

TRICONEX TOPICAL REPORT

Document No.: 7286-545-1

Revision 3

July 11, 2010

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

TRICONEX TOPICAL REPORT

Document Revision History

Revision Number	Date	Description of Changes
0	6/27/2000	Initial Issue
1	9/18/2000	Incorporate Triconex and STP comments
2	03/31/2010	Revised format of document incorporating new document template. Consolidated Revision 1 sections 2.0 thru 7.0 into new Section 2.0. Added new sections 3.0 thru 5.0. Revised report content including Appendices A and B to incorporate changes associated with Tricon V10.
3	07/11/2010	Revised Section 4 to incorporate Tricon V10.5.1 and TriStation 1131, V4.7.0. Section 2.5.34 and Section 5.0 updated for consistency with supporting communications and security documents. Appendix B, Section 4.1 clarification added for guidance on chassis installation. Made minor typographical corrections throughout document

TRICONEX TOPICAL REPORT

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1.0 INTRODUCTION	5
2.0 TRICON NUCLEAR QUALIFICATION PROJECT	6
2.1 SYSTEM DESCRIPTION	9
2.1.1 Tricon System Overview	9
2.1.2 Tricon System Hardware	11
2.1.3 Tricon System Software	21
2.1.4 Qualified Tricon Modules	26
2.1.5 Qualification of Newer Versions of the Tricon System	27
2.2 HARDWARE QUALIFICATION	28
2.2.1 Tricon Test Specimen Configuration	30
2.2.2 Radiation Qualification	31
2.2.3 Environmental Qualification	32
2.2.4 Seismic Qualification	35
2.2.5 Electromagnetic and Radio Frequency Interference Qualification	39
2.2.6 Electrical Fast Transient	43
2.2.7 Surge Withstand	44
2.2.8 Electrostatic Discharge	48
2.2.9 Class 1E to Non-1E Isolation	51
2.2.10 Performance Proof Testing	53
2.2.11 Failure Modes and Effects Analysis	55
2.2.12 Reliability and Availability Analysis	56
2.2.13 Cable Similarity Analysis	57
2.2.14 System Accuracy Specifications	57
2.2.15 Component Aging Analysis	58
2.3 SOFTWARE QUALIFICATION	58
2.3.1 Software Documentation	59
2.3.2 Software Development Process	61
2.3.3 Software Verification and Validation Process	62
2.3.4 Safety Analysis	65
2.3.5 Configuration Management and Error Notification	65
2.4 SYSTEM APPLICATION	66
2.5 REFERENCES	82
2.5.1	

TRICONEX TOPICAL REPORT

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
3.0 DIFFERENCES BETWEEN V9.5.3 AND V10.2.1 SYSTEMS	87
3.1 BACKGROUND	87
3.2 SYSTEM ARCHITECTURE & SYSTEM LEVEL DIFFERENCES BETWEEN V9.5.3 & V10.2.1	88
3.3 COMPARISON OF V9/V10 DIFFERENCES	88
4.0 TRICON V10.5.1 UPGRADE	92
4.1 INTRODUCTION	92
4.2 PURPOSE	92
4.3 DISCUSSION	92
4.3.1 Tricon Firmware Changes	96
4.3.2 TriStation 1131 Changes	104
4.3.3 Process Change Review	104
4.4 CONCLUSION	106
5.0 INVENSYS PROCESSES AND POLICIES FOR NUCLEAR PRODUCTS	107
5.1 MAINTENANCE OF QA AND PRODUCT DEVELOPMENT PROCESSES	107
5.1.1 Quality Assurance Program	107
5.1.2 Product Development Process	107
5.2 INVENSYS PROJECT INTEGRATION PROCESSES	109
5.3 SECURITY	109
5.4 DIVERSITY AND DEFENSE-IN-DEPTH ISSUES (ISG-02)	110
5.5 HIGHLY INTEGRATED CONTROL ROOMS – COMMUNICATION ISSUES (ISG-4)	111
5.6 INVENSYS TRICONEX TOPICAL REPORT/SER MAINTENANCE PROCESS	112

APPENDICES

- A EPRI TR-107330 REQUIREMENTS COMPLIANCE AND TRACEABILITY MATRIX
- B APPLICATION GUIDE

TRICONEX TOPICAL REPORT

1.0 INTRODUCTION

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

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

The staff concludes that the Tricon PLC system meets the requirements of 10 CFR 50.55a(a)(1) and 55a(h). It also meets GDC 1, 2, 4, 13, 20-24, and 29, and IEEE Std 603 for the design of safety-related reactor protection systems, engineered safety features systems, and other plant systems, and the guidelines of RG 1.152 and supporting industry standards for the design of digital systems.

On that basis, the staff concludes that, when properly installed and used, the Tricon PLC system is acceptable for safety-related use in nuclear power plants.

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

This report is organized as follows:

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

TRICONEX TOPICAL REPORT

- SER/Topical Report Maintenance Process

2.0 TRICON NUCLEAR QUALIFICATION PROJECT

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

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

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

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

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

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

TRICONEX TOPICAL REPORT

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

- Identifying the specific PLC modules and supporting devices to be qualified. The Tricon hardware included in the qualification are listed in the Master Configuration List, Reference 2.5.39. This hardware was integrated in a complete test system that was intended to demonstrate capabilities typical of various nuclear safety systems. The design of the test system is documented in the System Description, Reference 2.5.41 and associated drawings, References 2.5.43 through 2.5.45.
- Developing an application program to support the required testing. The Test Specimen Application Program (TSAP) was developed to simulate operation of the Tricon in typical nuclear facility applications. Development, including verification and validation (V&V) of the TSAP was done in accordance with the Triconex QA program and a project-specific Software QA Plan, Reference 2.5.40. The TSAP program and associated V&V activities are documented in References 2.5.66 through 2.5.70.
- Specifying the set of qualification tests to be performed on the test specimen, including defining a set of operability tests to be performed at suitable times in the qualification process. Operability tests are required to determine the baseline system performance and to demonstrate satisfactory system operation under the stresses applied during qualification testing. The specific tests performed are defined in the Master Test Plan, Reference 2.5.38. Test procedures are provided in References 2.5.46 through 2.5.54, Reference 2.5.73, and Reference 2.5.74.
- Performing the qualification tests and documenting the results. Results of these tests, documented in References 2.5.55 through 2.5.61 and 2.5.75 through 2.5.79, define the qualification envelope and form the basis for the application guidance contained in this report.
- Performing other technical evaluations as needed to demonstrate compliance with regulatory requirements and other technical requirements in EPRI TR-107330. Evaluation of the embedded operating system and programming software is documented in the Software Qualification Report, Reference 2.5.65. Evaluation of new hardware modules (MP 3008, NGAID 3721, NGDO 3625, and Tricon Communication Module (TCM)) is documented in Critical Digital Review (CDR), Reference 2.5.80. A failure modes and effects analysis evaluating the effects of component failures on Tricon operation is provided in Reference 2.5.63. Reference 2.5.62 documents an analysis of Tricon system reliability. Reference 2.5.64 provides a summary of the accuracy specifications for the Tricon system for use in calculating instrument measurement uncertainties and establishing critical control setpoints.

TRICONEX TOPICAL REPORT

2.1 SYSTEM DESCRIPTION

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

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

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

2.1.1 Tricon System Overview

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

TRICONEX TOPICAL REPORT

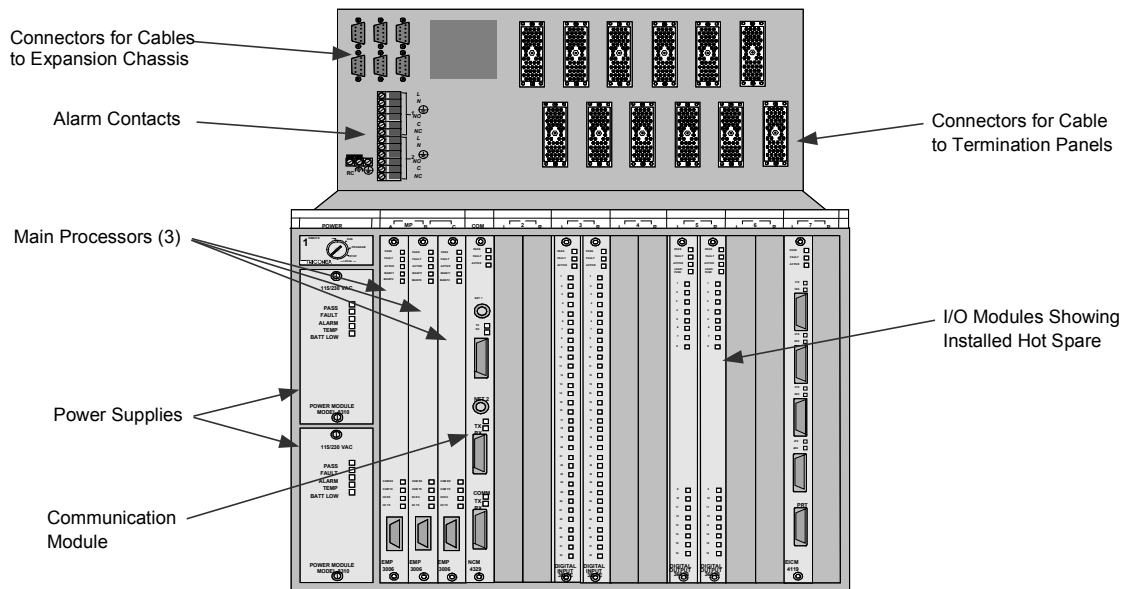


Figure 2-1. Tricon Main Chassis

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

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

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

TRICONEX TOPICAL REPORT

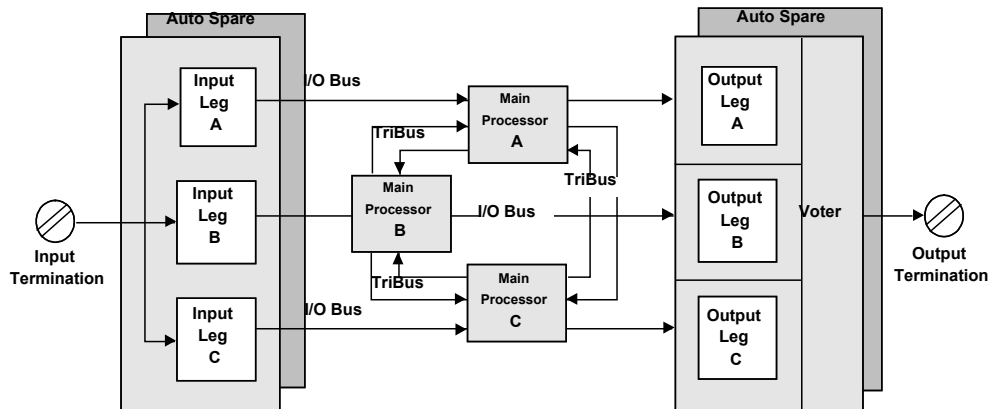


Figure 2--2. Triple Modular Redundant Architecture.

