

TRICONEX TOPICAL REPORT

7286-545-1-A

QUALIFICATION SUMMARY REPORT

**NUCLEAR QUALIFICATION OF TRICON
TRIPLE MODULAR REDUNDANT PLC SYSTEM**

Includes Triconex Report 7286-546-1-A
Amendment 1 to Qualification Summary Report

NRC Accepted Version
Issue date: March 8, 2002



TRICONEX TOPICAL REPORT 545-1-A

March 8, 2002

CONTENTS

Part 1. NRC Approval Letter dated December 12, 2001 and attached
NRC Safety Evaluation Report dated December 12, 2001

Part 2. Requests for Additional Information and Responses

Part 3. Abstract of Qualification Summary Report

Part 4. Qualification Summary Report, Triconex Document 7286-545, Revision 1,
dated September 18, 2000 (also published as EPRI Technical Report 1000799)

Part 5. Amendment 1 to Qualification Summary Report, Triconex Document 7286-546,
Revision 1, dated June 25, 2001 (Re-designated 7286-546-1-A)



UNITED STATES
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

December 12, 2001

Mr. J. Troy Martel, P.E.
Triconex Nuclear Qualification Project Director
Triconex Corporation
15345 Barranca Parkway
Irvine, California 92618

SUBJECT: REVIEW OF TRICONEX CORPORATION TOPICAL REPORTS 7286-545, "QUALIFICATION SUMMARY REPORT" AND 7286-546, "AMENDMENT 1 TO QUALIFICATION SUMMARY REPORT," REVISION 1 (TAC NO. MA8283)

Dear Mr. Martel:

The NRC staff has completed its review of the subject topical report which was submitted by Triconex Corporation by letter dated October 2, 2000. This document was also submitted to the NRC by the Electric Power Research Institute (EPRI) as a technical report entitled, "Generic Qualification of the Triconex Corporation Tricon Triple Modular Redundant Programmable Logic Controller System for Safety-Related Application in Nuclear Power Plants," document number 1000799, dated November 2000. By letter dated March 20, 2001, Triconex Corporation amended its original qualification summary report by submitting Topical Report 7286-546, "Amendment 1 to Qualification Summary Report," Revision 0, dated March 19, 2001. This amendment requested that the NRC review and approve an update of the Triconex Programmable Logic Controller (PLC) from Version 9.3.1 to Version 9.5.3.

By letter dated June 26, 2001, Triconex Corporation again revised its qualification summary report by submitting Topical Report 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1, dated June 25, 2001. This revision updated the Triconex part number for the 3636TN relay output module and the 3601TN 115 Vac digital output module, and revised the EAO software listing used in the 3805EN analog output module. In addition, together with the original qualification summary report, this revision asked the staff to approve the Triconex system and several module types for safety-related use in nuclear power plants.

The staff has found that Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1 are acceptable for referencing in licensing applications for nuclear power plants to the extent specified and under the limitations delineated in the report and in the associated safety evaluation. The safety evaluation defines the basis for acceptance of the reports.

Pursuant to 10 CFR 2.790, we have determined that the enclosed safety evaluation does not contain proprietary information. However, we will delay placing the safety evaluation in the public document room for a period of ten (10) working days from the date of this letter to provide you with the opportunity to comment on the proprietary aspects only. If you believe that any information in the safety evaluation is proprietary, please identify such information line by line and define the basis pursuant to the criteria of 10 CFR 2.790.

We do not intend to repeat our review of the matters described in the subject reports, and found acceptable, when the reports appear as a reference in license applications, except to ensure that the material presented applies to the specific plant involved. Our acceptance applies only to matters approved in the reports.

In accordance with procedures established in NUREG-0390, the NRC requests that Triconex Corporation publish accepted versions of the submittals, proprietary (-P) and non-proprietary (-NP), within 3 months of receipt of this letter. The accepted versions shall incorporate (1) this letter and the enclosed safety evaluation between the title page and the abstract, and (2) all requests for additional information from the staff and all associated responses, and (3) an "-A" (designating "accepted") following the report identification symbol.

Should our criteria or regulations change so that our conclusions as to the acceptability of the reports are invalidated, Triconex Corporation and/or the applicants referencing the topical reports will be expected to revise and resubmit their respective documentation, or submit justification for the continued applicability of the topical reports without revision of their respective documentation.

Sincerely,

A handwritten signature in black ink, appearing to read 'S. Richards', with a large, stylized flourish at the end.

Stuart A. Richards, Director
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Project No. 709

Enclosure: Safety Evaluation

Contents	Page
1.0 INTRODUCTION	1
2.0 SYSTEM DESCRIPTION	4
2.1 Hardware Description	5
2.1.1 Chassis	5
2.1.1.1 Main Chassis	5
2.1.1.2 Expansion Chassis	6
2.1.1.3 Remote Extender Chassis	6
2.1.1.4 External Termination Assemblies	7
2.1.1.5 Power Supply Modules	7
2.1.2 Main Processor Subsystem	8
2.1.3 Input and Output Modules	10
2.1.3.1 Digital Input Modules	12
2.1.3.2 Analog Input Modules	13
2.1.3.3 Digital Output Modules	13
2.1.3.4 Analog Output Module	14
2.1.3.5 Pulse Input Module	14
2.1.3.6 Thermocouple Input Modules	14
2.1.3.7 Relay Output	15
2.1.4 Communications Modules	15
2.2 Software Description	16
2.2.1 Safety-Related Operating System Software Description	17
2.2.1.1 Main Processor Module Software	17
2.2.1.1.1 TSX Operating Environment Software	17
2.2.1.1.2 IOC Software	19
2.2.1.1.3 COM Software	19
2.2.1.2 I/O Module Software	19
2.2.1.3 Communications Module Software	21
2.2.2 Safety-Related Plant-Specific Application Software	22
2.2.3 TriStation 1131 Software	22
2.3 Tricon PLC Product Qualifications	24
2.3.1 Environmental Requirements	24
2.3.2 EMI/RFI Requirements	25
2.3.3 Electrostatic Discharge (ESD) Withstand Requirements	25
2.3.4 Seismic Withstand Requirements	25
2.3.5 Surge Withstand Requirements	25
2.3.6 Class 1E to Non-1E Isolation Requirements	25
3.0 REVIEW CRITERIA	26
3.1 General Standards	26
3.2 Method of Review	28
4.0 EVALUATION	29
4.1 Tricon PLC Hardware Design Review	29
4.1.1 Hardware Architecture and Signal Flow	29
4.1.2 Hardware Quality	30

4.1.3	Environmental Testing and Qualification	32
4.1.3.1	Pre-qualification Testing	32
4.1.3.2	Temperature and Humidity Testing	33
4.1.3.3	Radiation Withstand Testing	35
4.1.3.4	Seismic Withstand Testing	35
4.1.3.5	Electromagnetic Compatibility Testing	36
4.1.3.6	Surge Withstand Testing	38
4.1.3.7	ESD Withstand Testing	39
4.1.3.8	Class 1E to Non-1E Isolation Testing	40
4.2	Tricon PLC Software Design Review	41
4.2.1	Software Documentation	41
4.2.2	Software Development and Life Cycle Planning	42
4.2.2.1	Software Management Plan	44
4.2.2.2	Software Development Plan	44
4.2.2.3	Software Quality Assurance Plan	44
4.2.2.4	Software Integration Plan	45
4.2.2.5	Software Installation Plan	45
4.2.2.6	Software Maintenance Plan	45
4.2.2.7	Software Training Plan	45
4.2.2.8	Software Operations Plan	46
4.2.2.9	Software Safety Plan	46
4.2.2.10	Software Verification and Validation Plan	46
4.2.2.11	Configuration Management and Error Notification	49
4.2.3	Evaluation of TriStation 1131 Programming Software	50
4.2.4	Application Programs	51
4.3	Tricon PLC System Design Review	51
4.3.1	Failure Modes and Effects Analysis	52
4.3.2	Reliability and Availability Analysis	52
4.3.3	Component Aging Analysis	52
4.3.4	Thread Audit	53
4.3.5	Response Time Characteristics	54
4.3.6	Tricon PLC System Self-Diagnostic Capacity	55
4.3.7	Training	56
4.3.8	Repair of Tricon PLC System Modules	58
4.3.9	Historic Data on Tricon PLC System Use	58
4.3.10	Defense-in-Depth and Diversity	58
5.0	CONCLUSION	60
5.1	Regulatory Compliance	60
5.2	Plant-Specific Requirements	63
5.3	Approval	66

LIST OF FIGURES

Figure 1-	Tricon PLC Architecture	4
Figure 2-	Main Chassis Backplane	6
Figure 3-	Main Processor Architecture	9



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

TOPICAL REPORTS 7286-545 AND 7286-546

"QUALIFICATION SUMMARY REPORT" AND "AMENDMENT 1 TO QUALIFICATION

SUMMARY REPORT," REVISION 1

TRICONEX CORPORATION

PROJECT NO. 709

1.0 INTRODUCTION

By letter dated October 2, 2000, Triconex Corporation (Triconex) submitted Topical Report 7286-545, "Qualification Summary Report," dated September 18, 2000 (ADAMS Accession Number ML003757032), for review by the staff of the U. S. Nuclear Regulatory Commission.

This document was also submitted to the NRC by the Electric Power Research Institute (EPRI) as a technical report entitled, "Generic Qualification of the Triconex Corporation Tricon Triple Modular Redundant Programmable Logic Controller System for Safety-Related Application in Nuclear Power Plants," document number 1000799, dated November 2000.

By letter dated March 20, 2001, Triconex amended its original qualification summary report by submitting Topical Report 7286-546, "Amendment 1 to Qualification Summary Report," Revision 0, dated March 19, 2001 (ADAMS Accession Number ML010810143). This amendment requested that NRC review and approve an update of the Triconex Programmable Logic Controller (PLC) from Version 9.3.1 to Version 9.5.3.

By letter dated June 26, 2001, Triconex again revised its qualification summary report by submitting Topical Report 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1, dated June 25, 2001 (ADAMS Accession Number ML011790327). This revision updated the Triconex part number for the 3636TN relay output module and the 3601TN 115 Vac digital output module, and revised the EAO software listing used in the 3805EN analog output module. In addition, together with the original qualification summary report, this revision asked the staff to approve the Triconex system and the following module types for safety-related use in nuclear power plants:

<u>MODULE TYPE</u>	<u>MODEL</u>	<u>DESCRIPTION</u>
Chassis	8110N	Main Chassis
	8111N	Expansion Chassis
	8112N	Remote Expansion Chassis

Main Processor	3006N	Enhanced Main Processor 11, V9, 2 Mb
Remote Extender	4210N	Remote Extender Module (Primary)
	4211N	Remote Extender Module (Remote)
Communication	4119AN	Enhanced Intelligent Communications Module (EICM) V9, Isolated
	4329N	Network Communications Module (NCM), V9
	4609N	Advanced Communications Module (ACM)
Analog Input	3700AN	Analog Input (AI) Module, 0/5 Vdc, 6% Overrange
	3701N	AI Module, 0/10 Vdc
	3703EN	Enhanced Isolated Analog Input (EAI) Module
	3704EN	High-Density Analog Input (HDAI) Module, 0-5/0-10 Vdc
Analog Output	3805EN	Analog Output Module, 4/20 mA
Digital Input	3501TN	Enhanced Digital Input (EDI) Module, 115V ac/dc
	3502EN	EDI Module, 48V ac/dc
	3503EN	EDI Module, 24V ac/dc
	3504EN	High-Density Digital Input (HDDI) Module, 24/48 Vdc
	3505EN	EDI Module, 24 Vdc, Low-Threshold
Digital Output	3601TN	Enhanced Digital Output (EDO) Module, 115 Vac
	3603TN	EDO Module, 120 Vdc
	3604EN	EDO Module, 24 Vdc
	3607EN	EDO Module, 48 Vdc
	3623TN	Supervised Digital Output (SDO) Module, 120 Vdc
	3624N	SDO Module, 24 Vdc
Pulse Input	3510N	Pulse Input Module
Thermocouple Input	3706AN	Non-Isolated Thermocouple (NITC) Input Module
	3708EN	Isolated Thermocouple (ITC) Input Module
Relay Output	3636TN	Enhanced Relay Output (ERO) Module, Simplex
Power Supply	8310N	120 Vac/DC Power Supply
	8311N	24 Vdc Power Supply

Since March 21, 2000, Triconex has also provided a variety of related documents under cover of the following eleven letters:

<u>Date</u>	<u>Adams Accession Number</u>
March 21, 2000	ML003702538
March 21, 2000	ML003721491
April 3, 2000	ML003700550
July 17, 2000	ML003733651

<u>Date</u>	<u>Adams Accession Number</u>
August 29, 2000	ML003746068
September 29, 2000	ML003756705
November 14, 2000	ML003769998
November 15, 2000	ML003769918
February 27, 2001	ML010610188
August 30, 2001	ML012490183
September 25, 2001	ML012700039

These submittals provided the following documents:

<u>Document Title</u>	<u>Triconex Document Number</u>
Quality Plan (Nuclear Qualification Project)	QPL-0 I
Quality Assurance Manual	QAM
Master Test Plan	7286-500
Setup and Check-out Test Procedure	7286-502
Operability Test Procedure	7286-503
Prudency Test Procedure	7286-504
Environmental Test Procedure	7286-506
Seismic Test Procedure	7286-507
Surge Withstand Test Procedure	7286-508
1E/Non-1E Isolation Test Procedure	7286-509
EMI/RFI Test Procedure	7286-510
TSAP Validation Test Procedure	7286-513
TSAP Functional Specification	7286-517
TSAP Design Specification	7286-518
TSAP Program Listing	7286-519
Pre-Qualification Test Report	7286-524
Environmental Test Report	7286-525
Seismic Test Report	7286-526
EMI/RFI Test Report	7286-527
Surge Test Report	7286-528
1E/Non-1E Isolation Test Report	7286-529
Performance Proof Test Report	7286-530
Reliability/Availability Study	7286-531
Failure Modes & Effects Analysis	7286-532
Radiation Hardness Evaluation	7286-533
Tricon PLC System Accuracy Specification	7286-534
Software Qualification Report	7286-535
TSAP V&V Report	7286-536
Software Quality Assurance Plan	7286-537
Master Configuration List	7286-540
Tricon PLC Test Specimen Description	7286-541
Certificate of Conformance	7286-542
Maximum Response Time Calculation	426-001/SCS-01
Triconex Training Manual	5600-0020/99
Technical Product Guide, V 8	9791007-002
Technical Product Guide, V 9	9791007-005

<u>Document Title</u>	<u>Triconex Document Number</u>
Tricon Planning and Installation Guide	9720051-006
Test System Loop Diagrams	Various
Type Approval of Tricon Version 9.5.3	TÜV-Rheinland 968/EZ 105.02/01
Advanced Communications Module	None (commercial manual)
Intelligent Communications Module	None (commercial manual)
TriStation Multi System Workstation	None (commercial manual)
TriStation Developers Workbench	None (commercial manual)

For documents that contained proprietary information, Triconex also submitted nonproprietary versions.

2.0 SYSTEM DESCRIPTION

The Tricon PLC system is a fault-tolerant PLC that uses a triple modular redundant (TMR) architecture in which three parallel control paths are integrated into a single overall system. The system is designed to use two-out-of-three voting with the intent of providing uninterrupted process operation with no single point of random hardware failure. However, since all three of the parallel paths use identical hardware and software, common- cause failure is possible in both hardware and software.

A Tricon PLC system consists of 1 main chassis and up to 14 expansion chassis. The main chassis contains: (1) two redundant power supply modules, (2) three main processor modules, (3) communications modules, and (4) input and output (I/O) modules.

Figure 1 shows the data flow in the TMR architecture of the Tricon PLC system. When entering the input module, the signals from each attached sensor are separated into three isolated paths and sent to one of the three main processor modules. The TriBus inter-processor bus performs a two-out-of-three vote on data and corrects any discrepancies. This process ensures that each main processor uses the same voted data to execute its application program.

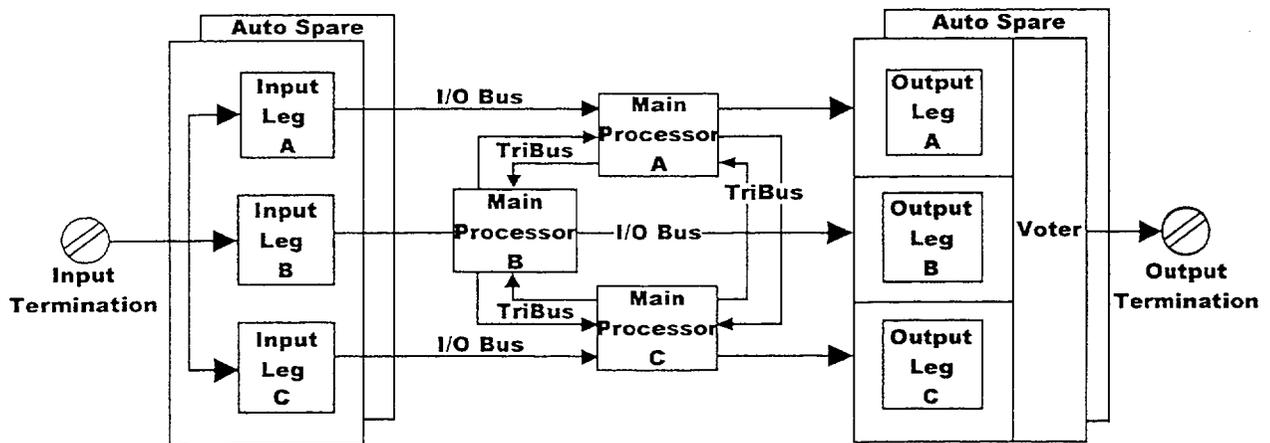


Figure 1. TMR Architecture of the Tricon PLC System

Similarly, process outputs are sent via triplicated paths to the output modules, which in turn send the data to a voter using two-out-of-three logic. The voted output is then sent to the actuation devices by an output termination board.

2.1 Hardware Description

The hardware which makes up the Tricon PLC system consists of the three types of chassis, the external termination assemblies, the power supply modules, the main processor subsystem, and various I/O and communication modules, depending on the configuration and use of the system. These components are described in Sections 2.1.1- 2.1.4.

2.1.1 Chassis

The Tricon PLC system can accommodate various combinations of the main chassis and up to 14 expansion chassis and/or remote extender chassis. The main chassis contains the main processor modules and a combination of I/O and communications modules. The expander chassis is used locally to increase the number of I/O modules in the system, and is connected via RS-485 communication links. The remote extender chassis is used for remote locations up to several miles away, and is connected via fiber optic links.

2.1.1.1 Main Chassis

The main chassis of the Tricon PLC system contains two power supplies, three main processor modules, and communications and I/O modules as needed. It also has a key switch with the following positions to set the system's operating mode:

- RUN is the normal operating mode, which gives read-only capability by externally connected systems including the TriStation. The switch is normally set to this position, and the key is removed and stored in a secured location.
- PROGRAM mode allows the Tricon PLC system to be controlled from an externally connected personal computer (PC) running the TriStation software. This mode is needed to download application programs to the Tricon PLC system.
- STOP terminates the execution of the current application program.
- REMOTE allows a TriStation PC or a Modbus master or external host to write values to application program variables.

The main chassis backplane of the Tricon PLC system has dual power rails, each of which has an independent power supply with sufficient capacity to power the entire chassis. Under normal circumstances, each main processor module and each of the three legs on I/O modules draw power from both power supplies through the dual power rails and the dual voltage regulators. If either of the power supplies or its supporting power line fails, the other power supply will increase its output to support the power needs of all modules in the chassis. Figure 2 shows the power supply architecture of the main chassis backplane.

The Tricon PLC system also has two 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 6 months. The system will generate an alarm when the battery power is too low to support the system.

2.1.1.2 Expansion Chassis

The expansion chassis are used locally to increase the number of I/O modules in the Tricon PLC system. Each expansion chassis is connected to the main chassis via three RS-485 communication links (one for each of the three I/O legs). If communications modules are installed, three separate RS-485 links are required for the three communications buses. The maximum length of the RS-485 cables is 100 feet. The Tricon PLC expansion chassis has the same type of power supplies as the main chassis, and the same dual and redundant power bus arrangement. Each expansion chassis can support I/O modules, but only the first expansion chassis can support communications modules.

2.1.1.3 Remote Extender Chassis

The remote extender chassis are similar to the expansion chassis, but are used for remote locations (up to several miles away), rather than locally. As such, each remote extender chassis has remote extender modules (RXMs) that serve as repeaters or extenders of the Tricon PLC I/O bus to allow communications with the main chassis and expansion chassis. The RXMs are single-mode fiber optic modules that allow the expansion chassis to be located up to 7.5 miles away from the main chassis. Each RXM module has separate transmit and receive cabling ports, requiring two unidirectional fiber optic cables (one to transmit and one to receive), for each module. Since the RXM modules are connected by fiber optic cables and not electrical

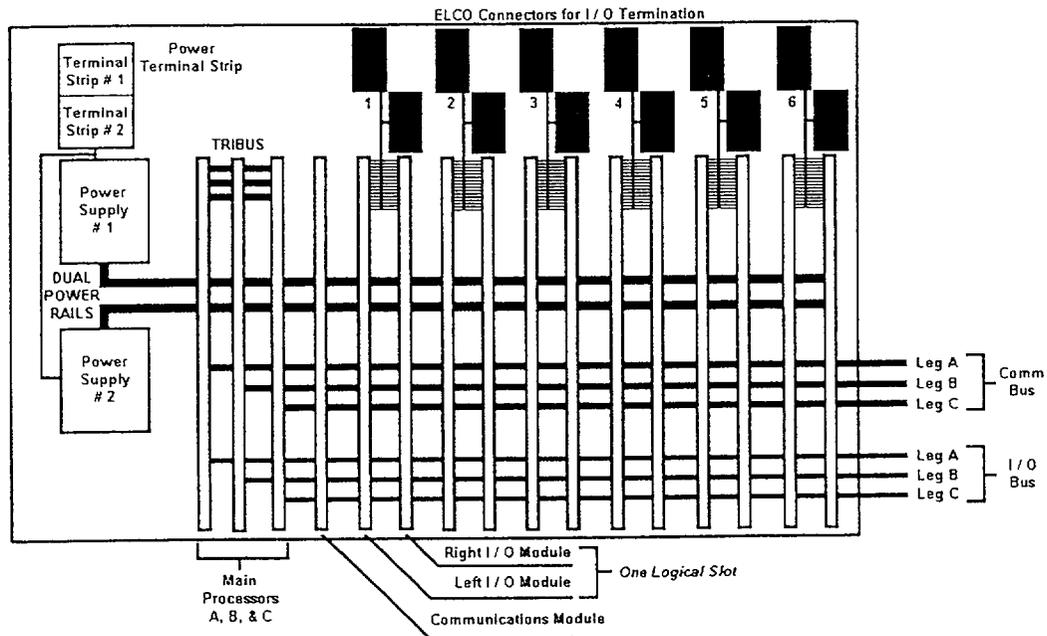


Figure 2. Main Chassis Backplane

cables, they provide ground loop isolation and immunity against electrostatic and electromagnetic interference, and they can be used as 1E-to-non-1E isolators between a safety-related main chassis and a non safety-related expansion chassis. The Tricon PLC remote extender chassis uses the same type of power supplies as the main chassis, and has the same dual and redundant power bus arrangement.

2.1.1.4 External Termination Assemblies

Each I/O module in the Tricon PLC system has an external termination assembly (ETA) mounted on the chassis in which it is contained. These are printed circuit board panels that are used to terminate field wiring. The panels contain terminal blocks, resistors, fuses, and blown fuse indicators. The panels are configured for specific applications, depending on which I/O modules are used. Thermocouple input termination panels provide cold-junction temperature sensors and are available with upscale, downscale, or programmable burnout detection. Resistance temperature detector (RTD) termination panels include signal conditioning modules. Each ETA panel includes an interface cable that connects the panel to the chassis backplane.

2.1.1.5 Power Supply Modules

All power supply modules are rated for 175 watts, which is sufficient to supply the power requirements of a fully populated chassis. A single chassis can accommodate the two different types of power supply modules available for nuclear power plants. Specifically, the available types of power supplies are the 120 V ac/dc Model # 8310N and the 24 V dc Model #8311N. Each of these power supply modules possesses built-in diagnostic circuitry to check for out-of-range voltages and over-temperature conditions. Light-emitting diodes (LEDs) on the front face of each power supply module indicate the module status.

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 power supply modules will alarm on the following states:

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

The system alarm contacts on at least one of the power supply modules will also actuate when any of the following power conditions exist(s):

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

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

2.1.2 Main Processor Subsystem

The main processor (MP) subsystem contains three MP modules, each of which is independent, resides on a separate printed circuit board, controls a separate leg of the system, and operates in parallel with the other two main processors. Each MP module contains three microprocessors, which are the 8-bit I/O communications (IOC) processor, the 8-bit communications (COM) processor for external communications, and the 32-bit primary processor. The primary processor manages execution of the control program and all system diagnostics at the main processor module level and has a 32-bit math co-processor. Each 8-bit processor and the 32-bit primary processor are connected via a dedicated dual port random access memory (RAM) allowing for direct memory access data exchanges. The operating system, run-time library, and fault analysis for the main processor are fully contained in read-only memory (ROM) on each MP module.

As shown in Figure 3, the Tricon PLC system has four separate bus structures, the Tribus, the communications bus, the I/O bus, and the bus internal to each of the main processor modules. Each of these bus structures is triplicated. The Tribus interconnects the three MP modules with each other, and is used for data transfer, voting, and program loading. The communications bus connects the MP modules with the communications modules and is used to send non-safety data to other Tricon PLC and non-Tricon PLC systems. The I/O bus connects the MP modules to the I/O modules, both within the main chassis and from chassis to chassis by means of I/O bus cables. The internal bus in each MP module interconnects the processors with the dual-port RAM, erasable programmable read only memory (EPROM), static random access memory (SRAM), direct memory access (DMA) devices, the timing generator and the interrupt controller.

The MP subsystem makes limited use of interrupts. The interrupt controller sends periodic interrupts to the background diagnostics and fault analysis tasks to trigger execution of the foreground task containing the control program. The "watchdog" can trigger an interrupt to inform the MP of a problem. In addition, the I/O processor uses interrupts generated by the I/O bus to request data from the I/O modules.

The MP modules communicate with each other through the Tribus. Each MP module has an I/O bus channel to allow communication with one of the three legs of each I/O module. Each MP module also has an independent clock circuit and clock selection mechanism that enables all three MP modules to synchronize their operations during each scan to allow voting of data and exchange of diagnostic information.

The I/O processor polls each I/O input module using the attached leg of the I/O bus, and stores the received value in the memory that is dual-ported to the I/O processor and the main processor. This makes the received value available for retrieval by the main processor.

In a similar manner, the communications processor manages the data exchanged between the main processors and the communications modules. The communications bus supports a broadcast mechanism, and stores the received value in the dual-ported memory, where it is available for retrieval by the main processor. The values in each MP module are transferred to the next MP module over the Tribus. Hardware voting also takes place during this transfer. The Tribus uses direct memory access to synchronize, transmit, vote, and compare data among the three main processors. If a disagreement occurs, the value found in two out of three tables prevails, and the third table is corrected accordingly. One-time differences that result from sample timing variations are distinguished from a pattern of differing data. Each main processor maintains data about the necessary corrections in local memory. Any disparity is flagged and used at the end of the scan by the built-in fault analyzer routines of the Tricon PLC system to determine whether a fault exists in a particular module.

