TRICONEX

Triconex Corporation
15091 Bake Parkway
Irvine, California 92618
United States of America

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

November 14, 2000

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

Subject: Nuclear 1E Qualification of the TRICON TMR Programmable Logic Controller (PLC) – Revised Project Proprietary Documents

Reference: 1. Letter, T. Martel (Triconex) to NRC, July 17, 2000, subject; Nuclear Qualification of the TRICON TMR PLC – Project Qualification Document Submittal (Proprietary Documents)

2. Project Number 709

Gentlemen:

In the referenced letter, Triconex submitted 12 proprietary documents for the NRC's review in connection with our TRICON 1E Qualification Project, as listed below. These documents were accompanied by a request for withholding from public disclosure per 10CFR2.790 and the required affidavit.

1. Software Qualification Report	7286-535	Rev 1
2. Pre-Qualification Test Report	7286-524	Rev 0
3. Environmental Test Report	7286-525	Rev 0
4. Seismic Test Report	7286-526	Rev 0
5. EMI/RFI Test Report	7286-527	Rev 0
6. Surge Test Report	7286-528	Rev 0
7. 1E/Non 1E Isolation Test Report	7286-529	Rev 0
8. Performance Proof Test Report	7286-530	Rev 0
9. Master Test Plan	7286-500	Rev 3
10. TSAP V&V Report	7286-536	Rev 0
11. Failure Modes & Effects Analysis	7286-532	Rev 0
12. Master Configuration List	7286-540	Rev 20

Non-proprietary versions of these documents were not provided at the time. Also, the proprietary portions of these documents were not specifically identified as requested by the staff. To resolve these documentation concerns, we are enclosing revised copies of documents 1-11 listed above, marked up as requested to show areas of proprietary information (please note that content has not changed). Also provided are non-proprietary versions of these documents for the public record with proprietary areas deleted. Document 12 above, the Master Configuration List, will be addressed in a separate submittal.

D062 1 Prop Version 1 NP Version

These enclosed documents replace and supersede earlier versions provided. As indicated in the July 17, 2000 letter, the enclosed documents are considered proprietary where so marked and should be withheld from public disclosure per 10CFR2.790. The affidavit provided in the July 17, 2000 letter still applies to these documents.

Reference 1 also addressed Triconex proprietary documents submitted to the NRC for information in earlier letters. These earlier documents included detailed test procedures, test software (TSAP) development documents, and test system configuration drawings. Due to the content of these documents being predominantly proprietary details of test process, method, and apparatus (reference section 5a of the July 17 affidavit), it is not considered practical to provide versions of these documents with the proprietary information removed.

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

Sincerely,

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

Enclosures
cc: L. Raynard Wharton, NRC (w/o attachments)
P. Loeser, NRC (w/o attachments)

TRICONEX DOCUMENTS

NON-PROPRIETARY VERSIONS

---

1. Software Qualification Report	7286-535	Rev 1
2. Pre-Qualification Test Report	7286-524	Rev 0
3. Environmental Test Report	7286-525	Rev 0
4. Seismic Test Report	7286-526	Rev 0
5. EMI/RFI Test Report	7286-527	Rev 0
6. Surge Test Report	7286-528	Rev 0
7. 1E/Non 1E Isolation Test Report	7286-529	Rev 0
8. Performance Proof Test Report	7286-530	Rev 0
9. Master Test Plan	7286-500	Rev 3
10. TSAP V&V Report	7286-536	Rev 0
11. Failure Modes & Effects Analysis	7286-532	Rev 0

TRICONEX

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

FAILURE MODES AND EFFECTS ANALYSIS (FMEA) FOR TRICON VERSION 9 PROGRAMMABLE LOGIC CONTROLLER

Document No: 7286-532

Revision 0

March 27, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Bruce Nickel		Project Engineer
Reviewer:	Tim Hurst		Engineer
Approvals:	Mitch Albers		Project Manager
	Troy Martel		Triconex Project Director
	Aad Faber		Director, Product Assurance

Document Change History			
Revision	**Date**	**Change**	**Author**
0	03/27/2000	Initial Issue	B. Nickel

TABLE OF CONTENTS

1.0 PURPOSE

EPRI TR-107330 "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants" (Reference 5.1) defines the requirements for qualifying commercially available programmable logic controllers (PLCs) for safety-related nuclear power plant applications. The Reference 5.1 guidelines require the performance of a Failure Modes and Effects Analysis (FMEA) to evaluate the effects of failures of components in the PLC modules on PLC performance.

The Triconex Corporation is qualifying the commercial grade "TRICON" Version 9 Triple Modular Redundant (TMR) Programmable Logic Controller for safety-related nuclear power plant applications. This report documents the methodology and results of the FMEA performed for the generic qualification of the TRICON Version 9 TMR PLC.

2.0 OBJECTIVE

The objective of this report is to document the methodology and results of the generic FMEA for the TRICON Version 9 TMR PLC. The FMEA is performed in accordance with the applicable guidelines of Reference 5.1, Section 6.4.1, "FMEA".

3.0 SCOPE

3.1 This analysis is prepared as a part of the TRICON Nuclear Qualification Program as defined in Reference 5.2.

3.2 The system analyzed by the FMEA is identical to the Test Specimen configuration that was used in the Qualification Test Program. The Test Specimen includes one TRICON Main Chassis, two RXM Chassis and one Expansion Chassis. The Test Specimen configuration was established to simulate a single channel/train of a typical nuclear power plant safety-related protection system installation. Specific hardware configurations, application programs, supporting drawings and documents are identified in the Generic Qualification Master Configuration List (Reference 5.3).

3.3 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 analysis does not address failure modes associated with application of multiple PLC systems in redundant safety trains. Although application-specific mitigating design features are described for certain failures, this analysis should not be considered as a bounding analysis applicable to actual safety-related applications and installations.

3.4 The Model 8107 Seismic Balance Module used in the qualification test specimen is passive in nature and provides no operational functionality. This module is therefore not included in the scope of the FMEA.

4.0 METHOD OF ANALYSIS

The subject FMEA is performed in accordance with the applicable guidelines of EPRI TR-107330 Section 6.4.1, "FMEA" (Reference 5.1). In general, the techniques of Appendix A of ANSI/IEEE Std. 352-1987 (Reference 5.4), have been used in this analysis. These techniques included definition of functional areas of PLC operation, as described later in this section. The effect of both single failures and common mode failures on each functional area were then analyzed, as summarized in Section 7.0.

This FMEA is 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. In addition, the TRICON self-diagnostic features, described in References 5.5 and 5.6 and summarized in Section 6.0 of this report, have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate that the diagnostics detect all possible single failures within each module.

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

a) Power Supplies (including chassis power supplies and I/O loop power supplies)
b) PLC Chassis (including internal power and communication buses)
c) Main Processors and Communications Modules
d) PLC Cables
e) PLC I/O Modules
f) Termination Panels

Figure 1 is a simplified block diagram of a typical TRICON chassis showing the arrangement of these major components. The approach used in this FMEA is to postulate credible failures of these components, identify the mechanisms that could cause these failure modes, 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, this FMEA 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).

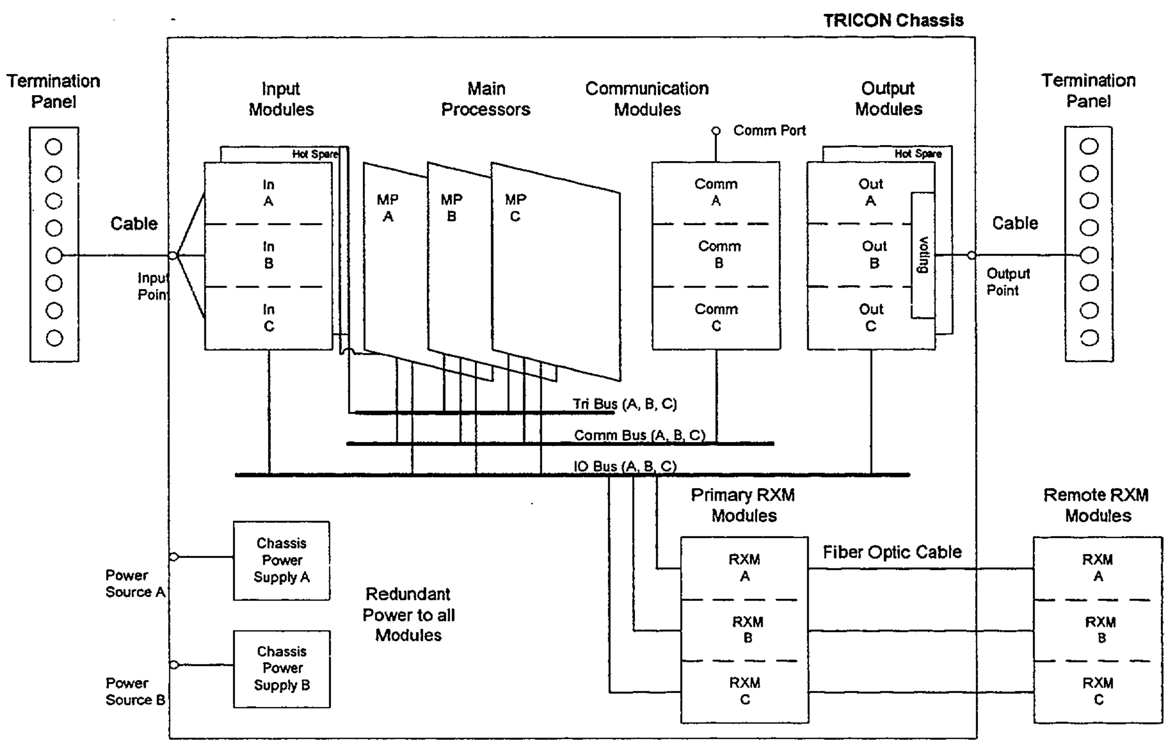


Figure 1. Simplified Block Diagram of Typical TRICON System

In order to identify the effect of failures on system operation (i.e., to prioritize types of failures), Section 4.2.3.5.C of Reference 5.1 recommends the following categories of failure states be identified as a part of the FMEA for redundant PLCs: *(a)*

Reference 5.1 also recommends identification of failures detected by the system diagnostics, and those that will only be detected by surveillance testing. For this FMEA, (a)

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

The FMEA tabulation in Section 7.0 of this report includes a column that documents the appropriate failure category assignment for each postulated PLC failure mode. The tabulation in Section 7.0 provides the following data for each type of failure, as required by the guidance of Reference 5.1.

a) Affected Components
b) Failure Mode
c) Failure Mechanism
d) Failure Category
e) Effect on PLC Inputs and Outputs
f) Effect on PLC Operability

Section 6.0 of this report provides a description of the PLC diagnostics that aid in detection of postulated failures, as well as a summary of the failures determined in Section 7.0.

5.0 REFERENCES

5.1 EPRI Report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants", Final Report dated December 1996

5.2 Triconex Document 7286-500, Master Test Plan

5.3 Triconex Document 7286-540, Generic Qualification Master Configuration List

5.4 ANSI/IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems"

5.5 Triconex Part No. 9720051-005, TRICON Planning and Installation Guide, Manual Release 5, March 1998.

5.6 Triconex Part No. 9791007-004, TRICON Technical Products Guide, Version 9.2 Systems, June 1997.

6.0 PLC MODULE DIAGNOSTIC DESCRIPTION

This section provides a basic description of the TRICON processor, communications and input/output module operation and diagnostic functions. This description of the diagnostic operations is provided to augment the FMEA tabulation provided in Section 7.0. A more detailed description of this information is presented in References 5.5 and 5.6.

6.1 INPUT MODULES

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. Any 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.

6.1.1 DIGITAL INPUT MODULES

This discussion is applicable to the following digital input (DI) modules:

Model 3501E; 115 Vac/Vdc Opto-isolated, non-commoned (32 points)
Model 3502E; 48 Vac/Vdc Commoned in groups of 8, Self Test (32 points)
Model 3503E; 24 Vac/Vdc Commoned in groups of 8, Self Test (32 points)
Model 3504E; 24/48 Vdc High Density, DC Coupled (64 points)
Model 3505E; 24 Vdc Low Threshold Commoned, Self Test (32 points)

Each DI module contains the circuitry for three identical legs. The three legs are completely isolated from each other and operate independently, so a fault on one leg cannot pass to another. There is an 8-bit microprocessor, called the I/O communication processor on each Main Processor Module to control communication with all I/O modules on a specific leg.

The three input legs independently measure each input signal, determine the respective state of each input signal, and place the values into input tables A, B, and C. Each input table is regularly interrogated over the leg-specific I/O busses by the I/O communication processor located on the corresponding main processor module. For TMR digital modules, all critical signal paths are triplicated. Each leg conditions signals independently and provides optical isolation between the field and the TRICON. The one exception is the Model 3504E; 24/48 Vdc High Density (64 points) module, which has no isolation.

Each DI module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module Fault Indicator, which in turn activates the chassis alarm signal. The module is designed to operate correctly in the presence of a single fault and may continue to operate properly with some multiple faults.

(b)

(b)

toggling will test the module's ability to transition to the opposite state in order to diagnose problems such as "Stuck On" / "Stuck Off" signals due to failed or faulted leg components. Since normal opto-isolator failures are random and detectable due to the TMR sampling of inputs, only a single failure per input is likely. Even with stuck on faults on a single input leg, the other two input legs would vote out the failed opto-isolator.

The Model 3502E, 3503E and 3505E DI modules extend fault coverage by self-diagnosing "Stuck On" leg signals. The DI modules are designed to monitor field signals that remain in the "On" state for long periods of time. The extended diagnostics verify the leg can process a transition to the "Off" commanded state.

(b)

The Model 3504E DI Modules extend fault coverage even further by the on-line ability to self-diagnose "Stuck On" and "Stuck Off" leg signals. The extended diagnostics verify each leg can process a commanded state transition in either direction.
Each leg contains "High" and "Low" reference signals as multiplexer inputs that momentarily drive the input signal for the leg under test to the "High" or "Low" state.

This test, which verifies the proper operation of leg signal processing and conditioning circuitry by ensuring the proper commanded state is propagated throughout the leg, is continually rotating among the three legs. Should a leg fail the test, the module fault indicator will be illuminated.

The DI module diagnostics are specified to operate as follows, as defined in Reference 5.5:

(b)

6.1.2 PULSE INPUT MODULE

This discussion is applicable to the following pulse input (PI) module:

Model 3510; Pulse Input, AC Coupled (8 points)

For the PI module, the extent of the diagnostic routine is the comparison across the three legs of the respective signal values.

Any leg signal value outside a set tolerance with the signal values in neighboring legs is reported to its respective Main Processor Module. The Main Processor Module fault analyzer routines determine whether a fault exists on a particular module at the end of each scan. One-time differences that result from sample timing variations are distinguished from a pattern of differing data. Should a Main Processor Module diagnose a faulty leg on a particular module, it will signal the pulse input module to illuminate its fault LED.

The PI module diagnostics are specified to operate as follows, as defined in Reference 5.5:

(b)

For a single input reading, a leg-to-leg deviation may result if the measured values of the three legs differ by the minimum input change specified. If the deviations continue for the specified minimum period, an input fault may be declared.

6.1.3 ANALOG INPUT MODULES

This discussion is applicable to the following analog input (AI) modules:

Model 3700A; 0-5 Vdc Differential, DC Coupled (32 points)
Model 3701; 0-10 Vdc Differential, DC Coupled (32 points)
Model 3703E; 0-5/0-10 Vdc Differential, Isolated (16 points)
Model 3704E; 0-5/0-10 Vdc High Density Differential, DC Coupled (64 points)

Each of the three AI legs asynchronously measure the input signal and place the results into an input table of values, which is passed to its associated main processor module using the corresponding I/O bus. The input table in each main processor module is transferred to its neighbor across the TRIBUS. The median value is selected by each main processor (in a duplex mode, the average value is used), and the input table in each main processor is corrected accordingly. Signals outside an internally specified error band in this median signal selection process will be alarmed by the Main Processor on the input module. Each AI module leg is automatically calibrated using multiple reference voltages read through the multiplexer, which determine the gain and bias required to adjust the readings of the A/D converter.

Each AI module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module Fault Indicator, which in turn activates the chassis alarm signal. The module is designed to operate correctly in the presence of a single fault, and may continue to operate properly with some multiple faults. (b)

(b)

Processor Module diagnose a faulty leg on a particular module, it will signal the input module to illuminate its Fault LED.

The AI module diagnostics are specified to operate as follows, as defined in Reference 5.5: (b)

For a single input reading, a leg-to-leg deviation may result if the measured values of the three legs differ by the minimum input change specified. If the deviations continue for the specified minimum period, an input fault may be declared.