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

2.1.2 Tricon System Hardware

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

2.1.2.1 Main Chassis

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

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

TRICONEX TOPICAL REPORT

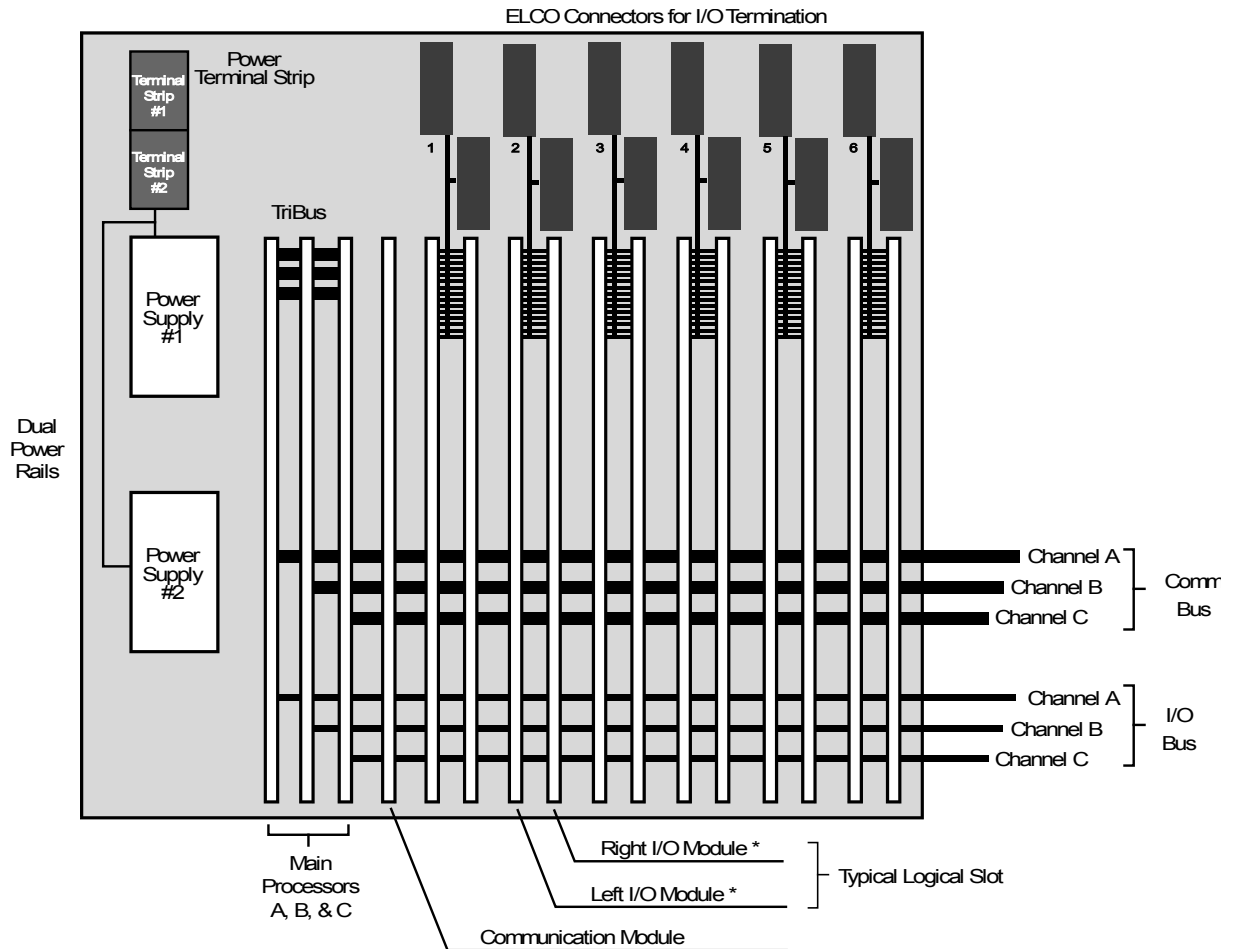
The main chassis also has a key switch that sets the system operating mode:

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

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

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

TRICONEX TOPICAL REPORT



* Either the left module or right module functions as the active or hot-spare module.

Figure 2-3. Tricon Chassis Backplane Configuration

2.1.2.2 Expansion Chassis

Expansion chassis are interconnected via three separate RS-485 data links, one for each of the three I/O legs. If communication modules are installed, three separate RS-485 data links are required for the three communications busses. The Tricon expansion chassis can support the following modules:

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

TRICONEX TOPICAL REPORT

2.1.2.3 Remote Extender Modules

The Remote Extender Modules (RXM) are single-mode fiber optic modules that allow expansion chassis to be located several kilometers away from the main chassis. An RXM connection consists of three identical modules, serving as repeaters/extenders of the Tricon I/O bus, that also provide ground loop isolation.

Each RXM module has single channel transmit and receive cabling ports. Each of the three primary RXM modules is connected to the remote RXM modules housed in the remote chassis. Each pair of RXM modules is connected with two fiber optic cables operating at a communication rate of 375 Kbaud. The interfacing cabling is unidirectional for each channel. One cable carries data transmitted from the primary RXM to the remote RXM. The second cable carries data received by the primary RXM from the remote RXM. The RXM modules provide immunity against electrostatic and electromagnetic interference. Since the RXM modules are connected with fiber optic cables, they may be used as 1E-to-non 1E isolators between a safety-related main chassis and a nonsafety-related expansion chassis.

2.1.2.4 External Termination Assemblies

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

2.1.2.5 Power Supply Modules

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

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

<u>Indicator</u>	<u>Color</u>	<u>Description</u>
PASS	Green	Input Power is OK
FAULT	Red	Power Module is not OK
ALARM	Red	Chassis Alarm Condition

TRICONEX TOPICAL REPORT

TEMP	Yellow	Over-temperature Condition
BATT LOW	Yellow	Battery Low Condition

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

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

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

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

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

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

2.1.2.6 Main Processor Modules

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

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

TRICONEX TOPICAL REPORT

The operating system, run-time library, and fault analysis for the main processor is fully contained in flash memory on each module. The main processors communicate with one another through a proprietary, high speed, voting, bi-directional serial channel called TriBUS. Each main processor has an I/O channel for communicating with one of the three legs of each I/O module. Each main processor has an independent clock circuit and selection mechanism that enables all three main processors to synchronize their operations each scan to allow voting of data and exchange of diagnostic information.

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

At the beginning of each scan, each primary processor takes a snapshot of the input data table in dual port RAM, and transmits the snap shots to the other main processor modules over the TriBUS. This transfer is synchronized using the TriClock. Each module independently forms a voted input table based on respective input data points across the three snapshot data tables. If a main processor module receives corrupted data or loses communication with a neighbor, the local table representing that respective leg data will default to the de-energized state.

For digital inputs, the voted input table is formed by a 2 out of 3 majority vote on respective inputs across the three data tables. The voting scheme is designed for de-energize to trip applications, always defaulting to the de-energized state unless voted otherwise. Any single leg failure or corrupted signal feeding a main processor module is corrected or compensated for at the main processor module level when the voted data table is formed.

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

TRICONEX TOPICAL REPORT

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

2.1.2.7 Input/Output Modules

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

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

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

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

A detailed description of each type of input module, including fault detection and data validation processes, is provided in the Planning and Installation Guide, Reference 2.5.30.

TRICONEX TOPICAL REPORT

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

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

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

A detailed description of the output modules, the voting processes, and fault detection processes is provided in the Planning and Installation Guide, Reference 2.5.30.

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

If a standby module is installed and both it and its pair are deemed healthy by the main processors, each of the modules is exercised on a periodic basis. The main processors will swap control between the two modules. By periodically using both modules, any faults are detected, alarmed, and the failed module replaced while a standby module is

TRICONEX TOPICAL REPORT

in place. This use of standby modules does not cause any interruption of protection or control functions.

2.1.2.8 Communication Module

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

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

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

The TCM provides functional isolation by handling all the communications with external devices, and it has been qualified under the Invensys Appendix B program for nuclear applications. In addition, the TCM has been designed for high-reliability and contributes to the overall reliability of the communication link through the use of Cyclic Redundancy Checks (CRCs), and testing has demonstrated that it will protect the safety core from network storms and other communication failures. Upon total loss of all TCMs, the safety core will continue to function. Furthermore, the Tricon has been tested by Wurldtech and it has been shown to be resilient against the communication faults listed in ISG-04 (Invensys document NTX-SER-09-10).

Invensys has developed a Communication Application Safety Layer for safety-related communication between a client and the Tricon system. This is an additional layer of protection provided by the communication protocols at the Application Layer of the network stack. The P2P and SAP protocols ensure end-to-end integrity of safety-critical messages. System architectures requiring data transfer between safety-related Tricons over a network would use the P2P protocol over an isolated, point-to-point network. Architectures requiring safety-critical

TRICONEX TOPICAL REPORT

data exchange with safety-related video display units would utilize the SAP. Invensys document NTX-SER-09-10 describes the Tricon V10 conformance to ISG-04.

2.1.3 Tricon System Software

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

2.1.3.1 Tricon Operating System

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

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

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

TRICONEX TOPICAL REPORT

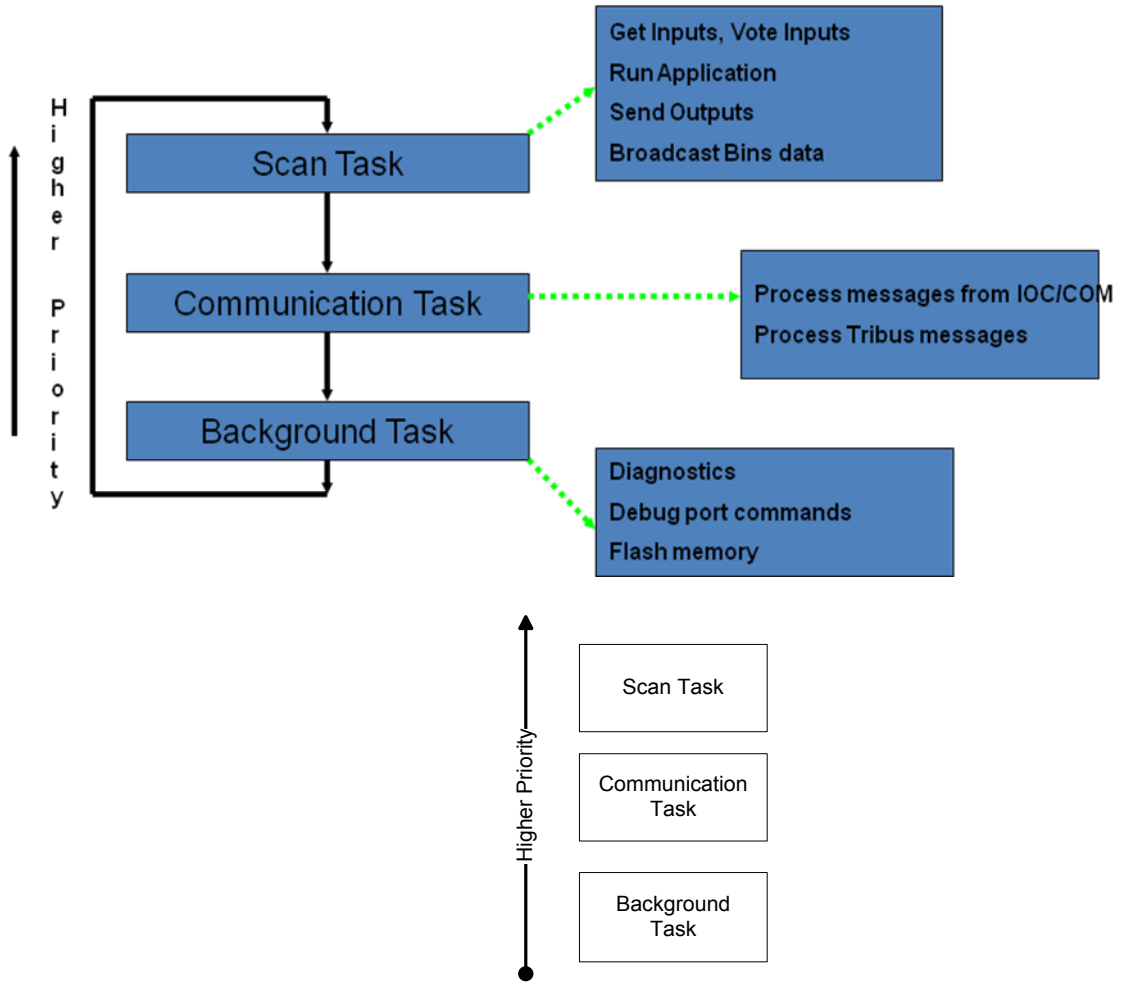


Figure 2-4 - ETSX tasks and priorities

TRICONEX TOPICAL REPORT

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

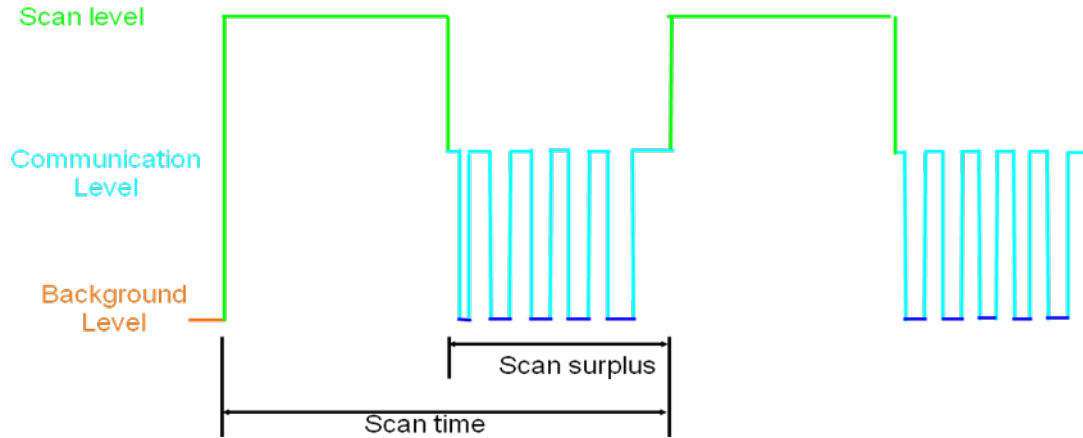


Figure 2-5 - ETSX task scheduling

The Scan task performs the following steps:

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

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

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

TRICONEX TOPICAL REPORT

8. Handle any TriBUS Messages from other MPs.

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

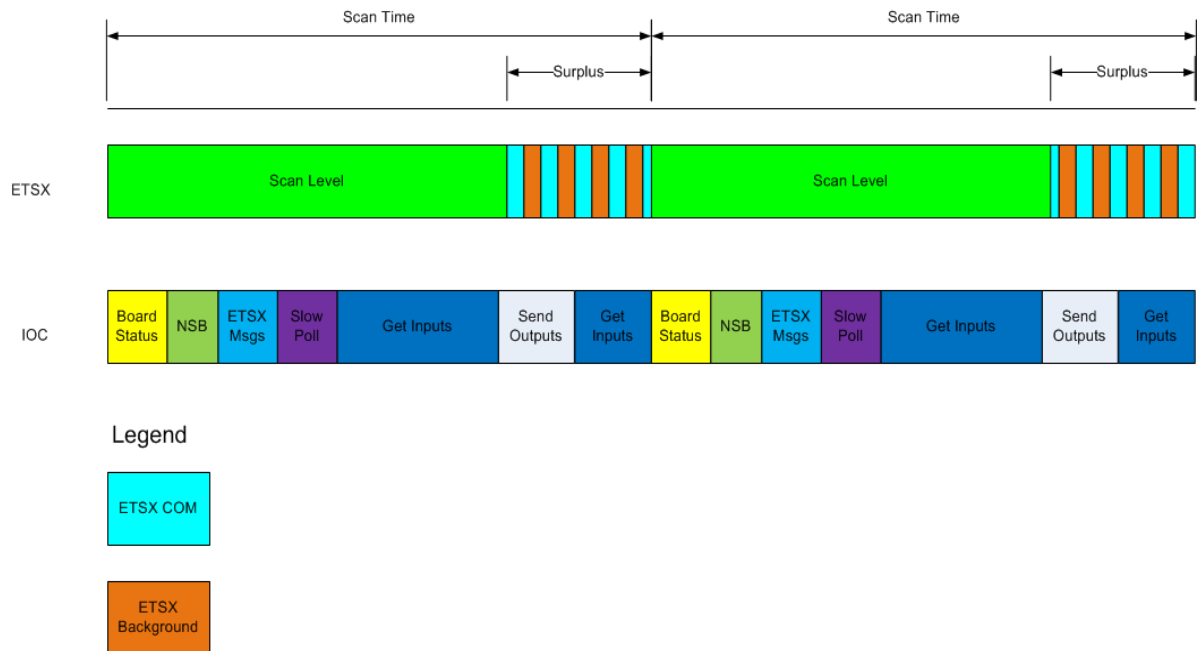


Figure 2-6 - ETSX and IOCCOM synchronization

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

As described in the preceding sections, the design of the software includes features to detect and mitigate system faults. These features include hardware and software based diagnostics. The diagnostic capabilities of the system are validated when hardware or software changes are made in any module. The validation requires that the stuck at zero, stuck at one, and contact noise from the automated fault injection system produce

TRICONEX TOPICAL REPORT

the pre-defined, expected diagnostic result. Failure to produce the correct result is evaluated and corrected exactly like a failure to produce any diagnostic result.

The extensive diagnostics comply with the requirements established in BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions." The diagnostics are integrated into the base Tricon and require no special application programming. In addition, data is made available to the application program concerning program operation, results of arithmetic operations, and other internal faults, consistent with the requirements of NUREG-0800 Branch Technical Position 7-17 (BTP 7-17). Thus, requirements imposed on the application program relating to error detection are limited to providing appropriate error recovery and annunciation of faults. Use of several of the diagnostic data inputs are mandated in the application guidelines in this report.

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

2.1.3.2 TriStation 1131 Programming Software

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

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

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

The TriStation 1131 Developer's Workbench also provides emulation capabilities for the Tricon. The tool provides a capability for running an emulation code version of the program on the PC. Capabilities exist for manual input of program variables and observation of program outputs on the PC screen, with the inputs and output values

TRICONEX TOPICAL REPORT

merged and displayed with the program blocks. This simulation can be used as part of the validation process for new or modified application code.

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

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

2.1.3.3 Application Program

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

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

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

2.1.4 Qualified Tricon Modules

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

TRICONEX TOPICAL REPORT

Table 2-1. Qualified Tricon Modules

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

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

2.1.5 Qualification of Newer Versions of the Tricon System

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

TRICONEX TOPICAL REPORT

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

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

2.2 HARDWARE QUALIFICATION

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

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

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

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

Pre-qualification testing included the following:

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

TRICONEX TOPICAL REPORT

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

- Operability tests are defined in Reference 2.5.47, to establish the baseline performance and to demonstrate the functionality of the Tricon in accordance with its specifications. The operability test procedure included tests for analog module accuracy, system response time, operation of discrete inputs and outputs, performance of timer functions, failover tests (due to failure of redundant components), loss of power, detection of failure to complete a scan, power interruption, and power quality tolerance.
- Prudency testing is described in Reference 2.5.48, to establish baseline performance and to demonstrate the ability of the Tricon to operate within specifications under dynamic conditions. The prudency test included a burst of events test, a serial port receiver failure test, and a serial port noise test.

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

Qualification testing included the following:

- Radiation Exposure testing, Reference 2.5.76, is performed to demonstrate the ability of the Tricon V10 PLC to operate properly after being exposed to radiation. The operability tests and prudency tests were performed immediately after to demonstrate proper operation of the system.
- Environmental testing, Reference 2.5.50, is performed to demonstrate the ability of the Tricon to operate properly under the extremes of temperature and humidity. The operability test was performed at the high and low temperature and humidity conditions and also immediately after the environmental test (at ambient conditions) to demonstrate proper system operation. The prudency test was also performed at the high temperature conditions.
- Seismic testing, Reference 2.5.51, is performed to demonstrate the ability of the Tricon to operate properly during and after design basis seismic events, and therefore demonstrate the suitability of the device for qualification as Seismic Category I equipment. The operability and prudency tests were performed immediately after the seismic test to demonstrate continued proper operation of the system.
- Electromagnetic interference (EMI) and radio frequency interference (RFI) testing, Reference 2.5.58, is performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility

TRICONEX TOPICAL REPORT

- Electrical Fast Transient (EFT) testing, Reference 2.5.73, is performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to susceptibility to repetitive electrical fast transients on the power and signal input/output leads.
- Surge testing, Reference 2.5.52, is performed to demonstrate the suitability of the Tricon for qualification as a safety-related device with respect to AC and DC power, signal and communication line electrical surge withstand capability.
- Electrostatic Discharge (ESD) testing, Reference 2.5.78,, is performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related device with respect to immunity to electrostatic discharge exposure
- Class 1E-to-non 1E electrical isolation testing, Reference 2.5.53, is performed to demonstrate the suitability of the Tricon V10 PLC for qualification as a safety-related, Class 1E device with respect to providing electrical isolation at Non-1E field connections.

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

- Operability test as described above.
- Prudency test as described above.

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

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

2.2.1 Tricon Test Specimen Configuration

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

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

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

TRICONEX TOPICAL REPORT

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

Analog and digital inputs to the test specimen were generated using a two-chassis simulator **Tricon**. This system was configured with a simulator application program that was used to create a variety of static and dynamic input signals as described in Reference **2.5.67**. Appropriate test equipment was used to provide additional analog inputs to the TUT.

Analog and digital outputs from the TUT were monitored with indicator lights and a PC-based data acquisition system (DAS). The DAS also monitored analog and digital inputs to the TUT. Data was recorded and analyzed by the DAS during the various tests to verify proper operation of individual input and output points.

Two PCs running the TriStation software were used to communicate with and monitor the status of the TUT and the simulator Tricon. The TriStation software used for this purpose was TriStation 1131, which is Windows based software.

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

2.2.2 Radiation Qualification

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

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

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

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

TRICONEX TOPICAL REPORT

- The TUT shall pass the post radiation operability test following the completion of radiation exposure testing.
- The TUT shall pass the post radiation prudency test following the completion of radiation exposure testing.

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

Conclusions from this test are as follows:

1. Radiation Exposure Testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977. All of the tested TUT components were exposed to Co60 gamma radiation doses of 1000 rads, plus margin.
2. The TUT met all applicable acceptance requirements of the post-radiation exposure visual inspections performed as part of Radiation Exposure Testing.
3. Results of the post-radiation operability and prudency tests demonstrate that the applied Radiation Exposure Test conditions had no adverse effect on the TUT performance.
4. The Radiation Exposure Test results demonstrate that the Tricon V10 PLC will not experience failures due to normal and abnormal service conditions of gamma radiation exposure. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List.

2.2.3 Environmental Qualification

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

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

- The PLC under qualification shall meet its performance requirements during and following exposure to abnormal environmental conditions of 40°F to 140°F and 5% to 95% relative humidity (non-condensing) according to a time varying profile (see Figure 4-4 of EPRI TR-107330).
- Environmental testing shall be performed with the power supply sources set to values that maximize heat dissipation in the test PLC.

TRICONEX TOPICAL REPORT

- Power supplies shall be loaded such that nominal current draws at nominal power supply output voltages are equal to the power supply rating.
- The test PLC shall be powered with its TSAP operating during environmental testing, with half of the discrete and relay outputs ON and loaded to their rated current. In addition, all analog outputs shall be set to between 1/2 and 2/3 of full scale.

Section 4.3.6.2 of EPRI TR-107330 (Reference 2.5.5) requires that the generic PLC meet its performance requirements over abnormal environmental conditions of 40°F to 120°F and 10% to 95% relative humidity (non-condensing). Section 4.3.6.3 of EPRI TR-107330 (Reference 2.5.5) requires that the test PLC operate for the environmental (temperature and humidity) withstand profile given in Figure 4-4 of the TR. The profile includes a beginning ramp-up period (unspecified in duration) from ambient to 140°F and 90% relative humidity (non-condensing). These conditions are held for 48 hours minimum, after which the Operability and Prudency tests are run. Conditions are then ramped down over a four hour minimum period to 40°F and 5% relative humidity. These conditions are held for 8 hours minimum, after which a second Operability test is run. Conditions are then ramped up over a four hour minimum period to ambient temperature and relative humidity. The equipment is stabilized at ambient conditions, after which a final Operability test is run. Section 6.3.3 of EPRI TR-107330 (Reference 2.5.5) requires that Environmental Testing be performed with margins of 5°F and 5% applied to the temperature and humidity values given above.

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

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

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

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

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

TRICONEX TOPICAL REPORT

Conclusions from this test are as follows:

1. Environmental testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977.
2. The TUT met all applicable performance requirements during and after application of the environmental test conditions.
3. One digital output module fault occurred during environmental. The fault indication was cleared through the Enhanced Diagnostic Monitor (EnDM) and did not return for the remainder of the Environmental Test. Because of the fault tolerant design of the Tricon V10 PLC, the monitored digital output point of the module (Model 3623T) continued to perform as expected during the fault condition.
4. The environmental test results demonstrate that the Tricon V10 PLC will not experience failures due to abnormal service conditions of temperature and humidity. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List.

2.2.4 Seismic Qualification

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

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

Additional requirements include the following:

- The test PLC shall meet its performance requirements during and following the application of the SSE.
- The test PLC shall be mounted on a structure whose configuration meets the manufacturer's mounting requirements. The structure is required to be stiff enough so there are no resonances below 100 Hz.
- Seismic testing shall be performed with the power sources to the test PLC power supply modules set to operate at minimum AC and DC source voltages and frequencies

TRICONEX TOPICAL REPORT

- The test PLC shall be powered with its TSAP operating during seismic testing, with 1/2 of its solid-state discrete outputs ON and loaded to their rated current, 1/2 of its relay outputs ON, and 1/2 of its relay outputs OFF. In addition, 1/4 of its relay outputs shall transition from OFF to ON and 1/4 shall transition from ON to OFF during the OBE and SSE tests.
- The seismic test table shall be instrumented with a control accelerometer, and each chassis of the test PLC shall be instrumented with one or more response accelerometers located to establish maximum chassis accelerations.
- The test PLC shall operate as intended during and following the application of an SSE, all connections and parts shall remain intact and in-place, and relay output contacts shall not chatter.