The main processors enter the corrected data into the control program. The 32-bit main microprocessor and math coprocessor execute the control program in parallel with the other two main processor modules. The control program generates output values on the basis of input values according to customer-defined rules that are built into the application. The I/O communication processor on each main processor manages the transmission of output data to the output modules by means of the I/O bus.

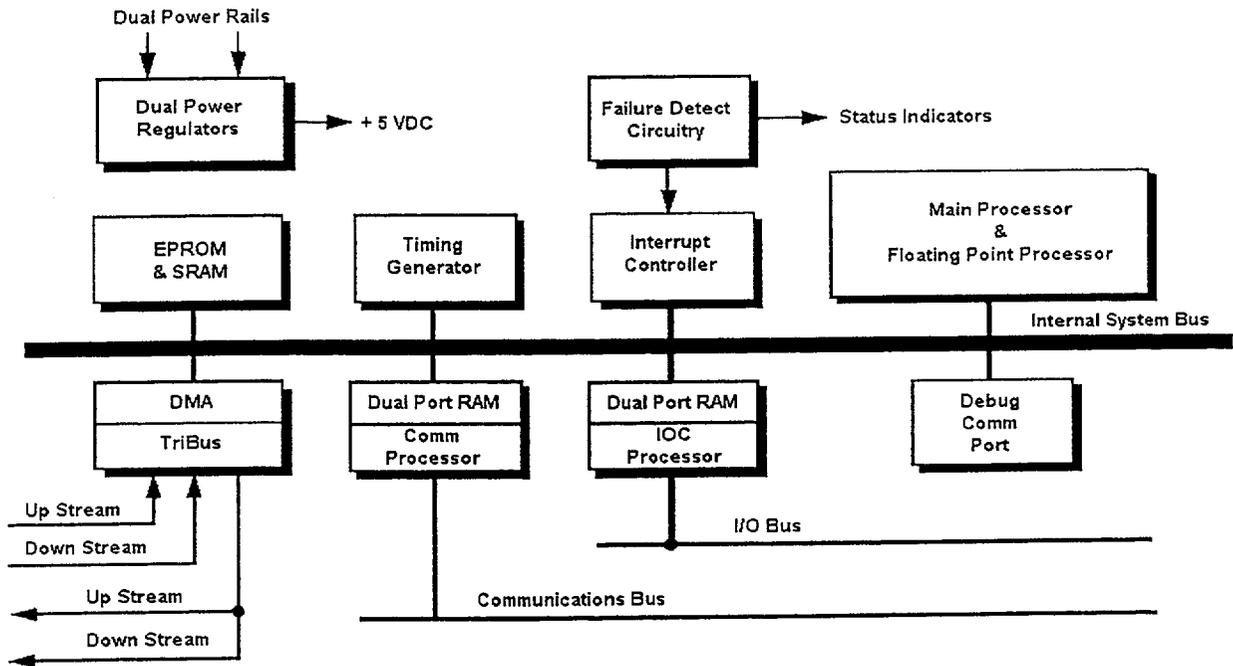


Figure 3. Main Processor Architecture

Each MP module has the following indicator lights on the front panel of each card:

- Pass: If on, the module has passed its self-diagnostic tests.
- Fault: If on, the module has a fault.
- Active: If on, the module is running the user-written control program.
- Maint1: The module is re-educating when this indicator light is blinking.
- Maint2: If on, the module has a high soft-error count.

The front panel also has four lights that show communication status, when the card is transmitting or receiving on either the communications bus or the I/O bus. In addition, the front panel has a History/Status port that can be used to read the diagnostic information on the given board. The History/Status port is generally not available for users, but is provided for depot-level repair by personnel from Triconex.

The only model of MP module available for safety-related use in nuclear power plants is the model 3006N, which provides 2 MB of SRAM. This SRAM is used for the plant-specific control program, I/O data, diagnostics, and communication buffers. In the event of an external power failure, the SRAM is protected by batteries that reside on the main chassis backplane. In the absence of power to the Tricon PLC system, the batteries maintain the integrity of the program and the retentive variables for six months.

Triconex also offers the Model 3007 main processor, which is intended for use as a single chassis Tricon PLC system. However, Triconex did not submit the Model 3007 for staff review and therefore it is not qualified for safety-related use in nuclear power plants.

2.1.3 Input and Output Modules

Each input module consists of three identical and independent circuits, called legs, contained on a single input card. The isolated input on each leg of each input module receives sensor outputs that are received on a field termination point. The microprocessor in each leg continually polls the input points, and constantly updates an input data table in the local memory of each leg. Any required signal conditioning, isolation, and processing are also performed independently for each leg. Each input module has leg-to-leg isolation and independence within the I/O board to ensure that a component failure in one leg will not affect the signal processing in the other two legs. Each of the triplicated I/O buses communicates with a single, hardware-defined MP and with one of the triplicated microprocessors on each I/O module. In each MP, the I/O bus microprocessor reads the data and provides it to the MP through a dual port RAM interface. Each MP then transfers and votes on all data over the Tribus.

All input modules include self-diagnostic features designed to detect single failures within the given 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 reference voltage sources that are used to continually self-calibrate the analog-to-digital converters. A diagnostic alarm is generated if a converter is found to be out of tolerance.
- Some input modules also include diagnostics to detect field device failures.

Output modules are similar to the input modules, in that each has three identical and independent circuits contained on a single card. All output modules include self-diagnostic features designed to detect single failures within the given 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.
- Each supervised digital output module includes a voltage and current loopback circuit that checks for open circuits (e.g., blown fuse) and short circuits in the field wiring.
- Each analog output module includes 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's output current is correct.

If one of the three legs within an I/O module fails to function, an alarm is raised to the main processors and is displayed on the power supply module. 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 are unaffected. To remove the fault in this event, a replacement unit is inserted into the system in the logically paired slot associated with the failed module. When the main processors detect the presence of a replacement module, they initiate diagnostics and, if the module is functioning correctly, 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 used on a periodic basis. The main processors will automatically swap control between the two modules. By periodically using both modules, any faults are detected and alarmed, and the failed module is replaced when a standby module is in place. This use of standby modules does not cause any interruption of protection or control functions.

The front panel of each I/O module has the following indicator lights that show the status of the card:

- Pass: If on, the module has passed its self-diagnostic tests.
- Fault: If on, one leg within the module has a fault.

- Active: If on, the module is running. (If modules are installed in pairs, one of each pair will be active, and the other in standby.)

The system firmware resident on the I/O modules is designed in a modular fashion, based around a common core. Specific customization, including integral diagnostic capabilities, are applied to fit the needs of a given module and the data to be acquired. All three microprocessors on a module run exactly the same firmware. Each microprocessor interfaces to only one leg of the I/O bus and, thus, to only one MP.

All I/O modules require a cable interface to an external termination panel. Each module is mechanically keyed to prevent improper installation in a configured chassis.

2.1.3.1 Digital Input Modules

The following types of digital input modules are available for safety-related use in nuclear power plants:

- Model 3501TN is a 115 Vac/dc digital input module with 32 isolated input points. This model has standard diagnostics, but does not have the ability to verify the transition of a normally energized circuit to the off state. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 input points is on or off.
- Model 3502EN is a 48 Vac/dc digital input module with 32 inputs. Four groups of 8 inputs use a common reference point. Unlike the Model 3501TN, this model can continuously verify the transition of a normally energized circuit to the off state. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 input points is on or off.
- Model 3503EN is a 24 Vac/dc digital input module with 32 inputs. Four groups of 8 inputs use a common reference point. Like the Model 3502EN, this model can continuously verify the transition of a normally energized circuit to the off state. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 input points is on or off.
- Model 3504EN is a 24/48 Vdc high-density digital input module with 64 inputs that all use a common reference point. Like the Model 3502EN and 3503EN, this model can continuously verify the transition of a normally energized circuit to the off state. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 64 input points is on or off.
- Model 3505EN is a 24 Vdc low-threshold digital input module with 32 inputs. Four groups of 8 inputs use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 input points is on or off.

2.1.3.2 Analog Input Modules

The following types of analog input modules are available for safety-related use in nuclear power plants:

- Model 3700AN is a 0-5 Vdc analog input module with 32 differential dc-coupled inputs. This model has a +6 percent over-range measurement capability.
- Model 3701N is a 0-10 Vdc analog input module with 32 differential dc-coupled inputs.
- Model 3703EN is a 0-5 or 0-10 Vdc isolated analog input module with 16 differential isolated inputs. This module has a selectable voltage range and upscale or downscale open-input detection and a +6 percent over-range measurement capability.
- Model 3704EN is a 0-5 or 0-10 Vdc high-density analog input module with 64 dc-coupled inputs using a common reference. This module has selectable voltage range and a +6 percent over-range measurement capability.

2.1.3.3 Digital Output Modules

The following types of digital output modules are available for safety-related use in nuclear power plants:

- Model 3601TN is a 115 Vac digital output module with 16 outputs that do not use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off.
- Model 3603TN is a 120 Vdc digital output module with 16 outputs that use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off.
- Model 3604EN is a 24 Vdc digital output module with 16 outputs that do not use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off.
- Model 3607EN is a 48 Vdc digital output module with 16 outputs that do not use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off.
- Model 3623TN is a 120 Vdc supervised digital output module with 16 outputs that use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off.
- Model 3624N is a 24 Vdc supervised digital output module with 16 outputs that use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 16 output points is on or off.

Each digital output module executes an "output voter diagnostic," in which the state of each point is momentarily reversed to verify that the output is not stuck on or off. Loop-back on the module allows each microprocessor to read the output value for the point to determine whether a latent fault exists within the output circuit. On dc voltage digital output modules, the output signal transition is 2 milliseconds or less and transparent to most field devices. On ac voltage digital output modules, the diagnostic process will cause the output signal to transition to the opposite state for a maximum of half an ac cycle. This transition may not be transparent to all field devices. This feature can be disabled for applications in which the attached devices cannot tolerate a signal transition of this type. Determining the suitability of this feature is a plant-specific requirement.

Supervised digital output modules provide both voltage and current loopback for fault coverage of both energized-to-trip and de-energized-to-trip conditions and verify the presence of the field load through continuous circuit-continuity checks.

2.1.3.4 Analog Output Module

The only analog output module available for safety-related use in nuclear power plants is the Model 3805EN 4-20 mA analog output module. This model has eight dc-coupled outputs, all with a common return. This module provides for redundant loop power sources with individual indicators. If this option is used, the licensee must provide external loop power supplies for analog outputs.

2.1.3.5 Pulse Input Module

The only pulse input module available for safety-related use in nuclear power plants is the Model 3510N pulse input module with 8 inputs that do not use a common reference point. This module senses voltage transitions from magnetic transducer input devices, and counts the number of transitions (or pulses) during a selected period of time. The pulse count is measured to a resolution of 1 microsecond. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the eight input points is on or off.

2.1.3.6 Thermocouple Input Modules

The following types of thermocouple input modules are available for safety-related use in nuclear power plants:

- Model 3706AN is a non-isolated thermocouple input module with 32 differential dc-coupled inputs. This module can support thermocouple types J, K, and T, and can provide upscale or downscale burnout detection depending on the selected field termination.
- Model 3708EN is an isolated thermocouple input module with 16 differential isolated inputs. This module can support thermocouple types J, K, T, and E, and can be programmed to provide upscale or downscale burnout detection. In addition to the Pass/Fault/Active indicator lights, this module has an indicator light that shows a failure of a cold-junction transducer.

Thermocouple input modules are programmable to select the thermocouple type and engineering units (either Celsius or Fahrenheit). Each module can support a variety of thermocouple types, as indicated in the specifications.

Triplicated temperature transducers residing on the field termination module support cold-junction compensation. Each leg of a thermocouple module performs auto-calibration and reference-junction compensation every 5 seconds using internal voltage references. On the Model 3708EN isolated thermocouple module, a cold-junction indicator shows a failure of a cold-junction transducer. On the Model 3706AN non-isolated thermocouple module, a fault indicator shows a transducer fault.

2.1.3.7 Relay Output

The only relay output module available for safety-related use in nuclear power plants is the Model 3636TN relay output module, which has 32 normally open non-common simplex outputs. This is a non-triplicated module for use on non-critical points that are not compatible with "high-side" solid-state output switches. The Model 3636TN relay output module receives output signals from the main processors on each of the three legs. The three sets of signals are then voted, and the voted data is used to drive the 32 individual relays. Each output has a loopback circuit that verifies the operation of each relay switch, independent of the presence of a load. Ongoing diagnostics test the operational status of the relay output module, which is not intended for use on critical points or switching of field loads. In addition to the Pass/Fault/Active indicator lights, this module has indicator lights showing if each of the 32 output points is on or off.

2.1.4 Communications Modules

The communications modules of the Tricon PLC system have three separate communication buses which are controlled by three separate communication processors, one connected to each of the three main processors. All three bus interfaces merge into a single microprocessor on each communications module, so the modules lose their triple redundancy feature at this point. The microprocessor on each communications module votes on the messages from the three main processors and transfers only one of them to an attached device or external system. If two-way communication is enabled, messages received from the attached device are triplicated and transmitted to the three main processors.

The communication paths to external systems have cyclic redundancy checks (CRC), handshaking, and other protocol-based features, depending on which devices are attached to the communication modules, and how the communication modules are programmed. These features are supported in both hardware and firmware.

Three types of communications modules are available for safety-related use in nuclear power plants. Specifically, these are:

- The Model 4119AN enhanced intelligent communications module allows the Triconex PLC system to communicate with other licensee systems using a Modbus interface. The enhanced intelligent communications module contains four serial ports and one parallel port that can operate concurrently. Each serial port is uniquely addressed and supports

either the Modbus or TriStation interface. The parallel port provides a Centronics interface to a printer.

- The Model 4609N advanced communications module is an interface between the Triconex PLC system and the Foxboro Intelligent Automation Series distributed control system. The Triconex system appears as a "control processor" node on the Foxboro Intelligent Automation communication network. The advanced communications module can be configured for one-way information transmission.
- The Model 4329N network communications module allows the Triconex PLC system to communicate with other Triconex PLC systems and with external hosts over IEEE 802.3 (Ethernet) networks. This includes PCs running the TriStation programming software. The network communications module has two BNC port connectors; Net 1 supports Peer-to-Peer and time synchronization protocols, and Net 2 supports open networking to external systems using Triconex applications.

In the Model 4609N advanced communications module, the microprocessor votes on the communication messages from the three MPs and transfers only one of them to an attached external system. By contrast, the Model 4119AN enhanced intelligent communications module and the Model 4329N network communications module (NCM) use the most recent information without voting. For two-way communications, messages received from the attached external system are triplicated and transmitted to the three MPs.

By means of these communications modules, the Triconex PLC system can interface with Modbus masters and slaves, other Triconex PLC systems in peer-to-peer networks, external hosts running applications over IEEE 802.3 networks, and Honeywell and Foxboro distributed control systems. For data sent out to other systems, the main processors broadcast data to the communications modules across the communication bus. Data is typically refreshed during every scan, and is never more than two scan-times old.

As a practical matter, for safety-related applications in nuclear power plants, these modules are limited to communicating non-safety-related information from the Tricon PLC system to other plant systems, and for the TriStation 1131 programming computer to load information or programs to the Tricon PLC system. In this instance, the Model 4329N NCM would be used with the IEEE 802.3 Ethernet. The staff notes that the IEEE 802.3 protocol is by its nature not deterministic in the general case. However, the IEEE 802.3 protocol is acceptable for applications downloading because: (1) there are only two nodes on the network (the Tricon PLC system and the TriStation); (2) the PLC is off-line, and (3) a CRC check is performed to ensure that the application program has not been modified during the download operation.

2.2 Software Description

The Tricon PLC system uses three types of software, including the safety-related operating system software, the safety-related plant-specific applications programs, and the non-safety-related TriStation 1131 software used to develop and generate those application programs. The following subsections describe each of these types in greater detail.

2.2.1 Safety-Related Operating System Software Description

In the Triconex PLC system, safety-related operating system software resides in the main processor modules, I/O modules, and communications modules. All safety-related software exists permanently in electronically erasable programmable read only memory (EEPROM) and, therefore, can be considered firmware.

2.2.1.1 Main Processor Module Software

Each Triconex PLC system has three MP boards, each of which contains a separate copy of identical software. Each main processor board contains three microprocessors, the main microprocessor, the IOC, and the COM. Each of these microprocessors has different software (as shown in the following table), but each is safety-related. The main microprocessor is a 32-bit microprocessor that runs both the TSX operating environment software and the plant-specific application software. The IOC and the COM are 8-bit microprocessors that run communication-related software to control one of the external bus functions of the Tricon PLC system. Specifically, the IOC manages the I/O bus, while the COM manages the communications bus.

2.2.1.1.1 TSX Operating Environment Software

The main processor on the Model 3006N module uses TSX Version 5211 operating environment firmware, which is responsible for performing built-in self-diagnostics, managing the triple-redundancy features, and executing the application software. The operating system executes a sequence of steps in four main blocks, known as Power Up, Background, Scan Level, and Loader. A detailed description of the operating system is provided in Triconex document number 7286-535, "Software Qualification Report." The four main blocks perform the following:

- Power Up performs memory, clock, and Tribus communication tests. These functions are only performed when the system is powered up or reset, and are not performed during normal operation.
- Background performs runtime diagnostic and fault analysis functions, including microprocessor checks, verification of constants stored in RAM, checks of the I/O and communication bus interfaces, checksum checks on the application programs, and Tribus fault analysis tests.
- Scan Level obtains and votes on input data, executes the application programs, and generates outputs at the scan cycle interval set by the application programs. The input data validation checks described above are completed during this step.
- Loader processes any TriStation messages when the key switch on the main chassis is in the "remote" position.

Safety-related Software

Type	Identification	Ver.	Used in
Main Micro Processors	TSX	5211	3006N Enhanced main processor II
	IOC	5212	3006N Enhanced main processor II
	COM	5206	3006N Enhanced main processor II
Communication	ICM	4930	4119AN EICM, V9, Isolated 4329N Network Communication Module 4609N Advanced Communication Module
	ACMX	5203	4609N Advanced Communication Module
	NCMX	5028	4329N Network Communication Module
	IICX	5276	4119AN EICM, V9, Isolated
	RXM	3310	4210N Remote Extender Module, Primary 4211N Remote Extender Module, Remote
Input/Output	AI/NITC	4873	3700AN AI Module, 0-5 Vdc, 6% Overrange 3701N AI Module, 0-10 Vdc 3706AN NITC Input Module
	EIA/ITC	5491	3703EN EAI Module, Isolated 3708EN ITC Thermocouple Input Module
	PI	4559	3510N Pulse Input Module
	EDI	5490	3501TN EDI Module, 115V ac/dc 3502EN EDI Module, 48V ac/dc 3503EN EDI Module, 24V ac/dc 3505EN EDI Module, 24 Vdc, Low Threshold
	HDI	5499	3704EN HDDI Module, 24/48 Vdc 3504EN HDAI Module, 0-5/0-10 Vdc
	EAO	5595	3805EN Analog Output Module, 4-20 mA
	EDO	5488	3601TN EDO Module, 115 Vac 3604EN EDO Module, 24 Vdc 3607EN EDO Module, 48 Vdc
	ERO	5497	3636TN ERO Module, N.O., Simplex
	TSDO	5502	3603TN EDO Module, 120 Vdc 3623N SDO Module, 120 Vdc 3624N SDO Module, 24 Vdc

The TSX software operates primarily on a continuous loop basis, and does not use a real time kernel. However, the TSX software does use some interrupts to periodically trigger execution of the application software, manage the Tribus and the Triclock mechanism and trigger the

watchdog timer. A diagnostic failure also generates an interrupt signal. The TSX software comprises about 45,000 lines of code developed in C programming language.

2.2.1.1.2 IOC Software

The IOC on the Model 3006N main processor module uses IOC version 5212 firmware which provides the interface between the main processor and the system I/O modules via the I/O bus. The IOC interchanges data with the MP using the shared RAM data structures based on the I/O module configuration.

2.2.1.1.3 COM Software

The COM on the Model 3006N main processor module uses COM version 5206 firmware, which provides an interface between the main processor and the system communications modules via the communications bus. The COM interchanges data with the MP using the shared RAM data structures based on the COM module configuration.

2.2.1.2 I/O Module Software

The Tricon PLC input modules are responsible for receiving sensor data from the attached instrumentation, manipulating the data as required, and passing the data to the IOC via the I/O bus. The output modules receive data from the IOC via the I/O bus, convert it as required, and pass it on to the connected output devices.

On each I/O module the firmware is replicated on each of the three legs, for use by the three leg-specific microprocessors, which exchange diagnostic data but not field data. The I/O modules do not contain plant-specific application software; however, an I/O module can be dedicated to a specific use in a plant-specific system by setting the parameters within this firmware. The firmware of the input modules continuously polls the input points from the field sensors and updates the input database for its own leg. The firmware of the output modules continuously reads the output data provided by the main processor and updates the output registers of its own leg.

In both the input and output modules, the firmware is responsible for performing self diagnostics and handling communication with the main processor via each leg's individual I/O bus. This bus is a serial bus, and the I/O modules operate as slaves responding to requests from the master main processor board.

The I/O data is continuously updated using an infinite loop that also runs diagnostics. Communication with the main processors is performed via interrupts from the I/O processor.

Even though each type of I/O module has its own specific firmware, all I/O modules have the same basic design and share common parts of the source code. The code was originally written in assembly language and is now progressively being replaced by C code. All I/O modules have both software and hardware watchdog timers to monitor and verify bus and module activity.

The staff reviewed the following I/O module firmware:

- AI/NITC version 4873, used in: 3700AN AI Module, 0-5 Vdc
3701N AI Module, 0-10 Vdc
3706AN NITC Input Module

This firmware converts analog input voltage signals to digital values and transmits the values to the IOC on demand. Automatic calibration is performed on the analog-to-digital converters. For the Model 3706AN thermocouple module, linearization of the selected thermocouple type and cold junction compensation are performed and the resultant temperature is passed to the IOC.

- EIAI/ITC version 5491, used in: 3703EN EAI Module
3708EN ITC Thermocouple Input Module

This firmware converts the analog input voltage signals to digital values and transmits the values to the IOC on demand. Automatic calibration is performed on the analog-to-digital converters.

- PI version 4559, used in: 3510N Pulse Input Module

This firmware counts voltage transitions during a time window, converts the raw counts to either frequency or revolutions per minute (RPM), and transmits the values to the IOC on demand.

- EDI version 5490, used in: 3501TN EDI Module, 115Vac/dc
3502EN EDI Module, 48Vac/dc
3503EN EDI Module, 24Vac/dc
3505EN EDI Module, 24 Vdc, Low-Threshold

This firmware converts the input voltage signals to digital values and transmits the values to the IOC on demand. The inputs are transmitted using optical isolation circuitry. For the Model 3502EN and 3505EN, the module can perform a self-test to check for conditions where the input circuitry is "stuck on."

- HDI version 5499, used in: 3704EN HDDI Module, 24/48 Vdc (24V)
3504EN HDAI Module, 0-5/0-10 Vdc

This firmware converts the isolated, variable analog input voltage signals to digital values and transmits the values to the IOC on demand.

- EAO version 5595, used in: 3805EN Analog Output Module, 4-20 mA

This firmware receives data from the IOC, performs a digital-to-analog conversion, and votes on which of the three hardware channels is to be provided to the single output point. Each output is checked for accuracy, and any of the three outputs that fail(s) to produce the correct current output value is replaced.

- EDO version 5488, used in: 3601TN EDO Module, 115 Vac
3604EN EDO Module, 24 Vdc
3607EN EDO Module, 48 Vdc

This firmware receives data from the IOC and outputs data to the output switches. A quadruplicated voter exists on each output point. The output of the voter is then provided to the field devices. The voltage on each output is checked, independently of any attached load. Failure of the detected field voltage to match the commanded state is considered an error and annunciated. Additional diagnostics are performed on the module.

- ERO version 5497, used in: 3636TN ERO Module, N.O., Simplex

This firmware receives data from the IOC, votes on it, and outputs it to the individual relays. Each output has a loopback circuit, which does not depend on the presence of a load. This loopback feature is used by diagnostics to test the operational status of the module.

- TSDO version 5502, used in: 3603TN EDO Module, 120 Vdc
3623N SDO Module, 120 Vdc
3624N SDO Module, 24 Vdc

This firmware receives data from the IOC and outputs data to the output switches. A quadruplicated voter on each output point provides its output to the field devices. The voltage on each output is checked, independent of any attached load. The current flowing through the output switch is also checked. Diagnostics are provided to verify the operation of each element in the output voter and the presence of a load.

2.2.1.3 Communications Module Software

The firmware in the Tricon PLC communications modules is somewhat different from that in the I/O modules in that each module has two types of firmware, one that is common to all three communications modules, and the one that is module-specific. The staff reviewed the following communications module firmware:

- ICM version 4930, used in: 4609N Advanced Communication Module
4119AN EICM, Isolated
4329N Network Communication Module

This firmware is common to all communications modules. It provides the interface to the triplicated communication buses, votes on output messages, and replicates the input messages to the three communication buses. It also includes common module diagnostics.

- ACMX version 5203, used in: 4609N Advanced Communication Module

This firmware provides the Triconex-generated portion of the software that is needed for module hardware interfaces and communication protocols required to communicate with

the Foxboro Intelligent Automation (IIA) system and the TriStation 1131. This firmware also provides the diagnostic interfaces to the module-specific hardware.

- NCMX version 5028, used in: 4329N Network Communication Module

This firmware provides the module hardware interfaces and communication protocols required for peer-to-peer communication and time synchronization with other Tricon PLC systems, with external hosts over IEEE 802.3 Ethernet networks, and with the TriStation 1131. This firmware also provides the diagnostic interfaces to the module-specific hardware.

- IICX version 5276, used in: 4119AN EICM, V9, Isolated

This firmware provides the module hardware interfaces and communication protocols required to communicate with Modbus masters and slaves, as well as printers. This firmware also provides the diagnostic interfaces to the module-specific hardware.

Except when downloading application software or updating parameters such as setpoints, a plant system built with a Tricon PLC does not need or use these communications modules or features to perform safety-related functions.

A special case of communications module firmware is used by the primary and remote extender modules. This firmware, RXM version 3310, is used by both the 4210N Remote Extender Module and the 4211N Remote Extender Module. This firmware allows extending the copper I/O Bus over extended distances.

2.2.2 Safety-Related Plant-Specific Application Software

The plant-specific application software implements the desired safety-related functions. This software is developed on a PC with the TriStation 1131 Developers Workbench (discussed in Section 2.2.3) and downloaded to the main processor boards. The application software consists of a sequence of calls to the basic functions that are available on libraries stored in the TriStation 1131. Those basic functions that are used by the applications programs are downloaded to the main processor boards along with the application software. As this software is plant specific (not generic) in nature, the staff did not review or approve any applications programs. Plant-specific reviews will be required for approval of applications software.

2.2.3 TriStation 1131 Software

The TriStation 1131 Developers Workbench is a software tool designed to generate the plant-specific application programs. The software runs on a standard commercial PC using the Windows NT operating system. The TriStation 1131 Developers Workbench does not perform safety-related functions, but allows the user to generate safety-related software for the Tricon PLC. The TriStation 1131 PC is not normally connected while the Tricon PLC system is running safety-critical functions. The only time that the TriStation PC and TriStation 1131 should be connected to the safety-related system is while new or modified programs are being downloaded to the Tricon PLC system. (It is physically possible for the TriStation PC to be connected at other times, and this should be prevented via administrative control.)

The TriStation 1131 Developers Workbench can use any one of four programming languages. Specifically, these are Structured Text, Function Block Diagrams, and Logic Diagrams, as well as the Triconex-defined Cause-and-Effect Matrix Language (CEMPLE). The first three of these programming languages conform to the requirements of the International Electrotechnical Commission (IEC) Standard 61131-3, "Programming Languages," dated 1993. The Developers Workbench uses a graphical user interface, and has language editors; compilers; linkers; emulation, communication, and diagnostic capabilities for the Tricon PLC system.