6.1.4 THERMOCOUPLE INPUT MODULES

This discussion is applicable to the following thermocouple input modules:

Model 3706A; Thermocouple Differential, DC Coupled (32 points)
Model 3708E; Thermocouple Differential, Isolated (16 points)

The diagnostic routine for the Model 3706A Thermocouple Input Modules consists of the automatic or self-calibration of each leg using internal-precision reference voltages. The microprocessors on each leg test for known or expected signal values within a certain tolerance. If the leg microprocessors receive signals within the allowed tolerance, the leg will self-calibrate its A/D converter to null out any undesirable offsets or gains. The module will flag any out of tolerance signal received.

The thermocouple input modules also perform automatic cold or reference junction temperature compensation. Solid state temperature sensors on the termination panel produce a current for each leg that is proportional to the temperature at the field contact

(b)

In addition, the Model 3708E interrogates the reference or cold junction temperature measurements across the three legs. Microprocessors on each leg compare the measured compensation temperature across the three legs. Each microprocessor will select the middle of the three temperatures for use in compensating field input point data.

The Thermocouple Input module diagnostics are specified to operate as follows, as defined in Reference 5.5: (b)

6.2 OUTPUT MODULES

6.2.1 DIGITAL OUTPUT MODULES

This discussion is applicable to the following digital output (DO) modules:

Model 3601E; 115 Vac Opto-isolated, Non-commoned (16 points)
Model 3603E; 120 Vdc Opto-isolated, Commoned (16 points)
Model 3604E; 24 Vdc Opto-isolated, Non-commoned (16 points)
Model 3607E; 48 Vdc Opto-isolated, Non-commoned (16 points)

(b)

Failure of any test within the three steps will result in the illumination of the fault LED on the output module. The modules additionally compare output table data across the three legs, with any discrepancies reported back to respective Main Processor Modules. The Main Processor Module fault analyzer routine diagnoses failed legs on output modules at the end of each scan, with a faulty output module annunciated by the system. The modules are specifically designed for applications that hold points in one state for long periods of time. The routine guarantees full fault coverage even if the commanded state at the field terminals never change.

(b)

The maximum output toggle rate enables proper operation of I/O diagnostics and detection of all normally detectable faults. The minimum toggle rate provides fault coverage of normally undetectable faults within 10% of the calculated Mean Time Between Failure (MTBF).

6.2.2 SUPERVISED DIGITAL OUTPUT MODULES

This discussion is applicable to the following supervised digital output (SDO) modules:

Model 3611E; 115 Vac Galvanically Isolated, Commoned, Supervised (8 points)
Model 3623; 120 Vac Opto-isolated, Commoned, Supervised (16 points)
Model 3624; 24 Vdc Opto-isolated, Commoned, Supervised (16 points)

The Model 3623 and 3624 SDO modules perform all three steps of the OVD routine, as discussed in the previous Section 6.2.1. However, these modules extend Step One of the routine to include fault coverage of the field load device. In addition to voltage loopback circuitry, the SDO modules contain additional current loopback circuitry allowing each leg to measure the current flowing to the load.

The current loopback circuitry allows the SDO modules to self-diagnose possible open or short circuit conditions at the field load terminals. The modules perform continuous continuity checks of the field load by verifying that when energized, current is actually flowing and the current is below a certain threshold value. The module annunciates any faulty switch or loss of field load. The modules are designed to provide complete fault coverage for both energize-to-trip and de-energize-to-trip applications.

The Model 3611E SDO module also performs all three steps of the OVD routine discussed in the previous Section 6.2.1. These modules also extend Step One of the routine to include fault coverage of the field load device. In addition to voltage loop-back circuitry, the modules contain additional current loop-back circuitry allowing each leg to measure the current flowing to the load. This module is also designed to provide complete fault coverage for both energize-to-trip and de-energize-to-trip applications.

The current loop-back circuitry allows the 3611E SDO module to self-diagnose possible open or short circuit conditions at the field load terminals. The module performs continuous continuity checks of the field load by verifying that when the loop-back circuit is energized, current is actually flowing and the current is below a certain threshold value. The module annunciates all switch failures or any loss of field load problems. This SDO module also compares output table data across the three legs, with any discrepancies reported back to the respective Main Processor Modules. The Main Processor Module fault analyzer routine diagnoses failed legs on SDO modules at the end of each scan, with a faulty SDO module annunciated by the system.

The SDO module diagnostics are specified to operate as follows, as defined in Reference 5.5:

(b)

6.2.3 RELAY OUTPUT MODULE

This discussion is applicable to the following relay output (RO) module:

Model 3636R; Relay Output, Non-triplicated, Normally Open, 32 points

RO modules are designed for use on non-critical points that are not compatible with "high-side" solid-state output switches. The modules do not possess the series-parallel switch configuration, designed to accommodate single switch failure without affecting the signal driving the load. Therefore, the RO module is not single fault tolerant, and is not intended for use in critical safety-related applications. This module may be used to provide contact inputs to a non-safety annunciator system and is qualified as a 1E to non-1E isolator.

The RO modules have three legs that receive signals from respective Main Processor Modules. The three leg signal sets are voted, and the voted signals are used to drive the 32 individual output relays. Each output contains loopback circuits that verifies the operation of each relay independent of the load. Ongoing diagnostics test the operational status of the module. Failure of any diagnostic activates a Fault indicator on the module, which in turn activates the chassis alarm.

6.2.4 ANALOG OUTPUT MODULE

This discussion is applicable to the following Analog Output (AO) module:

Model 3805E; 4-20ma Current Loop, DC Coupled (8 points)

AO modules contain three separate and isolated legs, with each leg equipped with a D/A converter. One of the legs is selected to drive the analog output, and the output is continuously checked for correctness by loopback inputs on each point which are read by (b)

Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module Fault Indicator, which in turn activates the chassis alarm signal. The module is designed to operate correctly in the presence of a single fault and may continue to operate properly with some multiple faults.

The health of each leg is verified by monitoring output current via a voltage loopback

(b)

6.3 MAIN PROCESSOR MODULE

This discussion is applicable to the following Main Processor Module:

Model 3006; Enhanced TRICON Main Processor, 2 Mbytes SRAM

A TRICON system utilizes three Main Processor Modules to control 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 I/O 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

(b)

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 will be corrected or compensated for at the Main Processor Module level when the voted data table is formed.

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 will be compensated for at the Main Processor Module level when the voted data table is formed. Significant errors will be alarmed.

The primary processors on the Main Processor Modules execute the application program in parallel on the voted input table data and produce an output table of values in shared memory. The voting schemes explained above for analog and digital data ensure the process control programs are executed on the same or equal 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 to the corresponding output module over the I/O data bus.

(b)

At the beginning of each scan, the Main Processor Modules transmit/receive copies of the previous scan Output Tables to/from neighbors over the TRIBUS. At the end of the scan, the modules vote on the previous scan output data to diagnose any faults. Extensive diagnostics validate the health of 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. The Main Processor Modules also 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 latent faults. The Main Processor diagnostics perform the following:

(b)

(b)

6.4 COMMUNICATIONS MODULES

6.4.1 EICM MODULE

This discussion is applicable to the following Communications Module:

Model 4119; Enhanced Intelligent Communications Module (EICM), Isolated

The EICM allows the TRICON to communicate with Modbus masters and slaves, and PCs running the TriStation programming software that is used to develop and download application programs to the TRICON controller. 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.

6.4.2 ACM MODULE

This discussion is applicable to the following Communications Module:

Model 4609; Advanced Communications Module (ACM), Foxboro I/A Series Nodebus Interface

The ACM acts as an interface between a TRICON and the Foxboro Intelligent Automation (I/A) Series system. The TRICON system appears to the Foxboro system as "Control Processor" node on the I/A 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.

6.4.3 NCM MODULE

This discussion is applicable to the following Communications Module:

Model 4329; Network Communications Module (NCM), 802.3 Port

The NCM allows the TRICON to communicate with other TRICONs and with external hosts over 802.3 networks. The NCM provides two BNC port connectors: NET 1 supports Peer-to-Peer and time synchronization protocols, Net 2 supports open networking to external systems using Triconex applications. Note that in a Peer-to-Peer configuration, communication between TRICONs is not triplicated and this communication is therefore subject to a single failure of the communication port or cable.

6.4.4 RXM MODULES

This discussion is applicable to the following Remote Extender Modules:

Model 4210-3; Primary RXM, Multi-mode Fiber Optics (set of 3 modules)
Model 4211-3; Remote RXM, Multi-mode Fiber Optics (set of 3 modules)

The RXM Multi-mode Fiber Optics modules allow I/O modules to be located several kilometers away from the Main Chassis. The RXM 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. A Primary RXM module set is connected to the Remote RXM module set housed in a remote chassis. The RXM sets are available for fiber optic cables with a communication rate of 375 Kbaud. These sets provide maximum immunity against electrostatic and electromagnetic interference, and support configurations with optical modems and fiber optic point-to-point cabling. The interfacing cabling is unidirectional for each channel. One cable carries data transmitted from the Primary RXM to the Remote RXM. The second cable carries data received by the Primary RXM from the Remote RXM.

6.5 POWER SUPPLY MODULES

This discussion is applicable to the following Power Supply Modules:

Model 8310; 120 Vac/Vdc – 175-Watt Power Module
Model 8311; 24 Vdc – 175-Watt Power Module
Model 8312; 230 Vac – 175-Watt Power Module

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

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

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

The chassis backplane provides terminal strip interfaces for power and alarm connections. The alarm feature operates independently for each power module. The alarm contacts on both main chassis power modules are actuated on the following states:

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

The alarm contact on at least one Main Chassis power module is actuated 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 overtemperature condition

The alarm contacts on at least one power module of an expansion chassis actuates when the following conditions exist:

- A power module fails
- Primary power to a power module is lost
- A power module has a overtemperature condition

The alarm contacts on both power modules of an expansion chassis actuate when an I/O module fails.

6.6 TRICON CHASSIS ASSEMBLIES

A TRICON system consists of one Main Chassis and up to fourteen additional chassis. The TRICON main chassis can support the following modules:

- Two Power Modules
- Three Main Processors

- Communications Modules (EICM, NCM, ACM, etc.)
- I/O Modules

The TRICON expansion chassis can support the following modules:

- Two Power Modules
- Communications Modules (in expansion chassis #2 only)
- I/O Modules

Each TRICON chassis houses two Power Modules containing independent power supplies arranged in a dual redundant configuration.

Dual independent power rails are etched on the back plane of each chassis in a TRICON system. Both power rails feed each of the three legs on each I/O module and each Main Processor Module residing within the chassis through dual independent voltage regulators. 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. A short on a voltage rail disables the power regulators for that leg rather than affecting the power bus.

Each Power Supply module is capable of supporting all the power requirements for all the modules in the chassis within which it resides. All models of power modules are protected against reverse connection of the DC inputs.

The TRICON also has dual redundant batteries located on the Main Chassis backplane. If a total power failure occurs, these lithium batteries can maintain data and programs on the Main Processor modules for a cumulative period of six months. When less than 30 days of battery life remains, the system will generate an alarm.

6.7 TRICON TERMINATION PANELS

The termination panels are printed circuit boards utilized to facilitate landing of field wiring. This panel contains 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.

Each termination panel is packaged with a matched interface cable that connects between the termination panel and the TRICON backplane.

6.8 FMEA SUMMARY AND CONCLUSIONS

The failure modes and effects analysis (FMEA) tabulation is provided in Section 7.0 of this report. As shown, 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.

About 25% of the failures analyzed fall into Category C1, as defined by Section 4.0 of this report. The general effect of failures in this category are single failures detected by PLC diagnostics that do not affect PLC operability and I/O capability, as detailed in the Section 7.0 tabulation. Application-specific design features should be implemented to monitor the TRICON diagnostic alarms so that these failures can be annunciated and repaired in a timely manner.

The second failure category defined by Section 4.0 is Category C2, which includes single and multiple failures, not detected by PLC diagnostics, which do not affect PLC operability. Approximately 19% of the failures analyzed fall into this classification, which may be categorized as follows:

a) Failures that would be detected by periodic surveillance testing in accordance with the manufacturer's standard recommendations as described in the preceding sections.
b) Failures associated with PLC functions not intended for safety-related applications (e.g., relay outputs).
c) Failures that could be detected by application-specific design considerations (e.g., monitoring for loss of external communications links or loss of loop power supplies).

The third failure category defined by Section 4.0 is Category C3a, which includes single failure conditions where the PLC is unable to perform all of its safety functions. These failures, which comprise approximately 22% of the analyzed total, are generally related to loss of a single I/O point or function. These failures are caused by loss of a non-redundant loop power supply, I/O point fuse failure, or cable failure. The majority of these failures would be detected by the PLC diagnostics, as described in Section 7.0. Only four items, identified with the combination of failure categories C2 and C3a, are not detected by the PLC. These can be detected by either application-specific design features or by periodic channel checks and surveillance testing .

The next failure category defined by Section 4.0 is Category C3b, which includes multiple failure conditions where the PLC is unable to perform all of its safety functions. About 27% of the failures analyzed fall into this category. These failures include the effects of fire, flooding and missiles, which are minimized by applying standard industry design practices in specific system applications. The remaining failures are either common-mode or multiple failure scenarios, which are considered as low-probability events beyond the limits of credible failure scenarios. These types of multiple failure scenarios are recognized as being very unlikely but are included to describe system behavior in the presence of severe failures and to provide guidance for application design.

The final failure category defined by Section 4.0 is Category C4, which includes single or multiple failure conditions where the PLC self-diagnostic capability is reduced, but the PLC remains operable. These failures, which comprise about 7% of the total analyzed population, all fall in the category of single or double failures of triple redundant components, such as Main Processor modules, I/O Bus links, TRIBUS links or RXM modules.

As stated in Section 4.0 of this report, the PLC utilizes a fault-tolerant triple modular redundant architecture. This system design identifies and compensates for failed system elements, which facilitates its use in critical and safety-related process applications. The TRICON self-diagnostic features, described in References 5.5 and 5.6 and summarized in Section 6.0 of this report, have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate that the diagnostics detect all possible single failures within each module.

The TRICON system design information presented in References 5.5 and 5.6 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 specified methods and frequencies of Reference 5.5 and 5.6 to maximize system reliability and operability.