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

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

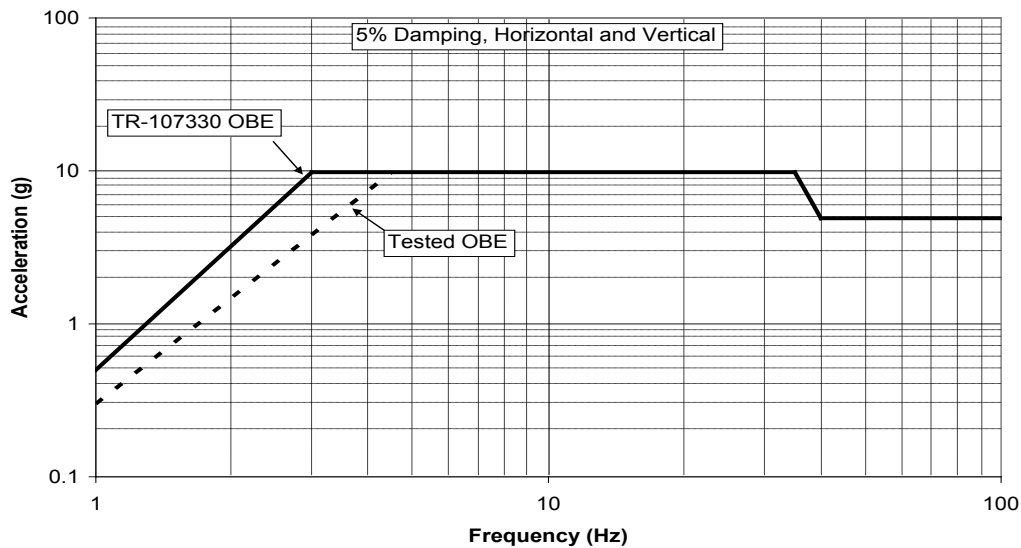
The seismic test acceptance criteria are as given below. These criteria were developed based on EPRI TR-107330, Section 4.3.9, and the Master Test Plan.

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

TRICONEX TOPICAL REPORT

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

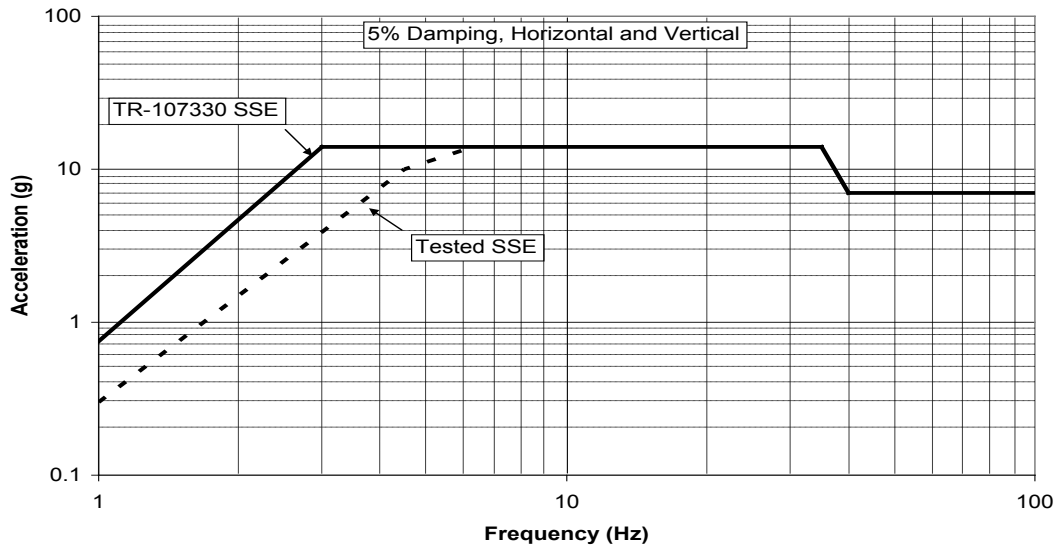
- Resonance search testing was performed as described in IEEE Standard 344, Section 7.1.4. The tests were performed to provide information on the dynamic response of the equipment mounted on the seismic test table. Over most of the 1 Hz to 10 Hz test frequency range, the accelerations experienced at the response accelerometer attachment points equaled or exceeded the acceleration applied to the seismic test table (as measured by the control accelerometers) in each of the three orthogonal directions.
- Five OBE tests and one SSE test were performed using the test response spectrum (TRS) which are shown in Figures 2-7 and 2-8.



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

Figure 2-7: OBE Test Acceleration

TRICONEX TOPICAL REPORT



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

Figure 2-8: SSE Test Acceleration

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

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

The results of the seismic test show that:

TRICONEX TOPICAL REPORT

1. Seismic testing of the TUT was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 344-1987.
2. The TUT met all applicable performance requirements during and after application of the seismic test vibration levels
3. Results of the Operability Test performed after Seismic Testing show that exposure to the Seismic Test conditions had no adverse effect on the TUT performance.
4. The seismic test results demonstrate that the Tricon PLC platform is suitable for qualification as Category 1 seismic equipment.
5. The horizontal and vertical seismic withstand response spectrum of the TUT as determined by testing is shown in Figures 2-7 and 2-8. The figures are based on a damping value of 5% used in the data analysis.
6. The seismic test results demonstrate that the equipment mounting configurations shown in Triconex Drawing No. 9600164-102 are adequate to support seismic qualification of the Tricon V10 PLC.
7. The manner in which the TUT chassis alarm relay contacts were monitored was determined to have the potential to mask contact chatter during Seismic Testing. Therefore, the TUT chassis alarm relays were not seismically qualified as part of Seismic Testing. It is important to note that these contacts do not provide a safety function.

2.2.5 Electromagnetic and Radio Frequency Interference Qualification

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

All of the TUT components were subjected to EMI/RFI testing as required.

EMI/RFI testing of the TUT was performed inside a shielded enclosure. The testing was performed in accordance with the EMI/RFI Test Procedure, Reference 2.5.54, and in accordance with the EPRI TR-107330 and NRC RG 1.180 test method requirements.

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

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

TRICONEX TOPICAL REPORT

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

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

The TUT was installed in the EMI/RFI chamber in open-frame racks as required by EPRI TR-107330. Wiring connections and grounding were in accordance with the manufacturer's recommendations. Additional EMI/RFI protective and mitigating devices such as power or I/O line filters, enclosed cabinets, and extra cable shielding were not used so that the specific emissions and susceptibilities of the equipment could be determined.

During EMI/RFI testing, the Tricon Test Specimen was powered with TSAP operating. The AC and DC power sources to the TUT chassis power supplies were set at nominal source voltage and frequency conditions. In order to minimize transmission of outside EMI/RFI sources into the EMI/RFI test chamber, all power, signal, and communications cables entering the EMI/RFI test chamber were passed through filters located in the chamber walls. Because the number of pass-through filters was limited, only one circuit per I/O module was connected. The specific configuration of the TUT is described in the EMI/RFI Test Procedure, Reference 2.5.54.

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

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

TRICONEX TOPICAL REPORT

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

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

Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) demonstrated operation as intended, including the following specific operational performance from Section 4.3.7 of EPRI TR-107330:

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

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

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

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

- 120 V ac Chassis Power Supply Line Lead. Conducted emission exceeded at:

179.7 Hz by 11.2 dB μ A	538.8 Hz by 8.9 dB μ A
299.8 Hz by 13.8 dB μ A	659.7 Hz by 2.1 dB μ A
419.7 Hz by 13.0 dB μ A	899.6 Hz by 1.5 dB μ A
- 120 V ac Chassis Power Supply Neutral Lead. Conducted emission exceeded at:

179.9 Hz by 11.0 dB μ A	539.7 Hz by 9.6 dB μ A
299.8 Hz by 14.9 dB μ A	659.9 Hz by 2.8 dB μ A
419.3 Hz by 13.1 dB μ A	

TRICONEX TOPICAL REPORT

- 230 V ac Chassis Power Supply Line Lead. Conducted emission exceeded at:
179.9 Hz by 4.0 dB μ A 539.7 Hz by 7.6 dB μ A
299.8 Hz by 8.3 dB μ A 659.7 Hz by 6.0 dB μ A
419.7 Hz by 8.7 dB μ A 779.6 Hz by 1.7 dB μ A
- 230 V ac Chassis Power Supply Neutral Lead. Conducted emission exceeded at:
179.9 Hz by 3.8 dB μ A 539.7 Hz by 7.5 dB μ A
299.8 Hz by 8.2 dB μ A 659.7 Hz by 5.9 dB μ A
419.7 Hz by 8.6 dB μ A 779.6 Hz by 1.6 dB μ A

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

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

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

The TUT discrete and analog input/output hardware does not fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for the EMI/RFI susceptibility tests as listed below:

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

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

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

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

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

TRICONEX TOPICAL REPORT

2.2.6 Electrical Fast Transient

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

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

As described in the EFT Test Procedure, Reference 2.5.73, the TUT was subjected to the following EFT tests:

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

The EFT test acceptance criteria are based on Appendix 8 of the Master Test Plan, Reference 2.5.38, and EPRI TR-107330, Section 4.3.7, Reference 2.5.5:, which require:

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

IEC 61000-4-4: Power Leads, Level 3 Test Voltage Level: 2 kV max.

IEC 61000-4-4: Signal Leads, Level 2 Test Voltage Level: 1 kV max.

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

TRICONEX TOPICAL REPORT

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

During EFT testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during, and after each test to verify normal operation of the system and all peripheral communication interfaces. Results of the EFT testing are described in the EFT Test Report, Reference 2.5.77. Data collected during and after each voltage test demonstrate that the TUT operated as intended throughout the testing.

Conclusions from this test are as follows:

1. EFT Testing of the TUT was performed in accordance with the applicable requirements of NRC Regulatory Guide 1.180, Rev. 1 and IEC 61000-4-4. The following EFT tests were performed:
 - 120 V ac Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
 - 230 V ac Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
 - 24 V dc Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
 - Peripheral Communications Cables: ± 0.5 kV and ± 1.0 kV
 - ETA Input Power Wires: ± 0.5 kV and ± 1.0 kV
 - Analog Input/Output Wires: ± 0.5 kV and ± 1.0 kV
 - RTD, T/C, and Pulse Input Wires: ± 0.5 kV and ± 1.0 kV
 - Discrete Input/Output Wires: ± 0.5 kV and ± 1.0 kV
2. The TUT met all applicable operational and performance requirements during and after each application of the EFT Tests voltages.
3. The EFT Test results demonstrate that the Tricon V10 PLC will not experience operational failures or susceptibilities due to exposure to repetitive electrical fast transients on the power and signal input/output leads. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List.

2.2.7 Surge Withstand

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

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

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

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

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

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

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

The surge withstand testing was performed at National Technical Systems in Boxborough, Massachusetts. Prior to the start of testing, all of the TUT modules (Main Processors (MPs), communication, and input/output) were removed and replaced with spare modules. This was done to protect the modules which had been through environmental, seismic, and EMI/RFI testing from damage that could occur during surge withstand testing, and preserve the condition of the original modules for final performance proof testing. Change-out of the modules was appropriate because surge withstand tests are design tests as opposed to conditioning (or aging) tests and therefore do not have to be performed on aged hardware.

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

TRICONEX TOPICAL REPORT

Operation of TUT was monitored by the DAS. The recorded data was evaluated in detail before, during, and after each test to verify normal operation of the system and all peripheral communication interfaces. The test details are described in the Surge Withstand Test Report, Reference 2.5.59. Data collected during and after each surge withstand test demonstrates that the TUT operated as intended throughout the testing.

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

- Applying the surge test voltages to the specified test points shall not damage any other module or device in the TUT, or cause disruption of the operation of the TUT backplane signals or any other signals that could result in a loss of the ability to generate a trip. Evaluation of normal operating performance data (inputs, outputs, and diagnostic indicators) shall demonstrate satisfactory operation of the Tricon Test Specimen following application of the surge test voltage. Per Section 6.3.5 of TR-107330, failures of one or more redundant devices are acceptable so long as the failures do not result in the inability of the Tricon Test Specimen to operate as intended.

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

1. Surge withstand testing of the Tricon Test Specimen was performed in accordance with the applicable requirements of the IEC 61000-4-5 and IEC 61000-4-12 test methods. The following Surge Withstand tests were performed:

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

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

TRICONEX TOPICAL REPORT

IEC 61000-4-12 Ring Wave: ± 2.0 kV

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

IEC 61000-4-12 Ring Wave: ± 1.0 kV

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

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

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

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

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

TRICONEX TOPICAL REPORT

2. In all cases, the Tricon Test Specimen continued to operate in accordance with the test acceptance criteria following application of the surge test voltages with no damage to components.
3. The Surge Withstand Test results demonstrate that the Tricon V10 PLC will not experience operational failures or susceptibilities that could result in a loss of the ability to generate a trip due to exposure to Ring Wave and Combination Wave electrical surges to the components listed above. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List.