The TriStation 1131 Developers Workbench translates the program written in one of the four languages into native mode executable code. Logic Diagrams, Function Block Diagrams, and CEMPLE are translated into Structured Text. The Structured Text is then translated into an emulated code, which can in turn be translated into native mode assembly language. The assembly language code is then assembled and linked with native mode code libraries to generate an executable program. Up to this point, all application development may be performed off line, with no physical connection between the TriStation PC and the Tricon PLC system. After the executable program is tested and verified, the TriStation PC can be attached to the Tricon PLC system, and the executable application program can be downloaded to the PLC via the NCM module.

During the download process, the individual communication blocks of programs and translated code are protected by 32-bit CRC and communication blocks are rejected if the CRC fails to match. In addition, 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 PLC system.

The TriStation 1131 Developers Workbench has the ability to emulate a given applications program running on the Tricon PLC system. This emulation allows manual input of program variables and observation of program outputs on the PC screen, with the input and output values merged and displayed with the program blocks. This emulation can be used in the validation of new or modified application code.

These features of the TriStation 1131 Developers Workbench enable the developer to perform the following tasks:

- Develop programs and other executable elements (such as functions, function blocks, data types) using any of the available language editors.
- Select functions and function blocks from the IEC-compliant libraries and/or custom libraries.
- Graphically configure the I/O modules and points for each chassis in a Tricon PLC system.
- Configure a Tricon PLC system to use the integrated sequence of events (SOE) capability.
- Apply password protection to projects and programs according to user names and security levels.

- Debug program logic by emulating execution.
- Download the newly created applications programs to the Tricon PLC system.
- Display diagnostic information about system performance and fault details.

2.3 Tricon PLC Product Qualifications

The Tricon PLC hardware is qualified for a mild environment, such as a main control room and auxiliary electrical equipment rooms. Triconex performed pre-qualification, environmental, seismic, electro magnetic interference/radio frequency interference (EMI/RFI), surge withstand, and Class 1E to non-1E isolation tests; these tests were performed in the listed order and in accordance with the requirements of EPRI TR-107330. A test system (as described below) was assembled and used for all tests; this system was reconfigured as necessary to support the protocol and worst-case loading scenario for each test.

The Tricon PLC test system contained the following components for which Triconex has requested qualification for safety-related use in nuclear power plants:

- 19-inch Chassis, Models 8110 (Main), 8111 (Expansion), and 8112 (Remote Expansion)
- Power Modules, Models 8310 (115 V), 8311 (24 Vdc), and 8312 (230 Vac)
- Main Processor Module, Model 3606
- Analog Input Modules, Models 3700A, 3701, 3703E, and 3704E
- Digital Input Modules, Models 3501E, 3502E, 3503E, 3504E, and 3505E
- Pulse Input Module, Model 3510
- Thermocouple Input Modules, Models 3706A, and 3708E
- Analog Output Module, Model 3805E
- Digital Output Modules, Models 3601E, 3603E, 3603T, 3604E, 3607E, 3611E, 3623, and 3624
- Relay Output Module, Model 3636R
- Remote Extender Modules, Models 4210, and 4211
- Communications Modules, Models 4119A, 4329, and 4609

The test system also included various ETAs, signal and communication cables, an RTD input signal conditioning panel, and a third-party 24 Vdc field power supply (Lambda Model LNS-P-24).

2.3.1 Environmental Requirements

The objective of the environmental testing was to demonstrate that the Tricon PLC will not experience failures due to abnormal service conditions of temperature, humidity, power source variation, or radiation. EPRI TR-107330, section 4.3, provides the environmental requirements for commercial PLC equipment.

Criteria for environmental qualifications of safety-related equipment are provided in General Design Criterion (GDC) 2, "Design Bases for Protection Against Natural Phenomena," and GDC 4, "Environmental and Dynamic Effects Design Bases," as specified in Appendix A to 10 CFR Part 50. The staff conducted its reviews in accordance with the guidance provided in Appendix

7.1-A to NUREG-0800, the NRC's Standard Review Plan (SRP) Revision 4, dated June 1997, which references Appendix 7.1-B, item 5, and Appendix 7.1-C, item 9. These two items reference American National Standards Institute (ANSI)/IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," dated January 1997.

2.3.2 EMI/RFI Requirements

Section 4.3.7 of EPRI TR-107330 states that PLC systems shall be able to withstand the EMI/RFI levels as given in EPRI TR-102323.

2.3.3 Electrostatic Discharge (ESD) Withstand Requirements

Section 4.3.8 of EPRI TR-107330 requires that when installed in its chassis, the PLC platform and associated devices shall have the capability to withstand ESD as required by EPRI TR-102323 without disrupting operation or causing any damage.

2.3.4 Seismic Withstand Requirements

Section 4.3.9 of EPRI TR-107330 requires that the PLC platform must be qualified as a Category I seismic device, and therefore must perform as required and remain operational for the specified level of vibration during and following the application of a safe shutdown earthquake applied in three orthogonal directions.

2.3.5 Surge Withstand Requirements

Section 4.6.2 of EPRI TR-107330 requires that the PLC platform be capable of withstanding surges with a characteristic of both the standard 0.5 μ s-100 kHz ring wave and the standard 1.2/50 μ s-8/20 μ s combination wave described in IEEE C62.41. The withstand level shall be consistent with Section 9 of IEEE C62.41 for location "B" and "medium exposure" except that the applied voltage shall be 3,000 V peak. The testing requirements are shown in Section 6.3.5 of EPRI TR-107330. Additional requirements are found in EPRI TR-102323.

2.3.6 Class 1E to Non-1E Isolation Requirements

Section 4.6.4 of EPRI TR-107330 provides the Class 1E to Non-1E isolation requirements, stating that the PLC modules must provide an isolation capability of at least 600 Vac and 250 Vdc applied for 30 seconds. Additional requirements are provided in IEEE Std 384-1977, "Criteria for Independence of Class 1E Equipment and Circuits."

3.0 REVIEW CRITERIA

The acceptance criteria for this review is defined in NUREG-0800, the NRC's SRP, Revision 4, dated June 1997. The subsections below will list which portions of 10 CFR Part 50, general industry standards, Branch Technical Positions (BTPs), and other guidance used in this review, as well as the methodology used when conducting this review.

3.1 General Standards

The staff performed this review using the acceptance criteria defined in NUREG-0800, the NRC's SRP, Revision 4, dated June 1997. Specifically, Section 7 of the SRP addresses the requirements for instrumentation and control (I&C) systems in light-water nuclear power plants. Revision 4 is particularly notable, in that it refined the procedures for reviewing digital systems, which principally appear in SRP Appendices 7.0-A, 7.1-A; Sections 7.1, 7.8, 7.9; and BTPs HICB-14, HICB-17, HICB-18, HICB-19, and HICB-21. SRP Appendix 7.1-C and Sections 7.2 through 7.7 provide additional criteria that the staff applied in the review of the appendices to Triconex's topical report.

Because the Tricon PLC system is a commercial, off-the-shelf (COTS) PLC system, two EPRI documents apply. The first is EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial-grade Digital Equipment for Nuclear Safety Applications," dated October 1996, reviewed by the staff and approved in a safety evaluation report (SER) dated April 1997. The second document is EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Application in Nuclear Power Plants," which the staff approved on July 30, 1998. Triconex has stated that its submittals follow the guidance of both of these documents.

SRP Table 7-1 lists a number of codes and standards that apply to the review of digital I&C systems. Many of these deal with plant-specific requirements and, therefore, cannot be addressed in the review of a generic topical report. These plant-specific requirements were not considered in performing this safety evaluation, but will be subject to the reviews of future plant-specific applications when submitted by licensees. Many of the other codes and standards listed in SRP Table 7-1 assume that the equipment and systems to be evaluated are specifically designed as nuclear safety-related equipment in accordance with Appendix B of 10 CFR Part 50. This was not the case for the Tricon PLC system. For this reason, these codes and standards were used as guidance during the review of the Tricon PLC system, but not as absolute requirements. The overriding criterion for this review was that in the case where the methods and techniques used by Triconex were not identical to the approved methodology, those methods and techniques were of sufficient quality to provide the staff with reasonable assurance that the quality and operability of the Tricon PLC are suitable for safety-related use in nuclear power plants.

Specifically, the staff considered the following codes and standards, and used them as a yardstick against which to measure the Triconex design effort and the Tricon PLC system when reaching this determination of suitability:

- 10 CFR 50.55a(a)(1)

- 10 CFR 50.55a(h)
- 10 CFR 50, Appendix A, GDC as follows:
 - GDC 1, Quality Standards and Records
 - GDC 2, Design Basis for Protection Against Natural Phenomena
 - GDC 4, Environmental and Missile Design Bases
 - GDC 13, Instrumentation and Control
 - GDC 20, Protection System Functions
 - GDC 21, Protection System Reliability and Testability
 - GDC 22, Protection System Independence
 - GDC 23, Protection System Failure Modes
 - GDC 24, Separation of Protection and Control Systems
 - GDC 29, Protection Against Anticipated Operational Occurrences
- RG 1.22, "Periodic Testing of Protection System Actuation Functions"
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"
- RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems"
- RG 1.62, "Manual Initiation of Protection Actions"
- RG 1.75, "Physical Independence of Electrical Systems"
- RG 1.89, "Qualification for Class 1E Equipment for Nuclear Power Plants"
- RG 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"
- RG 1.100, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants"
- RG1.105, "Instrument Spans and Setpoints"
- RG 1.118, "Periodic Testing of Electric Power and Protection Systems"
- RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
- RG 1.153, "Criteria for Power Instrumentation and Control Portions of Safety Systems"
- RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

- RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.172, "Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

3.2 Method of Review

In addition to reviewing Triconex's topical report, the staff held several public meetings at NRC and at MPR Associates in Alexandria, Virginia. The staff also conducted an audit on February 12-15, 2001, at the Triconex design and manufacturing site in Irvine, California, to discuss various aspects of the Tricon PLC design. These meetings successfully yielded answers to the staff's questions, making it unnecessary for the staff to request additional information.

The suitability of a digital platform for use in safety systems depends on the quality of its components; design quality; and system implementation aspects such as real-time performance, independence, and online testing. Section 4 of this safety evaluation discusses the staff's review of these system implementation aspects and the quality of the Tricon PLC platform components.

The acceptance process for most commercial-grade digital components typically comprises a variety of complicated technical activities. Consequently, the staff applied the guidance in EPRI TR-106439 and TR-107330 in reviewing the Triconex program for qualifying the Tricon PLC hardware and software. In evaluating the Tricon PLC platform for use in safety-related applications in a nuclear power plant, the staff reviewed (1) the hardware design, (2) the firmware and programming software design, (3) the qualification testing, (4) the qualification analyses, and (5) the history of commercial use of the Tricon PLC system. At this stage, the staff was looking programmatically at the design process and making comparisons to the applicable review guidance. The staff also reviewed the specific verification and validation performed on the software by the German Technischer Überwachungs-Verein (TÜV) Rheinland, and the critical design review performed by MPR Associates and ProDesCon. In addition, the staff performed a "thread audit," which involved selecting samples of assumed plant parameters and tracing the implementation of those parameters through the hardware and software. This review included evaluating actual sections of the code on a sample basis, and following the signal path through the hardware circuitry.

4.0 EVALUATION

Triconex designed and built the Tricon PLC system as a commercial-grade system, rather than specifically for use in safety-related systems in nuclear power plants. As a result, the design process was not governed by Appendix B to 10 CFR Part 50, and the related process documentation is not consistent with BTP HICB-14. EPRI TR-106439 and TR-107330 recognize that commercial design practices differ from nuclear specific design practices, and discuss how the essential technical characteristics of commercial PLC and digital system products meet the requirements, intent and quality characteristics needed for safety-related systems in nuclear power plants.

The Tricon PLC system design has evolved into a mature product over more than 15 years, and Triconex's software quality assurance (QA) program has also improved significantly over that period. The current QA program satisfies the provisions established by BTP HICB-14. In addition, Triconex has developed the TriStation 1131 Developers Workbench for engineering support and programming of the Tricon PLC system over the past 7 years, under a process that is compatible with the intent of BTP HICB-14.

4.1 Tricon PLC Hardware Design Review

The review of the Tricon PLC system hardware design included the hardware architecture and signal flow, quality provisions for the hardware, and the environmental testing and qualification methodology and results.

4.1.1 Hardware Architecture and Signal Flow

The staff reviewed the Tricon PLC hardware design, as well as the signal flow through that design. The Tricon PLC system uses a triple-redundant architecture to provide fault tolerance and uninterrupted control in the presence of either hard failures of components or transient faults from internal or external sources. Sensor signals are received on termination assemblies, which are constructed as electrically passive circuit boards to which field wiring is attached. The termination module passes input signals from the field to an input module. Each input module consists of three identical and independent circuits, all contained on a single printed circuit assembly. Each of the three input legs asynchronously measures the input signals from the input termination module and places the values into input tables. Each input table is regularly interrogated over the I/O bus by the I/O communication processor which is located on the corresponding main processor module.

As each input module is polled, the appropriate leg of the I/O bus transmits new input data to the main processor, where it is assembled into a table that is stored in memory for use in the hardware voting process. The input table in each main processor is transferred to its neighboring main processors over the Tribus. Hardware voting takes place during this transfer. The Tribus uses direct memory access to synchronize, transmit, vote, and compare data among the three main processors. If a disagreement occurs, the signal value found in two out of three tables prevails, and the third table is corrected accordingly. One-time differences that result from sample timing variations are distinguished from a pattern of differing data. Each main processor maintains data about necessary corrections in local memory. Any disparity is

flagged and used at the end of the scan by the built-in fault analyzer routines of the Tricon PLC system to determine whether a fault exists on a particular module.

The main processors enter corrected data into the control program, which the main microprocessor and a math coprocessor execute in parallel with the neighboring main processor modules. The control program generates trip or control signals on the basis of licensee specific application programs. The I/O communication processor on each main processor module sends the output data to output modules via the I/O bus. In the event of a trip signal, the output modules use termination assemblies to transfer the trip signal to the actuation devices.

If an I/O module channel fails to function, an alarm is raised to the MPs. If a redundant module is installed in the paired slot with the faulty module, and that module is deemed healthy by the MPs, 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 control is unaffected. The user obtains a replacement unit and plugs it into the system in the paired slot associated with the failed module. (This position is logically paired with the failed module's location.) When the MPs 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 user then removes the faulty module for repair or replacement.

If redundant modules are installed and both are deemed healthy by the MPs, the MPs will swap control between the redundant modules so that each is used on a periodic basis. By periodically using each module, any faults will be detected and alarmed, and the failed module will be replaced while a redundant module is in place. This use of redundant modules does not cause process upsets, and is undetectable outside of the Tricon PLC system.

The staff finds that the design is suitable for use in nuclear power plants when appropriately implemented.

4.1.2 Hardware Quality

The Tricon PLC system was initially developed in 1986. The vendor, Triconex, states that it uses good practices consistent with the objective of producing a highly reliable safety system, and the first Triconex QA Manual was developed in 1986 on the basis of the requirements established in the standard formerly titled American Society of Mechanical Engineers "Quality Assurance Program Requirements for Nuclear Facilities," NQA-1. In addition, Triconex has specifically developed all quality-related manuals and procedures for the Tricon PLC system. Specifically, the following manuals that describe the processes and procedures for the various aspects of the Tricon PLC system manufacture were reviewed as part of the staff audit:

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

The QAM provides the overall corporate QA requirements for the Tricon PLC system, including specific procedures for the Triconex QA organization. The first revision of the QPM, in 1992, contained procedures specific to manufacturing activities, while the 1994 revision included procedures specific to product development. The EDM provides the procedures pertinent to the development, configuration control, maintenance, and modification of the Tricon PLC system.

The QAM requires that all materials and services that are incorporated into or directly related to Triconex products must be procured from approved vendors. Potential vendors are assessed by the Vendor Assessment Team (VAT) on the basis of the vendor's responses to a questionnaire. The VAT may also perform a follow-up in-depth audit and/or a vendor site survey to evaluate the vendors' manufacturing and QA capabilities. The Quality Assurance Review Board then makes the final decision regarding vendor approval, and Purchasing and Manufacturing maintains a list of approved vendors. Nuclear vendors are evaluated and audited to verify their capability to meet the QA requirements of Appendix B to 10 CFR Part 50.

Two other documents are part of the Triconex QA system. The Triconex General Manual (TGM) requires that critical characteristics of the parts be identified. The Invensys Process System (IPS) is used to document the engineering evaluation of commercially procured items, and an evaluation must consider the item's intended use, its safety-related function, its traceability requirements, and its critical characteristics. The acceptance of any IPS item is contingent on verification of the critical characteristics. The method of acceptance may include: (1) source inspection and/or special testing as part of the receiving inspection, (2) a certificate of conformance, (3) pre-established tests or checks as part of installation or integration, and/or (4) evaluation of historical performance. For nuclear parts, TGM D-4 notes that historical performance cannot be used as the sole basis for acceptance.

The purchasing data for nuclear safety-related equipment and services are to be so identified, and must include a vendor QA program meeting the criteria of Appendix B to 10 CFR Part 50 and 10 CFR Part 21. Purchasing records consisting of (1) vendor approval documentation, (2) vendor audit reports, (3) the approved vendor list, (4) the approved material list, (5) source inspection reports, (6) first article inspection reports, (7) purchase orders, and (8) the IPS are assigned to responsible departments in the Triconex organization.

Triconex procures the commercial-grade items used in the Tricon PLC platform from various commercial-grade vendors. As part of the commercial-grade dedication (CGD) of these items, Triconex teams conducted reviews at the vendors' facilities to assess the quality of the vendors' activities. These reviews focused on the vendors' hardware and software life cycle with regard to the following:

- well-defined system hardware and software requirements;
- comprehensive hardware and software development methodologies;
- comprehensive test procedures;
- strict configuration management and maintenance procedures; and
- complete and comprehensive documentation.

The findings of the Triconex review teams were documented in Triconex proprietary reports and records which the staff reviewed as part of its hardware QA audit.

On the basis of its review of the manuals and audit of the Triconex facility and manuals with its walkthrough of purchasing and parts quality, the staff concludes that the quality of the Tricon PLC platform components is adequate for safety-related use in nuclear power plants.

4.1.3 Environmental Testing and Qualification

To comply with the requirements of GDC-4, 10 CFR 50.49, and IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," environmental qualification must demonstrate that the design basis and performance requirements of the I&C system are met when the equipment is exposed to normal and adverse environments. The subsections below will discuss the staff review of the Tricon PLC system environmental testing performed by Triconex.

4.1.3.1 Pre-qualification Testing

Triconex performed pre-qualification testing to (1) confirm that the Tricon PLC test system was properly configured and operational, (2) provide baseline performance data for comparison with data obtained during and after qualification testing, and (3) validate the test procedures. Pre-qualification testing included the following assessments:

- The system setup and checkout test documented proper configuration and operation of the Tricon PLC test system, including hardware, software, input and output simulators; test and measurement equipment; and interconnecting cabling.
- The operability test to establish baseline performance included tests for analog module accuracy, system response time, operation of discrete inputs and outputs, performance of timer functions, failover tests (associated with the failure of redundant components), loss of power, detection of failure to complete a scan, power interruption, and power quality tolerance.
- Prudency testing demonstrated the ability of the Tricon PLC system test system 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.

Triconex performed these pre-qualification tests in accordance with Section 5.2 of EPRI TR-107330, with two exceptions. Specifically, Triconex did not test the software objects in the PLC library. (The topical report justifies this exception by taking credit for the extensive software object testing that was previously performed by Triconex and TÜV Rheinland.) Also, Triconex performed only limited burn-in testing. (The topical report justifies this exception by taking credit for routine burn-in testing that is performed as part of the manufacturing process for the Tricon PLC system hardware.) Details of the testing can be found in the following Triconex documents:

<u>Document Title</u>	<u>Triconex Document Number</u>
Set-up & Checkout Test Procedure	7286-502
Operability Test Procedure	7286-503
TSAP Validation Test Procedure	7286-513
TSAP Functional Specification	7286-517
TSAP Design Specification	7286-518
TSAP Program Listing	7286-519
Pre-Qualification Test Report	7286-524

The staff concluded, after reviewing these documents, that the pre-qualification testing met the intent of TR-107330.

4.1.3.2 Temperature and Humidity Testing

Triconex performed environmental tests as identified in Section 6.3.3 of EPRI TR-107330 to demonstrate that the Tricon PLC system will not experience failures as a result of abnormal service conditions of temperature and humidity. Specifically, the Tricon PLC system was required to operate under the environmental conditions defined in Section 4.3.6 of EPRI TR-107330, as follows:

The operating environment where the PLC must meet the performance requirements given in Sections 4.3.2 through 4.3.4 are as follows:

- A. Temperature Range. *The PLC shall remain operable over an ambient temperature of 16 to 40°C (60 to 104°F) near the fan inlet if forced circulation is used or at the bottom of the chassis if natural circulation cooling is used.*
- B. Humidity. *The PLC must operate over a 40 to 95% (non-condensing) relative humidity range.*
- C. Power Sources. *The PLC must operate within specification for the power source ranges given in items A and B of Section 4.6.1.1.*
- D. Radiation. *The PLC must operate within specification for radiation exposure of up to 10³ rads.*

The abnormal operating environment where the PLC must meet the performance requirements given in Sections 4.3.2 through 4.3.4 are as follows:

- A. Temperature Range. *The PLC shall remain operable over an ambient temperature of 4 to 50°C (40 to 120°F) near the fan inlet if forced circulation is used or at the bottom of the chassis if natural circulation cooling is used.*
- B. Humidity. *The PLC must operate over a 10 to 95% (non-condensing) relative humidity range.*

- C. Power Sources. *The PLC must operate within specification for the power source ranges given in items A and B of Section 4.6.1.1.*
- D. Radiation. *The PLC must operate within specification for radiation exposure of up to 10^3 rads.*

The PLC shall operate for the temperature/humidity environmental profile given in Figure 4-4 with operability as given in Section 5.3. Evaluations, which provide confidence that none of the components in the PLC platform are degraded by exposure to the radiation level given in the previous section, are adequate for establishing radiation withstand capability.

Triconex performed the temperature and humidity tests using the Tricon PLC test system described in Section 2.3 of this SE and documented the test procedures and results in the "Environmental Test Procedure," document number 7286-506 and in the "Environmental Test Report," document number 7286-525. The test system was configured to maximize internal heat generation, power supply loading, and module point loading during the tests. At least one point on each input/output module was monitored for proper operation during testing. Communications modules were exercised through the interface with external monitoring devices. The third-party field power supply was loaded to 90 percent rated current output and monitored for output voltage variations. Operability and prudency testing was repeated several times during testing and one time after testing to demonstrate that throughout the testing, the Tricon PLC system was operating acceptably. The Triconex topical report stated that, in accordance with Section 5.9.8 of IEEE 381-1977, replacement of faulted or failed modules using spare modules constituted replacement with a similar test component, and allowed continuation of the test from the point of replacement.

Although the relative humidity at the low-temperature condition was not established because of a malfunction in the measuring equipment, the actual moisture content in the test chamber environment at the low-temperature condition was substantially lower than that at the high temperature condition. Accordingly, the test achieved the objective of exposing the tested equipment to a wide range of humidity conditions.

Two hardware faults occurred during the environmental qualification testing of the Tricon PLC system, however, because of the fault tolerant system design, these faults did not affect the expected operation of the system. Specifically, the Model 3603E 120 Vdc digital output module showed a voter fault diagnostic, and the Model 3611E 115 Vac digital output module showed a diagnostic fault message. Both of these faults resulted from component failures. During the environmental testing, Triconex replaced the Model 3603E 120 Vdc digital output module with a spare module, and that spare demonstrated acceptable performance during the remainder of the test. By contrast, on the basis of the post-test inspection results, Triconex withdrew the Model 3611E module from consideration for nuclear safety-related application; therefore the topical report does not list the Model 3611E as one of the modules for which Triconex requested approval. The Model 3601TN provides comparable functionality to the Model 3611E and demonstrated acceptable performance during environmental testing.

By subjecting the test system to a controlled temperature and humidity for the specified time profile and monitoring the performance of the test specimen, these tests demonstrated that the

Tricon PLC system hardware and third party field power supply will function under abnormal temperature and humidity conditions. However, these tests did not demonstrate that the Tricon PLC system is suitable for any particular plant usage, and plant-specific assessment of the suitability of the Tricon PLC system for an application is the responsibility of the licensee.

4.1.3.3 Radiation Withstand Testing

Triconex conducted an analysis to demonstrate that the Tricon PLC system hardware will continue to perform its safety-related function after a cumulative radiation exposure of 1000 rads over a 40-year operating period. This analysis is contained in Triconex Report No. 7286-533, "Radiation Hardness Evaluation." The level of exposure is consistent with installation in a "mild environment" as specified in Section 4.3.6 of EPRI TR-107330. On the basis of that analysis, the staff concludes that the Tricon PLC system hardware is qualified to the radiation exposure levels specified in Section 4.4 of EPRI Technical Report 1000799; however, before installing plant-specific Tricon PLC system equipment, licensees will need to verify that the expected radiation exposure for the equipment is enveloped by the radiation withstand capacity of the Tricon PLC system equipment. In addition, the staff notes that the Triconex analysis did not address the radiation withstand capability of the third-party field power supply. Therefore, the staff finds that before installing the third-party field power supply, a licensee needs to demonstrate the power supply is capable of withstanding the radiation exposure expected in the intended application.

4.1.3.4 Seismic Withstand Testing

To demonstrate that the Tricon PLC system hardware and third-party field power supply will function under seismic motion conditions, Triconex subjected the test system to a series of seismic simulation tests using a triaxial seismic simulator shake table. These tests included resonance search tests and random triaxial multifrequency tests designed to simulate a series of earthquake motions, as specified in IEEE Std 344-1987. The testing is required to include a resonance search followed by five simulated operating basis earthquakes and one simulated safe shutdown earthquake (SSE) at 9.75 g's and 14 g's respectively, based on 5 percent damping. The simulation vibrations are required to be applied triaxially (in three orthogonal directions), with random frequency content. Triconex documented these tests in the "Seismic Test Procedure," Triconex document number 7286-507 and in the "Seismic Test Report," Triconex document number 7286-526.

Triconex configured the chassis to represent lightly loaded to fully loaded module fill conditions. At least one point on each I/O module was monitored for proper operation during testing. A portion of the digital output module points were loaded to rated current carrying capacity and were cycled during testing to demonstrate continued operability. Mechanical relay output points were monitored for contact bounce. Communications modules were exercised through interface with external monitoring devices. The third-party field power supply was loaded to 90 percent rated current output and monitored for voltage and frequency variations. Operability and prudency testing was performed following seismic testing to demonstrate acceptable operation.

With one exception, seismic testing demonstrated that the Tricon PLC equipment can withstand the cumulative effects of a minimum of five operating-basis earthquakes, followed by a safe

shutdown earthquake, without loss of either safety function or physical integrity. The exception is to the maximum acceleration force of the SSE. The acceleration capability of the Triaxial Seismic Simulator Table was limited to a maximum of 10 g's based on 5 percent damping with the equipment tested, and therefore SSE tests were performed using a maximum acceleration level of 10 g's. Seismic testing was performed in accordance with IEEE Std 344-1987 and Section 6.3.4 of EPRI TR-107330.