Refer to Section 7.0 of this report for the detailed FMEA results.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
POWER SUPPLY-RELATED FAILURES					
1) All chassis power supplies	Loss of all input power	Facility blackout	C3b	Input signals will not be read. Analog and digital outputs fail low.	PLC fails to operate
2) Main Chassis power supply: Model 8310; 120Vac/Vdc Model 8311; 24Vdc Model 8312; 230Vac	Loss of one power supply output	Electronic component or fuse failure	C1	None	PLC continues operation via redundant main chassis power supply. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.5.
3) Main Chassis power supply: Model 8310; 120Vac/Vdc Model 8311; 24Vdc Model 8312; 230Vac	Power supply output fails high or low	Electronic component or fuse failure	C1	None	PLC continues operation via redundant main chassis power supply. Main (b)
4) RXM or Expansion Chassis power supply: Model 8310; 120Vac/Vdc Model 8311; 24Vdc Model 8312; 230Vac	Loss of one power supply output	Electronic component or fuse failure	C1	None	PLC continues operation via redundant RXM/Expansion chassis power supply. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.5.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
5) RXM or Expansion Chassis power supply: Model 8310; 120Vac/Vdc Model 8311; 24Vdc Model 8312; 230Vac	Power supply output fails high or low	Electronic component or fuse failure	C1	None	PLC continues operation via redundant RXM/Expansion chassis power supply. Main processor diagnostics will detect [redacted] (b)
6) Loop power supply for DC digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	DC power supply output voltage fails low (both DC power supplies fail)	Fire; flood; missile	C3b	Affected digital inputs will fail low	PLC continues operation. Condition will not be detected unless: (a) power supply failure was alarmed, or (b) DI point failures triggered alarms associated with measured parameters; or (c) by periodic channel checks or surveillance testing. DI point could also be wired as a power failure alarm to provide detection (application-specific). See Sec. 6.1.1.
7) Loop power supply for DC digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	DC power supply output voltage fails low (one DC power supply fails)	Electronic component or fuse failure	C1, C2	None	PLC continues operation. Condition will not be detected unless: (a) power supply failure was alarmed, or (b) by periodic channel checks or surveillance testing. DI point could also be wired as a power failure alarm to provide detection (application-specific). See Sec. 6.1.1.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
8) Loop power supply for AC digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc	AC power supply output voltage fails low	Electronic component or fuse failure; fire; flood; missile	C3a, C3b	Affected digital inputs will fail low	PLC continues operation. Condition will not be detected unless: (a) power supply failure was alarmed, or (b) DI point failures triggered alarms associated with measured parameters; or (c) by periodic channel checks or surveillance testing. DI point could also be wired as a power failure alarm to provide detection (application-specific). See Sec. 6.1.1.
9) Loop power supply for AC/DC digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Power supply output voltage fails high	Electronic component failure	C3a	Affected digital inputs may fail low; provided failure voltage is high enough to burn out affected DI points	PLC continues operation. Main processor [redacted] (b) circuit. Application specific monitoring required to detect and alarm the failure for remaining modules. See Sec. 6.1.1.
10) Loop power supply for digital outputs: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Power supply output voltage fails low	Electronic component or fuse failure	C3a	Affected digital outputs will fail low	PLC continues operation. Condition will be detected by the output voter diagnostics on the affected DO module, and by the DO module's field voltage detection circuit, which will activate the LOAD/FUSE alarm since the commanded DO state will not match the detected field voltage. Redundant loop power supplies may be installed for 9661-510 and 9661-910 termination cards (application-specific). See Sec. 6.2.1.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
11) Loop power supply for digital outputs: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Power supply output voltage fails high	Electronic component failure	C3a	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.1.
12) Loop power supply for supervised digital outputs: Model 3611E; 115 Vac Model 3623; 120 Vac Model 3624; 24 Vdc	Power supply output voltage fails low	Electronic component or fuse failure	C3a	Affected digital outputs will fail low	PLC continues operation. Loss of power will be detected by SDO circuitry, which will generate a Power Alarm and/or a Load Alarm. See Sec. 6.2.2.
13) Loop power supply for supervised digital outputs: Model 3611E; 115 Vac Model 3623; 120 Vac Model 3624; 24 Vdc	Power supply output voltage fails high	Electronic component failure	C3a	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	PLC continues operation. Loss of power will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2.
14) Loop power supply for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Power supply output voltage fails low	Electronic component or fuse failure	C3a	Affected analog inputs will fail low (downscale)	PLC continues operation. Low range (b) supplies may be installed for analog input termination cards (application-specific). See Sec. 6.1.3.
15) Loop power supply for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Power supply output voltage fails high	Electronic component failure	C3a	Affected analog inputs may fail low (downscale); assuming failure voltage is high enough to burn out affected AI points	PLC continues operation. Low range (b) diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.3.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
16) Loop power supply for analog output module: Model 3805E; 4-20ma	Power supply output voltage fails low	Electronic component or fuse failure	C3a	Affected analog outputs will fail low (downscale)	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Fault Indicator, which in turn activates the chassis alarm signal. Redundant loop power supplies may be installed for analog output termination cards (application-specific). See Sec. 6.2.4.
17) Loop power supply for analog output module: Model 3805E; 4-20ma	Power supply output voltage fails high	Electronic component failure	C3a	Affected analog outputs may fail low (downscale); assuming failure voltage is high enough to burn out affected AO points	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Fault Indicator, which in turn activates the chassis alarm signal. See Sec. 6.2.4.
18) Loop power supply for relay output module: Model 3636R; Relay Output	Power supply output voltage fails low	Electronic component or fuse failure	C2	Affected field loads from relay outputs will fail to the de-energized state	PLC continues operation. Condition will not be detected unless: (a) power supply failure was alarmed, or (b) RO point failures triggered alarms associated with controlled parameters; or (c) by periodic channel checks or surveillance testing. Module not intended for safety-related applications. See Sec. 6.2.3.
19) Loop power supply for relay output module: Model 3636R; Relay Output	Power supply output voltage fails high	Electronic component failure	C2	Affected field loads from relay outputs may fail to the de-energized state; assuming failure voltage is high enough to burn out field devices (application-specific failure).	PLC continues operation. Relay contacts may flash over if failure voltage exceeds maximum specified voltage. Module not intended for safety-related applications. See Sec. 6.2.3.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
PLC CHASSIS-RELATED FAILURES					
1) Main Chassis System Control keyswitch	Switch shorts or is closed to "STOP" position	Electrical power transient; fire; flood; missiles	C3b	Input signals will not be read. Analog and digital outputs fail low.	PLC fails to operate. STOP position shall [redacted]
2) Main Chassis power supply rails	Both rails fail open or short to ground	Electrical power transient; fire; flood; missiles	C3b	Input signals will not be read. Analog and digital outputs fail low.	PLC fails to operate. All analog, digital and relay outputs turn off.
3) Main Chassis power supply rails	One rail fails open or shorts to ground	Electrical power transient and/or motherboard insulation failure	C1	None	PLC continues operation via redundant main chassis power supply. Main processor diagnostics will detect and flag power rail fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.6.
4) Main Chassis TRIBUS serial links	All links open or short to ground	Electrical power transient; fire; flood; missiles	C3b	Input signals will not be read. Analog and digital outputs fail low.	PLC fails to operate
5) Main Chassis TRIBUS serial links	One or two links open or short to ground.	Electrical power transient and/or motherboard insulation failure	C1, C4	None	PLC continues to operate via intact TRIBUS. Main processor diagnostics will detect and flag TRIBUS link fault. See Sec. 6.3.

(b)

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
6) Main Chassis I/O Bus	All buses open or short to ground	Electrical power transient; fire; flood; missiles	C3b	I/O signals downstream of an open bus will not be read. I/O signals will not be read for a shorted bus condition. Analog and digital outputs fail low at and past an open bus.	PLC microprocessors continue to operate, with I/O limitations as noted. Main processor diagnostics will detect and flag I/O bus fault. See Sec. 6.3.
7) Main Chassis I/O Bus	One or two buses open or short to ground	Electrical power transient and/or motherboard insulation failure	C1, C4	None	PLC continues to operate via intact I/O bus(es). Main processor diagnostics will detect and flag I/O bus fault. See Sec. 6.3.
8) Main Chassis Communications Bus	All buses open or short to ground	Electrical power transient; fire; flood; missiles	C4	None	PLC continues to operate as a standalone device. Communications to external terminals is interrupted. Main processor diagnostics will detect and flag communications bus fault. Would require logic in the external system to detect and alarm this failure (application-specific). See Sec. 6.3.
9) Main Chassis Communications Bus	One or two buses open or short to ground	Electrical power transient and/or motherboard insulation failure	C1, C4	None	PLC continues to operate. Communications to external devices continues via intact communications bus(es). Main processor diagnostics will detect and flag communications bus fault. See Sec. 6.3.
10) Main Chassis Communications Bus	Communication from one MP to the two others differs at the two other MPs	Failure of receiver at one receiving MP	C1, C4	None	Voted out and alarmed. See Sec. 6.3.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER					
Affected Components	**Failure Mode**	**Failure Mechanism**	**Failure Category**	**Effect on PLC Inputs and Outputs**	**Effect on PLC Operability**
11) Main Chassis battery pack	Output voltage fails low	Battery aging or short circuit	C1	None	PLC continues to operate, unless failure is concurrent with loss of all input power. Battery failure concurrent with all power failure will result in loss of main program memory from SRAM. Main processor diagnostics will detect and flag low battery voltage prior to failure. See Sec. 6.6.
12) RXM or Expansion Chassis power supply rails	Both rails fail open or short to ground	Electrical power transient; fire; flood; missiles	C3b	Input signals will not be read. Analog and digital outputs fail low for shorted rails, and fail low at and past the failure points for open rails.	PLC continues to operate, with loss of I/O function in the failed RXM or Expansion chassis as noted, and all downstream chassis assemblies. Main processor diagnostics will detect and flag power rail fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.6.
13) RXM or Expansion Chassis power supply rails	One rail fails open or shorts to ground	Electrical power transient and/or motherboard insulation failure	C1	None	PLC continues operation via redundant RXM/Expansion chassis power supply. Main processor diagnostics will detect and flag power rail fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.6.
14) RXM or Expansion Chassis I/O Bus	All buses open or short to ground	Electrical power transient; fire; flood; missiles	C3b	Input signals downstream of an open bus will not be read. Input signals will not be read for a shorted bus condition. Analog and digital outputs fail low.	PLC microprocessors continue to operate, with I/O limitations in the specific RXM or Expansion chassis as noted, and all downstream chassis assemblies. Main processor diagnostics will detect and flag I/O bus fault. See Sec. 6.4.4.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
15) RXM or Expansion Chassis I/O Bus	One or two buses open or short to ground	Electrical power transient and/or motherboard insulation failure	C1, C4	None	PLC continues to operate via intact I/O bus(es). Main processor diagnostics will detect and flag I/O bus fault. See Sec. 6.4.4.
CONTROL AND COMMUNICATIONS MODULE-RELATED FAILURES					
1) Main Chassis Processor Module: Model 3006; Enhanced TRICON Main Processor, 2 Mbytes SRAM	Loss of all three processor modules	Fire; flood; missiles; software common mode failure	C3b	Input signals will not be read. Analog and digital outputs fail low.	PLC fails to operate
2) Main Chassis Processor Module: Model 3006; Enhanced TRICON Main Processor, 2 Mbytes SRAM	Loss of one or two processor modules	Electronics or software failure	C1, C4	None	PLC continues to operate via intact processor module(s). Main processor diagnostics will detect and flag processor fault. See Sec. 6.3.
3) Main Chassis Communications Module: Model 4119A; Enhanced Intelligent Communications Module (EICM)	Failure of module to transmit or receive data	Electronics or software failure	C1	None	PLC continues to operate. Communications to external RS-232, RS-422 terminals and system printer is interrupted. Main processor diagnostics will detect and flag communications fault. Requires application-specific alarming in the external system. See Sec. 6.4.1.
4) Main Chassis Communications Module: Model 4609, Advanced Communications Module (ACM)	Failure of module to transmit or receive data	Electronics or software failure	C1	None	PLC continues to operate. Communications to external Foxboro Intelligent Automation (I/A) system is interrupted. Main processor diagnostics will detect and flag communications fault. Requires application-specific alarming in the external system. See Sec. 6.4.2.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
5) Main Chassis Communications Module: Model 4329, Network Communications Module (NCM)	Failure of module to transmit or receive data	Electronics or software failure	C1	None	PLC continues to operate. Communications to external network devices is interrupted. Main processor diagnostics will detect and flag communications fault if application software is so designed. Requires application-specific alarming in the external system. See Sec. 6.4.3.
6) Model 4210-3; Primary Remote Extender Module (RXM), Multi-mode Fiber Optics (set of 3 modules)	Loss of all three RXM modules	Fire; flood; missiles; software common mode failure	C3b	Input signals in affected RXM chassis will not be read. Analog and digital outputs fail low.	PLC continues to operate, with loss of I/O function in the failed RXM chassis as noted, and all downstream chassis assemblies. Main processor diagnostics will detect and flag RXM communications fault. See Sec. 6.4.4.
7) Model 4210-3; Primary Remote Extender Module (RXM), Multi-mode Fiber Optics (set of 3 modules)	Loss of one or two RXM modules	Electronics or software failure	C1, C4	None	PLC continues to operate via intact RXM module(s). Main processor diagnostics will detect and flag RXM module fault. See Sec. 6.4.4.
8) Model 4211-3; Remote Extender Module (RXM), Multi-mode Fiber Optics (set of 3 modules)	Loss of all three RXM modules	Fire; flood; missiles; software common mode failure	C3b	Input signals in affected RXM chassis will not be read. Analog and digital outputs fail low.	PLC continues to operate, with loss of I/O function in the failed RXM chassis as noted, and all downstream chassis assemblies. Main processor diagnostics will detect and flag RXM communications fault. See Sec. 6.4.4.
9) Model 4211-3; Remote Extender Module (RXM), Multi-mode Fiber Optics (set of 3 modules)	Loss of one or two RXM modules	Electronics or software failure	C1, C4	None	PLC continues to operate via intact RXM module(s). Main processor diagnostics will detect and flag RXM module fault. See Sec. 6.4.4.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
PLC CABLE-RELATED FAILURES					
1) Main Chassis-to-RXM Chassis I/O Expansion Cables (set of 3 cables)	Open circuit, short circuit or hot short in all three cables	Fault in adjacent power cable; fire; flood; missiles	C3b	Input signals downstream of the faulted cables will not be read. Analog and digital outputs fail low.	PLC microprocessors continue to operate, with I/O limitations downstream of the I/O Expansion cable fault as noted. Main processor diagnostics will detect and flag I/O cable fault. See Sec. 6.4.4.
2) Main Chassis-to-RXM Chassis I/O Expansion Cables (set of 3 cables)	Open circuit, short circuit or hot short in one or two cables	Fault in adjacent power cable; cable cut	C1, C4	None	PLC continues to operate via intact I/O cable(s). Main processor diagnostics will detect and flag I/O cable fault. See Sec. 6.4.4.
3) RXM Chassis-to-Expansion Chassis I/O Expansion Cables (set of 3 cables)	Open circuit, short circuit or hot short in all three cables	Fault in adjacent power cable; fire; flood; missiles	C3b	Input signals downstream of the faulted cables will not be read. Analog and digital outputs fail low.	PLC microprocessors continue to operate, with I/O limitations downstream of the I/O Expansion cable fault as noted. Main processor diagnostics will detect and flag I/O cable fault. See Sec. 6.4.4.
4) RXM Chassis-to-Expansion Chassis I/O Expansion Cables (set of 3 cables)	Open circuit, short circuit or hot short in one or two cables	Fault in adjacent power cable; cable cut	C1, C4	None	PLC continues to operate via intact I/O cable(s). Main processor diagnostics will detect and flag I/O cable fault. See Sec. 6.4.4.
5) Main Chassis Communications Module: Model 4119A; Enhanced Intelligent Communications Module (EICM) – Modbus terminal cable	Open circuit, short circuit or hot short in cable	Fault in adjacent power cable; cable cut	C1, C2	None	PLC continues to operate. Communications to external Modbus terminal is interrupted. Requires application-specific alarming in the external system. See Sec. 6.4.1.
6) Main Chassis Communications Module: Model 4119A; Enhanced Intelligent Communications Module (EICM) – Tristation terminal cable	Open circuit, short circuit or hot short in cable	Fault in adjacent power cable; cable cut	C1, C2	None	PLC continues to operate. Communications to external Tristation terminal is interrupted. Requires application-specific alarming in the external system. See Sec. 6.4.1.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
7) Main Chassis Communications Module: Model 4119A; Enhanced Intelligent Communications Module (EICM) – printer cable	Open circuit, short circuit or hot short in cable	Fault in adjacent power cable; cable cut	C1, C2	None	PLC continues to operate. Communications to external printer is interrupted. See Sec. 6.4.1.
8) Main Chassis Communications Module: Model 4609, Advanced Communications Module (ACM) – Foxboro I/A cables	Open circuit, short circuit or hot short in either cable	Fault in adjacent power cable; cable cut	C1, C2	None	PLC continues to operate. Communications to external Foxboro Intelligent Automation (I/A) system is interrupted. Requires application-specific alarming in the external system. See Sec. 6.4.2.
9) Main Chassis Communications Module: Model 4329, Network Communications Module (NCM) – network cable	Open circuit, short circuit or hot short in cable	Fault in adjacent power cable; cable cut	C1, C2	None	PLC continues to operate. Communications to external network devices is interrupted. Main processor diagnostics will detect and flag communications fault. Requires application-specific alarming in the external system. See Sec. 6.4.3.
10) Model 4210-3; Primary Remote Extender Module (RXM) to Model 4211-3; Remote Extender Module, Multi-mode Fiber Optics (set of 6 fiber optic cables)	Loss of all three RXM transmit or receive cables	Fire; flood, missiles	C3b	Input signals in affected RXM chassis will not be read. Analog and digital outputs fail low.	PLC continues to operate, with loss of I/O function in the failed RXM chassis as noted. Main processor diagnostics will detect and flag RXM communications fault. See Sec. 6.4.4.
11) Model 4210-3; Primary Remote Extender Module (RXM) to Model 4211-3; Remote Extender Module, Multi-mode Fiber Optics (set of 6 fiber optic cables)	Loss of one or two RXM transmit or receive cables	Fire or cable cut	C1, C4	None	PLC continues to operate via intact RXM cable(s). Main processor diagnostics will detect and flag RXM communications fault. See Sec. 6.4.4.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER					
Affected Components	**Failure Mode**	**Failure Mechanism**	**Failure Category**	**Effect on PLC Inputs and Outputs**	**Effect on PLC Operability**
12) Chassis to termination cable for digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Open circuit or short circuit to ground	Fault in adjacent power cable; cable cut; fire; flood; missiles	C2, C3b	Affected digital inputs will fail low	PLC continues operation. Condition will not be detected unless: (a) DI point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.1.
13) Chassis to termination cable for digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Short circuit across DI point	Fire or cable cut; term panel short	C2, C3a	Affected digital inputs will fail high	PLC continues operation. Condition will not be detected unless: (a) DI point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing; or (c) a single DI point has been used to indicate supply of external power as an application specific alarm. See Sec. 6.1.1.
14) Chassis to termination cable for digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected digital inputs may fail low; provided failure voltage is high enough to burn out affected DI points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.1.
15) Chassis to termination cable for digital outputs: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Open circuit	Fault in adjacent power cable; cable cut; fire; flood; missiles	C2, C3b	PLC digital outputs will not be affected, but field devices will fail low	PLC continues operation. Condition will not be detected unless: (a) DO point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.2.1.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
16) Chassis to termination cable for digital outputs: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Short circuit to ground	Fault in adjacent power cable; fire; flood; missiles	C3a, C3b	Affected digital outputs will fail low	PLC continues operation. Condition will be detected by DO module field voltage detection circuit, which will activate the LOAD/FUSE alarm since the commanded DO state will not match the detected field voltage. See Sec. 6.2.1.
17) Chassis to termination cable for digital outputs: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.1.
18) Chassis to termination cable for supervised digital outputs: Model 3611E; 115 Vac Model 3623; 120 Vac Model 3624; 24 Vdc	Open circuit	Fault in adjacent power cable; cable cut; fire; flood; missiles	C3a, C3b	PLC digital outputs will not be affected, but field devices will fail low	PLC continues operation. Loss of field loops will be detected by SDO circuitry, which will generate a Power Alarm and/or a Load Alarm. See Sec. 6.2.2.
19) Chassis to termination cable for supervised digital outputs: Model 3611E; 115 Vac Model 3623; 120 Vac Model 3624; 24 Vdc	Short circuit to ground	Fault in adjacent power cable; fire; flood; missiles	C3a, C3b	Affected digital outputs will fail low	PLC continues operation. Fault will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2.
20) Chassis to termination cable for supervised digital outputs: Model 3611E; 115 Vac Model 3623; 120 Vac Model 3624; 24 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	PLC continues operation. Fault will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
21) Chassis to termination cable for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Open circuit or short circuit to ground	Fault in adjacent power cable; cable cut; fire; flood; missiles	C3a, C3b	Affected analog inputs will fail low (downscale)	PLC continues operation. Low range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.3.
22) Chassis to termination cable for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected analog inputs may fail low (downscale); assuming failure voltage is high enough to burn out affected AI points	PLC continues operation. Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.3.
23) Chassis to termination cable for analog output module: Model 3805E; 4-20ma	Open circuit	Fault in adjacent power cable; cable cut; fire; flood; missiles	C3a, C3b	Affected analog output end devices will fail low (downscale)	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Load Indicator, which in turn activates the chassis alarm signal. See Sec. 6.2.4.
24) Chassis to termination cable for analog output module: Model 3805E; 4-20ma	Short circuit to ground or hot short	Fault in adjacent power cable; fire; flood; missiles	C3a, C3b	Affected analog outputs will fail downscale for a short circuit, and may fail low for a hot short; assuming failure voltage is high enough to burn out affected AO points	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Fault Indicator, which in turn activates the chassis alarm signal. See Sec. 6.2.4.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
25) Chassis to termination cable for relay output module: Model 3636R; Relay Output	Open circuit or short circuit to ground	Fault in adjacent power cable; cable cut; fire; flood; missiles	C2	Affected field loads from relay outputs will fail to the de-energized state	PLC continues operation. Condition will not be detected unless: (a) RO point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. Module not intended for safety-related applications. See Sec. 6.2.3.
26) Chassis to termination cable for relay output module: Model 3636R; Relay Output	Hot short	Fault in adjacent power cable	C2	Affected field loads from relay outputs may fail to the de-energized state; assuming failure voltage is high enough to burn out field devices (application-specific failure).	PLC continues operation. Relay contacts may flash over if failure voltage exceeds maximum specified voltage. Module not intended for safety-related applications. See Sec. 6.2.3.
27) Chassis to termination cable for pulse input module: Model 3510; 8 pulse input	Open circuit or short circuit to ground	Fault in adjacent power cable; cable cut; fire; flood; missiles	C2, C3b	Affected pulse inputs will fail low	PLC continues operation. Condition will not be detected unless: (a) PI point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.2.
28) Chassis to termination cable for pulse input module: Model 3510; 8 pulse input	Hot short	Fault in adjacent power cable	C2, C3a	Affected pulse inputs may fail low; assuming failure voltage is high enough to burn out field devices (application-specific failure).	PLC continues operation. Condition will not be detected unless: (a) PI point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.2.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
PLC I/O MODULE-RELATED FAILURES					
1) Digital input modules: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Input point(s) stuck OFF on one leg.	Electronic component, or multiple components on different points.	C1; C2 if point is normally OFF for all modules except 3504E	None	PLC continues operation. If point is [redacted] (b)
2) Digital input modules: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Input point(s) stuck OFF on multiple legs.	Multiple electronic component failures on same point or fuse failure	C2, C3b	Affected digital input(s) will fail low	PLC unable to correctly determine the state of the affected point(s). If point is [redacted] (b)
3) Digital input modules: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Input point(s) stuck ON for one leg	Electronic component failure, or multiple component failures on different points.	C1; C2 only for 3501E if point is normally ON.	None	PLC continues operation. Condition will [redacted] (b)
4) Digital input modules: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Input point(s) stuck ON for multiple legs	Multiple electronic component failures on same point or fuse failure	C2, C3b	Affected digital input(s) will fail high.	PLC unable to correctly determine the [redacted] (b)

