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 TCXNRC-09-01, Affidavit, Section 4.)

EQUIPMENT QUALIFICATION SUMMARY REPORT

Document No: 9600164-545

Revision 3

August 03, 2009

	Name	Signature	Title
Author:	Frank Kloer	[signature]	Qualification Engineer
Reviewers:	Alan Sands	[signature]	Project QA Engineer
Approval:	Naresh Desai	[signature]	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.

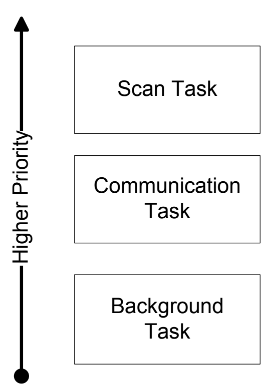

Figure 8 - ETSX tasks and priorities

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.

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

a, b

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.

a, b

a, b

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.

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.

a, b

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."

a, b

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.

a, f

a, b

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

a, b

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.

a, b

a, b

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.

a, b

a, b

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.

a, b

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.

a, b

a, b

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) Power Source Range: As given in Section 4.6.1.1 Radiation Exposure: Up to 1000 Rads	Comply Exception Comply	Tricon is rated for 0 to 60ºC (32 to 140ºF), 5% to 95% humidity (non-condensing). See Table Section 4.6.1.1 for exceptions to power source range. 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) Power Source Range: As given in Section 4.6.1.1 Radiation Exposure: Up to 1000 Rads	Comply Exception Comply	Tricon is rated for 0 to 60ºC (32 to 140ºF), 5% to 95% humidity (non-condensing). See Table Section 4.6.1.1 for exceptions to power source range. 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	
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).

a, b

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	
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.

a, b

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	

a, b

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."

a, f

a, f

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