On the basis of this review, the staff concludes that the tested Tricon PLC system equipment and third-party field power supply are qualified to the triaxial seismic simulator table limits shown in Figure 4-2 of EPRI Technical Report 1000799, with the exception of the maximum acceleration of an SSE. For this reason the staff finds that the Tricon PLC system did not fully meet the requirements of EPRI TR-107330 for seismic requirements, and before using Tricon PLC system equipment in safety-related systems in a nuclear power plant, licensees must determine that the plant-specific seismic requirements are enveloped by the capabilities of the Tricon PLC system. This determination, and the suitability of the Tricon PLC system for a particular plant and application is the responsibility of the licensee.

4.1.3.5 Electromagnetic Compatibility Testing

In order to simplify the plant-specific determination of electromagnetic compatibility, EPRI submitted Topical Report TR-102323, "Guideline for Electromagnetic Interference Testing in Power Plants" for staff review in 1994. That report provided alternatives to performing site-specific EMI surveys to qualify digital plant safety I&C equipment in a plant's electromagnetic environment. Specifically, the recommended alternatives in TR-102323 include (1) a set of EMI/RFI susceptibility testing levels, (2) EMI eliminating practices, and (3) equipment EMI/RFI emission testing levels. In 1996, the NRC staff issued a safety evaluation concluding that the recommendations and guidelines in TR-102323 provide an adequate method for qualifying digital I&C equipment for a plant's electromagnetic environment without the need for plant-specific EMI surveys if the plant-specific electromagnetic environment is confirmed to be similar to that identified in TR-102323. The Tricon PLC system does not meet the guidance of TR-102323.

Triconex performed electromagnetic compatibility (EMC) tests and measurements on the Tricon PLC system test system in accordance with EPRI TR-102323 and Section 6.3.2 of EPRI TR-107330. The details of the tests and measurements are described in the "EMI/RFI Test Procedure," Triconex document number 7286-510, and the "EMI/RFI Test Report," Triconex document number 7286-527. Specifically, Triconex performed the following tests:

- Low-Frequency Conducted Emissions, 30 Hz to 50 kHz (Test Method CE101)
- High-Frequency Conducted Emissions, 50 kHz to 400 MHz (Test Method CE102)
- Radiated Magnetic Field Emissions, 30 Hz to 100 kHz (Test Method RE101)
- Radiated Electric Field Emissions, 10 kHz to 1 GHz (Test Method RE102)
- Low-Frequency Conducted Susceptibility, 30 Hz to 50 kHz (Test Method CS101)
- High-Frequency Conducted Susceptibility, 50 kHz to 400 MHz (Test Method CS114)
- Radiated Magnetic Field Susceptibility, 30 Hz to 100 kHz (Test Method RS101)
- Radiated Electric Field Susceptibility, 10 kHz to 1 GHz (Test Method RS103)
- Conducted Electrical Fast Transient (EFT) Susceptibility (Test Method IEC 801-4)

With the exception of the 230 Vac Model 8312 chassis power supply modules and the third party field power supply, Triconex subjected all of the Tricon PLC system test system components to EMI/RFI testing as required. At present, Triconex does not offer these two components for safety-related use at nuclear power plants. During EMI/RFI testing, the Tricon PLC system test system was mounted in open instrument racks. No additional cabinet or cable shielding was installed, and no additional noise filters or suppression devices were used on the input/output interfaces. At least one point on each I/O module was monitored for proper operation, and the communications modules were exercised through interfaces with external monitoring devices. Operability and prudency testing was performed following EMI/RFI testing to demonstrate acceptable operation.

Triconex Report No. 7286-527 identifies the following operational anomalies that were recorded during the EMI/RFI testing:

- Figure 2-1 in Triconex Report No. 7286-527 showed that the radiated magnetic field susceptibility test (Test Method RS101) was performed at lower test levels than those required in TR-102323. As a result, this test did not meet the guidance of TR-102323.
- The high-frequency conducted susceptibility test (Test Method CS114) was performed at a maximum noise test level of 95 dB microamps rather than the 103 dB as required by TR-102323. As a result, this test did not meet the guidance of TR-102323.
- Compared to the maximum emission allowed by TR-102323, the Tricon PLC system test system showed higher levels of emissions during the low and high-frequency conducted emissions tests (Test Methods CE101 and CE102) and the radiated electric field emissions tests (Test Method RE102). As a result, this test did not meet the guidance of TR-102323.
- Some of the Tricon PLC system test system input, output, and communications modules exhibited susceptibilities during the low and high-frequency conducted susceptibility tests (Test Methods CS101 and CS114), radiated electric field susceptibility tests (Test Method RS103), and EFT susceptibility tests (Test Method IEC 801-4). In addition, there were several instances in which testing on one cable bundle resulted in susceptibility in another unit. As a result, these tests did not meet the guidance of TR-102323.

In most instances where a susceptibility was noted, Triconex performed sufficient threshold testing to identify the noise level at which acceptable equipment operation was achieved. These threshold levels are defined in Triconex Report No. 7286-527.

Given the problems noted above, the staff finds that the Tricon PLC system did not meet the guidance of EPRI TR-102323 for conducted or radiated EMI/RFI emissions or susceptibility. For this reason, before using Tricon PLC system equipment in safety-related systems in a nuclear power plant, licensees must perform sufficient testing and analysis to ensure that the plant-specific EMI/RFI environment is enveloped by the capabilities of the Tricon PLC system, and that the Tricon PLC system will not affect surrounding equipment.

4.1.3.6 Surge Withstand Testing

EPRI TR-102323 lists capabilities of equipment used in safety-related digital systems in nuclear power plants to withstand electrical surges. The NRC staff concludes that the recommendations in TR-102323 provide an adequate method for qualifying digital I&C equipment for a plant's electromagnetic environment without the need for plant-specific EMI surveys provided that the plant-specific electromagnetic environment is confirmed to be similar to that identified in TR-102323.

Triconex tested the ability of the Tricon PLC test system to withstand electrical surges in accordance with EPRI TR-102323 and Section 6.3.5 of EPRI TR-107330. The details of the tests are described in the "Surge Withstand Test Procedure," Triconex document number 7286-508, and the "Surge Test Report," Triconex document number 7286-528. In summary, Triconex performed the following tests:

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

Triconex Report No. 7286-528 stated that EPRI TR-102323 requires surge testing to be performed in accordance with IEEE C62.41 using applied surge test voltages of 3,000 V peak. However, IEEE C62.41 does not address surge testing of signal and data communication lines. Therefore, Triconex tested these circuits in accordance with IEC 801-5 at peak voltage levels of 500 V and 1,000 V, as recommended for demonstration of basic immunity of I/O circuits. The staff concludes that the surge withstand test levels applied during testing are adequate to demonstrate this level of surge withstand capability. However, before installing Tricon PLC system equipment in safety-related applications in a nuclear power plant, licensees must ensure that the applied test levels envelope the plant surge environment.

Triconex subjected all of the Tricon PLC test system components to surge withstand testing as required, except for the Model 8312 230-Vac chassis power supply modules and the third-party field power supply. At present, Triconex does not offer these two components for safety-related use in nuclear power plants. During surge withstand testing, the Tricon PLC system was mounted in open instrument racks. No additional surge suppression devices were used on the I/O interfaces. At least one point on each I/O module was monitored for proper operation, and the communications modules were exercised through interfaces with external monitoring devices. Operability and prudency testing was performed following surge withstand testing to demonstrate acceptable operation.

Triconex Report No. 7286-528 concludes that throughout all surge withstand testing, the Tricon PLC test system continued to operate in accordance with the acceptance criteria given in EPRI TR-107330. The report notes that although the test acceptance criteria were met, the following five digital output modules exhibited vulnerability (permanent damage) to the applied surge test levels:

- Model 3611E, 115-Vac digital output;
- Model 3604E, 24-Vdc digital output;
- Model 3624, 24-Vdc digital output;
- Model 3607E, 48-Vdc digital output; and
- Model 3623, 120-Vdc digital output.

Report No. 7286-528 concludes that the above modules are not acceptable for safety-related applications, which are susceptible to surge voltages on the discrete output lines unless qualified surge suppression devices are installed.

The staff accepts the surge withstand test results reported in Triconex Report No. 7286-528 and concludes that the Tricon PLC system is acceptable to the levels to which the equipment was tested. However, the five models listed above are not approved for safety-related use in a nuclear power plant unless licensees can demonstrate by test or analysis that the plant surge withstand requirements for the specific use and in the specific location are enveloped by the demonstrated surge withstand capabilities of the Tricon PLC system. In addition, before installing Tricon PLC system equipment for any use in a nuclear power plant, licensees must ensure that the test levels envelop the plant-specific electrical surge environment.

4.1.3.7 ESD Withstand Testing

EPRI TR-102323 recommends levels of ESD capability for safety-related digital I&C equipment. The staff concludes that those recommendations provide an adequate method for qualifying digital I&C equipment for a plant's electromagnetic environment without the need for plant-specific EMI surveys provided that the plant-specific electromagnetic environment is confirmed to be similar to that identified in TR-102323.

Triconex did not perform ESD withstand testing of the Tricon PLC test system as part of the equipment qualification program. Triconex document number 7286-500, "Nuclear Qualification of Tricon PLC System, Master Test Plan," explains that per TR-102323, test points for ESD testing are selected on the basis of accessibility during operation. Because the Tricon PLC system is intended for installation in a fully surrounding cabinet, all points of accessibility during operation are eliminated. In addition, EPRI TR-1000799 includes requirements for installation and operation of the Tricon PLC system that addresses control of ESD sources.

The staff accepts Triconex's position on ESD withstand capability, with the requirement that the licensees must have in place administrative or physical controls to ensure that no activity that would require opening the cabinet (including maintenance, repair, or calibration) can take place while the Tricon PLC system is required to provide its protective function, unless the particular cabinet and all channels within that cabinet are placed in trip or bypassed condition according to plant procedures. The alternative solution is for licensees to perform sufficient testing and analysis to demonstrate that the ESD withstand capability of the Tricon PLC system envelops the plant-specific ESD withstand requirements. In either case (administrative and physical controls or test and analysis), the staff will review the licensee's ESD provisions.

4.1.3.8 Class 1E to Non-1E Isolation Testing

Triconex performed isolation testing on the Tricon PLC test system in accordance with IEEE Std 384 and Section 6.3.6 of EPRI TR-107330. The details of the tests are described in the "1E/Non-1E Isolation Test Procedure," Triconex document number 7286-509, and in the "1E/Non-1E Isolation Test Report," Triconex document number 7286-529.

Through its testing, Triconex showed that the following Tricon PLC system modules are capable of acting as electrical isolation devices between the designated safety-related hardware of the PLC system and non-safety-related field circuit connections:

- Model 4119AN, EICM Module, RS-232 Serial Port (MODBUS) Interface
- Model 4329N, NCM Module, IEEE 802.3 Interface
- Model 4609N, ACM Module, Dual Nodebus (DNBI) and RS-423 Interfaces
- Model 3636RN, Relay Output Module

The Class 1E to non-1E isolation tests performed on the modules listed above demonstrated isolation capability complying with Section 7.2.2.1 of IEEE 384, including: (1) 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 (2) the isolation device prevents application of the maximum credible voltage on the non-1E side from unacceptably degrading the operation of the circuits on the 1E side. Triconex also tested the EICM, ACM and NCM modules for a maximum isolation capability of 250 Vac and 250 Vdc applied for 30 seconds, consistent with the maximum credible voltage that could be imposed on the non-1E interfaces if routed separately from high-voltage (>120 Vac) cables. In addition, Triconex tested the Model 3636R module for a maximum isolation capability of 600 Vac and 250 Vdc applied for 30 seconds, consistent with the maximum test levels provided in EPRI TR-107330.

During electrical isolation testing, the Tricon PLC test system was mounted in open instrument racks. No additional electrical protection devices were used on the I/O interfaces. At least one point on each I/O module was monitored for proper operation, and the communications modules were exercised through interfaces with external monitoring devices. Operability and prudence testing was performed following electrical isolation testing to demonstrate acceptable operation.

The Tricon PLC test system used a fiber optic link to connect two of the expansion chassis to the system's main chassis. Triconex has demonstrated by analysis that the fiber optic cables provide electrical isolation between the main chassis and the fiber optically linked expansion chassis. The basis for this conclusion is that since the fiber optic cables do not conduct electricity, they are incapable of transmitting electrical faults. In addition, the operability and prudence testing demonstrated that faults and failures of the fiber optic link do not degrade operation of the main chassis hardware.

The staff determined that the Tricon PLC system design, which separates Class 1E modules from non-1E modules by the fiber optic link, has adequate electrical isolation between Class 1E and non-1E equipment and is suitable in this regard for safety-related use in nuclear power plants. However, the staff finds that before installing the plant-specific Tricon PLC system

equipment, licensees must verify that the maximum test voltages cited above envelop the maximum credible voltages applied to non-1E interfaces.

4.2 Tricon PLC Software Design Review

The bases used by the staff for the review of the Tricon PLC system software include SRP Chapter 7, BTP's 14 and 18, EPRI TR-107330 and TR-106439. Triconex documented the compliance of the Tricon PLC system with these standards in Triconex document number 7286-535, "Nuclear Qualification of Tricon PLC System, Software Qualification Report."

The software qualification consisted of evaluating the processes, procedures, and practices used to develop the software; reviewing the software architecture; and assessing the history of the software and its associated documentation and operating experience. The object of this software qualification was to give the staff reasonable assurance that the quality of the Tricon PLC system is similar to the quality expected of a product developed under a nuclear QA program complying with Appendix B to 10 CFR Part 50.

The staff used the following criteria to determine the acceptability of the software used in the Tricon PLC system:

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

Triconex submitted its evaluation of the Tricon PLC system and TriStation 1131 software, including documentation, development practices, and operating history against these criteria. Details of the Triconex evaluation are contained in the "Software Qualification Report," Triconex document number 7286-535. The staff reviewed this evaluation, as well as original design documents and Triconex procedures, as discussed in the following subsections.

4.2.1 Software Documentation

On the basis of NUREG/CR-6241 and ASME NQA-1-1994, Section 8.7 of EPRI TR-107330 lists the documents that are needed as a minimum to support software verification and validation (V&V) and the related software quality processes:

- 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

As with most commercial-grade equipment that is not designed in accordance with Appendix B to 10 CFR Part 50, these documents do not exist as separate entities; rather the required information is contained in various other documents. In the case of the Tricon PLC system, the staff determined that the required software documentation for the Tricon PLC system is contained within the following Triconex documents:

- Triconex quality and engineering procedures, which provide planning requirements for quality assurance, V&V, configuration management, and test activities.
- The original Tricon PLC system functional requirements specifications.
- A series of Tricon PLC system software design specifications that define the incremental changes to the system.
- Test procedures and test reports applicable to each system revision for both hardware and software.
- The Tricon PLC system software release definition documents that identify software changes made in each revision.
- The Tricon PLC system user documentation.

As part of the qualification effort, Triconex reviewed the documentation associated with Version 9.5.3 of the Tricon PLC system software, and documented the review in the Software Qualification Report. The NRC staff reviewed the Software Qualification Report and the associated documentation, and determined that the Triconex QA and engineering procedures were of sufficient quality to provide reasonable assurance that the development process met the provisions for software planning documents as defined in BTP-14. In addition, the NRC staff found that the software development, V&V, and test documentation of the Triconex PLC software was in compliance with both Triconex procedural requirements and the general requirements of current industry standards. The staff further determined that the Tricon PLC system software documentation is acceptable for software intended for safety-related use in nuclear power plants.

4.2.2 Software Development and Life Cycle Planning

One of the guiding principles for approving COTS software for use in nuclear safety-related applications is that there must be reasonable assurance that the equipment will perform its intended safety function and that it is equivalent to an item designed and manufactured under a quality assurance program consistent with Appendix B to 10 CFR Part 50. To accomplish this, the SRP emphasizes the implementation and evaluation of the COTS software development process and life cycle planning. To aid in the evaluation, HICB BTP-14 (Section 2.1) states that

the information to be reviewed for the software development and life cycle planning should include the following documents:

- Software Management Plan
- Software Development Plan
- Software Quality Assurance Plan
- Software Integration Plan
- Software Installation Plan
- Software Maintenance Plan
- Software Training Plan
- Software Operations Plan
- Software Safety Plan
- Software Verification and Validation Plan
- Software Configuration Management Plan

Like most COTS products, the Tricon PLC system was not developed to the provisions of BTP-14, and therefore the information provided in accordance with BTP-14 was not organized into the 11 documents as shown above, but was contained in the following documents showing the development and life cycle planning of the Tricon PLC system software:

- Triconex Quality Assurance Manual
- Triconex Quality Procedures Manual
- Triconex Engineering Department Manual

The QAM provides the overall Triconex corporate QA requirements, while the QPM contains specific procedures for the QA organization (including validation testing), and the EDM defines the specific procedures for development, verification, configuration control, maintenance, and enhancement of the Tricon PLC system product. While the QAM and QPM provide some software specific requirements, the EDM provides the specific procedures that relate to development, maintenance, and life cycle activities of the Tricon PLC system software. In general, Triconex has improved the Tricon PLC system manuals and procedures during the years in which the Tricon PLC system has been produced. The Triconex review of the QAM, QPM and EDM is discussed in the "Software Qualification Report," which shows continual refinement of the life cycle procedures to ensure a quality product and reliable Tricon PLC system.

The staff notes that current processes and procedures contained in the QAM, QPM, and EDM documents have previously been audited by the South Texas Project (STP) Nuclear Operating Company in accordance with the Nuclear Procurement Issues Committee (NUPIC) checklist, and that audit determined that the Triconex program complies with Appendix B to 10 CFR Part 50, as documented in STP Audit Report 97-047(VA). The three year follow-up audit was documented in STP Audit Report 00-067(VA). However, the staff did not review these reports and did not use them as a portion of the basis for approving the Tricon PLC system. On the basis of its review of Triconex documents, the staff finds that the software development and life cycle planning for the Tricon PLC system is adequate for software that is intended for safety-related use in nuclear power plants. The following subsections discuss specific aspects of the software documentation.

4.2.2.1 Software Management Plan

The Tricon PLC software management plan is not contained in a stand-alone document; rather, the QAM, QPM, and EDM provide the basis for overall product management of the Tricon PLC system software. Most of the software management details for the Tricon PLC system product are listed in the EDM. Section 3.1.2.1 of Appendix A to the Software Qualification Report assesses the Tricon PLC system software management plan contained in the QAM, QPM, and EDM against provisions in Section 3.1a of BTP-14. The staff reviewed the software management plan details as discussed in the Software Qualification Report, and concludes that the management structure presented in the related documents provides adequate project oversight, control, reporting, review, and assessment. Furthermore, the NRC staff determined that the QAM, QPM, and EDM documents meet the software management provisions outlined in BTP-14 and are, therefore, acceptable for software intended for safety-related use in nuclear power plants.

4.2.2.2 Software Development Plan

The QAM, QPM, and EDM procedures provide the basis for overall product management of the Tricon PLC system software. Most of the software management details of the Tricon PLC system product are listed in the EDM. The initial 1986 procedures, with some expansion and revision, were used to develop Version 6.2.3 of the Tricon PLC system, the first version to achieve TÜV-Rheinland certification on February 11, 1990. Subsequent versions of the Tricon PLC system software have continued the TÜV-Rheinland oversight and certification, as well as independent verifications. The latest version of the Tricon software, Version 9.5.3, was certified by TÜV on September 17, 2001 in report number 968/EZ 105.02/01.

Section 3.1.2.2 of Appendix A to the Triconex "Software Qualification Report" assesses the Tricon PLC system software development plan contained in the QAM, QPM, and EDM against provisions in Section 3.1b of BTP-14. Having reviewed the software development plan details discussed in the Software Qualification Report, the staff finds the related documents describe acceptable methods of organizing the software life cycle. The staff further finds that the software development plan details contained throughout the QAM, QPM, and EDM conform to the guidance of IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," endorsed by RG 1.173. The staff therefore concludes that the software development plan identified in the Triconex application is acceptable for software that is intended for safety-related use in nuclear power plants.

4.2.2.3 Software Quality Assurance Plan

The QAM, QPM, and EDM procedures provide the basis for overall quality assurance of the Tricon PLC system software. Most of the software quality assurance details of the Tricon PLC system product are listed in the QAM. Section 3.1.2.3 of Appendix A to the Triconex "Software Qualification Report," assesses the Tricon PLC system software management plan contained in the QAM, QPM, and EDM against provisions in Section 3.1c of BTP-14.

Triconex has had a QA program in place since 1985. The company revised this program in 1997 with the specific intent of making it compliant with the requirements of Appendix B to 10 CFR Part 50. Having reviewed the Triconex software quality assurance plan, the staff

concludes that the Triconex software quality assurance plan is acceptable for software that is intended for safety-related use in nuclear power plants.

4.2.2.4 Software Integration Plan

Having reviewed the Software Integration Plan defined in Section 3.1d of BTP-14, Triconex determined that a software integration plan is not applicable to the Tricon PLC system, since the system uses discrete embedded firmware chips for the various processing boards, such as the main processor and I/O boards. The software modules are small, independent, and run on dedicated microprocessors that do not utilize operating systems, and they require no special software integration activities. Software written for the embedded firmware must be burned onto PROMs that are installed onto processor boards. Having reviewed this discussion in the Triconex Software Qualification Report, the staff agrees that because of the nature of the Tricon PLC system software, no software integration is required or performed and, therefore, the software integration plan outlined in Section 3.1d of BTP-14 is not applicable to this product. No determination of adequacy was required.

4.2.2.5 Software Installation Plan

Having evaluated Section 3.1e of BTP-14, Triconex concluded that the installation characteristics apply to the application programs that would be developed and installed by the users of the Tricon PLC system platform but do not apply to the on-board embedded software. Having reviewed this discussion, the staff agrees that because of the nature of the Tricon PLC system and its firmware (software contained on a PROM), no software installation plan is required. The staff further concluded that the installation plan used by the licensee or other installer of plant-specific software must be evaluated by the staff before the Tricon PLC system software can be used for safety-related use in nuclear power plants.

4.2.2.6 Software Maintenance Plan

The QAM, QPM, and EDM procedures provide the basis for the Tricon PLC software maintenance plan. Most of the software maintenance details for the Tricon PLC system product are listed in the EDM. Section 3.1.2.6 of Appendix A to the Triconex Software Qualification Report assesses the Tricon PLC system software maintenance plan contained in the QAM, QPM, and EDM against provisions in Section 3.1f of BTP-14. The Software Qualification Report also discussed the Triconex review of the QAM, QPM, and EDM documents. The staff reviewed these documents and determined that the QAM, QPM, and EDM contain the necessary management, implementation, and resource characteristics related to software maintenance during the active phase of the product as set forth by BTP-14 and, therefore, are acceptable for software that is intended for safety-related use in nuclear power plants.

4.2.2.7 Software Training Plan

Having evaluated Section 3.1g of BTP-14, Triconex determined that the software training requirements focus on user applications. Triconex provides to its customers a technical training

brochure that describes various courses offered regarding the basic Tricon PLC system unit. These courses include maintenance, user application programming, and advanced technical topics. Having reviewed the software training program offered by Triconex, the staff concludes that the specified end users training plans for the Tricon PLC software meet the criteria outlined in BTP-14 and therefore are acceptable for software that is intended for safety-related use in nuclear power plants. System level training is discussed in Section 4.3.7 of this SE.

4.2.2.8 Software Operations Plan

The software operations plan is a plant-specific requirement of the software user. Licensees are required to have a software operations plan when installing or using the Tricon PLC system in safety-related applications. The staff reviewed the user documentation for the basic platform, described under the heading of Software Life Cycle Process Design Outputs, and found it to be suitable for use and reference when the licensee implements a plant-specific Software Operations Plan.

4.2.2.9 Software Safety Plan

Section 3.1i of BTP-14 characterizes the software safety plans as a requirement of the software user. Licensees are required to have a software safety plan when installing or using the Tricon PLC system in safety-related applications. The guidance for the software safety plan are outlined in the SRP and in IEEE Std 1228, "IEEE Std for Software Safety Plans." The staff reviewed the safety plans related to the Tricon PLC system software as contained in the EDM and discussed in Section 3.1.2.9 of the Triconex "Software Qualification Report," Triconex Report No. 7286-535, and found them to be suitable for use and reference when the licensees implement plant-specific software operations plans.

4.2.2.10 Software Verification and Validation Plan

The NRC's RG 1.168 endorses IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans," as an acceptable methodology for the verification and validation of safety system software. However, because the Tricon PLC system was originally designed as a commercial product rather than nuclear-grade equipment, not in accordance with Appendix B to 10 CFR Part 50, Triconex did not follow the verification and validation process shown in IEEE Std 1012. Instead, Triconex used a similar (but not identical) process that includes verification and validation. The staff reviewed this process to determine if it is adequate to produce software that is intended for safety-related use in nuclear power plants. The QAM, QPM, and EDM procedures provide the basis for the verification and validation of the Tricon PLC system software, and Triconex provided a detailed assessment of the processes in the Software Qualification Report.

Verification techniques used by Triconex include design document review and code walkthrough to verify the correctness of code modifications and functionality enhancements. Validation activities include functional tests, including 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 tests to validate the diagnostic capability and software associated with diagnostics. The TriStation 1131 software is tested by manual and automated tests in accordance with written functional test procedures

that validate correct operation of both the TriStation 1131 and the Tricon PLC system. Functional outputs, boundary conditions, value conversions, and other essential functions are validated in this test.

The Triconex V&V activities were supplemented by two independent reviews of the process and V&V activities, the first performed by TÜV-Rheinland, and the second by MPR and ProDesCon.

TÜV-Rheinland is a German third-party certification agency that verifies and validates equipment to existing international standards. In 1992, TÜV-Rheinland first certified Version 6.2.3 of the Tricon PLC system to meet standard DIN V VDE 19250, "Fundamental Safety Aspects to be Considered for Measurement and Control Protective Equipment," and DIN V VDE 0801, "Principles for Computers in Safety-Related Systems" (Test Report 945/EL 366/91), for level 5 equipment. Each new version has been inspected and tested by TÜV-Rheinland, with Version 9.5.3 being certified on September 17, 2001. The inspection and testing performed by TÜV-Rheinland is on both hardware and software. The system software for the main processors and associated communication and I/O support modules and the TriStation 1131 application development tools software were reviewed and tested with each new version.

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

The TÜV-Rheinland software analysis consists of examining the code and supporting documentation to ensure that specifications are met and that good practices are used during the development. The software/firmware modules are checked to verify that their functions are as 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 common-mode software failures. The emphasis is on examining the software development process and quality controls used by Triconex.

TÜV-Rheinland testing of the TriStation software consisted of checking the translation of the graphical or text user program to the final code. TÜV-Rheinland testing of the Tricon PLC system software consists of the following:

- Internal Fault Routines – Procedures such as the watchdog routines, control processing unit (CPU) test, etc., were checked by either monitoring execution of the routines or by forcing the routines by means of fault insertion. This was done to ensure that faults were properly diagnosed and handled.
- Noise on the Processor – A software module was developed to simulate noise on the processor by putting the CPU address pointer to arbitrary positions and verifying proper detection. This was to simulate what may occur if the address pointer was corrupted by noise on the address lines.
- Functional Verification – Portions of the Triconex functional verification procedures were performed to verify the software module's performance and validity of the test procedure.

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

Since Version 6.2.3, the TÜV-Rheinland certification process has provided a second layer of V&V, this time with the required independence. While the TÜV certification process focuses on obtaining a safety certification, the process requires a set of V&V activities. The staff reviewed the TÜV-Rheinland certification reports and noted that the standards referenced are not nuclear-specific standards, and have not been endorsed by the staff. The standards are, however, appropriate for high-reliability safety-related commercial equipment, and therefore appropriate for the intended usage at that time. The review was thorough, detailed, and adequate to show the high quality of the Tricon PLC system equipment and the supporting TriStation 1131 software tools.