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
5) Digital input modules: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Module communication failure on one or two legs.	Electronic component failure(s)	C1	None	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.1.
6) Digital input modules: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Module communication failure on all three legs.	Electronic component failures on all legs or comm. software failure	C3a, C3b	Affected digital inputs will not be read.	PLC will treat all affected input points as OFF. Main processor diagnostics will detect and flag board fault(s). Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.1.
7) Digital output modules: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Output point fails high or low on one leg	Electronic component failure	C1	None	PLC continues operation. DO module (b)
8) Digital output modules: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Output point fails high or low on multiple legs	Multiple electronic component failures or fuse failure	C3a, C3b	Affected digital outputs will fail to the corresponding output state, or will go OFF if fuse fault.	PLC unable to control the affected output (b)
9) Digital output modules: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Module communication failure on one or two legs	Electronic component failure(s)	C1	None	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.1.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
10) Digital output modules: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Module communication failure on all legs	Multiple electronics failures or comm. software failure	C3b	Affected output points will go OFF.	PLC unable to control the affected output points. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.1.
11) Supervised digital output modules: Model 3611E; 115 Vac Model 3623; 120 Vdc Model 3624; 24 Vdc	Output point fails high or low on one leg.	Electronic component failure	C1	None	PLC continues operation. SDO module [redacted] (b)
12) Supervised digital output modules: Model 3611E; 115 Vac Model 3623; 120 Vdc Model 3624; 24 Vdc	Output point fails high or low on multiple legs.	Multiple electronic component failures or fuse failure.	C3a, C3b	Affected digital outputs will fail to the corresponding output state, or will go OFF if fuse fault.	PLC unable to control the affected output [redacted] (b)
13) Supervised digital output modules: Model 3611E; 115 Vac Model 3623; 120 Vdc Model 3624; 24 Vdc	Module communication failure on one or two legs	Electronic component failure(s)	C1	None	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2.
14) Supervised digital output modules: Model 3611E; 115 Vac Model 3623; 120 Vdc Model 3624; 24 Vdc	Module communication failure on all legs	Multiple electronics failures or comm. software failure	C3b	Affected output points will go OFF.	PLC unable to control the affected output points. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
15) Analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Input point fails high or low on single leg	Electronic component failure	C1	None	PLC continues operation. Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.3
16) Analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Input point fails high or low on multiple legs	Multiple electronic component failures or fuse failure	C3a, C3b	Affected analog inputs will fail to the corresponding input state, or will go downscale if fuse fault.	PLC unable to correctly determine the value of the affected point(s). Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.3
17) Analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Module communication failure on one or two legs	Electronic component failure(s)	C1	None	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.3.
18) Analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Module communication failure on all legs	Multiple electronics failures or comm. software failure	C3b	Affected input points will go downscale.	PLC will treat all affected input points as downscale. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.3.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
19) Analog output module: Model 3805E; 4-20ma	Output signal fails high or low on one or two legs.	Electronic component failure(s)	C1	None	PLC continues operation. Each analog output module sustains complete 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. Failure of all three legs for a given output will activate the Load Indicator, and output will not be driven. See Sec. 6.2.4.
20) Analog output module: Model 3805E; 4-20ma	Output signal fails high or low on all three legs.	Multiple electronic component failures or firmware failure	C3b	Affected analog outputs will fail to unknown value.	PLC unable to control the affected output points. Each analog output module sustains complete 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. See Sec. 6.2.4.
21) Analog output module: Model 3805E; 4-20ma	Module communication failure on one or two legs	Electronic component failure(s)	C1	None	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.4.
22) Analog output module: Model 3805E; 4-20ma	Module communication failure on all three legs.	Multiple module electronics failure or comm. software failure	C3b	Affected analog outputs will fail downscale.	PLC unable to control the affected output points. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.4.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
23) Relay output module: Model 3636R; Relay Output	Relay output fails open or closed	Electronic component or fuse failure	C1, C2	If relay contact or fuse, affected field loads from relay outputs will fail to the corresponding output state. If internal fault, no effect on output.	PLC unable to control affected output points, if contact or fuse fault. Relay contact or fuse faults will not be detected. All internal faults will be detected by RO diagnostics and alarmed. Module not intended for safety-related applications. See Sec. 6.2.3.
24) Relay output module: Model 3636R; Relay Output	Module communication failure on one or two legs	Electronic component failure(s)	C1	None	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. Module not intended for safety-related applications. See Sec. 6.2.3.
25) Relay output module: Model 3636R; Relay Output	Module communication failure on all three legs.	Module electronics failure or comm. software failure	C1, C4	Affected relay outputs will be OPEN.	PLC unable to control the affected output points. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. Module not intended for safety-related applications. See Sec. 6.2.3.
26) Pulse input module: Model 3510; 8 pulse input	Input point fails high or low on single leg	Electronic component failure	C1	None	PLC continues operation. Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.2

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
27) Pulse input module: Model 3510; 8 pulse input	Input point fails high or low on multiple legs	Multiple electronic component failures	C3b	Affected inputs will fail to the corresponding input state.	PLC unable to correctly determine the value of the affected point(s). Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.2
28) Pulse input module: Model 3510; 8 pulse input	Module communication failure on one or two legs	Electronic component failure(s)	C1	None	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.2.
29) Pulse input module: Model 3510; 8 pulse input	Module communication failure on all legs	Multiple electronics failures or comm. software failure	C3b	Affected input points will go downscale.	PLC will treat all affected input points as downscale. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.2.
TERMINATION PANEL-RELATED FAILURES					
1) Termination panel for digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Open circuit or short circuit to ground	Fire; flood; missiles; term panel fuse failure or short	C2, C3b	Affected digital inputs will fail low	PLC continues operation. Condition will not be detected unless: (a) DI point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.1.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
2) Termination panel for digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Short circuit across DI point	Fire or cable cut; term panel short	C2, C3a	Affected digital inputs will fail high	PLC continues operation. Condition will not be detected unless: (a) DI point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.1.
3) Termination panel for digital inputs: Model 3501E; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc Model 3504E; 24/48 Vdc Model 3505E; 24 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected digital inputs may fail low; provided failure voltage is high enough to burn out affected DI points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.1.
4) Termination panel for digital outputs: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Open circuit	Fire; flood; missiles; term panel fuse failure	C2, C3b	PLC digital outputs will not be affected, but field devices will fail low	PLC continues operation. Condition will not be detected unless: (a) DO point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.2.1.
5) Termination panel for digital outputs: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Short circuit to ground	Fire; flood; missiles or cable fault; term panel short	C3a, C3b	Affected digital outputs will fail low	PLC continues operation. Condition will

(b)

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
6) Termination panel for digital outputs: Model 3601E; 115 Vac Model 3603E; 120 Vdc Model 3604E; 24 Vdc Model 3607E; 48 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.1.
7) Termination panel for supervised digital outputs: Model 3611E; 115 Vac Model 3623; 120 Vac Model 3624; 24 Vdc	Open circuit	Fire; flood; missiles; term panel fuse failure	C3a, C3b	PLC digital outputs will not be affected, but field devices will fail low	PLC continues operation. Loss of field loops will be detected by SDO circuitry, which will generate a Power Alarm and/or a Load Alarm. See Sec. 6.2.2.
8) Termination panel for supervised digital outputs: Model 3611E; 115 Vac Model 3623; 120 Vac Model 3624; 24 Vdc	Short circuit to ground	Fire; flood; missiles or cable fault; term panel short	C3a, C3b	Affected digital outputs will fail low	PLC continues operation. Fault will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2.
9) Termination panel for supervised digital outputs: Model 3611E; 115 Vac Model 3623; 120 Vac Model 3624; 24 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	PLC continues operation. Fault will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2.
10) Termination panel for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Open circuit or short circuit to ground	Fire; flood; missiles; term panel fuse failure or short	C3a, C3b	Affected analog inputs will fail low (downscale)	PLC continues operation. Low range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.3.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
11) Termination panel for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected analog inputs may fail high or low (downscale); assuming failure voltage is high enough to burn out affected AI points	PLC continues operation. Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit. See Sec. 6.1.3.
12) Termination panel for analog output module: Model 3805E; 4-20ma	Open circuit	Fire; flood; missiles; term panel fuse failure or short	C3a, C3b	Affected analog output end devices will fail low (downscale)	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module's Load Indicator, which in turn activates the chassis alarm signal. See Sec. 6.2.4.
13) Termination panel for analog output module: Model 3805E; 4-20ma	Short circuit to ground or hot short	Fault in adjacent power cable	C3a	Affected analog outputs will fail downscale for a short circuit, and may fail low for a hot short; assuming failure voltage is high enough to burn out affected AO points	PLC continues operation. Each analog output module sustains complete 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. See Sec. 6.2.4.
14) Termination panel for relay output module: Model 3636R; Relay Output	Open circuit or short circuit to ground	Fire; flood; missiles; term panel fuse failure or short	C2	Affected field loads from relay outputs will fail to the de-energized state	PLC continues operation. Condition will not be detected unless: (a) RO point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. Module not intended for safety-related applications. See Sec. 6.2.3.

SECTION 7.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V9 TMR PROGRAMMABLE LOGIC CONTROLLER

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
15) Termination panel for relay output module: Model 3636R; Relay Output	Hot short	Fault in adjacent power cable	C2	Affected field loads from relay outputs may fail to the de-energized state; assuming failure voltage is high enough to burn out field devices (application-specific failure).	PLC continues operation. Relay contacts may flash over if failure voltage exceeds maximum specified voltage. Module not intended for safety-related applications. See Sec. 6.2.3.
16) Termination panel for pulse input module: Model 3510; 8 pulse input	Open circuit or short circuit to ground	Fire; flood; missiles	C2, C3b	Affected pulse inputs will fail low	PLC continues operation. Condition will not be detected unless: (a) PI point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.2.
17) Termination panel for pulse input module: Model 3510; 8 pulse input	Hot short	Fault in adjacent power cable	C2, C3a	Affected pulse inputs may fail low; assuming failure voltage is high enough to burn out field devices (application-specific failure).	PLC continues operation. Condition will not be detected unless: (a) PI point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.2.

(a)

TRICONEX

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

TEST SPECIMEN APPLICATION PROGRAM VERIFICATION & VALIDATION REPORT

Document No.: 7286-536

Revision 0

March 17, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

See Attachments for proprietary designation

	Name	Signature	Title
Author:	R. C. Munter	[signature]	Engineer
Reviewer:	Tim Hurst	[signature]	Engineer
Approvals:	Mitchell Albers	[signature]	Project Manager
	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

Document Change History			
Revision	Date	Change	Author
0	3/17/00	Initial Issue	R. C. Munter

TABLE OF CONTENTS

1.0 SUMMARY AND CONCLUSIONS

This report describes the verification and validation (V&V) process which has been completed for development and integration of the Nuclear Qualification Project Test Specimen Application Program (TSAP) software. The TSAP is an application program developed specifically for the qualification project to simulate operation of the TRICON PLC in typical nuclear plant applications.

The requirements for V&V of the TSAP are documented in the Triconex Software Quality Assurance Plan (Ref. 2.5). The Software QA Plan describes how the software quality assurance requirements defined in the Triconex 10CFR50 Appendix B Quality Program and EPRI Report TR-107330 (Ref. 2.1) are implemented for V&V of the TSAP software. In preparing the Software Quality Assurance Plan, additional guidance provided by IEEE Std. 7-4.3.2-1993 (Ref. 2.2) and IEEE Std. 1012-1986 (Ref. 2.3) was considered.

Since established Triconex procedures address the activities required for V&V, a project specific V&V plan was not generated. Instead, the V&V plan, as described in Triconex procedure, TGM D-3 (Ref. 2.6) was used. Software V&V steps are described in the procedure and documented on Software Development Checklists (SDCs) which include independent verification of programming and QA sign-off on validation testing. SDCs are generated for each program and/or revision. The documentation attached to the SDC is commensurate with the task magnitude and importance to safety. The standard V&V package consists of the SDC with attached specifications, procedures, or reports, as appropriate. For the qualification effort, this TSAP V&V Report has been generated in addition to the documentation required by TGM D-3.

