements Specification

7.68 9600164-518, TSAP Software Design Description

7.69 9600164-513, TSAP Software V&V Plan

7.70 9600164-53**6**, TSAP Final V&V Report

7.71 9600164-720, Software Traceability Analysis

7.72 9600164-538, Cable Similarity Analysis

7.73 9600164-534, System Accuracy Specifications

7.74 9600164-539, Critical Digital Review (Proprietary)

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

7.76 TÜV-Rheinland Microelectronic and Process Automation, "Type Approval of Tricon Version 10.2.1," Report-No. 968/EZ 105.06/06, October 31, 2006

8.0 APPENDICES

A. EPRI TR-107330 Requirements Compliance and Traceability Matrix

B. Application Guide

C. Evaluation to IEEE 323-2003, as endorsed by USNRC Regulatory Guide 1.209