MPR and ProDesCon performed a second independent V&V effort. ProDesCon is an independent V&V contractor, and has been involved in evaluating safety-related software for the nuclear power industry for more than 10 years. In this instance, the review was consistent with the guidance provided in EPRI TR-107330, which states that qualification of software is to be performed using the guidance provided in EPRI TR-106439. This was not a complete line-by-line review of the software, but rather an evaluation of the processes, procedures, and practices used to develop the software; review of the history of the software itself and its associated documentation and operating experience; and analysis of the software architecture. The software included in the V&V effort was the embedded real time operating system with its associated communication and I/O modules and the PC-based system configuration software (TriStation 1131 Developers Workstation, Version 2.0, Service Pack 3).

The purpose of the MPR and ProDesCon review was to determine acceptability of the Tricon PLC system as a platform for implementing nuclear safety-related functions, acceptability of the Triconex development and maintenance processes, and to ensure that future Tricon PLC system releases will continue to have an equivalent level of integrity. For this purpose, the review was divided in two areas:

- Evaluation of the Triconex software development process, on the basis of guidance provided in HICB-BTP14.
- Evaluation of system design and integrity on the basis of guidance provided in IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations."

The evaluation by MPR and ProDesCon revealed strengths in the Triconex software development process, including the quality of the final product, design partitioning, product testing, error diagnosis and reporting, and change and configuration control. However, the evaluation also identified weaknesses in the maintenance of design basis documentation and in documentation review (or verification) of those documents. Specifically, the review determined that while design verification documentation has become more formal in the current versions of software documentation, the internal verification activities do not provide formal traceability from document to document. The MPR and ProDesCon reviewers determined that the TÜV certification activities provided this traceability, and therefore compensated for the weakness found in the Triconex V&V procedures. The reviewers concluded that "these weaknesses are

adequately compensated for by reviews provided by a classically independent external agency (TÜV-Rheinland) and the quality of the work performed by the Triconex design and validation staff." The evaluation stated that "...taken alone, the internal documentation would not be sufficient to meet the intent of an IEEE1012 in many areas, particularly for versions prior to 6.2.3...", but the evaluation also stated that since the issuance of Version 6.2.3, the TÜV-Rheinland certification process has provided a second layer of classically independent verification and validation. While the TÜV-Rheinland certification process focuses on obtaining a "safety" certification, the process requires a set of V&V activities. Together, the internal Triconex review and the TÜV-Rheinland reviews provides an equivalent level of confidence to that obtained in an IEEE Std 1012 compliant program.

The staff has reviewed the evaluation conducted by MPR and ProDesCon, and although Triconex did not strictly follow IEEE Std 1012 guidelines, the combination of the internal Triconex review, the TÜV certification, and the review by MPR and ProDesCon, gives the staff confidence that the verification and validation activities related to the Tricon PLC system software are adequate. The staff, therefore, concludes that the Tricon PLC system verification and validation activities are acceptable for software that is intended for safety-related use in nuclear power plants. It should be noted, however, that acceptance of the Tricon PLC system is based to a large degree on the TÜV-Rheinland independent review, and any future version of the Tricon PLC system will require an equivalent level of independent V&V in order to be considered acceptable for safety-related use in nuclear power plants.

4.2.2.11 Configuration Management and Error Notification

The QAM, QPM, and EDM provide the basis for overall configuration management of the Tricon PLC system software. Most of the software configuration management details for the Tricon PLC product are listed in the EDM. Section 3.1.2.11 of Appendix A to the Triconex Software Qualification Report comprises the Tricon PLC software configuration management plan contained in the QAM, QPM, and EDM against provisions in Section 3.1k of BTP-14.

Triconex has 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 PLC system has a number of firmware sets on several modules. A Tricon PLC system 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 PLC system and TriStation 1131 release. The firmware defined in each software release definition has been validated by both, Triconex Product Assurance and TÜV-Rheinland. The minimum supported hardware, software, and firmware levels are defined in the Product Release Notice.

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

The configuration control system includes a customer history tracking system, that lists each Tricon PLC 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 Part 21. Errors are classified according to severity, with product alert notices (PANs) being the most significant. Six PANs have been issued and all six were evaluated as part of this qualification process. Triconex uses a conservative approach to customer notification, in which all customers are notified of any potential problems, instead of attempting to determine which customers might be at risk. In addition to this safety-critical issue notification system, other notification systems exist to disseminate technical data. Triconex has committed to adopt 10 CFR Part 21 reporting requirements once the Tricon PLC system is in use at nuclear power plants.

Once entered into the automated error tracking system, errors are retrievable, changes are controlled, appropriate resolutions are generated, and all data are available. After review for implementation risk by the change control board, corrections 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.

The staff has reviewed the configuration management plan details discussed in the Software Qualification Report and the error notification processes discussed in the summary report. One of the PANs discussed above occurred during the staff's review of the Triconex product line, and the staff was able to review the PAN and the decision making methodology used by Triconex. The staff found that the PAN process and the configuration management and error notification practices of Triconex comply with the guidance identified in IEEE Std 828 and IEEE Std 1042, which are endorsed by RG 1.169. Furthermore, the NRC staff concludes that the QAM, QPM, and EDM meet the configuration management provisions outlined in BTP-14 and are, therefore, acceptable for software that is intended for safety-related use in nuclear power plants.

4.2.3 Evaluation of TriStation 1131 Programming Software

Application programs for the Tricon PLC system are generated using the TriStation 1131 Developers Workbench, which runs in a Windows NT environment on a standard PC. The TriStation 1131 is a software tool that allows end users to develop application programs, download those applications to the target Tricon PLC system, and determine the health of an attached Tricon PLC system. The TriStation 1131 PC would not normally be connected while the Tricon PLC system is performing safety-critical functions. The TriStation 1131 does not perform any safety-related functions itself, but it is used to generate the software which perform the safety-related functions. For tools that are not safety-critical, BTP-13 states that they "be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be developed using those tools."

A description of the TriStation 1131 software, and the functions it performs is contained in Section 2.2.3 of this SE.

For the development of the application programs, the TriStation 1131 provides IEC1131-3 compliant programming languages. It also performs a number of automatic checks on the internal coherence of the application programs and the match between I/O variables and their physical correspondences on the I/O modules. The simulation capabilities of the TriStation 1131 allow the programmer to detect errors in specification and coding. Application programs are downloaded to the Tricon PLC system using an IEEE Std 802.3 protocol with CRC check. Use of this protocol and the checksum verification on the whole message provides a level of confidence that corrupt packets will be detected and, therefore, what is downloaded and received by the PLC is actually what was intended to be downloaded.

The provisions for development tools are given in SRP Section 7.1, which states that computer tools used in the design of digital I&C systems shall not introduce faults into the software that are resident on the computer at the time the computer is performing its safety-related function. The Triconex PLC system is designed such that the Tricon PLC system should not be connected to a TriStation PC during safety-related operation.

As was the case for the operating software, there were three levels of review on the TriStation 1131 software. The first was the Triconex in-house review of the software tool, the second was the review and V&V of the software by TÜV-Rheinland, and the third was a review by MPR and ProDesCon. The staff reviewed the data on these three levels, and determined that (similar to the operating software) the three reviews were sufficient to provide a high degree of confidence that the TriStation 1131 software will not introduce faults into the Tricon PLC system and that should this occur, a proper software test of the plant-specific operational programs will reveal those faults. For this reason, the staff finds the TriStation 1131 tools acceptable to produce software that is intended for safety-related use in nuclear power plants. This approval is contingent on proper testing of the operational software, and these test plans, procedures, and results will be reviewed on a plant-specific basis.

4.2.4 Application Programs

The application program implements the desired protection, monitoring, and control functions defined by the design-basis documents for the plant-specific system. Therefore, the application programs are inherently plant-specific, and are not included within the scope of this SE. Section 5.0 of Appendix B to Triconex Document 7286-545, "Applications Guide," provides guidance on the preparation of application programs. In addition, BTP-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," provides additional guidance for use during the review of plant-specific applications programs.

4.3 Tricon PLC System Design Review

As the basis for review of the Tricon PLC system design, the staff used SRP Chapter 7 and the guidance in EPRI TR-107330 and EPRI TR-106439. Triconex documented their compliance with these standards in Triconex document number 7286-545, Revision 1, dated September 18, 2000, as well as Amendment 1, Revision 1 to that report.

4.3.1 Failure Modes and Effects Analysis

Triconex performed a failure modes and effects analysis (FMEA) on the Tricon PLC system platform, and documented that analysis in Triconex document number 7286-532. This FMEA was done in accordance with the guidelines of Section 6.4.1 of TR-107330 and the requirements of IEEE 352, Sections 4.1, 4.4, and 4.5. The FMEA reviewed possible failures of the Tricon PLC system components, identified the mechanisms that could cause those failures, and evaluated the consequences of those failures on the operation of the Tricon PLC system. Triconex stated that because of the architecture of the Tricon PLC system, failure mechanisms that affect a single leg of the triple-redundant system generally have no effect on system operation. Therefore, the FMEA also considered (1) failure mechanisms that are recognized as being highly unlikely but could affect multiple components, and (2) the coincident occurrence of otherwise single failures (i.e., multiple failures).

The staff reviewed this FMEA and concurs with the analysis. The results of the FMEA showed that, in general, failure modes that could prevent a Tricon PLC system from performing its safety function are detected by the built-in system diagnostics, or by periodic testing. The staff concluded that the FMEA shows that the Tricon PLC system is suitable for use in safety-related applications in a nuclear power plant. The analysis and results in the Triconex FMEA are also suitable for reference by licensees and for incorporation into plant-specific FMEA analyses.

4.3.2 Reliability and Availability Analysis

The *availability* of a system is the probability that the system will operate on demand, and in particular that it will initiate a protective action when required. The *reliability* of a system is the probability that the system will perform its required function under specified conditions for a specified period of time.

Triconex performed a reliability and availability analysis on the Tricon PLC system in accordance with Section 4.2.3 of EPRI TR-107330 and documented the results in Triconex document number 7286-531. The study determined that the calculated reliability and availability of a typical Tricon PLC system are greater than 99.9 percent, which exceeds the goal of 99.0 percent recommended by EPRI TR-107330. With an assumed periodic test interval of 18 months, typical of nuclear plant refueling outage cycles, the reliability and availability increase to greater than 99.98 percent. The staff reviewed this study, and agrees that the results of the reliability and availability analysis support use of the Tricon PLC system in safety-related applications in a nuclear power plant, and the analysis and its results are appropriate for incorporation in plant-specific risk analyses.

4.3.3 Component Aging Analysis

Triconex performed a component aging analysis on the Tricon PLC system in accordance with Section 4.7.8.2 of EPRI TR-107330. The analysis is contained in Section 4.12 of the Triconex Qualification Summary Report, document number 7286-545, with additional details provided in the August 30, 2001, letter from Triconex (Accession Number ML012490183). The intent of the analysis was to identify significant aging mechanisms; establish a qualified life for the hardware on the basis of the significant aging mechanisms; and/or specify surveillance, maintenance, and replacement activities to address significant aging-related degradation.

The component aging analysis concluded that the components of the Tricon PLC system that are susceptible to significant, undetected aging mechanisms include only the chassis power supplies and backup batteries. Aging-related degradation of these components can be effectively addressed through periodic replacement before the onset of significant loss of performance. Section 6.3, "Maintenance Procedures," of Appendix B, "Applications Guide," to Triconex Topical Report 7286-545, "Qualification Summary Report," recommends replacement of the backup batteries every 5 years, or when the battery life alarm occurs, and replacement of the power supplies every 10 years.

The staff agrees with the results of the component aging analysis. Before installing Tricon PLC system equipment in a nuclear power plant, licensees must ensure that procedures are in place to ensure periodic replacement of the components identified above at the manufacturer's recommended frequencies given in the Application Guide (Appendix B to the Triconex Qualification Summary Report).

4.3.4 Thread Audit

The staff conducted a "thread audit" walkthrough of the Tricon PLC system hardware and software. Since this review is of a topical report, and not of a plant-specific application, no specific user software was available upon which to base this thread audit. For this reason, during the plant visit at the Triconex site, the staff had Triconex assume a system with analog and digital inputs and a digital output. Triconex demonstrated the method and logic that would be used to select the appropriate modules, and how the application-specific software would be designed. The staff and Triconex design engineers then traced the signal path from the input, through the input modules, to the I/O processor via the I/O bus, to the main processor and the application-specific software; showed how a trip signal would be generated; and assessed how that trip signal would be processed out through the I/O processor, I/O bus, and output modules. This thread audit consisted of the following steps:

- (1) Trace the signal through the hardware components, and verify any transformations (such as analog to digital conversion).
- (2) Review the actual code within the various processors through which the signal passes.
- (3) Examine the various levels of software development documents (such as the software specification and the V&V report), and compare them to the actual code.
- (4) Review the final results of the hardware and software development processes.

During this audit, Triconex personnel were able to quickly retrieve the appropriate documentation; explain the specification, design, review, test, and V&V processes; and walk the staff through the signal and software flow. On the basis of the "thread audit" and the review of the Triconex V&V program, the staff finds that the process is suitable for development of high-quality software suitable for use in safety-related applications in nuclear power plants.

4.3.5 Response Time Characteristics

GDC 20, 21, 23, and 25 (defined in Appendix A to 10 CFR 50) constitute requirements for timely operation of the protection features. To meet these requirements, BTP-21 provides the following guidance:

- The feasibility of design timing may be demonstrated by allocating a timing budget to components of the system architecture (Annex E of IEEE Std 7-4.3.2) so that the entire system meets its timing requirements.
- Timing requirements should be satisfied by design commitments.

Section 4.2.1-A of EPRI TR-107330, "General Functional Requirements," Part A, "Response Time," states, "The overall response time from an input to the PLC exceeding its trip condition to the resulting outputs being set shall be 100 milliseconds or less." Section 5.3, "Operability Test Requirements," Part B, "Response Time" states, "The response time of the loop shall be measured per the requirements of Section 4.2.1, Item A. The response time between receiving a discrete input and setting a discrete output and from changing an analog input to changing an analog output and a discrete output shall be measured in a fashion that is expected to provide repeatable results. The acceptance criteria is that the measured response time shall not vary more than $\pm 20\%$ from the value calculated from the manufacturer's data for the baseline testing and the value measured following qualification testing shall not vary more than $\pm 10\%$ from the baseline. The baseline response time testing shall be performed for any variations in arrangements that result from requirements in Section 6.2.1.1."

MPR Associates performed an analysis of the test system as described in Section 2.3 of this SE, and determined that the theoretical maximum response time for that system was 177 ms for a digital input to digital output signal, and 264 ms for an analog input to digital output signal. This analysis is documented in MPR Calculation No. 426-001/SCS-01, "Test Tricon Maximum Response Time Test Calculation." Triconex performed actual baseline response time tests on the test system, and documented those tests in Triconex documents 7286-503, "Operability Test Procedure," and 7286-530, "Performance Proof Test Report." These tests did not show compliance with the guidance in EPRI TR-107330, but did validate the MPR analysis. Specifically, the test report showed that the test system exhibited digital input to digital output response time values of 144 to 162 ms, and analog input to digital output response time values of 199 to 216 ms.

On the basis of those values, the Tricon PLC system is not in compliance with Section 4.2.1-A of EPRI TR-107330. The actual response time for any particular system will depend upon the actual system configuration, and may vary significantly from simple to complex systems. The determination of the suitability of the Tricon PLC system response time characteristics for a particular plant application is a plant-specific requirement and, therefore is the responsibility of licensees and will be reviewed by the staff during the review of plant-specific applications to ensure that the Tricon PLC system satisfies its plant- and application-specific requirements for system response time presented in the accident analysis in Chapter 15 of the safety analysis report.

4.3.6 Tricon PLC System Self-Diagnostic Capacity

Digital computer-based I&C systems are prone to different kinds of failures than traditional analog systems. Properly designed self-test, diagnostic, and watchdog timers reduce the time to detect and identify failures, but do not guarantee hardware or software error detection. Computer self-testing is most effective at detecting random hardware failures. BTP-17 describes provisions for self-test capabilities for digital systems. The Tricon PLC system provides continuous self-testing, including monitoring memory and memory reference integrity, using watchdog timers, monitoring communication channels, monitoring central processing unit status, and checking data integrity. The Tricon PLC system performs self-tests and I/O validation on each module. The Tricon PLC system TMR architecture provides continuous self-testing to detect, tolerate, and alarm on single internal failures. The internal self-test functions are transparent to the application program and are an integral part of the base platform software. These diagnostics check each main processor, as well as each I/O module and communication channel. Transient faults are recorded and masked by the hardware majority-voting circuit. Persistent faults are diagnosed, and the faulted module can be replaced or operated in a fault-tolerant manner until replacement is completed. The main processor diagnostics do the following:

- Verify fixed-program memory;
- Verify the static portion of RAM;
- Test all basic processor instructions and operating modes;
- Test all basic floating-point processor instructions;
- Verify the shared memory interface with each I/O communication processor and communication leg;
- Verify handshake signals and interrupt signals between the CPU, each I/O communication processor, and communication leg;
- Check each I/O communication processor and communication leg microprocessor, ROM, shared memory access, and loopback of RS-485 transceivers;
- Verify the Triclock interface; and
- Verify the Tribus interface

Each I/O module also has ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module's fault indicator, which in turn activates the chassis alarm signal. The fault indicator points to a leg fault, not a module failure. The module will continue to operate properly in the presence of a single fault.

The digital input modules with self-test continuously verify the ability of the Tricon PLC system to detect the transition of a normally energized circuit to the off state. High-density digital input

modules continuously verify the ability of the Tricon PLC system to detect transitions to the opposite state.

The digital output module executes a particular type of output voter diagnostic (OVD) for every point. In general, during OVD execution, the commanded state of each point is momentarily reversed on one of the output drivers, one after another. Loop-back sensing on the module allows each microprocessor to read the output value for the point to determine whether a latent fault exists within the output circuit.

Supervised digital output modules provide both voltage and current loopback, allowing fault coverage for both energized-to-trip and deenergized-to-trip conditions. In addition, a supervised digital output module verifies the presence of the field load by doing continuous circuit-continuity checks. Any loss of field load is annunciated by the power module.

A dc voltage digital output module is specifically designed to control devices that hold points in one state for long periods of time. The OVD strategy for a dc voltage digital output module ensures fault coverage even if the commanded state of the points never changes. On this type of module, an output signal transition occurs during OVD execution, but is guaranteed to be less than 2.0 ms (500 μ s is typical) and is transparent to most field devices.

The Triconex Planning and Installation Guide, a commercial Triconex manual with a Triconex part number of 9720051-006, provides detailed descriptions of each diagnostic test and flag.

The staff reviewed these self-test capabilities, and finds them to be suitable for a digital system used in safety-related applications in nuclear power plants. It may also be possible to use some of these diagnostic capabilities to modify or eliminate certain TS-required periodic surveillance tests; however this is a plant-specific, application-dependent issue and, therefore, is not addressed in this SE. Any such surveillance test modifications or eliminations will be reviewed in plant-specific reviews.

4.3.7 Training

Triconex Quality Assurance Manual, Section QAM 1.2, "Triconex Organization," Revision 009, dated April 23, 1999, contains the description of the functional organization of the corporation, and their authorities and responsibilities. The Customer Satisfaction Department within the organization is responsible for technical support, customer service, worldwide service, and worldwide training. Additionally, the document also identifies training as the responsibility of Human Resources, Customer Satisfaction, and every department per the requirements of QAM 18.0, "Training," Rev. 012, dated January 5, 2001. Specifically, QAM 18.0 describes the procedures that apply to all personnel performing activities that affect the quality of Triconex products. It also identifies positions and processes that require the assignment of certified personnel, the company's training policy, training needs, and the requirements for training records. QAM 18.0 also identifies the training that is provided to Triconex customers for operation and maintenance of the Tricon PLC system. Within Triconex, the Human Resource Department is responsible for managing the overall employee training program, while each department supervisor is responsible for ensuring that his or her employees are appropriately trained and qualified to perform their assigned functions.

The services and warranty programs that Triconex generally provides to its customers include technical product support; system troubleshooting; diagnostic evaluations; onsite support; and software/firmware/hardware upgrades. The procedures for customer service activities are defined in QAM 19.0, Rev. 6, dated April 14, 2000. The Customer Service Department in Irvine, California, is the only location authorized to perform repair work on any Triconex TMR product. QAM 19.0 also requires that all repair activities by Triconex customer servicing groups will meet the same workmanship standards that applied to the manufacturing process for the original product.

The customer is generally responsible for operating and maintaining the Triconex product at a given plant. The Customer Satisfaction Department offers Triconex customers training courses on the operation and maintenance of Triconex products.

The Triconex Training Manual, Document No.5600-0020/99, 1999, describes the training offered by the Triconex Customer Satisfaction Department for all Triconex products. Training is offered at training centers at Houston, Texas, and Irvine, California, in the United States, and at training centers in Europe, the Middle East, and Singapore. Triconex also offers onsite training at customer sites tailored to fit project specific requirements.

The Triconex Training Manual also describes the Tricon/TriStation 1131 Maintenance Course. The course summary is as follows:

This 3-day hands-on course provides an introduction to Tricon PLC system implementation, with its primary focus on maintenance and troubleshooting of the Tricon PLC system. Students get practical experience with continuity checks, loop testing, and general field maintenance. Using TriStation 1131 (Windows NT) software, students monitor Tricon PLC system operations, perform diagnostic procedures, and force points in a real-time environment designed to simulate actual field conditions.

The course is meant for plant supervisors who are responsible for the Tricon PLC system, and plant technicians responsible for installing and maintaining the Tricon PLC system. The course outline includes an introduction to the Tricon PLC system; principles of Tricon PLC system design; Tricon PLC system components; and installing, operating, and maintaining the Tricon PLC system.

Given the review of the information provided and discussions with Triconex personnel, the staff finds that the training provided to Triconex personnel responsible for Tricon products is adequate to ensure that the quality of the products, services offered and overall work performed is acceptable for safety-related applications. For its customers, Triconex has a well-established training program at facilities that are accessible to customers worldwide for operating and maintaining Tricon products installed at customer sites. The training and customer services offered to Triconex customers is comprehensive and adequate for maintaining the quality of the products operating at the customers' plants.

4.3.8 Repair of Tricon PLC System Modules

The Tricon PLC system modules are generally not considered to be field repairable. It is expected that plant repair activities will be limited to replacing of modules, and all faulted or broken modules will be returned to Triconex for repair. Triconex has stated that its policy is that the Customer Service Department in Irvine, California, is the only location authorized to perform repairs on any Triconex TMR product.

4.3.9 Historic Data on Tricon PLC System Use

The staff reviewed the historic data available on the use of the Tricon PLC system in commercial and foreign nuclear applications. Triconex has an ongoing relationship with each customer and, therefore, maintains knowledge about the system configuration and any customer concerns regarding those systems. The operating experience with these systems indicates that the hardware and software is highly reliable. There are more than 2,000 systems in operation, with greater than 100 million operating hours. During this time, there have been no failures to perform the required protective action.

The staff believes that historic data is insufficient by itself to approve any system for safety-related use in nuclear power plants; however, this data does show a degree of quality in the Tricon PLC system design and the advantages of a triple-redundant system. This data also shows that while common-mode software failure of all three portions of a triple redundant system is possible (and may in fact still happen at some location), the quality of the Triconex software design, testing, and applications is such that this type of failure is highly unlikely. This staff observation does not, in any way, reduce or eliminate the need and regulatory requirement for diversity or defense-in-depth.

4.3.10 Defense-in-Depth and Diversity

The staff described concerns with common-mode failures and other digital system design issues in SECY-91-292. Common-mode failures could defeat the redundancy achieved by the hardware architectural structure, and also result in the loss of several echelons of defense in depth (provided by the monitoring, control, reactor protection, and engineered safety functions performed by the digital I&C systems).

The staff has established acceptance guidelines for Defense-in-Depth and Diversity (D-in-D&D) assessments and has identified four echelons of defense against common-mode failures:

- Control system – The control system echelon consists of non-safety equipment which routinely prevents reactor excursions toward unsafe operation, and is used for normal operation of the reactor.
- Reactor trip system (RTS) – The reactor trip echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.
- Engineered safety feature actuation system (ESFAS) – The ESFAS echelon consists of safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers (cladding, vessel, and containment) to radioactive release.

- Monitoring and indication – The monitoring and indication echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

As a result of the reviews of advanced light-water reactor (ALWR) design certification applications that used digital protection systems, the staff documented its position in SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Design," with respect to common-mode failure in digital systems and defense-in-depth for the advanced reactors. This position is also documented in the SRP BTP HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer Based Instrumentation and Control Systems." There are four points in the position as applied to ALWR design certification applications. These four positions are quoted below.

1. The applicant/licensee should assess the diversity and defense-in-depth of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.
2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of those events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
4. A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

The staff stated in BTP HICB-19 that Points 1, 2, and 3 of this position apply to digital system modifications for U.S. operating plants. Point 4 of this position applies only to ALWR and new reactor system design certification applications.

Since both diversity and defense-in-depth are plant specific topics, the Triconex Topical Report 7286-545, "Qualification Summary Report," did not address these topics, and they are therefore not within the scope of this SE. Sections 3.6.2 and 3.6.3 of Appendix B, "Applications Guide," to Triconex document number 7286-545, provides guidance in the preparation of a plant specific D-in-D&D evaluation. A review of the differences between the Tricon PLC system and

the non-safety control system implemented at a particular nuclear power plant, and the determination that plant specific required diversity and defense-in-depth continue to be maintained must be addressed in a plant-specific D-in-D&D evaluation. These determinations will be reviewed by the staff during the plant-specific safety evaluation.

5.0 CONCLUSION

The subsections below will discuss the degree of regulatory compliance met by the Tricon PLC system, as well as any licensee actions required before the system can be used for safety-related applications in nuclear power plants.

5.1 Regulatory Compliance

This safety evaluation discusses the acceptability of the Tricon PLC system. The GDC listed in Appendix A to 10 CFR Part 50 establish the minimum requirements for the design of nuclear power plants; 10 CFR 50.55a(h) incorporates IEEE Std 603-1991. The regulatory guides and endorsed industry codes and standards listed in the SRP, Table 7-1, are the guidelines used as the basis for this evaluation.

Section 50.55a(a)(1), "Quality Standards for Systems Important to Safety," is addressed by conformance with the codes and standards listed in the SRP. In the development of the Tricon PLC system, Triconex used codes and standards that are the same as or equivalent to the standards identified in the SRP. Therefore, the staff concludes that the Tricon PLC system conforms with this requirement.

Section 50.55a(h) endorses IEEE Std 603-1991, which addresses both system-level design issues and quality criteria for qualifying devices. Not every section of IEEE Std 603-1991 applies to a topical report with no plant-specific application. The staff has reviewed the requirements of IEEE Std 603-1991, and finds that the following sections apply:

- Section 5.1 requires that a single failure will not prevent proper operation of the protective action. To meet this criterion, a Tricon PLC system is used in each of multiple redundant process channels and trip logic trains for each function. These redundant channels and trains will be electrically isolated and physically separated. This requirement has been satisfied for single hardware failures.
- Sections 5.2 and 7.3 require that once a safety-related protective system action has been initiated, the actuations proceed to completion. Once initiated, the Tricon PLC system will proceed to completion. Return to normal operation requires deliberate operator action.
- Section 5.3 contains the requirement for high-quality systems. This requirement is satisfied by the Triconex Quality Assurance Program.
- Section 5.4 contains the equipment qualification requirements. The topical report describes the degree to which the Tricon PLC system hardware is environmentally and seismically qualified to ensure that the system is capable of performing its designated

functions while exposed to normal, abnormal, test, accident, and post-accident environmental conditions.