The following conclusions are made based on the results of the software V&V activities described in this report:

- The verification and validation activities described in this report demonstrate that the TSAP software was designed, implemented and tested based on the requirements described in the governing Quality Assurance and software plans and procedures.

- Changes made to the TSAP software following the completion of validation testing were based on documented problems. Changes made were confirmed to be appropriate, and testing was performed to confirm that the changes corrected the identified problem and introduced no new errors. The V&V activities further demonstrate that the software configuration was controlled throughout the revision process.

2.0 REFERENCES

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

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

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

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

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

2.6 Triconex General Manual Procedure, TGM D-3, "System Integration Programming Guidelines"

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

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

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

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

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

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

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

3.0 DESCRIPTION OF THE TSAP SOFTWARE

The Test Specimen Application Program (TSAP) is the application program developed specifically for the qualification project to simulate operation of the TRICON PLC in typical nuclear power plant applications. The software tool used to develop the TSAP and configure the TRICON PLC Test Specimen is the Tristation MSW 3.1.1 software. The TSAP is only associated with this testing program and is not being qualified for a specific nuclear power plant application. The TSAP provides the process logic to generate the specified PLC output response to simulated inputs. The documents which provide the detailed description and operation of the TSAP include the TSAP Functional Requirements Specification (Ref. 2.8), TSAP Design Specification (Ref. 2.9) and TSAP Program Listing (Ref. 2.10).

Provisions for configuration control of the TSAP are contained in the Triconex Quality Plan (Ref. 2.4) which invokes existing Triconex QA procedures. A Master Configuration List (Ref. 2.12) was established to document the specific configuration information for all hardware and software being qualified. The specific versions of the TSAP software used throughout qualification testing are provided in the Master Configuration List.

4.0 SUMMARY OF LIFE-CYCLE TASKS AND DOCUMENTATION

As part of the Triconex PLC Nuclear Qualification Project, Triconex contracted with Hurst Technologies, Corp. (Hurst) to prepare a TSAP validation procedure and provide independent reviews of the TSAP software. Triconex also contracted with MPR Associates, Inc. (MPR) to be the overall project manager for the qualification effort. The South Texas Project Nuclear Operating Company (STPNOC) was the sponsoring electric utility for the qualification effort.

As required by TGM D-3 (Ref. 2.6), the life-cycle phases associated with development of the TSAP software were:

- Input requirements
- Design
- Implementation
- Test

Each of these phases was completed as a part of the TSAP software development. The products for each phase were independently verified for completeness and correctness as required by the Software Quality Assurance Plan and TGM D-3. Evidence of the reviews is indicated by reviewer signoffs on the resulting life-cycle phase documentation. This documentation was issued as controlled documents with revision numbers.

Once the TSAP software was developed, evidence of verification and validation for the initial issue and subsequent revisions was provided by completion of the Software Development Checklists (SDCs). The SDCs describe the revisions to the programming input documents and software. In addition, an Application Software Log was maintained to document the current software version, release date, and description of changes.

Following the Test phase, the TSAP software was approved for use in supporting TRICON PLC qualification testing. Configuration control of the TSAP software was established by the Triconex Quality Plan (Ref. 2.4).

4.1 Input Requirements

Triconex Procedure TGM D-3 states that application program functional requirements are provided by the customer. However, because the TSAP was developed by Triconex specifically for the TRICON PLC Nuclear Qualification Program, Triconex project personnel generated the detailed functional requirements. These requirements are documented in the TSAP Functional Requirements Specification (Ref. 2.8) and a set of Function Diagrams (Ref. 2.7).

The Function Diagrams were developed to implement typical operations of a PLC in nuclear power plant applications. Typical operations included such tasks as bistable trips, flow control and load sequencing. The diagrams provide the logic design for each of these typical operations. The completed diagrams were independently verified to ensure that the logic correctly depicts the intended application.

The TSAP Functional Requirements Specification (Ref. 2.8) provides a detailed written description of the applications depicted by each of the Function Diagrams. A description of the functional requirements as well as input values and output acceptance criteria were developed from the Function Diagrams. The Functional Specification was independently reviewed to verify that the functional requirements for each operation were correctly defined.

4.2 Design

The TSAP Design Specification (Ref. 2.9) was developed from the logic depicted by the Function Diagrams and the requirements described by the TSAP Functional Requirements Specification. The Design Specification provides the general software design criteria and requirements and further defines the requirements for each of the typical operations that were to be programmed. For example, items defined were: field inputs and outputs, TRISTATION outputs, operator console outputs, internal variables, logic descriptions and logic truth tables (where applicable). The Design Specification was independently reviewed to verify that the design requirements for each operation were correctly translated into software design requirements.

4.3 Implementation

The TSAP software (Ref. 2.10) was developed from the detailed design requirements provided by the TSAP Design Specification. The Tristation MSW 3.1.1 software program was used to develop the TSAP application program. The TSAP Program Listing documents the software program and program database.

The TSAP was issued for internal review as Version 0.0 on 3/28/99. The program underwent several reviews. During these reviews, changes were made and documented for items such as correcting the input/output database, revising PID networks, assigning aliases, and revising scaling factors.

An independent verification review of the TSAP software and database was performed by Hurst. The results of this independent review are documented on the "TSAP Verification Checklists" included in Attachment 1.0. Each of these checklists documents the review of one TSAP function as defined on the Function Diagrams. The revision of the TSAP considered in the review is documented on the checklist. The scope of the review included tracing requirements defined by each of the Function Diagrams through to the Design Specification. The software and database were then reviewed against the requirements defined in the Design Specification. As part of this review effort, matrices were developed by Triconex and reviewed by Hurst for each function to document the expected behavior of each variable used in the function. These "Emulation Acceptance Test" matrices were developed for use in the preliminary validation test described below. These matrices also became part of the TSAP Validation Test Procedure. Finally, the software and database were reviewed for technical adequacy as follows:

1. Review the code to verify functionality in accordance with the Function Diagrams and software design description. The code was also verified to be free of "dead" (unused) code, flow control (GOTO, END) statements, and interrupts.

2. Review the database to ensure that all tags associated with the Function Diagrams were listed, all tag descriptions were complete, tag types were correct, I/O points were addressed correctly, and all points that are read by external devices were aliased.

3. Review the emulation matrix used during the preliminary software testing (prior to integration in the Test Specimen) and verify that a full range of analog variables is used to check for proper functionality, setpoints and reset points are accurate, and all input state possibilities are tested.

Comments are documented on the Verification Checklists and resolutions of these comments were incorporated as a part of the ongoing design effort and prior to the final verification review.

A preliminary validation test was performed by running the TSAP in a simulated operating mode using the Tristation software. The test consisted of executing all of the software logic except for the EDG Load Sequencer, Radiation Monitor NI, Saturation Monitor, PID, power loading and communications functions and validating that the outputs were as expected. Since the PID, power loading, and communication functions could not be executed external to the TRICON PLC, they were omitted from the preliminary test. In addition, the functional specifications for the EDG Load Sequencer, Radiation Monitor NI, and Saturation Monitor were not fully developed at the time of simulation testing. For this test, the "Emulation Acceptance Test" matrices (developed as described above) were used to manually set TRICON PLC inputs to specific values. The resulting values of the outputs from each function were then checked against the expected values from the matrix. The results of the preliminary validation test are documented in Attachment 2.0. Resolutions of comments from the test were incorporated prior to the final verification review.

Prior to integrated validation testing, Triconex performed a final verification review on the TSAP software and database. Initial issue of the TSAP software (Version 0.7) was made on 9/29/99. Subsequent changes to the software, as part of the final review, were documented in the SDCs. One SDC may account for several version changes of the TSAP software. Each version of the software included an independent verification. These verifications are documented in the SDCs. The TSAP Application Software Log, Attachment 3.0, provides the log of SDCs for the software. The individual SDCs are also included in Attachment 3.0. Review of the documentation for these revisions showed that configuration control was maintained and that appropriate revisions were produced.

4.4 Test

EPRI Report TR-107330 (Ref. 2.1) defines the testing to be performed for qualification of a generic PLC platform. A Master Test Plan (Ref. 2.11) was written to define a testing approach to meet the requirements of TR-107330. The TSAP Validation Test Procedure (Ref. 2.13) is identified in the Master Test Plan and provides the detailed test requirements for TSAP validation after integration in the TRICON PLC Test Specimen. The TSAP Validation Test Procedure was reviewed to verify that it included steps to test the software requirements defined by the previous life-cycle phases.

The TSAP Validation Test Procedure was written by Hurst and approved by Triconex and MPR. The procedure defines the test prerequisites, acceptance criteria and procedural steps to validate the TSAP software. The TSAP Validation Test Procedure was reviewed by MPR to verify that the procedure met the requirements of the Master Test Plan and EPRI Report TR-107330.

The TSAP was released for testing as Version 1.0 on October 7, 1999. The completed TSAP Validation Test Procedure (Appendix A) documents measuring and test equipment used, tables of expected to measured values, and test exception reports (TERs). When software problems were found, either the reason for the test exception was justified in the TERs or revisions to the software were made and documented with the SDCs. Portions of the TSAP Validation Test Procedure were re-run to test the revised TSAP code. Test results were documented until all test exceptions were justified or corrected. Results of validation testing were reviewed and problem resolutions have been verified to be complete by this review.

5.0 SUMMARY OF ANOMALIES AND RESOLUTIONS

Documents that form the basis for the TSAP software development (Function Diagrams, TSAP Functional Requirements Specification, TSAP Design Specification and TSAP Program Listing) went through the normal design evolution of revisions by incorporating comments received. Evidence of the reviews is indicated by reviewer signoffs on these documents. These documents were independently reviewed by Hurst. The majority of the comments made concerned the logic descriptions in the Functional Requirements Specification and Design Specification. The independent review is documented in Attachments 1.0 and 2.0. Review of the documentation for these comments showed that appropriate revisions were made to the applicable documents.

The TSAP software went through several internal reviews prior to initial issue. The software was independently reviewed by Hurst. The independent review is documented in Attachment 1.0. Review of the documentation for these comments showed that appropriate revisions were made to the software.

Subsequent to initial issue of the TSAP software as Version 0.7, several revisions were made as a result of additional reviews. Changes included items such as assigning aliases, reconfiguring module locations, changing overflow values, and scan times. These changes are documented on SDCs. Review of the documentation for these changes showed that appropriate revisions were made to the software.

The TSAP software was released for testing as Version 1.0 on 10/7/99. The TSAP Validation Test was started on 10/8/99. Output measurements were recorded on the Validation Test Tables that are a part of the TSAP Validation Test Procedure (Ref. 2.13). Section 4.0 of the Test Procedure provides the acceptance criteria. When measured values did not meet the acceptance criteria, a test exception report was generated. Each test exception was reviewed and the cause of the exception was determined. Fifteen test exception items were documented. Examples of test exceptions include incorrect expectation values in the test procedure, fluctuations and accuracy limitations of test equipment, and an incorrectly configured scaling factor. In all cases, exceptions were determined to be explainable and revisions to the software were made, when appropriate. All exceptions were dispositioned and verified to be appropriate. Revisions to the software were made and documented on SDCs with the appropriate reviews and verification. When necessary, the Test Procedure was re-run to validate the software change. The TSAP Validation Test results are included with this report as Appendix A that includes the Test Exception Reports.

ATTACHMENT 1.0

Verification Comment Sheets

(Page 1 of 29) [pages 2-29 deleted]

ENTIRE DATA ATTACHMENT 1.0
CONSIDERED PROPRIETARY

(a,b)

ATTACHMENT 2.0

Simulation Result Tables

(Page 1 of 39) [pages 2-39 deleted]

ENTIRE DATA ATTACHMENT 2.0
CONSIDERED PROPRIETARY

(a,b)

ATTACHMENT 3.0

TSAP Application Software Log and Software Development Checklists

(Page 1 of 47) [pages 2-47 deleted]

ENTIRE DATA ATTACHMENT 3.0
CONSIDERED PROPRIETARY

(a,b)

TRICONEX

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

MASTER TEST PLAN

Document No: 7286-500

Revision 3

March 8, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Gary McDonald	[signature]	Nuclear Quality Engineer
Approvals:	Mitch Albers	[signature]	Project Manager
	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

Document Change History

Revision	Date	Change	Author
0	6/5/98	Initial Issue	G. W. McDonald
1	7/23/99	Revision based on project restructuring	G. W. McDonald
2	8/3/99	Incorporation of STP comments.	G. W. McDonald
3	3/8/00	Incorporation of Pre-qualification and Qualification testing results.	G. W. McDonald

MASTER TEST PLAN

QUALIFICATION OF TRICONEX PLC FOR SAFETY RELATED APPLICATION IN NUCLEAR POWER PLANTS

TABLE OF CONTENTS

MASTER TEST PLAN

1. BACKGROUND

The nuclear power industry is currently facing increasing obsolescence issues with original equipment installed for instrumentation, control, and safety system applications. These systems, based on analog and relay, discrete component technology that is over twenty years old, are now difficult if not impossible to maintain. Industry goals are now focusing on the development of cost-effective replacement systems based on new technologies that can offer the added benefits of improved functionality, reliability and performance as well as to reduce operations and maintenance (O&M) costs and to enhance safety.

The nuclear power industry has identified Programmable Logic Controllers (PLCs) as a promising technology that may be used to retrofit current systems and achieve the desired benefits. The most significant barriers to the widespread, cost-effective application of PLCs in nuclear power plants are the lack of a generally accepted method for qualifying commercially available PLCs for safety grade service and the lack of sufficient industry experience in developing, qualifying, and licensing applications of these PLC platforms such that a critical replacement project could be categorized as a low risk task.

An EPRI and utility sponsored working group, using regulatory requirements, standards, guidelines, and expertise developed a specification EPRI TR-107330, titled "Generic Requirements Specification for Qualifying a commercially Available PLC for Safety-Related Applications in Nuclear Power Plants". The specification provides guidance on what is essential to qualify a commercially available PLC. It covers both functional and qualification requirements so it can be used by utilities for developing their bid specifications for a PLC-based application. After reviewing the specification, the NRC issued a Safety Evaluation Report (SER) in August 1998.

The objective of TR-107330 is to provide generic requirements for pre-qualifying commercial-off-the-shelf (COTS) PLC lines for use in safety-related applications in nuclear power plants. It defines the essential technical characteristics, (e.g., I/O points and options, 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 processes, are addressed in this specification primarily by reference to published standards and guidelines.

TR-107330 requirements are geared towards qualifying a PLC as a replacement for specific segments of safety systems at existing plants (for example, using a PLC in place of a large portion of the ESFAS). 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 elements.

The technical scope focus and content of TR-107330 is based on the steps involved in completing a generic qualification effort. Performing the qualification requires, in effect, creating a synthetic application so the steps are similar to those used in qualifying any device for nuclear safety-related service. Steps identified are:

A. Selecting a PLC product line that supports the requirements of this specification and the required functionality of nuclear safety-related applications. The selection process includes selecting the set of PLC modules to be qualified.

B. Evaluating the manufacturer's (including third party or sub-tier suppliers) hardware and software QA programs applied to the products of interest to determine if they are adequate to support nuclear safety-related applications with a reasonable set of supplementary activities. The evaluation includes factors relating to both generic qualification and future applications of the qualified products.

C. Procuring a set of modules and any required supporting devices and software from the PLC manufacturer or third party suppliers to be used as the qualification test specimen.

D. Defining and producing a Test Specimen Application Program (TSAP). The TSAP is, in effect; a synthetic application designed to aid in the qualification tests and operability testing.

E. Combining the modules and the TSAP into a suitable test configuration and performing a set of acceptance tests on the test specimen. This is, in effect, a system integration test for the test specimen.

F. 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. The operability tests are designed to demonstrate satisfactory operation under the stresses applied during qualification tests.

G. Performing the qualification tests and documenting the results. Results documentation includes producing documentation that defines the qualification envelope, specific products that were qualified, and other application information and application guidance for using the qualified PLC in a specific application.

In accordance with paragraph A, EPRI and South Texas Project Nuclear Operating Company (STPNOC) selected Triconex's TRICON TMR PLC as one of the first PLCs to be evaluated under the TR-107330 specification. STPNOC, in accordance with paragraph B, conducted an audit of Triconex's hardware and software QA programs in January 1998, judging them to be in compliance with 10CFR50 Appendix B and 10CFR21, and adequate to support nuclear safety-related applications.

This Master Test Plan addresses paragraphs B through G.

2. SCOPE

EPRI Specification TR-107330 defines the requirements for testing to be performed in connection with the qualification of a generic PLC platform. Testing of a sample PLC system, flexibly configured to encompass a broad range of potential safety related applications, will fulfill the major portion of the requirements for qualifying the equipment. Other required analytical information and documentation will be provided separately. This Master Test Plan provides an overview of the Triconex Testing Program and provides a bridge between the specification requirements and the test program results.