2.2.8 Electrostatic Discharge

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

EPRI TR-107330, Section 4.3.8, requires that the PLC under qualification be tested for immunity to the ESD test levels specified in EPRI TR-102323-R1, Reference 2.5.6. ESD Testing of the TUT was performed in accordance with IEC 61000-4-2, using the test levels defined in EPRI TR-102323-R1, Appendix B, Section 3.5.

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

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

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

TRICONEX TOPICAL REPORT

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

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

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

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

The ESD test acceptance criteria are as follows, based on Appendix 8 of the Master Test Plan, Reference 2.5.38, and EPRI TR-107330, Section 4.3.7 and 4.3.8, Reference 2.5.5:

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

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

IEC 61000-4-2: Contact Discharges Test Voltage Level: ± 8 kV max.

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

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

TRICONEX TOPICAL REPORT

During ESD testing, operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during, and after each test to verify normal operation of the system and all peripheral communication interfaces. Results of the ESD testing are described in the ESD Test Report, Reference 2.5.78. 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. ESD Testing of the TUT was performed in accordance with the applicable requirements of EPRI TR-102323-R1, Appendix B, Section 3.5 and IEC 41000-4-2. The following ESD tests were performed:

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

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

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

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

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

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

2. The TUT met all applicable operational and performance requirements during and after each application of the ESD Tests voltages.
3. The ESD Test results demonstrate that the Tricon V10 PLC will not experience operational failures or susceptibilities due to exposure to electrostatic discharges to the components listed above. The main processors continued to function. The transfer of I/O was not interrupted. The TCM Peer-to-Peer and MODBUS data links continued to operate correctly.

TRICONEX TOPICAL REPORT

2.2.9 Class 1E to Non-1E Isolation

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

The qualification of the Tricon V10 PLC is based on a system design that connects Non-1E input/output circuits to modules installed in one or more separate chassis which are interfaced to the Class 1E portion of the PLC by fiber optic cables. This design provides electrical isolation of the Non-1E input/output circuits because the fiber optic cables are incapable of transmitting electrical faults. Based on this system design, only the communication modules installed in the main chassis are required to provide Class 1E to Non-1E electrical isolation capability (if these module are used to interface to Non-1E communication equipment). Accordingly, the TCM Module, RS-232 (MODBUS) was tested for Class 1E isolation capability.

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

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

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

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

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

Operation of the TUT was monitored by the DAS. The recorded data was evaluated in detail before, during and after each isolation test to verify normal operation of the system and all

TRICONEX TOPICAL REPORT

peripheral communication interfaces. The test details are described in the Isolation Test Report, Reference 2.5.60.

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

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

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

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

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

The testing demonstrated electrical isolation capability of the communication ports to applied voltages of 250 V ac (at 10 amps maximum) and 250 V dc (at 5 amps maximum) for 30 seconds. The fiber optic module is considered an acceptable Class 1E to Non-1E isolation device by design, and was not tested.

4. The Class 1E to Non-1E isolation test results demonstrate that the Tricon PLC relay output module Model 3636T provides adequate electrical isolation per IEEE Standard 384-1981 between the safety related portions of the Tricon and connected non-safety related field circuits. The testing demonstrated electrical isolation capability of the relay output points to applied voltages of 600 Vac (at 5 amps maximum) and 250 Vdc (at 10 amps maximum).

TRICONEX TOPICAL REPORT

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

2.2.10 Performance Proof Testing

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

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

1. Analog Input/Output Module Accuracy – For all Operability Test runs, the accuracy of each analog input/output module was demonstrated to meet the published Triconex product specifications. In addition, the test results show no degradation in module accuracy from pre-qualification testing throughout qualification and performance proof testing.
2. Response Time – Response times for digital input to digital output, analog input to digital output, and "round robin" sequences of the TUT were measured during all runs of the Operability Test procedure. Triconex provides a method for calculating the maximum expected digital input to digital output, analog input to digital output, and analog output and "round-robin" response time for a specific Tricon hardware configuration and application

TRICONEX TOPICAL REPORT

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

3. Discrete Input Operation – For all Operability Test runs, the OFF to ON and ON to OFF voltage switching levels of each digital input module were demonstrated to meet the published Triconex product specifications. In addition, the test results show no degradation in discrete input module voltage switching levels from pre-qualification testing throughout qualification and performance proof testing.
4. Discrete Output Operation – For all Operability Test runs, each discrete output module was demonstrated to operate ON and OFF at the manufacturer’s published product specifications for maximum operating current, and minimum and maximum operating voltage. In addition, the test results show no degradation in operation of the discrete output modules from pre-qualification testing throughout qualification and performance proof testing.
5. Timer Function Accuracy – For all Operability Test runs, the time out periods of the application program timer functions were demonstrated to not vary from the measured pre-qualification baseline time-out periods by more than the greater of $\pm 1\%$ of the time out period or three application program scan cycles. In addition, the test results show no degradation in timer function variation from pre-qualification testing throughout qualification and performance proof testing.
6. Failover Performance – Tests were done to demonstrate automatic failover to redundant components on simulated failures of a main processor module, an RXM module, a chassis expansion port cable, and chassis power supplies. All test results demonstrated acceptable failover operation of the TUT.
7. Loss of Power Performance / Failure to Complete a Scan Detection – Each run of the Operability Test procedure included tests to demonstrate performance of the TUT on loss and restoration of power to the chassis power supplies. The test results demonstrated predictable and consistent response of the TUT to a loss of power. The test results also demonstrated predictable and consistent response of the TUT on recovery of power. In addition, successful restart of the TUT on restoration of power consistently indicated proper functioning of the watchdog timer mechanisms.
8. Power Interrupt Performance – Each run of the Operability Test procedure included tests to demonstrate power hold-up time performance of the Tricon PLC chassis power supplies on an interruption of source power for approximately 40 milliseconds. The test results demonstrated:
 - The 120 V ac and 230 V ac chassis power supplies meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 milliseconds when installed as the only

TRICONEX TOPICAL REPORT

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

- The 24 V dc chassis power supplies do not meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 milliseconds. The measured hold-up time capability of the 24 VDC chassis power supplies was less than 3 milliseconds.
9. Power Quality Tolerance – Tests to demonstrate tolerance of the Tricon V10 PLC power supplies to changes in the quality (voltage and frequency) of AC and DC source power were performed. Tests were performed over the manufacturer's allowable ranges of voltage and frequency for each type of power supply included in the testing. All test results demonstrated acceptable performance of the TUT. In addition, power quality tolerance tests demonstrated acceptable performance of processor memory writes prior to Tricon reset on gradual loss of source power voltage.
 10. Burst of Events Performance – Burst of Events testing demonstrated the ability of the PLC to process rapidly changing input and output signals based on the control logic of the TSAP.
 11. Communication Port Failure Performance – Communication port failure testing demonstrated no effect on digital input to digital output and analog input to analog output response times during simulated failures of communication lines connected to communication ports on the TCM.

2.2.11 Failure Modes and Effects Analysis

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

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

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

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

TRICONEX TOPICAL REPORT

components considered include the following:

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

The approach used in the FMEA was to postulate credible failures of these components, identify the mechanisms that could cause these failures, and evaluate the consequences of these failures on the operation of the Tricon system. Because of the architecture of the Tricon, failure mechanisms that affect a single leg of the triple redundant system generally have no effect on system operation. Therefore, the FMEA also considers (1) failure mechanisms that are recognized as being highly unlikely but that could affect multiple components, and (2) the coincident occurrence of otherwise single failures (i.e., multiple failures).

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

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

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

2.2.12 Reliability and Availability Analysis

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

TRICONEX TOPICAL REPORT

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

For the Tricon analysis, the two probabilities calculated include: (1) the probability that the system will fail in a given period of time (reliability), and (2) the probability that the system will fail on demand in a given period of time (availability). As required by the EPRI TR, the analysis was performed with the assumption that periodic testing of the system will uncover faults that are not normally detected by the system. As the periodic test interval is lengthened, the probability of failure increases. Calculations were done for periodic test intervals ranging from 6 to 30 months. In all cases, the calculated reliability and availability were greater than 99.9%, which exceeds the recommended goal of 99.0% from the EPRI TR. For a periodic test interval of 18 months (corresponding to the typical nuclear power plant refueling outage cycle), the reliability is 99.9987% and the availability is 99.9990%.

2.2.13 Cable Similarity Analysis

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

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

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

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

2.2.14 System Accuracy Specifications

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

The design of the Tricon enables it to maintain its rated reference accuracy specifications indefinitely. If the rated reference accuracy specifications are not met, the system will generate an alarm and the faulted module will be indicated. Response to the alarm would require replacement of the faulted module and restoration of normal operation. No field adjustments or

TRICONEX TOPICAL REPORT

calibrations of the Tricon are required or possible. The key in the Tricon design is its TMR architecture. By performing continuous cross comparisons between the triplicated values, a true and full verification of actual input and output values is maintained.

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

2.2.15 Component Aging Analysis

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

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

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

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

2.3 SOFTWARE QUALIFICATION

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

2.3.1 Software Documentation

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

TRICONEX TOPICAL REPORT

2.3.2 Software Development Process

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

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

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

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

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

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

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

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

2.3.3 Software Verification and Validation Process

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

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

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

TRICONEX TOPICAL REPORT

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

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

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

2.3.4 Safety Analysis

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

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

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

2.3.5 Configuration Management and Error Notification

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

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

TRICONEX TOPICAL REPORT

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

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

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

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

2.4 SYSTEM APPLICATION

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

TRICONEX TOPICAL REPORT

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

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

TRICONEX TOPICAL REPORT

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

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS	COMPLIANCE	COMMENTS
5.3.B	<p>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.</p>	Exception	<p>Based on Tricon design, it is not practicable to perform a test that provides consistent (within $\pm 20\%$) 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.</p>
5.3.E	<p>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.</p>	Partial Exception	<p>The TCM Module NET1 port and NET2 ports are included in the qualification envelope. Test equipment to measure degradation of bit rates, pulse shapes, and signal levels was not available at the time testing was performed. The port protocol is proprietary and not amenable to TR specified tests. Port operation is monitored for correct performance throughout all qualification tests.</p>

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

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

TRICONEX TOPICAL REPORT

2.5 REFERENCES

- 2.5.1 NUREG-800; Standard Review Plan, Section 7.0, "Instrumentation and Controls – Overview of Review Process," Rev. 5, March 2007
- 2.5.2 NUREG/CR-6241, "Using Commercial-Off-the-Shelf (COTS) Software in High-Consequence Safety Systems," November 10, 1995
- 2.5.3 NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," October 1997
- 2.5.4 U.S. Nuclear Regulatory Commission Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," October 2003
- 2.5.5 EPRI Report, TR-107330, "Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants"
- 2.5.6 EPRI Report TR-102323-R1, "Guidelines for Electromagnetic Interference Testing in Power Plants"
- 2.5.7 IEEE Std. 323-1983, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
- 2.5.8 IEEE Std. 344-1987, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
- 2.5.9 IEEE Std. 381-1977, "Standard Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations"
- 2.5.10 IEEE Std. 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits"
- 2.5.11 IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
- 2.5.12 IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation Plans"
- 2.5.13 IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
- 2.5.14 IEC 61000-4-2 "Electromagnetic Compatibility (EMC), Part 4-2: Testing and Measurement Techniques, Electrostatic Discharge Immunity Test," April 2001

TRICONEX TOPICAL REPORT

- 2.5.15** IEC 61000-4-3, “Electromagnetic Compatibility (EMC), Part 4-3: Testing and Measurement Techniques, Radiated, Radio-Frequency, Electromagnetic Field Immunity Test,” September 2002
- 2.5.16** IEC 61000-4-4, “Electromagnetic Compatibility (EMC), Part 4-4: Testing and Measurement Techniques, Electrical Fast Transient/Burst Immunity Test,” 2004
- 2.5.17** IEC 61000-4-5, “Electromagnetic Compatibility (EMC), Part 4-5: Testing and Measurement Techniques, Surge Immunity Test,” April 2001
- 2.5.18** IEC 61000-4-6, “Electromagnetic Compatibility (EMC), Part 4-6: Testing and Measurement Techniques, Immunity to Conducted Disturbances, Induced by Radio-Frequency Fields,” November 2004
- 2.5.19** IEC 61000-4-8, “Electromagnetic Compatibility (EMC), Part 4-8: Testing and Measurement Techniques, Power Frequency Magnetic Field Immunity Test,” March 2001
- 2.5.20** IEC 61000-4-9, “Electromagnetic Compatibility (EMC), Part 4-9: Testing and Measurement Techniques, Pulse Magnetic Field Immunity Test,” March 2001
- 2.5.21** IEC 61000-4-10, “Electromagnetic Compatibility (EMC), Part 4-10: Testing and Measurement Techniques, Damped Oscillatory Magnetic Field Immunity Test,” March 2001
- 2.5.22** IEC 61000-4-12, “Electromagnetic Compatibility (EMC), Part 4-12: Testing and Measurement Techniques, Oscillatory Waves Immunity Test,” April 2001
- 2.5.23** IEC 61000-4-13, “Electromagnetic Compatibility (EMC), Part 4-13: Testing and Measurement Techniques, Harmonics and Interharmonics Including Mains Signaling at A.C. Power Port, Low Frequency Immunity Tests,” March 2002
- 2.5.24** IEC 61000-4-16, “Electromagnetic Compatibility (EMC), Part 4-16: Testing and Measurement Techniques, Test for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz,” July 2002
- 2.5.25** IEC 61784-3, “Industrial Process Measurement and Control – Digital Communications,” July 2005