- Section 5.6 contains the requirements for physical, electrical, and communications independence. These criteria are met through redundancy and separation of the channels. Communication between channels is via a peer-to-peer communication protocol implemented using Tricon PLC system communications modules that have been demonstrated to be qualified isolation devices.
- Section 5.7 contains testing and calibration requirements. The testing and calibration capabilities of the Tricon PLC system have been demonstrated to be in compliance with RG 1.22, RG 1.118, and IEEE-338. The capability exists to permit testing of redundant channels during power operation. The design does not require disconnecting wires, installing jumpers, or otherwise modifying the installed equipment.
- Section 5.9 requires control of access to the system. Access to the hardware can be controlled via front and rear cabinet doors, which could normally be locked. Also, door positions can be monitored with an alarm to the operator if any door is opened.
- Section 5.15 discusses reliability. Availability and reliability of the Tricon PLC system have been assessed with probabilistic availability and reliability analyses using actual operating experience data. The probabilistic analysis has been used to quantify non-availability on demand. The staff has reviewed these calculations; however, the staff does not use probabilistic and deterministic reliability analyses as the sole means of determining the acceptability of a safety system. The calculations relate only to the hardware aspects of the Tricon PLC system. Despite the staff's determination that the software is of sufficiently high quality to be suitable for use in safety-related systems in nuclear power plants, there is no method to make a verifiable determination of the numeric value of software reliability.
- Sections 6.1 and 7.1 discuss the requirements for automatic control and Sections 6.2 and 7.2 discuss the requirements for manual control. The Tricon PLC system meets these automatic and manual control requirements. In a properly installed system, failure of the automatic controls would not interfere with separately provided manual controls.
- Section 6.8 discusses the determination of setpoints. Triconex has performed an analysis of accuracy, repeatability, thermal effects and other necessary data for use in a plant-specific setpoint analysis. Licensees must ensure that, when the Tricon PLC system is installed, setpoint calculations be reviewed and, if required, setpoints be modified to ensure that the Tricon PLC system equipment will perform within system specifications.

Therefore, the staff has determined that the Tricon PLC system satisfies the requirements of 10 CFR 50.55a(h) with regard to IEEE Std 603-1991.

The staff determined that the following GDCs specified in Appendix A to 10 CFR Part 50 are the applicable design criteria for this review:

- GDC 1: Quality Standards and Records
- GDC 2: Design Basis for Protection Against Natural Phenomena
- GDC 4: Environmental and Missile Design Bases
- GDC 13: Instrumentation and Control
- GDC 20: Protection System Functions
- GDC 21: Protection System Reliability and Test ability
- GDC 22: Protection System Independence
- GDC 23: Protection System Failure Modes
- GDC 24: Separation of Protection and Control Systems
- GDC 29: Protection Against Anticipated Operational Occurrences

The staff reviewed the equipment descriptions in the topical report for conformance to the guidelines in the regulatory guides and industry codes and standards that apply to this equipment. The staff concludes that Triconex adequately identified the guidelines that apply to this equipment. Given the review of the equipment designs for conformance to the guidelines, the staff finds that there is reasonable assurance that the Tricon PLC system conforms to the applicable guidelines. Therefore, the staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included identifying those components and assemblies of the Tricon PLC system that are designed to survive the effects of earthquakes and abnormal environments. On the basis of this review, the staff concludes that Triconex has identified those components and assemblies consistent with the design bases for the intended safety-related applications of the Tricon PLC system. Therefore, the staff finds that the identification of those components and assemblies satisfies the requirements of GDC 2 and 4.

On the bases of its review of the Tricon PLC system status information, manual interface capabilities, and provisions to support safe shutdown, the staff concludes that information is provided to monitor the Tricon PLC system over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions so as to ensure adequate safety. Appropriate controls can be provided for manual initiation of a reactor trip. The Tricon PLC system can appropriately support actions to safely operate a nuclear power unit under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the staff finds that the Tricon PLC system design satisfies the requirements of GDC 13.

Given its review of the topical report, the staff concludes that the Tricon PLC system conforms to the design-basis requirements of 10 CFR 50.34(f), and to the guidance of IEEE Std 603 and RG 1.105. The staff also concludes that the Tricon PLC system includes the necessary provisions to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown consistent with the accident analysis presented in Chapter 15 of a licensee's SAR. Licensee evaluation of plant-specific accident analyses is required. Therefore, the staff finds that the Tricon PLC system satisfies the requirements of GDC 20.

The Tricon PLC system conforms to the guidelines for periodic testing in RG 1.22 and RG 1.118. Bypassed and inoperable status indication can be supported to conform to the guidelines of RG 1.47. A Tricon PLC system installation can also conform to the guidelines regarding the application of the single-failure criterion in IEEE Std 379, as supplemented by RG 1.53. On the basis of this review, the staff concludes that the Tricon PLC system satisfies the

guidance of IEEE Std 603 with regard to system reliability and testability. Therefore, the staff finds that the Tricon PLC system satisfies the requirements of GDC 21.

On the basis of its review, the staff concludes that the Tricon PLC system satisfies the guidance of IEEE Std 603 and the guidance in RG 1.75 with regard to protection system independence. Therefore, the staff finds that the Tricon PLC system satisfies the requirements of GDC 22.

On the basis of its review of the FMEA for the Tricon PLC system, the staff concludes that the system is designed to fail into a safe mode if conditions such as disconnection of the system, loss of energy, or adverse environment are experienced. Therefore, the staff finds that the Tricon PLC system satisfies the requirements of GDC 23.

Based on its review of the interfaces between the Tricon PLC system and plant operating control systems, the staff concludes that the Tricon PLC system satisfies the guidance of IEEE Std 603 with regard to control and protection system interactions. Therefore, the staff finds that the Tricon PLC system satisfies the requirements of GDC 24.

On the basis of its review of all GDCs listed above, the staff concludes that the Tricon PLC system satisfies the requirements of GDC 29, "Protection Against Anticipated Operational Occurrences."

On the basis of its review of software development plans and inspections of the computer development process and design outputs, the staff concludes that the Tricon PLC system meets the guidance of RG 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the staff finds that the Tricon PLC system satisfies the requirements of GDC 1 and 21.

The staff determined that the Tricon PLC system meets the relevant requirements of GDCs 1, 2, 4, 13, 20-24, and 29.

5.2 Plant-Specific Requirements

Section 4.1.3.2 of this SE discusses the temperature and humidity conditions for which the Tricon PLC system is qualified. Licensees will be responsible for analysis of the plant-specific environment, and the determination that the Tricon PLC system is suitable for that particular plant usage. This determination will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.1.3.3 of this SE discusses the radiation exposure levels for which the Tricon PLC system is qualified. Licensees will be responsible for analysis of the plant-specific radiation environment, and the determination that the Tricon PLC system is suitable for that particular plant usage. This determination will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.1.3.4 of this SE discusses the seismic levels for which the Tricon PLC system is qualified. The staff found that the Tricon PLC system did not fully meet the guidance of EPRI TR-107330 for seismic requirements, and before using Tricon PLC system equipment in safety-related systems in a nuclear power plant, licensees must determine that the

plant-specific seismic requirements are enveloped by the capabilities of the Tricon PLC system. This determination, and the suitability of the Tricon PLC system for a particular plant and application is the responsibility of the licensee. This determination will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.1.3.5 of this SE discusses the conducted or radiated EMI/RFI emissions or susceptibility for which the Tricon PLC system is qualified. Since the Tricon PLC system did not satisfy the guidance of EPRI TR-102323, it is the responsibility of the licensees to measure or otherwise determine the worst case EMI/RFI environment that would exist at the time the protective function provided by the Tricon PLC system would be required, and then to ensure that the conducted and radiated EMI/RFI emissions and susceptibility capabilities of the Tricon PLC system envelop this environment, and that the system will not affect surrounding equipment. This determination will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.1.3.6 of this SE discusses the surge withstand capabilities for which the Tricon PLC system is qualified. Licensees will be responsible for the analysis of the plant-specific surge environment, and the determination that the Tricon PLC system is suitable for that particular plant usage. This determination will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.1.3.7 of this SE discusses the ESD withstand capability, and the fact that the Tricon PLC system was not tested for this capability. Before installing and using the Tricon PLC system, licensees must have in place administrative or physical controls to ensure that no activity which would require opening the cabinet can take place while the Tricon PLC system is required to provide its protective function, unless the particular cabinet and all channels within that cabinet are placed in a trip or bypassed condition according to plant procedures. An alternative solution is for licensees to perform sufficient testing and analysis to demonstrate that the ESD withstand capability of the Tricon PLC system envelops the plant-specific requirements. In either case, whether administrative and physical controls or test and analysis, the staff will review the licensees' ESD provisions during the plant-specific safety evaluation.

Section 4.1.3.8 of this SE discusses the Class 1E to non-1E isolation capabilities for which the Tricon PLC system is qualified. Licensees will be responsible for analysis of the plant-specific maximum credible applied voltages produced by non-1E interfaces, and for ensuring that this value is enveloped by the Tricon PLC system capacity, and that the Tricon PLC system is suitable for that particular plant usage. This determination will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.2.2.5 of this SE discusses the software installation plan. The staff determined that the software installation plan is the responsibility of the licensee, and must be developed before the Tricon PLC system software can be used for safety-related applications in nuclear power plants. This software installation plan will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.2.2.6 of this SE discusses the software maintenance plan. Although Triconex has an acceptable software maintenance plan, the staff determined that a plant-specific software maintenance plan is also required, and it is the responsibility of licensees to develop this

software maintenance plan before the Tricon PLC system software can be used for safety-related applications in nuclear power plants. This software maintenance plan will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.2.2.8 of this SE discusses the software operations plan. The staff determined that licensees will be required to develop a software operations plan before using the Tricon PLC system software for safety-related use in nuclear power plants. This software operations plan will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.2.2.9 of this SE discusses the software safety plan. The staff determined that licensees will be required to develop a software safety plan before using the Tricon PLC system software for safety-related applications in nuclear power plants. This software operations plan will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.2.2.10 of this SE discusses verification and validation. Although Triconex did not strictly follow guidelines of IEEE Std 1012, the staff determined that the combination of the internal Triconex review, the TÜV certification, and the review by MPR and ProDesCon provided acceptable verification and validation for software that is intended for safety-related use in nuclear power plants. However, the staff noted that a significant portion of its acceptance is predicated upon the independent review by TÜV-Rheinland, and licensees using any Tricon PLC system beyond Version 9.5.3 must ensure that similar or equivalent independent V&V is performed; without this, the Tricon PLC system will not be considered acceptable for safety-related use at nuclear power plants. Should licensees use future Tricon PLC systems beyond Version 9.5.3 which have not received TÜV-Rheinland certification, the staff will review the acceptability of the independent V&V during the plant-specific safety evaluation.

Section 4.2.3 of this SE discusses the use of the TriStation 1131. That section noted that the Triconex PLC system is designed such that the Tricon PLC system should not be connected to a TriStation PC during safety-related operation. The plant-specific procedures which ensure that the TriStation PC is not connected to the Tricon PLC system during safety-related operation will be reviewed by the staff during the plant-specific safety evaluation. In addition, the testing of the operational software produced by the TriStation 1131, and these test plans, procedures, and results will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.2.4 of this SE discusses the application programs, which are inherently plant specific, and therefore are not included in the scope of this SE. Plant-specific application programs will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.3.3 of this SE discusses the component aging analysis, which determined that the chassis power supplies and backup batteries are susceptible to significant, undetected aging mechanisms. Before installing Tricon PLC system equipment in a nuclear power plant, licensees must have procedures in place to ensure periodic replacement of these components. These procedures will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.3.5 of this SE discusses the response time characteristics of the Tricon PLC system software safety plan. The staff determined that the actual response time for any particular system will depend upon the actual system configuration, and may vary significantly from

simple to complex systems. The determination of the response time for the particular system intended for safety-related use for a particular plant application, and the determination that this response time satisfies the plant-specific requirements in the accident analysis in Chapter 15 of the safety analysis report is the responsibility of the licensee. These determinations will be reviewed by the staff during the plant-specific safety evaluation.

Section 4.3.10 of this SE discusses diversity and defense-in-depth. A review of the differences between the Tricon PLC system and the non-safety control system implemented at a particular nuclear power plant, and the determination that plant specific required diversity and defense-in-depth continue to be maintained must be addressed in a plant-specific D-in-D&D evaluation. These determinations will be reviewed by the staff during the plant-specific safety evaluation.

Triconex has made a number of determinations of items and criteria to be considered when applying the Tricon PLC system to a specific plant application. These are contained in the "Applications Guide," provided as Appendix B to the "Qualification Summary Report," Triconex document number 7286-545. A number of these are the same as those discussed above, but the "Applications Guide" goes beyond regulatory compliance to include good engineering practice and applications suitability determinations. It is expected that licensees intending to use the Tricon PLC system will consider each item in this guide, and document the appropriate decisions and required analysis. The staff will review these decisions and analysis during the plant-specific safety evaluation.

5.3 Approval

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.

Principle Contributors: P. Loeser
D. Spaulding

Date: December 12, 2001



TRICONEX TOPICAL REPORT 545-1-A
March 8, 2002

NRC REQUESTS FOR ADDITIONAL INFORMATION (RAIs) AND RESPONSES

(N/A – None Received)



TRICONEX TOPICAL REPORT 545-1-A

March 8, 2002

ABSTRACT – QUALIFICATION SUMMARY REPORT

The US nuclear power industry is faced with the challenges of market de-regulation, aging of facilities, obsolescence of instrument and control systems, and the consolidation of vendors. In order to facilitate the use of programmable logic controllers (PLCs) for safety applications, an EPRI and utility sponsored working group of utility and industry representatives developed EPRI report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."

The Triconex Corporation has successfully completed all testing and documentation requirements of TR-107330 for its TRICON TMR PLC platform. This report describes the methods employed to qualify the TRICON fault tolerant PLC against the established TR requirements. The report includes:

- a description of the TRICON product capabilities and history
- a description of the TRICON test specimen and the testing methods
- a description of qualification test acceptance criteria and results
- evaluation of Triconex quality assurance and software development processes
- evaluation of TRICON safety-critical software integrity
- evaluation of TRICON reliability, failure modes, and radiation withstand capability
- traceability to documentation and data supporting the conclusions of this report

The completed qualification tests and the specified engineering evaluations have successfully demonstrated the suitability of the TRICON system to perform with high reliability in a nuclear power plant environment. As reported, analysis of test data finds the TRICON acceptable for use as a generic Class 1E platform which can be used in a broad range of safety-related applications in nuclear power plants.

The report identifies the 1E qualified TRICON modules and provides data on their qualification envelopes. Specific guidance is provided for developing nuclear power plant applications, including hardware selection, design approaches, and development of application programs.

(Note: Qualification Summary Report 7286-545 has also been published as EPRI Technical Report 1000799. This Abstract is taken from that Technical Report.)



TRICONEX TOPICAL REPORT 545-1-A
March 8, 2002

Qualification Summary Report

Triconex Document 7286-545, Revision 1



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

QUALIFICATION SUMMARY REPORT

Document No.: 7286-545

Revision 1

September 18, 2000

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



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

QUALIFICATION SUMMARY REPORT

Document No.: 7286-545

Revision 1

September 18, 2000

QUALITY ASSURANCE DOCUMENT

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	2 of 60	Date:	09/18/00

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	3 of 60	Date:	09/18/00

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1.0 INTRODUCTION	5
2.0 TRICON NUCLEAR QUALIFICATION PROJECT	6
3.0 SYSTEM DESCRIPTION	8
3.1 TRICON System Overview	9
3.2 TRICON System Hardware	10
3.2.1 Main Chassis	11
3.2.2 Expansion Chassis	12
3.2.3 Remote Extender Modules	12
3.2.4 External Termination Assemblies	13
3.2.5 Power Supply Modules	13
3.2.6 Main Processor Modules	14
3.2.7 Input/Output Modules	17
3.2.8 Communication Modules	19
3.3 TRICON System Software	20
3.3.1 TRICON Operating System	20
3.3.2 TriStation 1131 Programming Software	21
3.3.3 Application Program	22
3.4 Qualified TRICON Modules	23
3.5 Qualification of Newer Versions of the TRICON System	24
4.0 HARDWARE QUALIFICATION	24
4.1 TRICON Test Specimen Configuration	26
4.2 Environmental Qualification	28
4.3 Seismic Qualification	31
4.4 Radiation Qualification	34
4.5 Electromagnetic Compatibility Qualification	35
4.6 Surge Withstand	38
4.7 1E to Non-1E Isolation	41
4.8 Electrostatic Discharge	44
4.9 Performance Proof Testing	44
4.10 Failure Modes and Effects Analysis	47
4.11 Reliability and Availability Analysis	48
4.12 Component Aging Analysis	48



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	4 of 60	Date:	09/18/00

5.0 SOFTWARE QUALIFICATION	49
5.1 Software Documentation	50
5.2 Software Development Process	51
5.3 Software Verification and Validation Process	53
5.4 Safety Analysis	55
5.5 Configuration Management and Error Notification	55
6.0 SYSTEM APPLICATION	56
7.0 REFERENCES	57

APPENDICES

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	5 of 60	Date:	09/18/00

1.0 INTRODUCTION

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

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

The TRICON system has been qualified on a generic basis to provide utilities and other users with a platform that has been shown to comply with the applicable requirements for digital safety systems. Where appropriate, compliance with the applicable requirements is defined in terms of a "qualification envelope." This envelope defines the range of conditions within which the TRICON system meets the acceptance criteria. In applying the TRICON to a specific safety-related application, the user must confirm that the qualification envelope bounds the plant-specific requirements. Additional guidance on use of the TRICON system in safety-related applications is provided in the Application Guide, Appendix B.

The generic qualification of the TRICON Version 9.3.1 system encompasses both the hardware and the software used in the system. The hardware includes termination panels, chassis, power supplies, main processor modules, communication modules, input/output modules, and interconnecting cabling. The specific TRICON modules selected for qualification are defined in the Master Configuration List, Reference 7.23. These modules provide the functionality that is typically required for safety-related control and protection systems in nuclear power plants. The TRICON software that has been qualified includes the embedded real time operating system and its associated communication and input/output modules, and the PC-based system configuration software, TriStation 1131.

The process of qualifying the TRICON system has involved technical evaluations and qualification tests (i.e., "type" tests). This report summarizes the results of these evaluations and tests and provides references to the applicable documents for more detailed information.



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	6 of 60	Date:	09/18/00

This report is organized as follows:

- Section 2 provides a summary of the TRICON nuclear qualification project, including background on the EPRI TR-107330 document and the overall approach used to demonstrate compliance with requirements specified in the EPRI document.
- Section 3 is an overview description of the TRICON system and its major components.
- Section 4 describes the basis for qualification of the TRICON system hardware, including results of environmental, seismic, electromagnetic compatibility, surge withstand, and Class 1E isolation testing.
- Section 5 describes the basis for qualification of the TRICON system software.
- Section 6 provides reference to the detailed system application guidance that is included in Appendix B of this report.

2.0 TRICON NUCLEAR QUALIFICATION PROJECT

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

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

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

The objective of EPRI TR-107330 is to provide generic requirements for qualifying commercial PLCs for use in safety-related applications in nuclear power plants. It defines the essential technical characteristics, (e.g., input and output point requirements, scan rates, software features, etc.) that must be included to cover the needs of a range of plant safety applications. Process-oriented considerations, including system and software development and quality



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	7 of 60	Date:	09/18/00

assurance, are addressed in this specification primarily by reference to published standards and guidelines. The process-oriented guidance is provided as a means of achieving adequate software and systems quality for safety related applications.

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

The TRICON Nuclear Qualification Project was initiated by Triconex, EPRI, and the South Texas Project Nuclear Operating Company (STPNOC) to qualify the TRICON system in accordance with the EPRI TR-107330 requirements. Quality assurance requirements and special procedures that were unique to the TRICON qualification project are documented in the Project Quality Plan, Reference 7.21. The major activities completed as part of this project include the following:

- Evaluating the quality assurance (QA) program established by Triconex. Triconex has had a QA program in place since 1985 modeled on the requirements of ASME NQA-1. This program was revised in 1997 to be fully compliant with 10CFR50, Appendix B and 10CFR21. STPNOC conducted an audit of Triconex's QA program and in January 1998 judged that the program complied with 10CFR50, Appendix B and 10CFR21.
- Identifying the specific PLC modules and supporting devices to be qualified. The TRICON hardware included in the qualification are listed in the Master Configuration List, Reference 7.23. This hardware was integrated in a complete test system that was intended to demonstrate capabilities typical of various nuclear safety systems. The design of the test system is documented in the System Description, Reference 7.25, and associated drawings, References 7.26 through 7.28.
- Developing an application program to support the required testing. The Test Specimen Application Program (TSAP) was developed to simulate operation of the TRICON in typical nuclear plant applications. Development, including verification and validation (V&V) of the TSAP was done in accordance with the Triconex QA program and a project-specific Software QA Plan, Reference 7.24. The TSAP program and associated V&V activities are documented in References 7.51 through 7.55.
- Specifying the set of qualification tests to be performed on the test specimen, including defining a set of operability tests to be performed at suitable times in the qualification process. Operability tests are required to determine the baseline system performance and to demonstrate satisfactory system operation under the stresses applied during qualification



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	8 of 60	Date:	09/18/00

testing. The specific tests performed are defined in the Master Test Plan, Reference 7.22. Test procedures are provided in References 7.29 through 7.37.

- Performing the qualification tests and documenting the results. Results of these tests, documented in References 7.38 through 7.44, define the qualification envelope and form the basis for the application guidance contained in this report.
- Performing other technical evaluations as needed to demonstrate compliance with regulatory requirements and other technical requirements in EPRI TR-107330. Evaluation of the TRICON operating system and programming software is documented in the Software Qualification Report, Reference 7.49. A failure modes and effects analysis evaluating the effects of component failures on TRICON operation is provided in Reference 7.46. Reference 7.45 documents an analysis of TRICON system reliability. An analysis of the effect of radiation exposure on system operation is provided in Reference 7.47. Reference 7.48 provides a summary of the accuracy specifications for the TRICON system for use in calculating instrument measurement uncertainties and establishing critical control setpoints.

3.0 SYSTEM DESCRIPTION

This section provides a brief description of the TRICON system. A more detailed description of the system is provided in the TRICON Product Guide, Reference 7.19, and the Planning and Installation Guide, Reference 7.20. The specific hardware and software that has been qualified is identified in the Master Configuration List, Reference 7.23. For convenience, Table 3-1 at the end of this section lists the TRICON modules that have been qualified for nuclear safety-related applications.

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

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

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	9 of 60	Date:	09/18/00

Throughout its life cycle, a quality assurance program and documented development process has been in place to control the design, verification and validation, and configuration management of the system (including both hardware and software). The quality assurance program and development process have been continually improved since 1985 and are compliant with the requirements of 10CFR50, Appendix B and 10CFR21. Demonstration of high quality, robust design, and accurate performance has been required from the first version of the TRICON system because of the safety-critical nature of the applications in which it is used. Qualification of the system for use in safety-critical systems has required evaluation by various safety certification agencies, including Factory Mutual, and TÜV Rheinland. Triconex's commitment to support the nuclear power industry is a natural extension of this corporate history.

3.1 TRICON System Overview

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

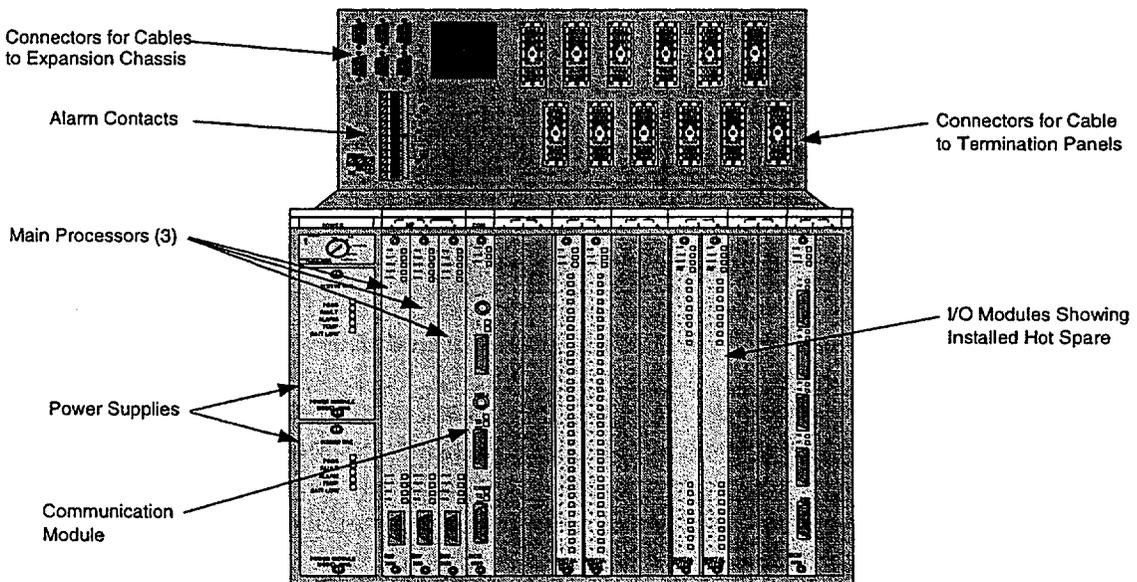


Figure 1. TRICON Main Chassis

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

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	10 of 60	Date:	09/18/00

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

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

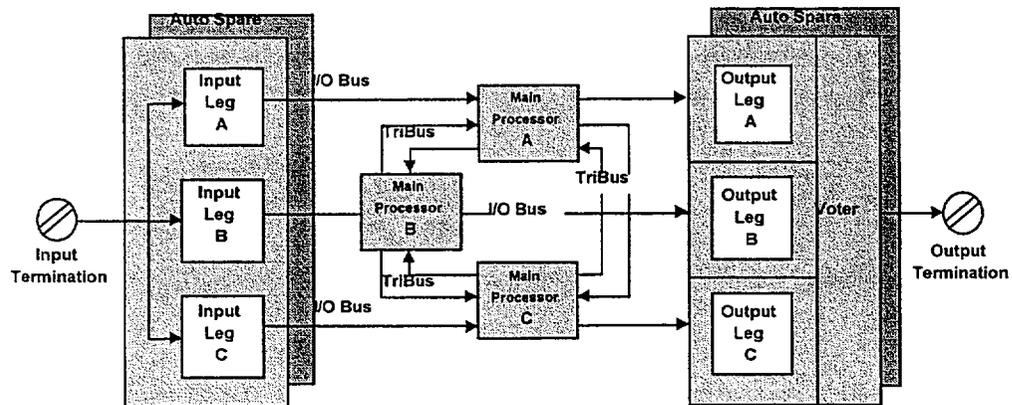


Figure 2. Triple Modular Redundant Architecture.