The qualification testing will demonstrate the suitability of the Tricon system, including hardware and operating software, to perform with high reliability in nuclear power plant environment. This Plan identifies equipment to be tested, tests to be performed, and procedures for conducting the testing. The project Quality Plan provides additional instructions (Nuclear Test Instructions) for administering test program activities.

The results of the tests will be evaluated against acceptance criteria and provide a basis for qualifying the generic equipment configuration. The data taken during testing will also provide configuration and qualification envelope information. This will be included in the final summary report to be used as a basis for evaluating specific applications of the equipment in nuclear power plants.

Figure 1 shows an overview of the Nuclear Qualification Project and shows the key project documents associated with each phase. The relationship of the test plans, procedures, and governing requirements can be seen in this figure. A Project Requirements Matrix will also be established to provide a road map from each EPRI specification section to the project documents which satisfy that requirement.

3. EQUIPMENT TO BE TESTED

A Qualification Test Specimen has been designed to be tested as a representative sample of a Triconex PLC system. This system is defined in Appendix 1 and is consistent with the technical requirements of EPRI specification TR-107330. In general, the system consists of a standard Tricon PLC system configured with a selection of modules needed to encompass a variety of applications. A third party field power supply will also be tested with the Test Specimen.

System equipment layout drawings, wiring diagrams, and other diagrams define the configuration of the test system (test specimen). Test plans and procedures provide specific details on hardware mounting and interfaces used in the qualification testing. A test specimen application program (TSAP) will be developed and integrated with the equipment. Detailed configuration information such as serial numbers, software versions, etc. are provided as part of the qualification documentation. A Master Configuration List (MCL) will capture all hardware and software configuration information.

4. SAFETY FUNCTIONS TO BE DEMONSTRATED

The safety functions to be demonstrated by the test program include:

1. The ability to perform to the requirements specified in EPRI specification section 4 under normal conditions.
2. The ability to perform the functions specified in EPRI specification TR-107330 under stressed conditions as defined in EPRI specification sections 5 and 6, including the ability to:
   - function during and after exposure to abnormal temperature and humidity conditions,
   - function during and after exposure to EMI/RFI conditions,
   - function during and after exposure to operating basis and design basis seismic events,
   - function during and after exposure to voltage surges,

- function under varying input power quality (voltage and frequency) conditions, and
- demonstrate class 1E/Non 1E electrical isolation capability of selected modules.

5. TEST REQUIREMENTS

Requirements for conducting testing activities are found in EPRI TR-107330 specification sections 5 and 6. These sections reference other sections, which detail further testing criteria. In addition to the EPRI TR-107330 specification, additional test criteria are provided by Triconex equipment specifications and published literature.

The EPRI specification provides a generic basis for qualifying PLCs from any manufacturer. Where items are not applicable due to unique Triconex equipment characteristics, deviations or exceptions will be identified in the Project Requirements Matrix. Alternate test methods or criteria will be defined in the Test Plan or Test Procedures.

As seen on the Master Test Plan flow chart (Figure 2), three categories of tests will be conducted to satisfy the requirements of EPRI TR-107330:

(1) **Pre-Qualification tests** conducted prior to qualification testing to determine that the system operates correctly and to provide baseline data on equipment performance,

(2) **Qualification tests** to demonstrate compliance with specification requirements and suitability of equipment while subject to stress conditions, and

(3) **Performance Proof tests** to confirm satisfactory operation after being subjected to Qualification test conditions. Performance proof tests are merely a repeat of selected pre-qualification baseline tests to identify any changes in equipment performance.

Tests to be performed are shown below. Table 1 also lists these tests along with the applicable EPRI TR-107330 references and corresponding Triconex test procedures.

Pre-Qualification Tests include:

1. System Set-up and Check-out Test
2. Operability Test
3. Prudency Test

Qualification Tests include:

1. System Set-up and Check-out Test (as needed following system disassembly/reassembly)
2. Environmental Test (including Operability and Prudency tests)
3. Seismic Test (including post-seismic Operability test)
4. EMI/RFI Test
5. Surge Test
6. Class 1E/Non-1E Electrical Isolation Test

Performance Proof Tests include:

1. Operability Test (retest)
2. Prudency Test (retest)

(a)

6. TEST PLANS AND PROCEDURES

Test Plans have been prepared for various tests or testing categories (Environmental, Seismic, etc.), as listed in appendices 3-8:

Appendix 3, Pre-qualification Test Plan
Appendix 4, Environmental Test Plan
Appendix 5, Seismic Test Plan
Appendix 6, Surge/Isolation Test Plan
Appendix 7, EMI/RFI Test Plan
Appendix 8, Proof Test Plan

Test Plans provide a link between the EPRI TR-107330 specification requirements and the procedures which conduct the tests. Test Plans address general testing approach, objectives, reference to requirements, general testing criteria, service conditions, environmental conditions, sequence of tests, and applicable procedures.

Test procedures control the detailed sequence of testing activities and document the results. The procedures define equipment set-up, environmental conditions, specific testing steps, performance data collection requirements, verifications, and measuring equipment used. A master list of the test procedures to be used is contained in the Master Configuration List.

Software, i.e., the Test Specimen Application Program (TSAP), which supports the testing will be identified, validated, and controlled in accordance with project procedures. Requirements for the TSAP are summarized in Appendix 2, Test Specimen Application Program.

Test plans and procedures will be approved by STPNOC.

7. TEST PROGRAM IMPLEMENTATION

7.1 Test sequence

(b)

Details of the individual tests and sequencing are found in Test Plans for the different testing categories (Environmental, Seismic, etc.). Pre-Qualification and Performance Proof testing will be done at the Triconex Irvine facility. Qualification testing will be performed at the Wyle test laboratories in Huntsville, AL.

(a)

7.2 Methodology

7.3 Test personnel

Testing activities will be conducted by qualified Triconex engineers and technicians. Contractors participating in qualification testing will be approved by Triconex. Provisions will be made for customer access and witnessing of testing activities, as specified by STPNOC.

8. AGE CONDITIONING

Age conditioning is an integral part of the qualification test program. Section 6.3.1 of the EPRI specification identifies the key aging mechanisms associated with the PLC system. These factors are:

1. Environmental (Abnormal Temperature & Humidity)
2. Seismic
3. Electromagnetic and Radio Frequency Interference (EMI/RFI)

The specification defines the required parameters and the order in which to perform the age conditioning procedures. This is factored into the Individual Test Plans (Appendices 3-8) and the test sequencing.

Radiation is addressed in the EPRI specification as a lesser aging factor. Per section 4.3.6.3, evaluations establishing radiation withstand capability to the level given in the specification are sufficient. Testing is not required.

(a)

9. MAINTENANCE/MODIFICATIONS DURING TESTING

10. TEST DEVIATIONS/FAILURES

Test failures or deviations from test program requirements will be documented and controlled in accordance with approved instructions (see NTI-2, Conduct of Test).

11. OTHER CONSIDERATIONS

While manufacturing and acceptance testing will be performed in the Irvine facility, qualification testing will be performed off-site at Wyle Laboratories in Huntsville, Alabama. The

(a)

12. DOCUMENTATION OF RESULTS

(a)

The primary deliverables for the testing phase of this project are:

(a)

Test program documentation will be maintained in accordance with Triconex procedures and will be provided to STP Nuclear Operating Company as provided for in the Purchase Order. Any other records generated as part of this project but not identified as a deliverable document will be available for audit in Triconex files.

TABLE 1 – OVERVIEW OF TESTS TO BE PERFORMED

(b)

Test Type & Description	Test Procedure	Test Plan
1.0 PRE-QUALIFICATION TESTS		
1.1 System Set-up and Check-out test	7286-502	App. 3, Pre-qualification test plan
1.2 TSAP Validation test	7286-513	App. 3, Pre-qualification test plan
1.3 Operability test	7286-503	App. 3, Pre-qualification test plan
1.4 Prudency test	7286-504	App. 3, Pre-qualification test plan
2.0 QUALIFICATION TESTS		
2.1 Environmental qualification test	7286-506	App. 4, Env Test Plan
2.2 Seismic qualification test	7286-507	App. 5, Seismic Test Plan
2.3 Surge test	7286-508	App. 6, Surge/Iso Test Plan
2.4 Isolation (1E to non-1E) test	7286-509	App. 6, Surge/Iso Test Plan
2.5 EMI/RFI tests	7286-510	App. 7, EMI/RFI Test Plan
3.0 PERFORMANCE PROOF TESTS		
3.1 Operability test from 1.3 above	7286-503	App. 10, Proof Test Plan
3.2 Prudency test from 1.4 above	7286-504	App. 10, Proof Test Plan

FIGURE 1
NUCLEAR QUALIFICATION PROJECT OVERVIEW

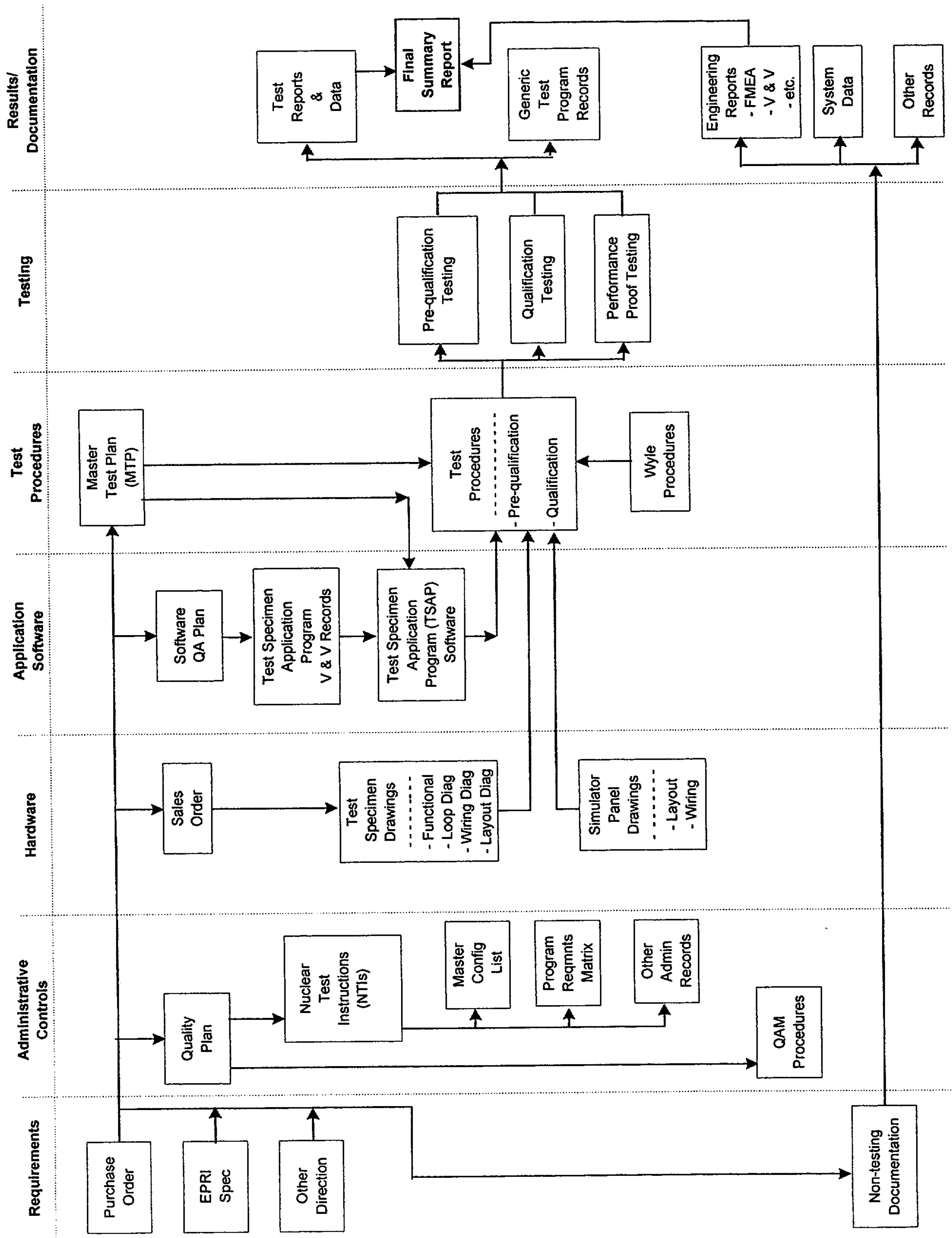
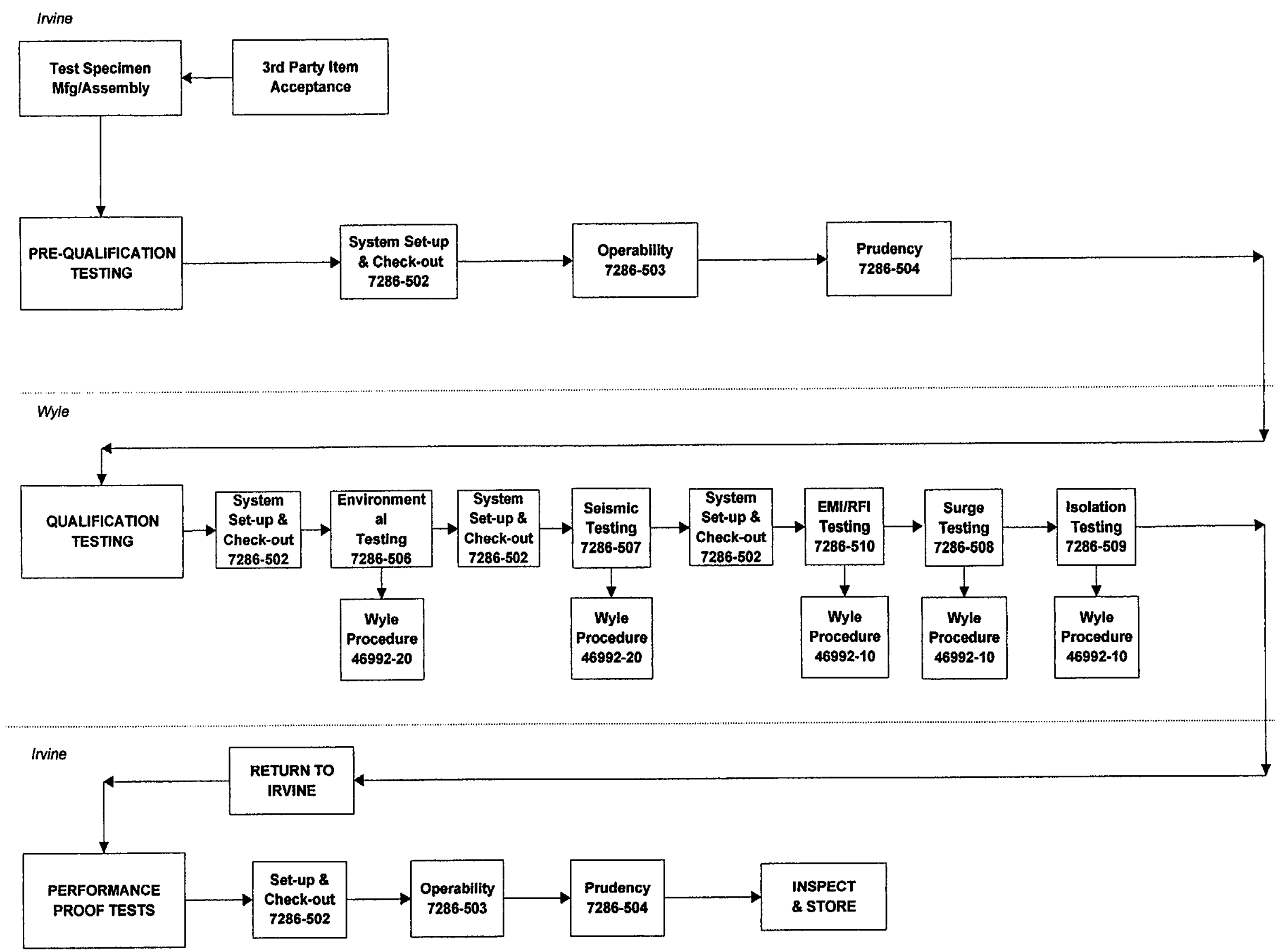


FIGURE 2
MASTER TEST PLAN - FLOW DIAGRAM



TRICONEX

Document:	7286-500	Title:	MASTER TEST PLAN		
Revision:	3	Page:	16 of 36	Date:	3/8/00

APPENDIX 1 - EQUIPMENT UNDER TEST

The equipment under test basically consists of 4 TRICON chassis containing selected functional modules, external termination panels (ETAs) appropriate to the included modules, and necessary connecting cables. A listing of the specific modules, firmware, and third party equipment to be qualified is provided below. (b)

Type	Model #	Description
Chassis	8110	Main Chassis
	8111	Expansion Chassis
	8112	Remote Expansion Chassis
Power	8310	High Density Power Module, 115 V
	8311	High Density Power Module, 24 VDC
	8312	High Density Power Module, 230 VAC
Main Processor	3006	Enhanced Main Processor II, V9, 2 Mb
Remote Extender	4210	Remote Extender Module
	4211	Remote Extender Module
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
	3603E	EDO Module, 120 VDC
	3604E	EDO Module, 24 VDC
	3607E	EDO Module, 48 VDC
	3611E	SDO Module, 115 VAC
	3623	SDO Module, 120 VDC
	3624	SDO Module, 24 VDC
Pulse Input	3510	Pulse Input Module
Thermocouple	3706A	NITC Input Module
	3708E	ITC Thermocouple Input Module
Relay Output	3636R	ERO Module, N.O., Simplex
Seismic Module	8107	Seismic Balance Module (Inactive)

Third Party Equipment

Field power supply		Lambda Power Supply, 24 VDC

(b)

The Master Configuration List (MCL) is a controlled project document which provides a listing of the specific modules, termination assemblies (ETAs), and cables which comprise the test specimen (not including testing equipment, which will be specified separately in the individual test procedures and drawings). The serial numbers of all modules and ETAs (all items which are serialized for traceability) are documented in the MCL and are maintained current with any required equipment changes.