TRICONEX DOCUMENTS

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

TRICONEX TOPICAL REPORT

- 2.5.29 Tricon Product Guide, Triconex Document No. 9791007-013
- 2.5.30 Tricon Planning and Installation Guide, Triconex Document No. 9720077-008
- 2.5.31 Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System, Invensys Document No. NTX-SER-09-05
- 2.5.32 Triconex Development Processes for PLDs in Nuclear Qualified Products, Invensys Document No. NTX-SER-09-06
- 2.5.33 Nuclear System Integration Program Manual, Invensys Document No. NTX—SER-09-021
- 2.5.34 **Tricon V10 Conformance to Regulatory Guide 1.152, Invensys Document No. NTX-SER-10-14**
- 2.5.35 Tricon Applications in Nuclear Reactor Protection Systems – Compliance with NRC ISG-2 and ISG-4, Invensys Document No. NTX-SER-09-10
- 2.5.36 Safety Evaluation Report (SER) Maintenance Process, Invensys Document No. NTX-SER-09-20

TRICONEX NUCLEAR QUALIFICATION PROJECT DOCUMENTS

- 2.5.37 Triconex Nuclear Qualification Quality Plan, Triconex Document No. 9600164--002.
- 2.5.38 Master Test Plan, Triconex Document No. 9600164-500
- 2.5.39 Master Configuration List, Triconex Document No. 9600164-540
- 2.5.40 Software QA Plan, Triconex Document No. 9600164-537
- 2.5.41 Tricon System Description, Triconex Document No. 9600164-541
- 2.5.42 Equipment Qualification Summary Report, Triconex Document No.. 9600164--545
- 2.5.43 Function Diagrams, Triconex Drawing Nos. 9600164-500 to 515
- 2.5.44 Wiring Schedule, Triconex Drawing No. 9600164-700
- 2.5.45 Test System Wiring Drawings, Triconex Drawing Nos. 9600164-100 to 300
- 2.5.46 Setup and Checkout Test Procedure, Triconex Document No. 9600164-502
- 2.5.47 Operability Test Procedure, Triconex Document No. 9600164-503
- 2.5.48 Prudency Test Procedure, Triconex Document No. 9600164-504

TRICONEX TOPICAL REPORT

- 2.5.49 Radiation Test Procedure, Triconex Document No. 9600164-511
- 2.5.50 Environmental Test Procedure, Triconex Document No. 9600164-506
- 2.5.51 Seismic Test Procedure, Triconex Document No. 9600164-507
- 2.5.52 Surge Withstand Test Procedure, Triconex Document No. 9600164-508
- 2.5.53 Class 1E to Non-1E Isolation Test Procedure, Triconex Document No. 9600164-509
- 2.5.54 EMI/RFI Test Procedure, Triconex Document No. 9600164-510
- 2.5.55 Pre-qualification Operability Test Report, Triconex Document No. 9600164-560
- 2.5.56 Environmental Test Report, Triconex Document No. 9600164-525
- 2.5.57 Seismic Test Report, Triconex Document No. 9600164-526
- 2.5.58 EMI/RFI Test Report, Triconex Document No. 9600164-527
- 2.5.59 Surge Test Report, Triconex Document No. 9600164-528
- 2.5.60 Class 1E to Non-1E Isolation Test Report, Triconex Document No. 9600164-529
- 2.5.61 Performance Proof Operability Test Report, Triconex Document No. 9600164-566
- 2.5.62 Reliability/Availability Study for Tricon PLC Controller, Triconex Document No. 9600164-532
- 2.5.63 Failure Modes and Effects Analysis (FEMA) for TRICON V10 PLC, Triconex Document No. 9600164-531
- 2.5.64 Tricon System Accuracy Specifications, Triconex Document No. 9600164-534
- 2.5.65 Software Qualification Report, Triconex Document No. 9600164-535
- 2.5.66 TSAP Software Requirements Specification, Triconex Document No. 9600164-517
- 2.5.67 TSAP Software Design Description, Triconex Document No. 9600164-518
- 2.5.68 TSAP Software V&V Plan, Triconex Document No. 9600164-513
- 2.5.69 TSAP Final V&V Report, Triconex Document No. 9600164-537
- 2.5.70 Software Traceability Analysis, Triconex Document No. 9600164-720

TRICONEX TOPICAL REPORT

- 2.5.71** TÜV-Rheinland Microelectronic and Process Automation, “Type Approval for the Tricon Triple Modular Redundant (TMR) Controller Tricon,” Report No. 945/EL 336/91, April 19, 1991
- 2.5.72** TÜV-Rheinland Microelectronic and Process Automation, “Type Approval of TriconVersion10.2.1,” Report No. 968/EZ 105.06/06, October 31, 2006
- 2.5.73** EFT Test Procedure, Triconex Document No. 9600164-514
- 2.5.74** ESD Test Procedure, Triconex Document No. 9600164-512
- 2.5.75** Pre-Qualification Prudency Test Report, Triconex Document No. 9600164-670
- 2.5.76** Radiation Test Report, Triconex Document No. 9600164-533
- 2.5.77** EFT Test Report, Triconex Document No. 9600164-521
- 2.5.78** ESD Test Report, Triconex Document No. 9600164-522
- 2.5.79** Performance Proof Prudency Test Report, Triconex Document No. 9600164-573
- 2.5.80** Critical Digital Review, Triconex Document No. 9600164-539
- 2.5.81** Cable Similarity Analysis, Triconex Document No. 9600164-538

TRICONEX TOPICAL REPORT

3.0 DIFFERENCES BETWEEN V9.5.3 AND V10.2.1 SYSTEMS

3.1 BACKGROUND

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

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

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

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

Upgraded/redesignated versions of existing modules:

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

Miscellaneous support hardware units added:

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

TRICONEX TOPICAL REPORT

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

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

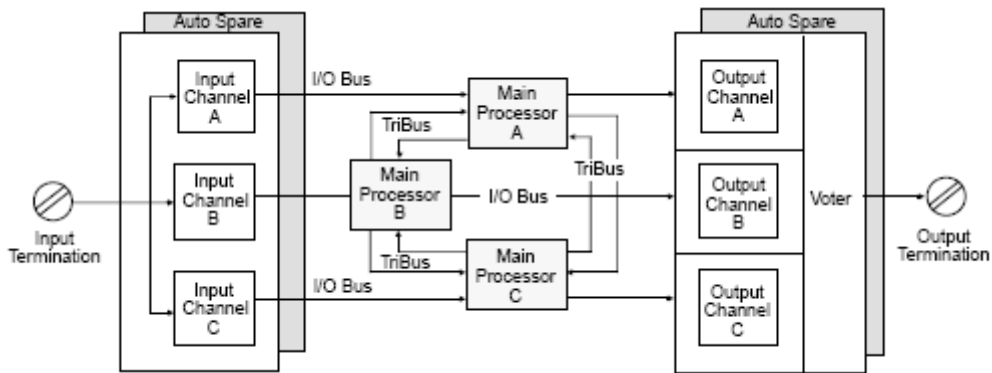


Figure 3-1: Triple Modular Redundant (TMR) architecture

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

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

3.3 COMPARISON OF V9/V10 DIFFERENCES

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

TRICONEX TOPICAL REPORT

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

Table 3-1 Hardware

Module	Tricon V9.5.3 System	Tricon V10.2.1 System
Main Processor	3006N Hardware floating point processor	3008N Embedded floating point software
Communication Module	Three modules: <ul style="list-style-type: none"> ▪ 4119AN (EICM) ▪ 4329N (NCM) ▪ 4609N (ACM) 	One module: <ul style="list-style-type: none"> ▪ 4352AN (TCM) Fiber Optic
I/O Modules Analog Input (AI)	3700AN (0-5 VDC)	3721N (0-5 or -5 to +5 VDC, Differential) Next Generation Module,
	3701N (0-10 VDC) – Through Hole	3701N2 (0-10 VDC) - SMT
	3510N (Pulse Input)	3511N (Pulse Input) – Faster Input Scan
	3703EN (Isolated)	Same
	3708EN (ITC)	Same
	3704EN (0-5/0-10 VDC, High Density)	Removed
	3706AN (NITC)	Removed
I/O Modules Analog Output (AO)	3805EN (4-20 mA)	3805HN (4-20 mA) – Supports increased inductive loads
I/O Modules Digital Input (DI)	3501TN 115V AC/DC – Through Hole	3501TN2 115V AC/DC – SMT
	3502EN 48V AC/DC – Through Hole	3502EN2 48V AC/DC – SMT
	3503EN 24V AC/DC – Through Hole	3503EN2 24V AC/DC – SMT
	3504EN 24/48 VDC – Through Hole	Removed
	3505EN 24 VDC – Through Hole	Removed
I/O Modules Digital Output (DO)	3604EN 24 VDC 3624N 24 VDC, Supervised	3625N 24 VDC, Supervised/ Unsupervised Next Generation Module
	3601TN 115 VAC	Same
	3603TN 120 VDC	Same
	3607EN 48 VDC	Same
	3623TN 120 VDC, Supervised	Same
	3636TN (Relay Output)	Same

TRICONEX TOPICAL REPORT

Table 3-1 Hardware

Module	Tricon V9.5.3 System	Tricon V10.2.1 System
Remote Extender Modules: Primary Remote	4210N (Single Mode Fiber Optic cable) 4211N (Single Mode Fiber Optic	4200N (Multi Mode Fiber Optic cable) 4201N (Multi Mode Fiber
I/O Module Term Panels	Version 8 Term Panels Version 9 Term Panels (various)	Removed Additional Version 9 Term Panels to support new I/O modules
Signal Conditioners	<ul style="list-style-type: none"> ▪ Signal Conditioner (-100 to 100 °C) Pt (7B34-01-1) ▪ Signal Conditioner (0 to 100 °C) Pt (7B34-02-1) ▪ Signal Conditioner (0 to 200 °C) Pt (7B34-03-1) ▪ Signal Conditioner (0 to 600 °C) Pt (7B34-04-1) 	Same
	Not included	Four additional Signal Conditioners: <ul style="list-style-type: none"> ▪ Signal Conditioner (0 to 200 °C) Pt (7B34-CUSTOM) ▪ Signal Conditioner (0 to 600 °C) Pt (7B34-CUSTOM) ▪ Signal Conditioner (0 to 100 mV) (7B30-02-1) ▪ Signal Conditioner (0 to 120 °C) Cu (7B14-C-02-1)
Power Supplies: 120 V 24 VDC 230 VAC	ASTEC Power Modules 8310N 8311N	Alternate Vicor Power Modules 8310N2 8311N2 8312N2
Chassis: Main Expansion Remote Expansion	8110N 8111N 8112N	8110N2 8111N 8112N

TRICONEX TOPICAL REPORT

Table 3-2 Software

Module	Tricon V9.5.3 System Software Version	Tricon V10.2.1 System Software Version
TriStation 1131 Developer's Workbench <i>(Application Development Software)</i>	V3.1	V4.1.437
Main Processor Software:		
Application Processor	TSX 5211	ETSX 6198 (Build 92)
I/O Processor	IOC 5212	IOCCOM 6054 (Build 92)
COM Processor	COM 5206	
Communication Module Software:		
TCM	Not Applicable	TCM 6136 (Build 92)
Common V9.5.3 COM	ICM 4930	Not Applicable
EICM	IICX 5276	Not Applicable
NCM	NCMX 5028	Not Applicable
ACM	ACMX 5203	Not Applicable
I/O Module Software		
AI 3721N	Not Applicable	AI 6200 (Build 92)
DO 3625N	Not Applicable	DO 6213 (Build 92)
AI 3701N/N2	AI/NITC 4873	AI/NITC 5661
IAI 3703EN	EIAI/ITC 5491	EIAI/ITC 5916
ITC 3708EN	EIAI/ITC 5491	EIAI/ITC 5916
PI 3510N	PI 4559	Not Applicable
PI 3511N	Not Applicable	PI 5647
AO 3805EN/HN	EAO 5595	EAO 5897
DI 3501TN/TN2		
DI 3502EN /EN2	EDI 5490	EDI 5909
DI 3503EN/EN2		
DI 3505EN	EDI 5490	Not Applicable
DI 3504EN	HDI 5499	
AI 3704EN	HDI 5499	
DO 3601TN		
DO 3607EN	EDO 5488	EDO 5781
DO 3604EN	EDO 5488	Not Applicable
RO 3636TN	ERO 5497	ERO 5777
DO 3603TN	TSDO 5502	Same
DO 3623TN	TSDO 5502	TSDO2 5940
DO 3624N	TSDO 5502	Not Applicable
Remote Extender Modules	RXM 3310	Same

TRICONEX TOPICAL REPORT

4.0 TRICON V10.5.1 UPGRADE

4.1 INTRODUCTION

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

The focus of the qualification effort was Tricon product version V10.2.1, and TriStation V4.1.437, which were the prevailing versions being marketed at the time the qualification project was being organized. As with any high-tech product, during the extended period of qualification testing and evaluation, the Tricon products continued to evolve such that upgraded versions beyond V10.2.1 and V4.1.437 are now being manufactured and provided to industry. For business reasons, it is now desired to obtain NRC approval of the current Tricon product offering, specifically Tricon V10.5.1 and its associated support software.