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

3.2 TRICON System Hardware

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	11 of 60	Date:	09/18/00

3.2.1 Main Chassis

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

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

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

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

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

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

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	12 of 60	Date:	09/18/00

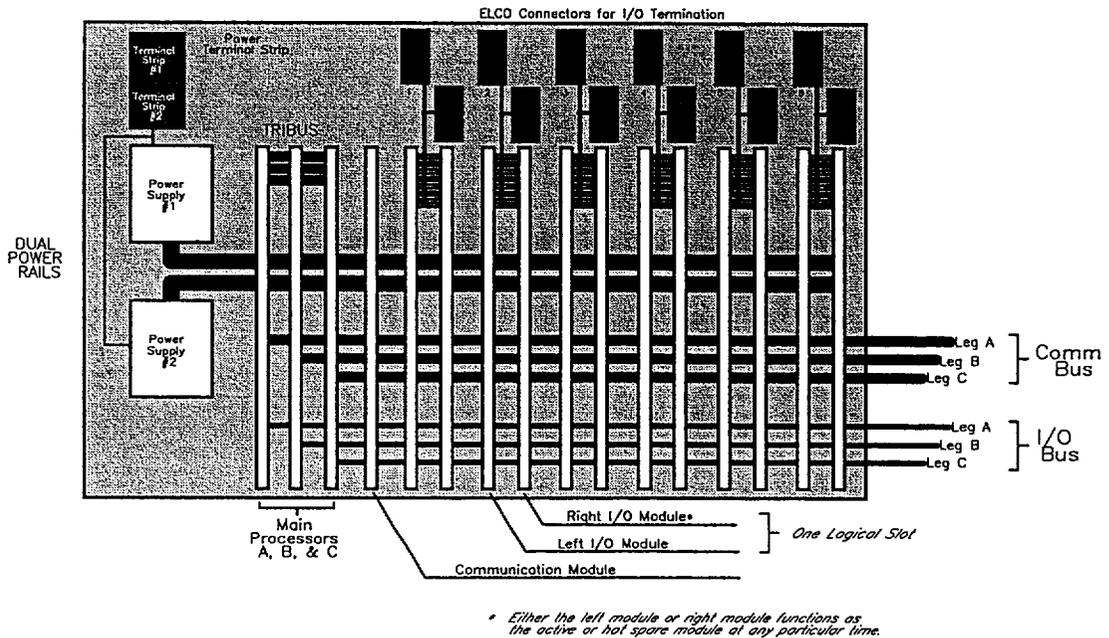


Figure 3. TRICON Chassis Backplane Configuration

3.2.2 Expansion Chassis

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

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

3.2.3 Remote Extender Modules

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

Each RXM module has single channel transmit and receive cabling ports. Each of the three primary RXM modules is connected to the remote RXM modules housed in the remote chassis. Each pair of RXM modules is connected with two fiber optic cables operating at a communication rate of 375 Kbaud. The interfacing cabling is unidirectional for each channel. One cable carries data transmitted from the primary



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	13 of 60	Date:	09/18/00

RXM to the remote RXM. The second cable carries data received by the primary RXM from the remote RXM. The RXM modules provide immunity against electrostatic and electromagnetic interference. Since the RXM modules are connected with fiber optic cables, they may be used as 1E-to-non 1E isolators between a safety-related main chassis and a nonsafety-related expansion chassis.

3.2.4 External Termination Assemblies

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

3.2.5 Power Supply Modules

All power supply modules are rated for 175 watts, which is sufficient to supply the power requirements of a fully populated chassis. Two different power supply modules can be used in a single chassis. Two qualified models are available to support different power sources: 120 V ac or V dc and 24 V dc. The 230 VAC power supply was successfully tested for environmental and seismic qualification, but was not tested for EMC and surge withstand. Testing of the 230 VAC power will be continued if justified based on utility demand.

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

<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
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:



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	14 of 60	Date:	09/18/00

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

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

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

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

3.2.6 Main Processor Modules

The TRICON system utilizes three main processor modules to control the three separate legs of the system. Each main processor module operates independently with no shared clocks, power regulators, or circuitry. Each module owns and controls one of the three signal processing legs in the system, and each contains two 8-bit processors and one 32-bit processor. One of the 8-bit processors is a dedicated, leg-specific I/O communication (IOC) microprocessor that processes all communication with the system I/O modules. The second 8-bit dedicated, leg-specific processor manages interfaces with all communication modules in the system.

The 32-bit primary processor manages execution of the control program and all system diagnostics at the main processor module level. Between each 8-bit processor and the 32-bit primary processor is a dedicated dual port RAM allowing for direct memory access data exchanges.

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	15 of 60	Date:	09/18/00

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

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

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

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	16 of 60	Date:	09/18/00

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

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

- Verification of fixed-program memory.
- Verification of the static portion of RAM.
- Testing of all basic floating-point processor instructions.
- Verification of the shared memory interface with each I/O communication processor and communication channel.
- Verification of handshake signals and interrupt signals between the CPU, each I/O communication processor and communication channel.
- Checking of each I/O communication processor and communication channel microprocessor, ROM, shared memory access and loopback of RS-485 transceivers.
- Verification of the TriClock interface.
- Verification of the TriBUS interface.

When a fault is detected on a main processor module, it is annunciated and voted out, and processing continues through the remaining two main processors. When the faulty main processor is replaced, it runs a self-diagnostic to determine its basic health. When the self-diagnostic is successfully completed, the main processor then begins the process of "re-education," where the control program is transferred from each of the working units into the returning main processor. All three main processors then resynchronize data and voting, and the replacement processor is allowed back in service.

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	17 of 60	Date:	09/18/00

3.2.7 Input/Output Modules

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

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

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

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

A detailed description of each type of input module, including fault detection and data validation processes, is provided in the Planning and Installation Guide, Reference 7.20.

After the main processors complete the control algorithm, data is sent out to the output modules. Outputs from the main processors are provided to the I/O bus microprocessors through dual port RAM. The I/O bus microprocessors then transfer that data to the triplicated microprocessors on the output modules. The output modules then set the

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	18 of 60	Date:	09/18/00

output hardware appropriately on each of the triplicated sections and vote on the appropriate state and/or verify correct operation. Discrete outputs use a unique, patented, power output voter circuit. This voter circuitry is based on parallel-series paths that pass power if the driver for legs A and B, or legs B and C, or legs A and C command them to close (i.e. 2-out-of-3 vote). Analog outputs use a switching arrangement tying the three legs of digital to analog converters to a single point.

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

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

A detailed description of the output modules, the voting processes, and fault detection processes is provided in the Planning and Installation Guide, Reference 7.20.

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

If a standby module is installed and both it and its pair are deemed healthy by the main processors, each of the modules is exercised on a periodic basis. The main processors will swap control between the two modules. By periodically using both modules, any faults are detected, alarmed, and the failed module replaced while a standby module is in place. This use of standby modules does not cause any interruption of protection or control functions.

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	19 of 60	Date:	09/18/00

3.2.8 Communication Modules

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

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

The three types of qualified communication modules are as follows:

- The Enhanced Intelligent Communications Module (EICM) allows the TRICON to communicate with Modbus masters and slaves. Each EICM contains four serial ports and one parallel port that can operate concurrently. Each serial port is uniquely addressed and supports either the Modbus or TriStation interface. The parallel port provides a Centronics interface to a printer.
- The Advanced Communications Module (ACM) acts as an interface between a TRICON and the Foxboro Intelligent Automation (I/A) Series distributed control system. The TRICON system appears to the Foxboro system as a "Control Processor" node on the I/A communication network (the "Nodebus"). The ACM communicates process information at full network data rates for use anywhere on the I/A Series system, transmitting all TRICON aliased data and diagnostic information to operator workstations in display formats. This module can be configured for one-way transmittal of information.
- The Network Communications Module (NCM) allows the TRICON to communicate with other TRICONs and with external hosts over IEEE 802.3 networks. This includes PCs running the TriStation programming software that is used to develop and download application programs to the TRICON controller. The NCM provides two BNC port connectors: Net 1 supports Peer-to-Peer and time synchronization protocols, and Net 2 supports open networking to external systems using Triconex applications.

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	20 of 60	Date:	09/18/00

3.3 TRICON System Software

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

3.3.1 TRICON Operating System

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

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

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	21 of 60	Date:	09/18/00

Each microprocessor interfaces to only one leg of the I/O bus, and thus to only one main processor.

As described in the preceding sections, the design of the software includes features to detect and mitigate system faults. These features include hardware and software based diagnostics. The diagnostic capabilities of the system are validated when hardware or software changes are made in any module. The validation requires that the stuck at zero, stuck at one, and contact noise from the automated fault injection system produce the pre-defined, expected diagnostic result. Failure to produce the correct result is evaluated and corrected exactly like a failure to produce any diagnostic result.

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

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

3.3.2 TriStation 1131 Programming Software

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

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

The TriStation 1131 Developer's Workbench translates the various languages into native mode executable code. The Cause and Effect Matrix, Logic Diagrams, and Function Block Diagrams are translated into Structured Text. The Structure Text is



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	22 of 60	Date:	09/18/00

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

The TriStation 1131 Developer's Workbench also provides emulation capabilities for the TRICON. The tool provides a capability for running an emulation code version of the program on the PC. Capabilities exist for manual input of program variables and observation of program outputs on the PC screen, with the inputs and output values merged and displayed with the program blocks. This simulation can be used as part of the validation process for new or modified application code.

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

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

3.3.3 Application Program

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

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

In addition to the support features offered by the TriStation 1131, the standardized language features will aid in development of safety critical functions. The TriStation 1131 function subset does not allow such constructs as looping and GOTO that could inadvertently result in infinite program flow loops or at least in non-deterministic



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	23 of 60	Date:	09/18/00

execution timing. This reduces the chance of bad programming constructs creating unexpected system hangs, further reducing the chance of system failures as well as software common cause failures.

3.4 Qualified TRICON Modules

For convenience, the specified TRICON modules that are qualified for nuclear safety-related use are listed in the table below. For more information on the specific revision levels of these modules and on other qualified hardware and software, refer to the Master Configuration List, Reference 7.23. Section 4 of this report summarizes the qualification testing of these modules and the specific qualification envelope applicable to each one.

Table 3-1. Qualified TRICON Modules

MODULE TYPE	MODEL NO.	MODULE TYPE/DESCRIPTION
Main Processor	3006	Enhanced Main Processor II, V9, 2 Mb
Remote Extender	4210	Remote Extender Module (Primary)
	4211	Remote Extender Module (Remote)
Communication	4119A	EICM, V9, Isolated
	4329	Network Communication Module, V9
	4609	Advanced Communication Module
Analog Input	3700A	AI Module, 0-5 VDC, 6% Overrange
	3701	AI Module, 0-10 VDC
	3703E	EAI Module, Isolated
	3704E	HDAI Module, 0-5/0-10 VDC
Analog Output	3805E	Analog Output Module, 4-20 mA
Digital Input	3501E	EDI Module, 115V AC/DC
	3502E	EDI Module, 48V AC/DC
	3503E	EDI Module, 24V AC/DC
	3504E	HDDI Module, 24/48 VDC (24V)
	3505E	EDI Module, 24 VDC, Low Threshold
Digital Output	3601E	EDO Module, 115 VAC
	3603T	EDO Module, 120 VDC
	3604E	EDO Module, 24 VDC
	3607E	EDO Module, 48 VDC
	3623	SDO Module, 120 VDC
	3624	SDO Module, 24 VDC
Pulse Input	3510	Pulse Input Module
Thermocouple Input	3706A	NITC Input Module
	3708E	ITC Thermocouple Input Module
Relay Output	3636R	ERO Module, N.O., Simplex
Power Supply	8310	120 VAC/VDC Power Supply
	8311	24 VDC Power Supply

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	24 of 60	Date:	09/18/00

Note: Specific termination panels, cable assemblies, and RTD signal conditioners that have also been qualified are listed in the Master Configuration List, Reference 8.21.

3.5 Qualification of Newer Versions of the TRICON System

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

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

4.0 HARDWARE QUALIFICATION

This section describes the qualification of the TRICON system hardware for nuclear safety-related applications. Qualification activities were performed as required by EPRI TR-107330, Reference 7.4. These activities conform to the requirements of IEEE Standard 323 for qualifying Class 1E equipment.

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

Qualification of the TRICON hardware was demonstrated primarily by conducting a series of qualification tests in accordance with EPRI TR-107330. The tests specified in the EPRI TR are required in order to comply with the applicable regulatory requirements and industry standards. For TRICON qualification, the required tests and their sequence was defined in the Master Test Plan, Reference 7.22. The test sequence included pre-qualification performance testing, qualification testing, and post-qualification performance proof testing.

Pre-qualification testing included the following:

- System setup and checkout test, described in Reference 7.29, which documented proper configuration and operation of the test system. This test was performed after manufacturing and assembly of the system, and as required, throughout the qualification process. This test includes verification of hardware, software, and cabling including interconnections to all equipment.
- Operability tests, defined in Reference 7.30, to establish the baseline performance and to demonstrate the functionality of the TRICON in accordance with its specifications. The operability test procedure included tests for analog module accuracy, system response time, operation of discrete inputs and outputs, performance of timer functions, failover tests (due



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	25 of 60	Date:	09/18/00

to failure of redundant components), loss of power, detection of failure to complete a scan, power interruption, and power quality tolerance.

- Prudency testing, described in Reference 7.31, to establish baseline performance and to demonstrate the ability of the TRICON to operate within specifications under dynamic conditions. The prudency test included a burst of events test, a serial port receiver failure test, and a serial port noise test.

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

Qualification testing included the following:

- Environmental testing, Reference 7.33, to demonstrate the ability of the TRICON to operate properly under the extremes of temperature and humidity. Proper operation of the system under high radiation levels is also an environmental concern; however this was demonstrated by analysis instead of testing, Reference 7.47. The operability test was performed at the high and low temperature and humidity conditions and also immediately after the environmental test (at ambient conditions) to demonstrate proper system operation. The prudency test was also performed at the high temperature conditions.
- Seismic testing, Reference 7.34, to demonstrate the ability of the TRICON to operate properly during and after design basis seismic events, and therefore demonstrate the suitability of the device for qualification as Seismic Category I equipment. The operability and prudency tests were performed immediately after the seismic test to demonstrate continued proper operation of the system.
- Surge testing, Reference 7.35, to demonstrate the suitability of the TRICON for qualification as a safety-related device with respect to AC power line electrical surge withstand capability.
- Class 1E-to-non 1E electrical isolation testing, Reference 7.36, to demonstrate the suitability of the TRICON for qualification as a safety-related, Class 1E device with respect to providing electrical isolation at Non-1E field connections.
- Electromagnetic compatibility (EMC) testing, described in Reference 7.37, to demonstrate the suitability of the TRICON for qualification as a safety-related device with respect to electromagnetic emissions and susceptibility.

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

- Operability test as described above.

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	26 of 60	Date:	09/18/00

- Prudency test as described above.

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

Engineering analyses were also performed to demonstrate compliance with additional hardware and system requirements specified in the EPRI report. In addition to the radiation withstand analysis noted above, a failure modes and effects analysis, Reference 7.46, and a reliability and availability analysis, Reference 7.45, were performed.

4.1 TRICON Test Specimen Configuration

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

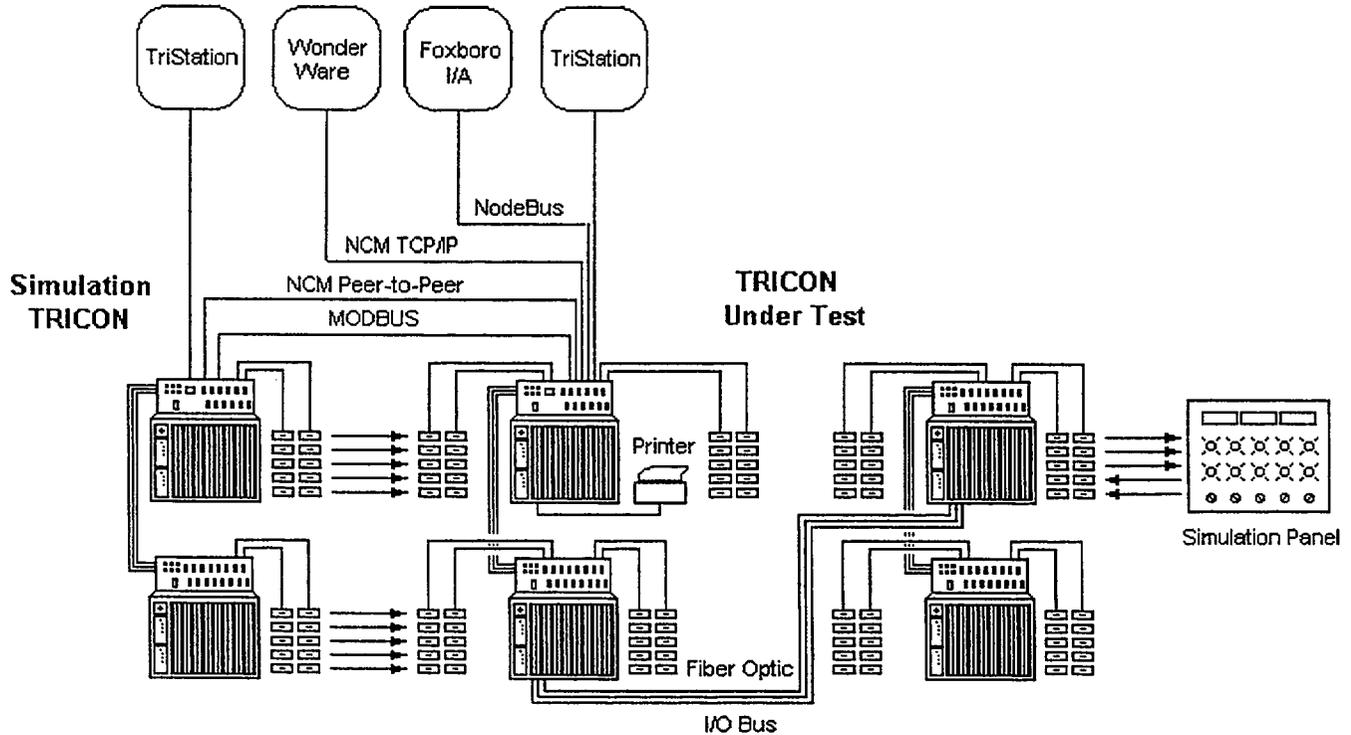


Figure 4. TRICON Test System



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	27 of 60	Date:	09/18/00

Triconex Drawing 7286-102 (Reference 7.28) shows the general arrangement and interconnection of the TRICON Test Specimen chassis. The System Description, Reference 7.25, provides an overview and description of the test specimen and test system. A detailed identification of the tested equipment is provided in the project Master Configuration List, Reference 7.23.

During testing, the test specimen was executing an application program (the TSAP) developed specifically for the qualification project and designed to exercise the test specimen in a manner that supported data collection requirements during testing. The TSAP is described in Reference 7.51. The Master Configuration List identifies the revision level of all test specimen software and firmware.

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

Analog and digital outputs from the TRICON test specimen were monitored with indicator lights and a data logger system. The data logger system also monitored analog and digital inputs to the TRICON test specimen. This data logger consisted of a PC-based data acquisition system with 29 analog channels and 107 digital channels. Data was recorded with this system during the various tests, and then analyzed to verify proper operation of individual input and output points.

Two PCs running the TriStation software were used to communicate with and monitor the status of the TRICON test specimen and the simulator TRICON. The TriStation software used for this purpose was the MSW version, which is a DOS-based program that is superseded by the TriStation 1131 software. The version of the TriStation software used to support the qualification testing has no effect on the results of this testing.

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

During each of the qualification tests, operation of the TRICON test system was monitored and recorded by the test system data logger and the Wonderware and Foxboro I/A workstations. The recorded data was evaluated in detail before, in some cases during, and after the test period. The data evaluation considered operation (per the TSAP) of at least one input or output point on each I/O module installed in the TRICON test system, and operation of all peripheral



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	28 of 60	Date:	09/18/00

communication interfaces including the Simulator TRICON Peer-to-Peer and MODBUS interfaces, the Wonderware and Foxboro I/A interfaces, and the test system printer interface. The data was monitored for deviations or trends from normal performance.

4.2 Environmental Qualification

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

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

- The PLC under qualification shall meet its performance requirements during and following exposure to abnormal environmental conditions of 40°F to 140°F and 5% to 95% relative humidity (non-condensing) according to a time varying profile (see Figure 4-4 of the EPRI TR).
- Environmental testing shall be performed with the power supply sources set to values that maximize heat dissipation in the test PLC.
- Power supplies shall be loaded such that nominal current draws at nominal power supply output voltages are equal to the power supply rating.
- The test PLC shall be powered with its TSAP operating during environmental testing, with 1/2 of the discrete and relay outputs ON and loaded to their rated current. In addition, all analog outputs shall be set to between 1/2 and 2/3 of full scale.

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

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

The environmental test acceptance criteria are as given below based on Appendix 4 of the Master Test Plan, Reference 7.22, and EPRI TR-107330, Section 4.3.6, Reference 7.4.



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	29 of 60	Date:	09/18/00

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

Environmental testing of the TRICON Test Specimen and Lambda field power supply was performed on October 24 through 30, 1999 at Wyle Laboratories in Huntsville, Alabama. The testing complied with the specific requirements of EPRI TR-107330, Sections 4.3.6 and 6.3.3, as described above, and the general requirements of IEEE 381-1977, Reference 7.9. Results of the testing are described in the Environmental Test Report, Reference 7.39.

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

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	30 of 60	Date:	09/18/00

Review of the data collected during the test shows that the TRICON Test Specimen operated as intended. A number of module diagnostic messages were indicated at the TriStation Console during testing. These messages included two indications of Test Specimen hardware faults and other indications that were due to operation of the system under abnormal conditions. A description of all diagnostic messages received during the testing is provided in the test report, Reference 7.39. It is important to note that the diagnostic messages did not indicate failures of the system, only faults. The system met its safety function throughout testing.

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

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

- The Model 3603E 120 VDC digital output module developed a voter fault diagnostic during the high temperature Operability test period. The spare 3603E module was installed, operated correctly throughout the remainder of the environmental test, and did not experience any faults.
- The Model 3611E 115 VAC digital output module developed a diagnostic fault message during the high temperature Operability test period. The fault remained into the ambient temperature hold period. The spare 3611E module was installed, operated correctly throughout the remainder of the environmental test, and did not experience any faults. However, the root cause of the module fault could not be determined, and it was therefore concluded that the module did not demonstrate acceptable operation during environmental testing.

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	31 of 60	Date:	09/18/00

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

Conclusions from this test are as follows:

1. Environmental testing of the TRICON Test Specimen was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977.
2. The TRICON Test Specimen met all applicable performance requirements during and after application of the environmental test conditions.
3. Two digital output module faults occurred during environmental testing which were the result of component failures. Because of the fault tolerant design of the TRICON PLC, the digital output points of the two modules (Model 3603E and Model 3611E) continued to perform as expected. However, based on post-test inspection results, the Model 3611E module is not recommended for nuclear safety related application. The Model 3601E module provides functionality comparable to the Model 3611E and demonstrated acceptable performance during environmental testing.
4. The environmental test results demonstrate that the TRICON PLC and the Lambda field power supply will not experience failures due to abnormal service conditions of temperature and humidity.

4.3 Seismic Qualification

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

EPRI TR-107330, Sections 4.3.9 and 6.3.4, requires that the test PLC be seismically tested in accordance with IEEE 344, Reference 7.8. The testing is required to include a resonance search followed by five simulated Operating Basis Earthquakes (OBEs) and one simulated Safe Shutdown Earthquake (SSE) at 9.75 g's and 14 g's respectively, based on 5% damping. The simulation vibrations are required to be applied triaxially (in three orthogonal directions), with random frequency content. Additional requirements include the following:

- The test PLC shall meet its performance requirements during and following the application of the SSE.
- The test PLC shall be mounted on a structure whose configuration meets the manufacturer's mounting requirements. The structure is required to be stiff enough so there are no resonances below 100 Hz.



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	32 of 60	Date:	09/18/00

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

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

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

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

- The TRICON Test Specimen shall operate as intended during and after application of the OBE and SSE vibrations. Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate operation as intended.
- During and after application of the OBE and SSE vibrations, all connections on the TRICON Test Specimen shall remain intact, all modules installed in the TRICON Test Specimen shall remain fully inserted, and no functional or non-functional parts of the TRICON Test Specimen shall fall off.
- The Model 3636R electromechanical relay contacts shall change state in accordance with the TSAP. Any spurious change of state of the relay contacts shall not exceed 2 milliseconds in duration.

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	33 of 60	Date:	09/18/00

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

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

- Resonance search testing was performed as described in IEEE-344, Section 7.1.4. The tests were performed to provide information on the dynamic response of the equipment mounted on the seismic test table. Over most of the 1 Hz to 50 Hz test frequency range, the accelerations experienced at the response accelerometer attachment points equaled or slightly exceeded the acceleration applied to the seismic test table (as measured by the control accelerometers) in each of the three orthogonal directions.
- Five OBE tests and one SSE test were performed using the same test response spectrum (TRS) which is shown in Figure 5. The acceleration capability of the Wyle Triaxial Seismic Simulator Table was limited to a maximum of 10 g's based on 5% damping with the equipment tested. Therefore, OBE and SSE tests were performed using a maximum acceleration level of 10 g's.

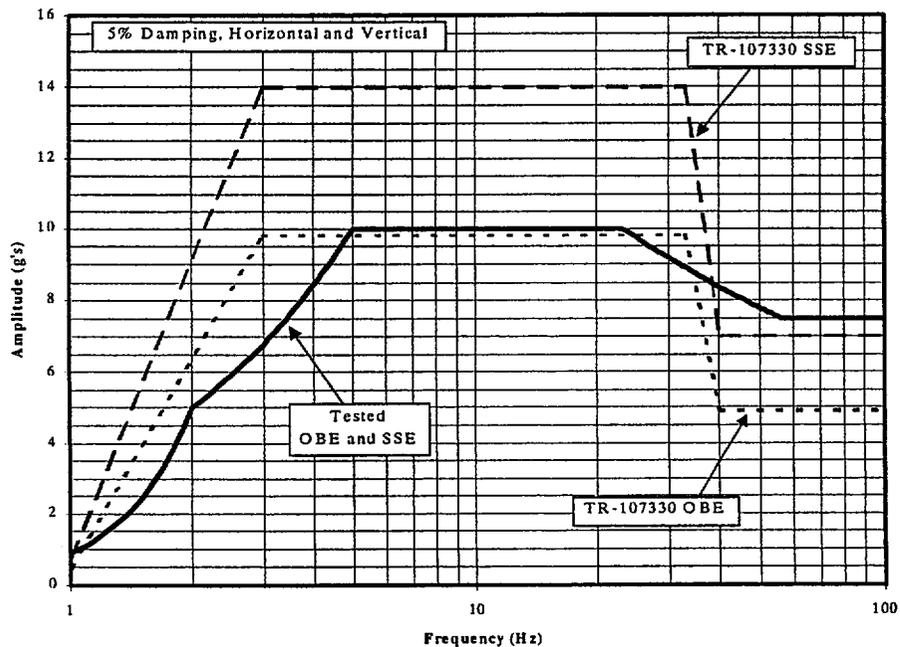


Figure 5. Seismic Test Accelerations

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	34 of 60	Date:	09/18/00

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

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

The TRICON Test Specimen was visually inspected for damage or degradation following each OBE and SSE test. Results of these inspections showed no physical damage or degradation of the test specimen.

The results of the seismic test show that:

1. Seismic testing of the TRICON Test Specimen was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 344-1987.
2. The TRICON Test Specimen met all applicable performance requirements during and after application of the seismic test vibration levels.
3. The seismic test results demonstrate that the TRICON PLC platform and the Lambda field power supply are suitable for qualification as Category 1 seismic equipment.
4. The horizontal and vertical seismic withstand response spectrum of the TRICON PLC and Lambda field power supply as determined by testing is shown in Figure 5. The figure is based on a damping value of 5% used in the data analysis.
5. The seismic test results demonstrate that the equipment mounting configurations shown in Triconex Drawing No. 7286-101 are adequate to support seismic qualification of the TRICON PLC and the Lambda field power supply.