The configuration and arrangement of the Test Specimen are defined on drawings which are listed in the MCL. The MCL also defines all software associated with the Test Specimen, including operating firmware, Tristation MSW 3.1.1 programming software, and application/test programs described in test plans and procedures. (b)

A third party power supply (Lambda [redacted]) will be tested with the Test Specimen to provide an available field power supply for external transmitters and devices. This will be reflected on the arrangement drawings and the MCL.

APPENDIX 2 – TEST SPECIMEN APPLICATION PROGRAM (TSAP)

1. GENERAL

A synthetic test specimen application program (TSAP) will be developed to establish PLC program logic and exercise selected input/output points to support testing activities. Governing regulations for development, content, and implementation are described below.

(b)

2. REFERENCES:

3. DEVELOPMENT:

a. The TSAP will be developed in accordance with the SQA plan (7286-537)

b. Objective:
The objective of the TSAP is to support the test procedures to demonstrate the functionality of the Test Specimen during pre-qualification testing and throughout qualification testing. *(a)*

c. Software Requirements:

4. VERIFICATION & VALIDATION: *(a)*

(a)

5. IMPLEMENTATION:

APPENDIX 3 - PRE-QUALIFICATION TEST PLAN

1. GENERAL

Upon completion of manufacturing of the test system, the pre-qualification testing phase will begin. Pre-qualification acceptance tests are those tests performed on the test specimen prior to the qualification tests to confirm that the test specimen is correctly configured, assembled and operational. Pre-qualification acceptance tests also provide baseline performance data for comparison to performance data obtained during and following the qualification tests. *(a)*

(a)

2. REFERENCES:

EPRI Specification TR-107330: *(b)*

3. EQUIPMENT

The equipment under test is the Triconex Test Specimen as documented in Appendix 1. During acceptance testing, the equipment will be configured as shown on the system drawings. Specific interfaces with the test equipment will be described in the individual test procedures.

4. SEQUENCE OF TESTING:

(a)

5. PROCEDURES:

The following test procedures will be utilized during pre-qualification testing:

1. <u>System Set-up and Check-out Test (7286-502)</u>
   Scope: This procedure verifies the proper assembly and configuration of the test system and confirms the proper functioning of the test system.

2. TSAP Validation Test (7286-513) *(a)*

3. Operability Test (7286-503) *(a)*

4. Prudency Test (7286-504) *(a)*

6. SERVICE CONDITIONS AND MARGINS:

Pre-qualification testing is performed in a mild environment. No unique service conditions (a)

7. PERFORMANCE AND ENVIRONMENTAL VARIABLES

Performance and environmental variables to be measured, including required accuracy, will be defined in the specific test procedures.

8. ACCEPTANCE CRITERIA

Specific acceptance criteria for individual tests are found in the procedures. Governing source (b) of acceptance criteria are indicated below:

1. System Set-up and Check-out Test
2. TSAP Validation Test
3. Operability Test
4. Prudency Test

9. RECORDS:

1. Pre-qualification Test Report
2. Completed procedures/attachments
3. System drawings

APPENDIX 4 - ENVIRONMENTAL TEST PLAN

1. GENERAL

The Tricon PLC system is required to operate under environmental conditions defined in sections 6.3.3 and 4.3.6 of the EPRI specification to assure that the system does not fail due to abnormal conditions of temperature and humidity. Testing shall be performed to simulate specified conditions, including margins, and confirm the capability of the Test System to meet its performance specifications. Figure 4-4 of the EPRI specification defines the environmental profile of varying temperature and humidity to which the test specimen should be subjected during environmental testing. (a)

[redacted]

2. REFERENCES

[redacted] (b)

3. EQUIPMENT

The equipment under test is the Triconex Test Specimen as documented in Appendix 1. The test set-up information in the Environmental Test Procedure will document the specific mounting methods and interfaces. The requirements of EPRI TR-107330, Section 6.3.3 will be followed for equipment arrangement and mounting requirements.

4. SEQUENCE OF TESTING

(a)

[redacted]

5. PROCEDURES

The following procedures will be utilized for environmental testing:

(a)

1. Environmental Test (7286-506)

2. Wyle Procedure, Environmental & Seismic Test
   Scope: This procedure is conducted by Wyle personnel to establish the specified environmental conditions in the test chamber and to vary the temperature and humidity in accordance with the profile specified in the EPRI specification.

6. SERVICE CONDITIONS AND MARGINS

(a)

7. PERFORMANCE AND ENVIRONMENTAL VARIABLES

Performance and environmental variables to be measured, including required accuracy, will be defined in the specific test procedures.

8. ACCEPTANCE CRITERIA

(b)

9. RECORDS

1. Environmental Test Report
2. Completed procedures/attachments
3. System Drawings

APPENDIX 5 - SEISMIC TEST PLAN

1. GENERAL

The Tricon PLC system is considered a Seismic Category 1 Safety System. The PLC platform represented by the test specimen shall meet its performance requirements during and following the application of a Safe Shutdown Earthquake (SSE) simultaneously applied in three orthogonal directions. The system shall withstand the SSE vibration following application of five Operating Basis Earthquakes (OBEs). These capabilities will be demonstrated by the seismic test. *(a)*

2. REFERENCES

(b)

(a)

3. EQUIPMENT

4. SEQUENCE OF TESTING

Testing sequence is projected as listed below.

[redacted]

(a)

5. PROCEDURES

The following test procedures will be utilized for Seismic testing:

(a)

1. <u>Seismic Test (7286-507)</u>

[redacted]

2. <u>Wyle Procedure, Environmental & Seismic Test</u>

   Scope: This procedure is conducted by Wyle personnel to initiate the specified seismic conditions with the test specimen mounted on the shaker table and obtain seismic data.

6. SERVICE CONDITIONS AND MARGINS

(a)

[redacted]

7. PERFORMANCE AND ENVIRONMENTAL VARIABLES

Performance and environmental variables to be measured, including required accuracy, will be defined in the specific test procedures.

(b)

8. ACCEPTANCE CRITERIA

9. RECORDS

1. Seismic Test Report
2. Completed procedures/attachments
3. Test response spectrum data
4. System drawings

APPENDIX 6 - SURGE AND ISOLATION TEST PLAN

1. GENERAL

The purpose of this plan is to define the requirements for Surge and Isolation testing conducted as part of the qualification tests for the Triconex Test Specimen. Testing shall demonstrate surge withstand capability and isolation capability as specified in the EPRI Specification, sections 4.6.2 and 4.6.4, respectively. Sections 6.3.5 and 6.3.6 provide the requirements for this testing.

Tests to be conducted under this plan are:

1. Surge Withstand Test
2. Isolation (1E/non-1E) Test

(a)

2. REFERENCES

(b)

(a)

3. EQUIPMENT

4. SEQUENCE OF TESTING

(a)

5. PROCEDURES

The following test procedures will be utilized for this testing: *(a)*

1. Surge Withstand Test (7286-508)

[redacted]

(a)

2. Isolation (1E/non-1E) Test (7286-509)

[redacted]

3. Wyle Procedure, Electromagnetic Interference (EMI) Testing

   Scope: Wyle personnel apply Surge Withstand and Isolation voltages to designated test points on the test specimen.

6. SERVICE CONDITIONS AND MARGINS *(a)*

[redacted]

7. PERFORMANCE AND ENVIRONMENTAL VARIABLES

Performance and environmental variables to be measured, including required accuracy, will be defined in the specific test procedures.

8. ACCEPTANCE CRITERIA

(b)

9. RECORDS

1. Surge and Isolation Test Report
2. Completed procedures/attachments
3. System drawings

APPENDIX 7 - EMI/RFI TEST PLAN

1. GENERAL

The purpose of this plan is to define the requirements for the EMI/RFI testing conducted as part of the qualification tests for the Triconex Test Specimen. Testing shall demonstrate the satisfaction of EMI/RFI criteria specified in EPRI Specification 6.3.2 and 4.3.7.

The EMI/RFI susceptibility and emissions withstand capability given in EPRI TR-102323 shall be tested as follows:

1. Radiated susceptibility per Appendix B, section 3.1.2.
2. Conducted susceptibility per Appendix B, section 3.2.2.
3. Radiated emissions per Section 7.
4. Conducted emissions per Section 7.

(a)

2. REFERENCES

(b)

(a)

3. EQUIPMENT

4. SEQUENCE OF TESTING

(a)

5. PROCEDURES

The following test procedures will be utilized for this testing: *(a)*

1. EMI/RFI Test (7286-510)

2. Wyle Procedure, Electromagnetic Interference (EMI) Testing

   Scope: Wyle personnel will subject the test specimen to specified levels of EMI and RFI radiation to establish susceptibility. In addition, conducted and radiated emissions by the test specimen will be measured and compared to acceptable levels.

6. SERVICE CONDITIONS AND MARGINS

(a)

7. PERFORMANCE AND ENVIRONMENTAL VARIABLES

Performance and environmental variables to be measured, including required accuracy, will be defined in the specific test procedures.

8. ACCEPTANCE CRITERIA

(b)

9. RECORDS

1. EMI/RFI Test Report
2. Completed procedures/attachments
3. System drawings

APPENDIX 8 - PERFORMANCE PROOF TEST PLAN

1. GENERAL

During pre-qualification testing (Appendix 3), acceptable operation of the test specimen is confirmed and baseline performance data is established for selected operating parameters through performance of the Operability and Prudency tests. Qualification testing (Appendices 4-7) subjects the test specimen to specified stresses and confirms operability during adverse conditions. Normal operating performance data, and in some cases Operability test and Prudency test data, is obtained during and/or after each qualification test. *(a)*

2. REFERENCES

EPRI Specification TR-107330: (*(b)*

(a)

3. EQUIPMENT

4. SEQUENCE OF TESTING

(a)

5. PROCEDURES

The following test procedures, as described in Appendix 3, will be utilized for this testing:

1. System Set-up and Check-out Test (7286-502)
2. Operability Test (7286-503)
3. Prudency Test (7286-504)

6. SERVICE CONDITIONS AND MARGINS

(a)

7. PERFORMANCE AND ENVIRONMENTAL VARIABLES

Performance and environmental variables to be measured, including required accuracy, will be defined in the specific test procedures.

(b)

8. ACCEPTANCE CRITERIA

9. RECORDS

1. Performance Proof Test Report
2. Completed procedures/attachments
3. System drawings

TRICONEX

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

PERFORMANCE PROOF TEST REPORT

Report No.: 7286-530

Revision 0

March 13, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Mitchell Albers	[signature]	Project Manager
Approvals:	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

Document Change History			
Revision	**Date**	**Change**	**Author**
0	03/13/00	Initial Issue	M. Albers

TABLE OF CONTENTS

1.0 PURPOSE

The purpose of this test report is to summarize the results of performance proof testing of the Triconex Tricon PLC. 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 testing involved a final performance of the Tricon Nuclear Qualification Project Operability and Prudency Test procedures (References 8.9 and 8.12). These procedures were developed in accordance with Sections 5.3 and 5.4 of EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants (Reference 8.6).

The format of this test report conforms to Section 8.3.(7) of IEEE Specification 323-1983 (Reference 8.2). Section 6 provides a detailed discussion of the test results, including a comparison of the performance proof testing Operability and Prudency test data to the data recorded during all other performances of the Operability and Prudency tests. This test report therefore serves as an evaluation and summary of the Operability and Prudency test data collected throughout the qualification testing process. Conclusions from the testing are provided in Section 7.0, including a summary of the specific manufacturer's performance specifications which were verified throughout qualification testing. These performance specifications will be included in the Final Summary Report Application Guide.

The following documents are included as appendices to this test report:

Appendix A: Completed Pre-Performance Proof Test Run of Triconex Procedure No. 7286-502, "System Set-Up and Check-Out Procedure". This completed procedure documents activities performed by Triconex personnel in setting up the Tricon Test Specimen for performance proof testing and verifying proper system operation prior to testing.

Appendix B: Completed Performance Proof Test Run of Triconex Procedure No. 7286-503, "Operability Test Procedure". This completed procedure documents the performance and results of performance proof operability testing of the Tricon Test Specimen, including evaluation of acceptable test results.

Appendix C: Completed Performance Proof Test Run of Triconex Procedure No. 7286-504, "Prudency Test Procedure". This completed procedure documents the performance and results of performance proof prudency testing of the Tricon Test Specimen, including evaluation of acceptable test results.

The Operability and Prudency tests were also performed during pre-qualification, environmental and seismic testing. These completed Operability and Prudency test procedures are included as appendices to the respective qualification test reports.

2.0 TEST OBJECTIVE

The objective of performance proof testing is to demonstrate the continued acceptable performance of the Tricon Test Specimen after exposure to the stresses applied during environmental, seismic and EMI/RFI qualification testing.

3.0 DESCRIPTION OF TEST SPECIMEN

The equipment tested consists of four Tricon PLC chassis populated with selected input, output, communication, chassis interface and chassis power supply modules. The tested equipment also includes external termination assemblies (ETA's) provided for connection of field wiring to the Tricon input and output modules, and a third party field power supply. Triconex Drawing 7286-102 (Reference 8.4) shows the general arrangement and interconnection of the Tricon Test Specimen chassis. Project document 7286-541 (Reference 8.3) 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 8.1).

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 completed Operability and Prudency Test Procedures (Appendices B and C) identify the TSAP revision used during performance proof testing. The Master Configuration List identifies the revision level of all test specimen firmware.

4.0 TEST SET-UP AND INSTRUMENTATION

The following sections describe the set-up of the Tricon Test Specimen and Lambda field power supply during performance proof testing, and the simulation and measuring instrumentation used during testing. The system set-up is documented in Appendix A. Results of the performance proof Operability and Prudency tests are documented in Appendices B and C. Specifications for test instrumentation are included in all three appendices.

4.1 Test Specimen Mounting

Performance proof testing was performed at the Triconex Irvine, California facility. The

(a)

4.2 Test Specimen Chassis and Module Configuration

(a)

4.3 Test Specimen Power Supply Configuration

(a)

4.4 Test Instrumentation

(a)

4.5 Instrument Calibration

All tests were performed using calibrated test instruments. Calibration certifications are held by Triconex. Appendices A, B and C document the calibration status of the test instrumentation used.

5.0 TEST PROCEDURE

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 testing was performed at the Triconex Irvine, California facility. This section describes the procedures used to conduct performance proof testing of the Tricon Test Specimen.

5.1 Test Method

Performance proof testing involved a final performance of the Tricon Nuclear Qualification Project Operability and Prudency Test procedures. These procedures were developed in accordance with Sections 5.3 and 5.4 of EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications (Reference 8.6). The tests include the following Test Specimen performance checks:

(a)

Section 6 of this report provides a detailed description of the tests performed by each section of the Operability and Prudency Test procedures.

5.2 Test Sequence

Figure 2 of the project Master Test Plan (Reference 8.8) shows the sequence of acceptance testing performed on the Tricon Test Specimen. These tests included pre-qualification

e

g,

y

(a)

5.3 Test Levels

Operability and Prudency testing involves exposing the Tricon Test Specimen to various normal and abnormal conditions of source power and input/output interface operation. Section 6 of this report provides a detailed description of the normal and abnormal operating conditions simulated during performance proof Operability and Prudency testing.

5.4 Test Specimen Operation

(a)

5.5 Test Specimen Performance Monitoring

(a)

5.6 Test Acceptance Criteria

The completed performance proof Operability and Prudency Test procedures (Appendices B and C) include detailed acceptance criteria in Section 4.0 of each test section. These acceptance criteria were developed from the applicable sections of EPRI TR-107330 and from Triconex product specifications for the Tricon PLC. Section 6 of this report provides a detailed listing and comparison of the measured test data to the applicable test acceptance

(a)

6.0 TEST RESULTS

This section discusses the results of performance proof testing of the Tricon Test Specimen and Lambda field power supply. The testing involved a final performance of the Operability and Prudency Test procedures developed as part of the Nuclear Qualification Effort. The discussion of test results includes comparison of the performance proof test data to Operability and Prudency test data collected during pre-qualification, environmental and seismic testing. This test report therefore serves as an evaluation and summary of the Operability and Prudency test data collected throughout the qualification testing process. This section also dispositions performance or data anomalies which were observed or recorded during Operability and Prudency testing of the Tricon Test Specimen.