4.2 PURPOSE

All data pertaining to testing and analysis of Tricon V10.2.1 have been provided to the NRC for review. The purpose of this Section of the report is to provide a listing of any pertinent differences between the V10.2.1 product discussed in section 2.0 and the current product upgrades (represented by V10.5.1). A discussion of impact to qualification testing already completed is also provided. This additional information is provided for the NRC’s consideration for inclusion in the SER approval.

4.3 DISCUSSION

No new hardware modules have been added since V10.2.1, i.e., the module listings and hardware descriptions applicable to V10.5.1 are the same as in section 2.1.4 of this report. Routine component and board changes to maintain production needs are ongoing and are reviewed by the Configuration Control Board (CCB) in accordance with Triconex Appendix B QA procedures. This review confirms that no significant changes have been made to modules or which would adversely affect performance specifications or qualification characteristics (e.g. seismic, environmental, electrical, etc.) as specified in EPRI TR 107330.

V10.5.1 essentially represents the further evolutionary upgrades and bug fixes made to platform software since V10.2.1 was released. Triconex document NTX-SER-09-05 (Reference 2.5.31)

TRICONEX TOPICAL REPORT

provides a development tree and table showing the stepwise progression of platform change releases between V9.5.3 and V10.2.1. Figure 4-1 provides an update to this platform history to reflect the further progression of operating software from V10.2.1 to V10.5.1. Table 4-1 shows the software differences between V10.2.1 and subsequently issued Versions (V10.2.2, V10.2.4, **V10.5**, and V10.5.1) that have been evaluated and qualified for nuclear use (placed on the NQEL) in accordance with Triconex QA procedures. As seen in Table 4-1, there are five software modules in V10.5.1 that are different from the modules qualified for the V10.2.1 release, i.e.:

ETSX 6271 (versus ETSX 6198)
TCM 6276 (versus TCM 6136)
AI 6256 (versus AI 5661)
DO 6255 (versus DO 6213)
TSDO/HVDO 6273 (versus TSDO 5502)

The interim revisions between V10.2.1 and V10.5.1 (i.e., V10.3, V10.4, V10.4.1, and V10.4.2) in the development tree shown in Figure 4-1 have not been released for use in nuclear modules. However, any changes in these releases affecting V10.5.1 operating software modules were reviewed to assure that these revisions had no negative impact on V10.5.1 software integrity. A discussion of each of these interim (non-nuclear) releases is provided in Section 4.3.1.5.

In addition, the TriStation 1131 programming software revision level for Tricon V10.5.1 is different (**currently at TriStation 1131 V4.7.0**). **Associated supporting software continues to evolve to address platform changes and maintenance issues. Qualification** evaluations have determined that the routine product upgrades have not altered the critical characteristics of the product, i.e., current modules have the same functional and environmental characteristics as the V10.2.1 Test Specimen (or better).

TRICONEX TOPICAL REPORT

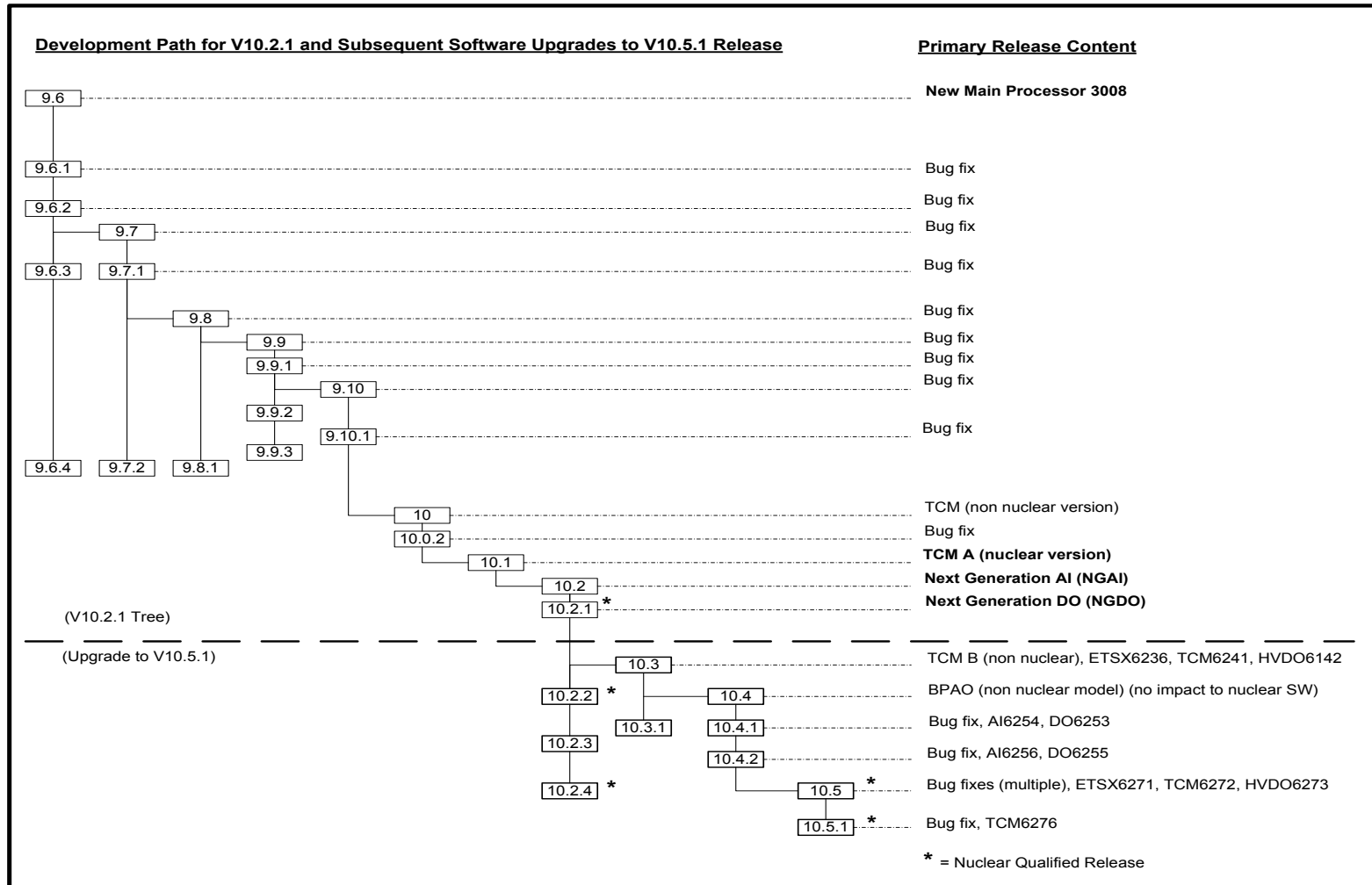


Figure 4-1: V10.2.1 to V10.5.1 Software Development Tree – Evolutionary Changes

TRICONEX TOPICAL REPORT

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

TYPE	IDENTIFICATION	VERSION (for V10.2.1)	VERSION (for V10.2.2)	VERSION (for V10.2.4)	VERSION (for V10.5)	VERSION (for V10.5.1)	USED IN
Main Processors	ETSX	6198	6198	6198	6271	6271*	3008N
	IOCCOM	6054	6054	6054	6054	6054	3008N
Communication Module	TCM	6136	6136	6136	6272	6276*	4352AN
I/O Modules	AI/NITC	5661	5661	5661	5661	5661	3701N2
	EIAI/ITC	5916	5916	5916	5916	5916	3703EN(AI), 3708EN (TC)
	AI	6200	6200	6256	6256*	6256*	3721N
	DO	6213	6213	6255	6255*	6255*	3625N
	PI	5647	5647	5647	5647	5647	3511N
	EDI	5909	5909	5909	5909	5909	3501TN2, 3502EN2, 3503EN2
	EAO	5897	5897	5897	5897	5897	3805HN
	EDO	5781	5781	5781	5781	5781	3601TN, 3607EN
	ERO	5777	5777	5777	5777	5777	3636TN
	TSDO/HVDO	5502	6142	6142	6273	6273*	3603TN
	TSDO2	5940	5940	5940	5940	5940	3623TN
	RXM	3310	3310	3310	3310	3310	4200N, 4201N
Application Program Development Software	TriStation 1131, Developer's Workbench Suite	4.1.437	4.1.437	4.1.437	4.6.134	4.7.0*	TriStation Workstation
(Bold=new revision released; * = V10.5.1 Software different from V10.2.1)							

TRICONEX TOPICAL REPORT

4.3.1 Tricon Firmware Changes

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

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

4.3.1.1.1 Detailed Review of Changes

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

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

4.3.1.1.2 Impact of Differences on Tricon Qualification

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

4.3.1.1.3 Conclusion

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

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

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

TRICONEX TOPICAL REPORT

4.3.1.1.4 References

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

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

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

4.3.1.2.1 Detailed Review of Changes

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

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

4.3.1.2.2 Impact of Differences on Tricon Qualification

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

TRICONEX TOPICAL REPORT

4.3.1.2.3 Conclusion

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

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

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

4.3.1.2.4 References

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

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

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

4.3.1.3.1 Detailed Review of Changes

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

TRICONEX TOPICAL REPORT

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

Table 4-2: Affected Firmware Releases

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

ETSX 6271, TCM 6272, TSDO/HVDO 6273

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

Reference documents:

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

Description of change:

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

Validation:

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

4.3.1.3.2 Impact of Differences on Tricon Qualification

Functional Characteristics

None. The functional characteristics of previously qualified revisions of the Firmware: ETSX, TCM, and TSDO/HVDO have not been changed. This was confirmed in validation testing. Maintenance release V10.5 removed previously identified errors and/or provided product enhancements for added functionality in the operating and programming software.

TRICONEX TOPICAL REPORT

Physical Characteristics:

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

Quality Characteristics:

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

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

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

4.3.1.3.3 Conclusion

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

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

4.3.1.3.4 References

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

TRICONEX TOPICAL REPORT

4.3.1.4 Upgrade Tricon version from V10.5 to V10.5.1

Maintenance Release V10.5.1 provides a more current version of Tricon System that incorporates an enhancement to the operating software as tabulated in SRD 6200003-221. This is considered a minor change to fix an observed anomaly (ref TAB 181).

4.3.1.4.1 Detailed Review of Changes

No additional hardware is being qualified. This change provides newer firmware for the 4352AN and 4352BN Modules, which incorporates resolutions to a PDR. Changes included correction of conditions noted in TAB 181. V10.5.1 corrected a condition with a TSAA Protocol BIN broadcast issue. Firmware changes were developed and implemented in accordance with V10.5.1 EPP 9100315-001. Verification and validation activities were performed in accordance with V&V Plans referenced below. Firmware was validated as documented in the V&V Test Reports listed. V10.5.1 was approved and released by the Change Control Board (CCB) on 6/16/10.

TCM 6276

TCM 6276 was released in the V10.5.1 update in June, 2010

Reference documents:

- Software Release Definition (SRD) for V10.5.1, 6200003-221
- Tricon V10.5.1 Validation Plan 9600310-001
- V10.5.1 Validation and Verification Report

Description of change:

The TCM firmware modules were revised to fix a PDR affecting the 4352AN and 4352BN modules (see SRD 6200003-221 for details).

Validation:

TCM 6276 was validated as part of the Tricon V10.5.1 Verification & Validation Plan 9600310-001. This plan included the validation and verification requirements for changes made to the TCM firmware. The firmware was released in V10.5.1 per SRD 6200003-221. The results of the V & V are documented in the Tricon V10.5.1 Validation and Verification Report.