4.4 Radiation Qualification

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

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	35 of 60	Date:	09/18/00

4.5 Electromagnetic Compatibility Qualification

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

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

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

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

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	36 of 60	Date:	09/18/00

During EMI/RFI testing, the TRICON Test Specimen was powered with a revised TSAP operating. In order to minimize transmission of outside EMI/RFI sources into the EMI/RFI test chamber, all power, signal, and communications cables entering the EMI/RFI test chamber were passed through filters located in the chamber walls. Because the number of pass-through filters was limited, only one circuit per I/O module was connected. The specific configuration of the TRICON Test Specimen is described in the EMI/RFI Test Procedure, Reference 7.37.

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

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

The EMI/RFI test acceptance criteria are as follows, based on Appendix 7 of the Master Test Plan, Reference 7.22, and EPRI TR-107330, Section 4.3.7, Reference 7.4:

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

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

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

EMI/RFI testing of the TRICON Test Specimen was performed from November 9 through December 9, 1999 at Wyle Laboratories in Huntsville, Alabama. Results of the susceptibility testing showed that the TRICON main processors and coprocessors continued to function correctly throughout all test exposure levels. The transfer of input and output data was not



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	37 of 60	Date:	09/18/00

interrupted. There were no interruptions or inconsistencies in the operation of the system or the software. However, some susceptibilities were identified in the TRICON input, output and communication modules during the following susceptibility tests:

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

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

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

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

Summary of EMI/RFI Test Results

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

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	38 of 60	Date:	09/18/00

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

- Notes:
- 1) EPRI TR-102323-R1 requires CS114 tests be performed at a test level of 103 dB μ A, which corresponds with CS114 Curve 4 from MIL-STD-461D. The TRICON was tested at a CS114 test level of 95 dB μ A, which corresponds with CS114 Curve 3 from MIL-STD-461D.
 - 2) EPRI TR-102323-R1 requires RS101 tests be performed using the MIL-STD-461D, Army Only test level. The TRICON was tested at levels closer to the RS101 Navy Only test levels. Figure 4-2 in the Application Guide (Appendix B of this report) provides a comparison of the as-required and as-tested levels.

4.6 Surge Withstand

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	39 of 60	Date:	09/18/00

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

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

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

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

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

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

The surge withstand testing was performed at Wyle Laboratories in Huntsville, Alabama. Prior to the start of testing, all of the TRICON Test Specimen modules (power, communication, chassis interface and input/output) were removed and replaced with spare modules. This was done to protect the modules which had been through environmental, seismic and EMI/RFI testing from damage that could occur during surge withstand testing, and preserve the condition of the original modules for final performance proof testing. Change-out of the modules was appropriate because surge withstand tests are design tests as opposed to conditioning (or "aging") tests and therefore do not have to be performed on "aged" hardware.



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	40 of 60	Date:	09/18/00

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

Operation of the TRICON test system was monitored by the test system data logger and the Wonderware and Foxboro I/A workstations. The recorded data was evaluated in detail before, during and after each test to verify normal operation of the system and all peripheral communication interfaces. The test details are described in the Surge Withstand Test Report, Reference 7.42.

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

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

Test results described in the Surge Withstand Test Report, Reference 7.42, show that:

1. Surge withstand testing of the TRICON Test Specimen was performed in accordance with the applicable requirements of EPRI TR-107330, IEEE Standards C62.41-1991 and C62.45-1987, and IEC Standard 801-5.
2. In all cases the TRICON Test Specimen continued to operate in accordance with the test acceptance criteria following application of the surge test voltages.
3. Six of the eight digital output modules included in the TRICON Test Specimen exhibited vulnerability (permanent damage) to the applied surge test levels. These modules included:
 - Model 3611E, 115 VAC digital output
 - Model 3604E, 24 VDC digital output
 - Model 3624, 24 VDC digital output
 - Model 3607E, 48 VDC digital output
 - Model 3603E, 120 VDC digital output
 - Model 3623, 120 VDC digital output

In all cases the damaged points were detected by system diagnostics and indicated by status LED's and alarm lamps. In no case did a valid test result in damage to a module other than



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	41 of 60	Date:	09/18/00

the module to which the surge test voltage was applied. In all but one case (digital output module 3603E) the damaged points were found to have failed in the OPEN (or Loss of Power) state. Based on this performance, the TRICON system meets the TR-107330 acceptance criteria for surge withstand. Because the digital output modules listed above exhibited surge voltage vulnerability, the modules are acceptable for use in safety-related applications as long as one (or more) of the following conditions is satisfied:

- Qualified surge suppression devices are used on the safety-related discrete output lines,
 - The safety-related application can be demonstrated not susceptible to surge voltages on the discrete output lines. These would likely include most applications powered from plant vital power supplies, which are typically located indoors and are segregated or isolated from the high voltage power distribution systems in the plant.
 - The safety-related function can be demonstrated not susceptible to a common mode surge which might disable the same safety function in all redundant trains, or
 - The discrete output modules are not controlling a safety-related function.
4. The Model 3603E digital output module and associated Model 9661-910 termination panel exhibited vulnerability (permanent damage) to applied surge voltages. The Model 3603T digital output module and associated Model 9661-910 (revised) termination panel are revised versions of the Model 3603E module and ETA. These revised components were tested and demonstrated to have acceptable surge withstand capability (i.e., no demonstrated vulnerability). By evaluation (Reference 7.58) it is determined that the design modifications incorporated in the Model 3603T module do not affect the environmental, seismic and EMI/RFI test results obtained for the Model 3603E module. Therefore, the Model 3603T digital output module and its associated termination panel are considered equivalent replacements for the Model 3603E module.

4.7 1E to Non-1E Isolation

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	42 of 60	Date:	09/18/00

Accordingly, the following communication modules were tested for Class 1E isolation capability:

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

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

Class 1E to Non-1E electrical isolation testing of the PLC was performed in accordance with the requirements of IEEE 384-1981, Reference 7.10. In particular, IEEE 384 requires that (a) the isolation device prevents shorts, grounds and open circuits on the Non-1E side from unacceptably degrading the operation of the circuits on the 1E side, and (b) the isolation device prevents application of the maximum credible voltage on the Non-1E side from degrading unacceptably the operation of the circuits on the 1E side.

Communication port testing performed as part of the Prudency Test Procedure, Reference 7.31, addresses the item (a) isolation requirements for the TRICON communication modules. During prudency testing, the TRICON response time was monitored and shown not to degrade. These results are documented in the Triconex Performance Proof Test Report, Reference 7.44.

The Class 1E to Non-1E Isolation Test Procedure, Reference 7.36, addresses the item (b) isolation requirements for the communication modules and both the item (a) and item (b) isolation requirements for the relay output module.

The isolation testing was performed at Wyle Laboratories in Huntsville, Alabama. During testing, the TRICON Test Specimen was powered with the TSAP operating. The AC and DC power sources to the TRICON Test Specimen chassis power supplies were set at nominal source voltage and frequency conditions. The arrangement and grounding of the system during isolation testing was the same as for the EMI/RFI tests.

Operation of the TRICON test system was monitored by the test system data logger and the Wonderware and Foxboro I/A workstations. The recorded data was evaluated in detail before, during and after each isolation test to verify normal operation of the system and all peripheral communication interfaces. The test details are described in the Isolation Test Report, Reference 7.43.

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	43 of 60	Date:	09/18/00

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

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

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

1. Class 1E to Non-1E isolation testing of the TRICON Test Specimen was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 384-1981.
2. The TRICON Test Specimen met all applicable performance requirements during and after application of the Class 1E to Non-1E isolation test voltages.
3. The isolation test results (together with the Prudency Test communication port fault tests) demonstrate that the following TRICON PLC communication module ports provide adequate electrical isolation per IEEE 384-1981 between the safety related portions of the TRICON and connected non-safety related communication circuits:
 - Enhanced Intelligent Communication Module (EICM) Model 4119A, Serial Port Modbus Interfaces
 - Advanced Communication Module (ACM) Model 4609, Dual Nodebus (DNBI) and RS-423 Serial Port Interfaces to a Foxboro I/A Console
 - Network Communication Module (NCM) Model 4329, IEEE 802.3 (TCP/IP) Net 2 Interface to a Wonderware Console

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

4. The Class 1E to Non-1E isolation test results demonstrate that the TRICON PLC relay output module Model 3636R provides adequate electrical isolation per IEEE 384-1981 between the safety related portions of the TRICON and connected non-safety related field circuits. The testing demonstrated electrical isolation capability of the relay output points to



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	44 of 60	Date:	09/18/00

applied voltages of 600 VAC (at 23.4 amps maximum) and 250 VDC (at 10 amps maximum).

5. The Model 4211 Remote RXM fiber optic module is considered an acceptable Class 1E to Non-1E isolation device by design, and was not tested. The fiber optic cables are incapable of transmitting electrical faults from the remote Non-1E RXM module to the primary RXM module (which would be installed in the safety related TRICON chassis), and therefore meet IEEE 384-1981 electrical isolation requirements.

4.8 Electrostatic Discharge

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

4.9 Performance Proof Testing

Performance proof testing was conducted at the completion of all qualification testing to demonstrate the continued acceptable performance of the TRICON Test Specimen after exposure to the various qualification test conditions. The proof testing involved performing the Operability Test, Reference 7.30, and the Prudency Test, Reference 7.31. These procedures were developed in accordance with Sections 5.3 and 5.4 of EPRI TR-107330. Results of these tests are documented in the Performance Proof Test Report, Reference 7.44. This test report serves as an evaluation and summary of the Operability and Prudency test data collected throughout the qualification testing process. The data evaluation included comparison of the performance proof test data to Operability and Prudency test data collected during pre-qualification, environmental and seismic testing. Conclusions from the testing are provided in the report, including a summary of the specific manufacturer's performance specifications which were verified throughout qualification testing.

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

1. Analog Input/Output Module Accuracy – For all Operability Test runs, the accuracy of each analog input/output module was demonstrated to meet the published Triconex product



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	45 of 60	Date:	09/18/00

specifications. In addition, the test results show no degradation in module accuracy from pre-qualification testing throughout qualification and performance proof testing.

2. Response Time – Response times for digital input to digital output and analog input to digital output sequences were measured during all runs of the Operability Test procedure. Triconex provides a method for calculating the maximum expected digital input to digital output and analog input to digital output response time for a specific TRICON hardware configuration and application program scan time. The test data demonstrates that the Triconex equation provides a reliable upper bound on the maximum expected response times for a specific hardware configuration and an appropriately structured application program.
3. Discrete Input Operation – For all Operability Test runs, the OFF to ON and ON to OFF voltage switching levels of each digital input module were demonstrated to meet the published Triconex product specifications. In addition, the test results show no degradation in discrete input module voltage switching levels from pre-qualification testing throughout qualification and performance proof testing.
4. Discrete Output Operation – For all Operability Test runs, each discrete output module was demonstrated to operate ON and OFF at the manufacturer’s published product specifications for maximum operating current, and minimum and maximum operating voltage. In addition, the test results show no degradation in operation of the discrete output modules from pre-qualification testing throughout qualification and performance proof testing.
5. Timer Function Accuracy – For all Operability Test runs, the time out periods of the application program timer functions were demonstrated to not vary from the measured pre-qualification baseline time-out periods by more than the greater of $\pm 1\%$ of the time out period or three application program scan cycles. In addition, the test results show no degradation in timer function variation from pre-qualification testing throughout qualification and performance proof testing.
6. Failover Performance – Tests were done to demonstrate automatic failover to redundant components on simulated failures of a main processor module, an RXM module, a chassis expansion port cable, and chassis power supplies. All test results demonstrated acceptable failover operation of the TRICON Test Specimen.
7. Loss of Power Performance / Failure to Complete a Scan Detection – Each run of the Operability Test procedure included tests to demonstrate performance of the TRICON PLC on loss and restoration of power to the chassis power supplies. The test results demonstrated predictable and consistent response of the TRICON Test Specimen to a loss of power. The test results also demonstrated predictable and consistent response of the TRICON Test Specimen on recovery of power. In addition, successful restart of the



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	46 of 60	Date:	09/18/00

TRICON Test Specimen on restoration of power consistently indicated proper functioning of the watchdog timer mechanisms.

8. Power Interrupt Performance – Each run of the Operability Test procedure included tests to demonstrate power hold-up time performance of the TRICON PLC chassis power supplies on an interruption of source power for approximately 40 milliseconds. The test results demonstrated:
 - The 120 VAC and 230 VAC chassis power supplies meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 milliseconds when installed as the only chassis power supply or when installed in combination with a second chassis power supply.
 - The 24 VDC chassis power supplies do not meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 milliseconds. The measured hold-up time capability of the 24 VDC chassis power supplies was less than 3 milliseconds.

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

9. Power Quality Tolerance – Tests to demonstrate tolerance of the TRICON PLC and Lambda field power supply to changes in the quality (voltage and frequency) of AC and DC source power was performed. Tests were performed over the manufacturer’s allowable ranges of voltage and frequency for each type of power supply included in the testing. All test results demonstrated acceptable performance of the TRICON Test Specimen. In addition, power quality tolerance tests demonstrated acceptable performance of processor memory writes prior to TRICON reset on gradual loss of source power voltage.
10. Burst of Events Performance – Burst of Events testing demonstrated the ability of the PLC to process rapidly changing input and output signals based on the control logic of the TRICON operating application program.
11. Communication Port Failure Performance – Communication port failure testing demonstrated no effect on digital input to digital output and analog input to analog output response times during simulated failures of communication lines connected to communication ports on the EICM, ACM, NCM, and Chassis I/O expansion RS-485 ports.



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	47 of 60	Date:	09/18/00

4.10 Failure Modes and Effects Analysis

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

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

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

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

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

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	48 of 60	Date:	09/18/00

The detailed results of the FMEA are tabulated in Reference 7.46. The results show that failure modes that can prevent the TRICON system from performing its function are detected by proper application-specific design, the built-in system diagnostics or by periodic testing. Provided the results of this FMEA are applied to specific control system designs, there will be no undetectable failure modes associated with safety-related functions.

The TRICON system design information presented in References 7.19 and 7.20 includes recommendations for periodic testing of field inputs and outputs. These recommendations establish general surveillance techniques and surveillance intervals intended to maintain the high reliability of the overall control system. It is strongly recommended that specific nuclear plant safety-related applications incorporate the manufacturer's recommended methods and frequencies to maximize system reliability and operability.

4.11 Reliability and Availability Analysis

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

The reliability and availability analysis for the TRICON system is documented in Reference 7.45. This analysis complies with the applicable requirements of EPRI TR-107330.

For the TRICON analysis, the two probabilities calculated include: (1) the probability that the system will fail in a given period of time (reliability), and (2) the probability that the system will fail on demand in a given period of time (availability). As required by the EPRI TR, the analysis was performed with the assumption that periodic testing of the system will uncover faults that are not normally detected by the system. As the periodic test interval is lengthened, the probability of failure increases. Calculations were done for periodic test intervals ranging from 6 to 30 months. In all cases, the calculated reliability and availability were greater than 99.9%, which exceeds the recommended goal of 99.0% from the EPRI TR. For a periodic test interval of 18 months (corresponding to the typical nuclear plant refueling outage cycle), the reliability is 99.9984% and the availability is 99.9853%.

4.12 Component Aging Analysis

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

Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	49 of 60	Date:	09/18/00

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

Based on review of the components used to assemble a TRICON PLC, and recognizing the extensive self monitoring and diagnostic features of the TRICON system, the components which are susceptible to significant, undetected aging mechanisms were determined to include only the chassis power supplies and the backup batteries.

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

5.0 SOFTWARE QUALIFICATION

Ultimately, the basis for the qualification of the TRICON system software is the U.S. Nuclear Regulatory Commission Standard Review Plan (SRP), provided in NUREG-0800, Section 7, “Instrumentation and Controls.” The approach used to demonstrate compliance with the requirements of the SRP is based on the guidance provided in EPRI TR-107330 and EPRI TR-106439. This approach, including the activities performed as part of the software qualification effort and the acceptance criteria established for these activities, is described in the Software Qualification Report, Reference 7.49.

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

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

- SRP, Section 7.1, “Instrumentation and Controls – Introduction”;
- SRP, Appendix 7.0-A, “Review Process for Digital Instrumentation and Control Systems”;



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	50 of 60	Date:	09/18/00

- Branch Technical Position HICB-18, “Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems”;
- Branch Technical Position HICB-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.”
- NRC Regulatory Guide 1.152, which endorses IEEE Std 7-4.3.2 “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations.”

The TRICON and TriStation 1131 software, including documentation, development practices, and operating history were evaluated against these criteria. Detailed results from this evaluation are provided in the Software Qualification Report, Reference 7.49. Key results are summarized in the following sections.

5.1 Software Documentation

EPRI TR-107330, Section 8.7 lists the minimum documents that are needed to support software verification and validation and the related software quality processes. This list is based on NUREG/CR-6241, which BTP HICB-18 describes as an acceptable process for qualifying existing software, and ASME NQA-1-1994. The minimum documents are:

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

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

- Triconex company quality and engineering procedures which provide planning requirements for quality assurance, V&V, configuration management, and test activities,



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	51 of 60	Date:	09/18/00

- The original TRICON System Functional Requirements Specifications,
- A series of TRICON Software Design Specifications that define the incremental changes to the system,
- Test procedures and test reports applicable to each system revision (whether it includes changes to hardware, software, or both),
- The TRICON Software Release Definition documents that identify software changes made in each revision, and
- The TRICON user documentation.

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

5.2 Software Development Process

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

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

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	52 of 60	Date:	09/18/00

The TRICON system was initially developed 15 years ago, evolving into the present day configuration. When the TRICON operating system was conceived there was very little guidance in the way of industry standards to base the software development and design. Good programming practices were used based on the objective of producing a highly reliable safety system.

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

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

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

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

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

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

The first release of the Engineering Department Manual was in 1986. The first procedures concentrated on configuration and change control issues. While the QAM and QPM do provide some software specific requirements, the EDM provides the specific procedures that relate to development and maintenance of the TRICON software. These engineering procedures define a product life cycle which includes the following phases:



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	53 of 60	Date:	09/18/00

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

To assess the processes used to produce the TRICON software, including pre-existing code from the initial release, the QAM, QPM, and EDM procedures were reviewed at various points in time between 1986 and 1999. The evolution of the various Engineering Procedures described in the Software Qualification Report, Reference 7.49, demonstrates the continual refinement and improvement of the procedures from an initial set of eight to the current set of 36.

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

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

5.3 Software Verification and Validation Process

An essential issue for acceptability is a defined, controlled process for software verification and validation (V&V). The requirements specified in IEEE Std 1012-1986 provide an approach that is acceptable to the NRC for meeting the requirements of 10 CFR 50, Appendix B and the guidance given in Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." NRC Regulatory Guide 1.168 endorses IEEE Standard 1012-1986 as an acceptable methodology for implementing the verification and validation of safety system software, subject to certain exceptions listed in that Regulatory Guide.

Triconex's verification and validation activities do not strictly follow the ANSI/IEEE 1012 model. However, a life cycle process is defined in the engineering procedures and this process includes verification and validation processes. A detailed assessment of the Triconex process is provided in the Software Qualification Report, Reference 7.49.



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	54 of 60	Date:	09/18/00

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

Validation activities include functional tests (with regression testing) of the integrated system in accordance with written test procedures. In addition, hardware and software design upgrades and enhancements are tested using the automated fault insertion test to validate the diagnostic capability and software associated with diagnostics. The TriStation software is tested by manual and automated tests in accordance with written functional test procedures. These tests validate correct operation of both the TriStation and the TRICON. Functional outputs, boundary conditions, value conversions, and other essential functions are validated in this test. Since the test is automated and runs in a PC Windows environment, any changes to the TriStation operator interface will be explicitly uncovered in the testing process.

The Triconex V&V activities are supplemented by the independent certification activities performed by TÜV-Rheinland. TÜV-Rheinland is a German third party certification agency that validates equipment to existing international standards. In 1992, TÜV-Rheinland first certified the TRICON Version 6.2.3 to meet standard DIN V VDE 19250, resp. DIN V VDE 0801 requirements for safety equipment, class 5 (Test Report 945/EL 366/91, Reference 7.56).

Each new version has been tested by TÜV-Rheinland, with Version 9.3 being certified in February of 1998 to class 5 and class 6 of the DIN standard (Test report 945/EZ 102/98). The testing 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 three aspects of software review and testing by TÜV-Rheinland are software analysis, software testing, and integrated system (software/hardware) testing.

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

TÜV-Rheinland testing of the TriStation software involves checking the translation of the graphical or text user program to the final code. TÜV testing of the TRICON software consists of the following:



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	55 of 60	Date:	09/18/00

- Internal Fault Routines – Procedures such as the watchdog routines, CPU test, etc. were checked by either monitoring execution of the routines or by forcing the routines by means of fault insertion.
- Noise on the Processor – A software module was developed to simulate noise on the processor by putting the CPU address pointer to arbitrary positions and verifying proper detection.
- Functional Verification – Portions of the Triconex functional verification procedures were performed to verify the software module’s performance and validity of the test procedure.

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

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

5.4 Safety Analysis

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

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

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

5.5 Configuration Management and Error Notification

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



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	56 of 60	Date:	09/18/00

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

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

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

Triconex also has an established error tracking and reporting program that is consistent with the requirements established in 10 CFR 21. Errors are classified according to severity, with Product Alert Notices (PAN) being the most significant. Only five PANs have been issued against the TRICON since the release of the system over 15 years ago. All of the Product Alert Notices were evaluated as part of this qualification process. An extremely conservative approach to customer notification was found. Most of the Product Alert Notices affected only a very small subset of users. Instead of attempting to determine which customers might be at risk, Triconex chose to notify all customers. None of the notices affect this qualification effort. In addition to this safety critical issue notification system, other notification systems exist which are used to disseminate technical data.

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

6.0 SYSTEM APPLICATION

This summary report describes tests, evaluations and analyses which were performed to demonstrate generic qualification of the TRICON system for use in safety-related nuclear power plant applications. In any actual nuclear plant application, plant-specific conditions must be evaluated to ensure that they are within the qualification envelope of the TRICON system as



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	57 of 60	Date:	09/18/00

described in this summary report. System-specific performance requirements must also be evaluated to ensure that the TRICON system accuracy, response time, and other performance attributes are adequate. Other important considerations for application of the TRICON system to specific plant applications include design, operation, and maintenance requirements needed to ensure high reliability. These requirements include, for example, annunciation of system faults and periodic testing to check for the limited number of abnormal conditions not detectable by the built-in self-diagnostics.

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

7.0 REFERENCES

- 7.1 NUREG-800; Standard Review Plan, Section 7.0, "Instrumentation and Controls – Overview of Review Process," Rev. 4 – June 1997
- 7.2 NUREG/CR-6241, "Using Commercial-Off-the-Shelf (COTS) Software in High-Consequence Safety Systems," November 10, 1995
- 7.3 NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," October 1997
- 7.4 EPRI Report, TR-107330, "Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."
- 7.5 EPRI Report, TR-106339, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications"
- 7.6 EPRI Report TR-102323-R1, "Guidelines for Electromagnetic Interference Testing in Power Plants"
- 7.7 IEEE Std. 323-1983, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
- 7.8 IEEE Std. 344-1987, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
- 7.9 IEEE Std. 381-1977, "Standard Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations"
- 7.10 IEEE Std. 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits"



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	58 of 60	Date:	09/18/00

- 7.11 IEEE C62.41-1991, "Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits"
- 7.12 IEEE C62.45-1987, "Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits"
- 7.13 IEC 801-5, January 1990, "Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment, Part 5 – Surge Immunity Requirements"
- 7.14 IEEE Std. 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
- 7.15 IEEE Std. 1012-1986, "IEEE Standard for Software Verification and Validation Plans"

TRICONEX DOCUMENTS

- 7.16 Triconex Quality Assurance Manual (QAM)
- 7.17 Triconex Quality Procedures Manual (QPM)
- 7.18 Triconex Engineering Department Manual (EDM)
- 7.19 TRICON Product Guide, Triconex Document No. 9791007-004
- 7.20 TRICON Planning and Installation Guide, Triconex Document No. 9720051-005

TRICONEX NUCLEAR QUALIFICATION PROJECT DOCUMENTS

- 7.21 Triconex Quality Plan, Triconex Document No. QPL-01.
- 7.22 Master Test Plan, Triconex Document No. 7286-500
- 7.23 Master Configuration List, Triconex Document No. 7286-540
- 7.24 Software QA Plan, Triconex Document No. 7286-537
- 7.25 Tricon Test Specimen Description, Triconex Document No. 7286-541
- 7.26 Function Diagrams, Triconex Drawing Nos. 7286-430 to 444
- 7.27 Test System Loop Diagrams, Triconex Drawing Nos. 7286-531 to 543



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	59 of 60	Date:	09/18/00

- 7.28 Test System Wiring Drawings, Triconex Drawing Nos. 7286-001 to 329
- 7.29 Setup and Checkout Test Procedure, Triconex Document No. 7286-502
- 7.30 Operability Test Procedure, Triconex Document No. 7286-503
- 7.31 Prudency Test Procedure, Triconex Document No. 7286-504
- 7.32 Burn-In Test Procedure, Triconex Document No. 7286-505
- 7.33 Environmental Test Procedure, Triconex Document No. 7286-506
- 7.34 Seismic Test Procedure, Triconex Document No. 7286-507
- 7.35 Surge Withstand Test Procedure, Triconex Document No. 7286-508
- 7.36 Class 1E to Non-1E Isolation Test Procedure, Triconex Document No. 7286-509
- 7.37 EMI/RFI Test Procedure, Triconex Document No. 7286-510
- 7.38 Pre-qualification Test Report, Triconex Document No. 7286-524
- 7.39 Environmental Test Report, Triconex Document No. 7286-525
- 7.40 Seismic Test Report, Triconex Document No. 7286-526
- 7.41 EMI/RFI Test Report, Triconex Document No. 7286-527
- 7.42 Surge Test Report, Triconex Document No. 7286-528
- 7.43 Class 1E to Non-1E Isolation Test Report, Triconex Document No. 7286-529
- 7.44 Performance Proof Test Report, Triconex Document No. 7286-530
- 7.45 Reliability/Availability Study for TRICON PLC Controller, Triconex Document No. 7286-531
- 7.46 Failure Modes and Effects Analysis (FEMA) for TRICON Version 9 PLC, Triconex Document No. 7286-532
- 7.47 Radiation Hardness Evaluation, Triconex Document No. 7286-533
- 7.48 TRICON System Accuracy Specifications, Triconex Document No. 7286-534
- 7.49 Software Qualification Report, Triconex Document No. 7286-535



Document:	7286-545	Title:	QUALIFICATION SUMMARY REPORT		
Revision:	1	Page:	60 of 60	Date:	09/18/00

- 7.50 Simulator Application Program (SAP) Functional Requirements and Program Listing, Triconex Document No. 7286-520
- 7.51 TSAP Functional Requirements Specification, Triconex Document No. 7286-517
- 7.52 TSAP Design Specification, Triconex Document No. 7286-518
- 7.53 TSAP Program Listing, Triconex Document No. 7286-519
- 7.54 TSAP Validation Test Procedure, Triconex Document No. 7286-513
- 7.55 TSAP V&V Report, Triconex Document No. 7286-536
- 7.56 TÜV-Rheinland Microelectronic and Process Automation, "Type Approval for the TRICON Triple Modular Redundant (TMR) Controller TRICON," Report-No. 945/EL 336/91, April 19, 1991
- 7.57 TÜV-Rheinland Microelectronic and Process Automation, "Type Approval of TRICON Version 9.3," Report-No. 945/EZ 102/98, February 18, 1998
- 7.58 E-Mail from Triconex (G. Hufton) to MPR Associates (M. Albers) dated March 22, 2000, "Revised Module Evaluation"