4.3.1.4.2 Impact of Differences on Tricon Qualification

Functional Characteristics

None. The functional characteristics of previously qualified revisions of the Firmware: TCM has not been changed. This was confirmed in validation testing. Maintenance release V10.5.1 removed a previously identified error in the operating and programming software.

TRICONEX TOPICAL REPORT

Physical Characteristics:

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

Quality Characteristics:

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

Based on the above, it is concluded that changes made in V10.5.1 did not introduce any changes to the TRICON systems:

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

4.3.1.4.3 Conclusion

V10.5.1 is considered equivalent to V10.5, which was previously qualified 1E. No changes were made to the basic functionality or reliability. Triconex has no reason to believe that any of the changes made from V10.5 to V10.5.1 invalidate the findings and results of the generic qualification of the Tricon in accordance with EPRI TR-107330.

No additional qualification steps are required to consider Tricon V10.5.1 qualified. TRICON V10.5.1 is considered to be qualified for nuclear safety related (Class 1E) application.

4.3.1.4.4 References

EPP 9100218-001
SRD for V10.5.1, 6200003-221
Tricon V10.5.1 Validation Plan 9600310-001
V10.5.1 Validation and Verification Report
TAB 181
TUV Certification for V10.5.1, dated 6/07/10

TRICONEX TOPICAL REPORT

4.3.1.5 Other Releases potentially affecting V10.5.1 Software

The Software development path from V10.2.1 to V10.5.1 shown in Figure 4-1 reflects the release of interim versions 10.3, 10.4, 10.4.1, and 10.4.2. These were commercial releases that were not specifically qualified for nuclear facility applications. However, two of the releases (V10.3 and V10.4.1) made changes to software modules that are used in nuclear qualified V10.5.1 but not described above. Records for these releases were reviewed to confirm that software changes were developed, controlled, and validated accordance with approved EDM development processes.

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

Reference documents:

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

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

Reference documents:

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

Conclusion: The referenced interim changes to the ETSX, TCM, AI, and DO software modules in V10.3 and V10.4.1 (between V10.2.1 and V10.5.1) were developed, controlled, and validated in accordance with approved EDM procedures, as evidenced in development

TRICONEX TOPICAL REPORT

records and TUV approvals, and therefore had no adverse impact on subsequent revisions of these modules in V10.5.1.

4.3.2 TriStation 1131 Changes

TriStation Programming software was upgraded to V4.7.0 as the current version that supports the V10.5.1 platform release. PDR fixes and product enhancements were incorporated, but no basic functional changes were made. Evaluation details and records for TriStation V4.7.0 are on file and available for review and audit. Upgrades were made in accordance with EDM procedures and reviewed by TÜV.

4.3.3 Process Change Review

Changes to the Triconex Quality Assurance program and development processes between V9.5.3 and V10.2.1 were reviewed in document NTX-SER-09-05, “Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System.” This section reviews changes to processes from V10.2.1 to V10.5.1 (developed during the period of 2006 to **2010**) for any impact on the V10.5 software changes described in sections 4.3.1 and 4.3.2 above.

4.3.3.1 QA program and procedures

For the period of 2001 to 2006, the “Differences Document” (NTX-SER-09-05) tabulated the changes to QA Manual (QAM) sections and Quality Procedure Manual (QPM) procedures to demonstrate that the Appendix B QA program continued to be consistent with QA program commitments, i.e., 10CFR50 Appendix B, 10CFR21, and NQA-1-1994. While ongoing procedure revisions occurred as part of the normal Triconex QA program maintenance, reflecting changes in implementation details and ongoing process improvements, the QA program continued to be compliant with nuclear industry commitments. This was independently confirmed by nuclear customer and agency audits over the period of 2001 to 2006.

Similarly, during the period from 2006 to **2010** (spanning development of software upgrades to V10.5.1), commitments to nuclear industry QA regulations and standards did not change. This can be seen by comparing the documented QA Program commitments contained in the 2006 version of the QA Manual (rev 029) and the 2009 QA Manual (revision 040). All revisions to the QAM continued to cite 10CFR50 Appendix B, 10CFR21, and NQA-1-1994 as governing regulations and standards. In addition, all QAM revisions contained reference to the Invensys Corporate Nuclear Quality Assurance Manual (IOM-Q2), which commits to the nuclear industry regulations and standards. **The current version of IOM-Q2 (Rev 3, 10/23/09) also continues to cite 10CFR50 Appendix B, 10CFR21, and NQA-1-1994 as governing regulations and standards among other international nuclear QA standards as the basis for the IOM Nuclear Quality Assurance Program.**

TRICONEX TOPICAL REPORT

Continuing compliance with nuclear quality program requirements during the 2006-**2010** period was confirmed by internal and external audits, including customer (NUPIC) and NRC audits that reflected continuing Triconex status as an approved nuclear supplier. QA processes and commitments have remained stable and compliant in the period spanning the development and production release of Tricon V10.5.1.

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

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

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

4.3.3.2 Engineering/Software Development Processes

Document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System" reviewed Product Development Processes in the EDM for the entire period from 2001 through 2009 (**inclusive of EDM Rev 042**) and concluded that no reductions or adverse changes to the previously approved development processes were made. This review encompassed the period of development and release of Tricon V10.5. **A subsequent review of EDM procedure changes from Rev 042 to current Rev 052 (May 2010) confirmed that, while routine procedure changes were made for process implementation clarifications, enhancements, and audit finding corrective action, no substantial changes to the basic development process elements have occurred during the period of development of Tricon V10.5.1. The Triconex Product Development processes continue to be consistent with previous process methodology, quality standards, and V9 SER commitments for ongoing independent reviews by TÜV.**

TRICONEX TOPICAL REPORT

4.3.3.3 Conclusion (Process Change Review)

No changes were made to the Quality Assurance or Development processes that reduced commitments or effectiveness of processes affecting the product upgrade from V10.2.1 to V10.5.1.

4.4 CONCLUSION

The Tricon V10.5.1 products and TriStation V4.7.0 Application Software continue to meet EPRI TR 107330 and IEEE requirements for Class 1E service and accurately represent the Tricon Qualification Test results as presented in the V10.2.1 Qualification Summary Report, 9600164-545. Changes made to the Tricon product since V10.2.1 and TriStation 4.1.437 are considered minor and evolutionary and have no adverse effect on qualification program results previously submitted for review.

TRICONEX TOPICAL REPORT

5.0 INVENSYS PROCESSES AND POLICIES FOR NUCLEAR PRODUCTS

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

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

5.1 MAINTENANCE OF QA AND PRODUCT DEVELOPMENT PROCESSES

5.1.1 Quality Assurance Program

At the time of the V9 Triconex Platform SER (December 2001), Triconex was operating under a 10CFR50 Appendix B Quality Assurance Program. The program had been established and approved by nuclear utility audits in early 1998. The V9 Tricon System, with existing legacy hardware and software, was not fully developed under the Appendix B program, as noted in the SER. However, all nuclear related activities, including hardware and software development, since 1998 have been implemented under 10CFR50 Appendix B controls. The Appendix B nuclear QA program has been maintained since the V9 qualification timeframe as evidenced by continued nuclear utility approvals of Invensys Triconex as a nuclear safety-related system supplier. Further discussion of audits by nuclear utilities (including NUPIC audits) and the NRC is found in Invensys document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System," (Reference 2.5.31). **Section 4.0 above reviews the Quality Assurance Program status from V10.2.1 timeframe to the current product version.**

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

5.1.2 Product Development Process

The V9 SER documented the NRC's review of Triconex procedures and process for hardware and software development. The SER concluded that procedures in the Engineering Department Manual (EDM), as part of the Appendix B Quality Assurance Program, were suitable for production of safety related hardware and software, with the caveat that an independent second

TRICONEX TOPICAL REPORT

level V&V review (such as by TÜV) would be required for future software to be considered acceptable.

Triconex development processes continue to be equivalent to (or better than) the processes reviewed as part of the V9 Qualification. Product development processes and software development activities continue to be controlled by procedures found in the Engineering Department Manual (EDM). All changes in engineering procedures since the 2001 timeframe were reviewed for any significant changes that may be construed to be a reduction in the rigor or effectiveness development processes as previously reviewed. No reductions were found. To the contrary, an ongoing improvement in process rigor and procedure completeness is evident. Significant improvements in the quality and formality of the EDM procedures have taken place since the SER was issued for Tricon V9.5.3, but no basic changes (reductions in commitment) were made to the design process. For more details, see further discussion of process changes in Invensys document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System," (Reference 2.5.31). **Section 4.0 above reviews the Quality Assurance Program status from V10.2.1 timeframe to the current product version.**

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

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

Any changes to the process described in EDM 12.00 (or any supporting procedures that deviate

TRICONEX TOPICAL REPORT

from the requirements of this procedure) shall be evaluated for impact on the SER and the need for topical report revision (see Section 5.6).

5.2 INVENSYS PROJECT INTEGRATION PROCESSES

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

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

Project procedures supporting the Nuclear System Integration Program Manual (NSIPM) govern all quality-affecting Project activities performed by personnel at the Irvine facility. The NSIPM implements the requirements of the Invensys Nuclear Quality Assurance Manual, 10CFR50 Appendix B, NQA-1, and applicable Regulatory Guides and industry Standards. Specific standards associated with software activities include, but are not limited to Regulatory Guide 1.168 and IEEE Standards 830 and 1012. The NSIPM may also be used by other Invensys facilities.

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

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

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

5.3 SECURITY

The increasing use of computers for various functions at nuclear facilities brings forth new technical challenges that must be addressed in a rigorous and balanced manner. Digital computers in nuclear facilities are used in safety-related and non-safety systems, where non-availability or malfunction could affect nuclear safety and continuity of power. Computers are

TRICONEX TOPICAL REPORT

also used to store important and sensitive data, where malfunction could lead to the loss or unavailability of data. As the complexity of these computer systems increases, comprehensive methods to assure computer system dependability and reliability need to be employed.

NRC Regulatory Guide (RG) 1.152, Rev 2, “Criteria for use of Computers in Safety Systems of Nuclear Power Plants,” describes a method that the NRC deems acceptable for complying with regulations for promoting high functional reliability, design quality, and security for the use of digital computers in safety systems for nuclear power plants. In the context of RG 1.152, “security” refers to protective actions taken against a predictable set of non-malicious acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system.

As a supplier of digital control systems for safety related applications in nuclear facilities, Invensys is committed to implementing **measures** to mitigate relevant security risks during the applicable life cycle phases of the digital computer systems. **Invensys document NTX-SER-10-14, “Tricon V10 Conformance to Regulatory Guide 1.152,”** (Reference 2.5.34), describes the **conformance of the V10 Tricon to NRC Regulatory Guide 1.152. NTX-SER-10-14 provides a discussion of the Tricon system characteristics related to security and also contains a conformance table providing details on Tricon V10 conformance to Regulatory Positions 2.1 through 2.5. Triconex commits to maintain conformance to the positions in this document with each new release of the Tricon, in accordance with the process described in NTX-SER-09-20, Invensys Triconex Safety Evaluation Report (SER) Maintenance Process (Reference 2.5.36).**

Any significant changes to the **provisions** described in **NTX-SER-10-14** (or procedures deviating from the **commitments** in this document) shall be evaluated for impact on the SER and need for topical report revision (see Section 5.6).

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

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

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

TRICONEX TOPICAL REPORT

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

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

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

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

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

The Invensys position and application philosophy in regard to NRC Interim Staff Guidance ISG-04 and related regulatory standards and guidance is described in Invensys Document NTX-SER-09-10, “Tricon Applications in Nuclear Reactor Protection Systems – Compliance with NRC ISG-2 and ISG-4,” (Reference 2.5.35).

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

In Section 1.0 of the document, a typical example illustrates the flexibility and many of the features of Tricon controllers configured for RPS and/or ESFAS applications. While not proposed for any specific facility architecture, the example is presented for discussion purposes

TRICONEX TOPICAL REPORT

of how Tricon controllers may be applied in reactor protection applications in compliance with regulatory requirements and to industry standards.

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

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

5.6 INVENSYS TRICONEX TOPICAL REPORT/SER MAINTENANCE PROCESS

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

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

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

To the extent that product or process changes are confirmed to be within the established criteria, the Triconex platform will be considered consistent and current with the latest SER/Topical Report and marketed as such. Where the SER Impact Review identifies unreviewed safety issues, i.e., issues considered to be outside the basic elements credited in the

TRICONEX TOPICAL REPORT

SER, the process will assure NRC review and approval of the changes by Topical Report revision. Similar to a 10CFR50.59 process, summary reports on Triconex SER impact reviews will be provided to the NRC on a 24 month basis.

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

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

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