6.1 Pre-Performance Proof Set-Up and Check-Out Testing

This testing directs set-up of the Tricon Test Specimen and Lambda field power supply for performance proof testing and verification of proper system operation prior to testing. Results of the testing are documented in the completed System Set-Up and Check-Out Test

Procedure (7286-502) included as Appendix A. Results of the testing showed that the system was set-up and operating correctly prior to start of performance proof testing.

6.2 Performance Proof Operability Testing

Performance proof operability testing of the Tricon Test Specimen was performed in accordance with Triconex Test Procedure 7286-503, "Operability Test Procedure." The completed test procedure is included as Appendix B. The following is a discussion of the results of performance of each section of the Performance Proof Operability Test.

(a)

(a)

(a)

(a)

(a)

(a)

(a)

(a)

(a)

(a)

6.3

(a)

(a)

n.

e.

/O

ed

6.4

(a)

(c)

(a)

(d)

(a)

7.0 CONCLUSIONS

1. The results of performance proof Operability and Prudency testing were compared to the results of Operability and Prudency testing performed throughout the pre-qualification and qualification test process. The following conclusions are made from review and comparison of the test results for each specific section of the Operability and Prudency tests:

   (a) Analog Input/Output Module Accuracy

   For all Operability Test runs, the accuracy of each analog input/output module was demonstrated to meet the following Triconex published product specifications:

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

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

   (b) 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.

(c) 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 following Triconex published product specifications:

Module	Description	Switching Level OFF to ON or ON to OFF
3504E	24 VDC Digital Input	6 VDC # V_{SWITCH} #18 VDC
3501E	115 VAC Digital Input	28 VAC # V_{SWITCH} #86 VAC

Continued from previous page:

Module	Description	Switching Level OFF to ON or ON to OFF
3502E	48 VDC Digital Input	11 VDC # V_{SWITCH} #32 VDC
3503E	24 VDC Digital Input	6 VDC # V_{SWITCH} #18 VDC
3505E	24 VDC Digital Input	4VDC # V_{SWITCH} #12 VDC

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.

(d) Discrete Output Operation

For all Operability Test runs, each discrete output module was demonstrated to operate ON and OFF at the following manufacturer's published product specifications for maximum operating current, and minimum and maximum operating voltage:

		Point Drive Capability		
Module	Description	Max. Current	Min. Voltage	Max. Voltage
3604E	24 VDC Digital Output	2.0 amp	22 VDC	45 VDC
3624	24 VDC Digital Output	0.7 amp	16 VDC	30 VDC
3607E	48 VDC Digital Output	1.0 amp	44 VDC	80 VDC
3603E	120 VDC Digital Output	0.8 amp	90 VDC	150 VDC
3623	120 VDC Digital Output	0.8 amp	90 VDC	150 VDC
3601E	115 VAC Digital Output	2.0 amp	80 VAC	155 VAC
3611E	115 VAC Digital Output	2.0 amp	90 VAC	155 VAC

3636R	115 VAC Relay Output	2.0 amp	N/A	155 VAC

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.

(e) Timer Function Accuracy

For all Operability Test runs, the time out periods of the application program timer functions were demonstrated to not vary from the measured pre-qualification baseline time-out periods by more than the greater of ±1% of the time out period or ±3 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.

(f) Failover Performance

The pre-qualification, ambient temperature environmental, post-seismic and performance proof runs of the Operability Test procedure included tests to demonstrate automatic failover to redundant components on simulated failures of the following components:

- Main Processor Module
- Fiber Optic Communication Modules (Primary and Remote)
- Chassis Expansion Port Cabling
- Chassis Power Supplies

All test results demonstrated acceptable failover operation of the Tricon Test Specimen based on observing:

(1) Uninterrupted operation of communication links to peripheral devices.
(2) No change in state of discrete and relay output points.
(3) No change in analog outputs greater than 5%.
(4) Actuation of chassis alarm circuits during simulated failure conditions.

(g) 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 including:

(1) Chassis alarm circuits actuate.
(2) Analog outputs points go to zero.

(3) Discrete and relay output points open.
(4) Communication links to peripheral devices disabled.

The test results also demonstrated predictable and consistent response of the Tricon Test Specimen on recovery of power including:

(1) Chassis alarm circuits de-actuate.
(2) Analog outputs points go to value commanded by application program.
(3) Discrete and relay output points go to state commanded by application program.
(4) Communication links to peripheral devices restored.

In addition, successful restart of the Tricon Test Specimen on restoration of power consistently indicated proper functioning of the watchdog timer mechanisms.

(h) 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 mseconds. Acceptable test results were based on observing:

(1) Uninterrupted application program execution.
(2) Uninterrupted operation of communication links to peripheral devices.
(3) No change of state of discrete and relay output points.
(4) No change in analog outputs greater than 5%.

The test results demonstrated:

(1) The 120 VAC and 230 VAC chassis power supplies meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 mseconds when installed as the only chassis power supply or when installed in combination with a second chassis power supply.

(2) The 24 VDC chassis power supplies do not meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 mseconds. The measured hold-up time capability of the 24 VDC chassis power supplies (a)

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 (a) Acceptable test results were based on observing a drop in the output voltage of the Lambda field power supply to (a) The test results demonstrated:

(1) The Lambda field power supply does not meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 mseconds. The measured hold-up time

(a)

(i) Power Quality Tolerance

The pre-qualification, high temperature environmental, post-seismic and performance proof runs of the Operability Test procedure included 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. Tests were performed over the following manufacturer's allowable ranges for each type of power supply included in the testing:

Chassis Power Supply Model 8310 (120 VAC):	85 VAC to 140 VAC,	47 Hz to 63 Hz
Chassis Power Supply Model 8312 (230 VAC):	185 VAC to 285 VAC,	47 Hz to 63 Hz
Chassis Power Supply Model 8311 (24 VDC):	22 VDC to 31 VDC	
Lambda Power Supply Model LNS-P-24:	105 VAC to 127 VAC,	57 Hz to 63 Hz

All test results demonstrated acceptable performance of the Tricon Test Specimen based on observing:

(1) Uninterrupted operation of the TSAP.
(2) No appreciable change in power supply output voltage.
(3) No change in state of discrete and relay output points.
(4) No change in analog outputs greater than 5%.

In addition, power quality tolerance tests demonstrated acceptable performance of processor memory writes prior to Tricon reset on gradual loss of source power voltage.

(j) Burst of Events Performance

Burst of Events testing performed during the pre-qualification, high temperature environmental, post-seismic and performance proof runs of the Prudency Test procedure demonstrated the ability of the Tricon PLC to process rapidly changing input and output signals based on the control logic of the operating application program.

(k) Communication Port Failure Performance

Communication Port Failure testing performed during the pre-qualification, high temperature environmental, post-seismic and performance proof runs of the Prudency Test procedure demonstrated no effect on digital input to digital output and analog input to analog output response times during simulated failures (transmit line opens, shorts, grounds and superimposed white noise) of communication lines connected to the following communication ports:

- EICM Module RS-232 ports 1 and 4.
- ACM Module I/A Nodebus AUI DNBI and RS-423 ports.
- NCM Module IEEE 802.3 Net 1 and Net 2 ports.
- Chassis I/O Expansion RS-485 ports.

2. The Tricon Test Specimen and Lambda field power supply met all Operability and Prudency test acceptance criteria throughout qualification and performance proof testing with the following exceptions:

   (a) The 24 VDC chassis power supplies do not meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 mseconds. The measured hold-up time capability of the 24 VDC chassis power supplies (a)

   (b) The Lambda field power supply does not meet the TR-107330 acceptance criteria for hold-up time capability of at least 40 mseconds. The measured hold-up time capability of the Lambda field power supply wa (a)

   These performance exceptions will be addressed in the Final Summary Report Application Guide to be developed as part of the Nuclear Qualification Effort.

8.0 REFERENCES

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

8.1 Triconex Document No. 7286-540, Nuclear Qualification of Tricon PLC System, Master Configuration List (MCL)

8.2 IEEE Standard 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

8.3 Triconex Document No. 7286-541, Nuclear Qualification of Tricon PLC System, System Description

8.4 Triconex Drawing No. 7286-102, Sheet 1, Rev. 1 and Sheet 2, Rev. 0, Generic Qualification System General Equipment Arrangement

8.5 MPR Calculation 426-001/MDA-02, Triconex PLC Qualification, Determination of Test Measurement Accuracies, Rev. 0

8.6 EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Final Report dated December, 1996

8.7 MPR Calculation 426-001/SCS-01, Triconex PLC Qualification, Test Tricon Maximum Response Time Calculation, Rev. 2

8.8 Triconex Document No. 7286-500, Nuclear Qualification of Tricon PLC System, Master Test Plan

8.9 Triconex Procedure No. 7286-503, Rev. 2, Nuclear Qualification of Tricon PLC System, Operability Test Procedure

8.10 Triconex Report No. 7286-525, Nuclear Qualification of Tricon PLC System, Environmental Test Report

8.11 MPR Calculation 426-001/MDA-01, Triconex PLC Qualification, Prudency Test Analog Input to Analog Output Accuracy Determination, Rev. 1

8.12 Triconex Procedure No. 7286-504, Rev. 2, Nuclear Qualification of Tricon PLC System, Prudency Test Procedure

8.13 Triconex Procedure No. 7286-502, Rev. 2, Nuclear Qualification of Tricon PLC System, System Set-up and Checkout Test Procedure

9.0 ATTACHMENTS

Attachment 1: Summary of Operability Test Results, Section 2: Analog Input/Output Accuracy Tests (20 pages)

Attachment 2: Summary of Operability Test Results, Section 3: Response Time Tests (2 pages)

Attachment 3: Summary of Operability Test Results, Section 4: Discrete Input Tests (3 pages)

Attachment 4: Summary of Operability Test Results, Section 5: Discrete Output Tests (9 pages)

Attachment 5: Summary of Operability Test Results, Section 6: Timer Tests (2 pages)

Attachment 6: Summary of Operability Test Results, Section 7: Failover Tests (5 pages)

Attachment 7: Summary of Operability Test Results, Section 8: Loss of Power/Failure to Complete Scan Detection Tests (2 pages)

Attachment 8: Summary of Operability Test Results, Section 9: Power Interruption Tests (8 pages)

Attachment 9: Summary of Operability Test Results, Section 10: Power Quality Tolerance Tests (13 pages)

Attachment 10: Summary of Prudency Test Results, Section 2: Burst of Events Tests (2 pages)

Attachment 11: Summary of Prudency Test Results, Section 3: Communication Port Failure Tests (13 pages)

10.0 APPENDICES

Appendix A: Completed Pre-Performance Proof Test Run of Triconex Procedure No. 7286-502, System Set-Up and Check-Out Procedure

Appendix B: Completed Performance Proof Test Run of Triconex Procedure No. 7286-503, Operability Test Procedure

Appendix C: Completed Performance Proof Test Run of Triconex Procedure No. 7286-504, Prudency Test Procedure

(a)

ATTACHMENT 1

(Page 1 of 20)

pages 2-20 deleted in non-proprietary version

Summary of Operability Test Results

Section 2: Analog Input/Output Accuracy Tests

(a)

page 2 deleted in non-proprietary version

ATTACHMENT 2

(Page 1 of 2)

Summary of Operability Test Results

Section 3: Response Time Tests

(a)

pages 2, 3 deleted in non-proprietary version

ATTACHMENT 3

(Page 1 of 3)

Summary of Operability Test Results

Section 4: Discrete Input Tests

(a)

ATTACHMENT 4

pages 2-9 deleted in non-proprietary version

(Page 1 of 9)

Summary of Operability Test Results

Section 5: Discrete Output Tests

(a)

page 2 deleted in non-proprietary version

ATTACHMENT 5

(Page 1 of 2)

Summary of Operability Test Results

Section 6: Timer Tests

(a)

ATTACHMENT 6

pages 2-5 deleted in non-proprietary version

(Page 1 of 5)

Summary of Operability Test Results

Section 7: Failover Tests

(a)

ATTACHMENT 7

(Page 1 of 2)

page 2 deleted in non-proprietary version

Summary of Operability Test Results

Section 8: Loss of Power/Failure to Complete Scan Detection Tests

(a)

ATTACHMENT 8

pages 2-8 deleted in non-proprietary version

(Page 1 of 8)

Summary of Operability Test Results

Section 9: Power Interruption Tests

(a)

ATTACHMENT 9

(Page 1 of 13)

pages 2-13 deleted in non-proprietary version

Summary of Operability Test Results

Section 10: Power Quality Tolerance Tests

(a)

page 2 deleted in non-proprietary version

ATTACHMENT 10

(Page 1 of 2)

Summary of Prudency Test Results

Section 2: Burst of Events Tests

(a)

ATTACHMENT 11

(Page 1 of 13)

pages 2-13 deleted in non-proprietary version

Summary of Prudency Test Results

Section 3: Communication Port Failure Tests

TRICONEX

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

CLASS 1E TO NON-1E ISOLATION TEST REPORT

Report No.: 7286-529

Revision 0

March 14, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Ralph Paul	[signature]	Engineer
Approvals:	Mitchell Albers	[signature]	Project Manager
	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

Document Change History			
Revision	**Date**	**Change**	**Author**
0	03/14/00	Initial Issue	R. Paul

TABLE OF CONTENTS

1.0 PURPOSE

The purpose of this test report is to summarize the results of Class 1E to Non-1E isolation testing of the Triconex Tricon PLC. This testing was performed in accordance with the requirements of Section 6.3.6 of EPRI TR-107330 (Reference 8.6). The format of this test report conforms to Section 8.3.(7) of IEEE Specification 323-1983 (Reference 8.2). Conclusions from the testing are provided in Section 7.0.

The following documents are included as appendices to this test report:

Appendix A: Wyle Laboratories Test Report Number 41339-01, Electromagnetic Interference (EMI) Test Report on a Tricon PLC System. This report documents the activities of Wyle Laboratories personnel in performing Class 1E to Non-1E isolation testing of the Tricon Test Specimen.

Appendix B: Completed Triconex Procedure No. 7286-509, "Class 1E to Non-1E Isolation Test Procedure". This completed procedure documents the activities performed by Triconex personnel in performing Class 1E to Non-1E isolation testing of the Tricon Test Specimen, including performance monitoring during testing and evaluation of acceptable test results on completion of testing.

2.0 TEST OBJECTIVE

The objective of Class 1E to Non-1E isolation testing is to demonstrate the capability of selected Tricon PLC modules to act as electrical isolation devices between the designated safety related hardware of the PLC and non-safety related field circuit connections. The qualification of the Tricon PLC is based on a system design that connects Non-1E input/output circuits to modules installed in one or more separate Non-1E 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 modules are used to interface to Non-1E communication equipment). The Tricon Test Specimen was configured with three communication modules in the main chassis. Each of these communication modules included the following interfaces to simulated Non-1E equipment:

- EICM Module, RS-232 Serial Port (MODBUS) interface to Simulator Tricon
- ACM Module, Dual Nodebus (DNBI) and RS-423 interface to Foxboro I/A Console
- NCM Module, IEEE 802.3 (TCP/IP) interface to Wonderware Operator Console

These interfaces were tested to demonstrate Class 1E to Non-1E electrical isolation capability. 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. The Model 3636R Relay Output Module was installed in Chassis 4, Slot 6 of the Tricon Test Specimen.

3.0 DESCRIPTION OF TEST SPECIMEN

The equipment tested consists of four Tricon PLC chassis populated with selected input, output, communication, chassis interface and chassis power supply modules. The tested equipment also includes external termination assemblies (ETA's) provided for connection of field wiring to the Tricon input and output modules. Triconex Drawing 7286-102 (Reference 8.4) shows the general arrangement and interconnection of the Tricon Test Specimen chassis. Project document 7286-541 (Reference 8.3) 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 8.1).

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 completed Class 1E to Non-1E Isolation Test procedure (Appendix B) identifies the TSAP revision used during testing. The Master Configuration List identifies the revision level of all test specimen firmware.

4.0 TEST SET-UP AND INSTRUMENTATION

The following sections describe the set-up of the Tricon Test Specimen during Class 1E to Non-1E isolation testing, and the instrumentation used to monitor the applied test conditions and the Tricon Test Specimen performance during and after testing. The system set-up is documented in Appendix B and References 8.10 and 8.11. Specifications for test instrumentation supplied by Wyle Laboratories are included in Appendix A and Reference 8.13. Specifications for test instrumentation supplied by Triconex are included or referenced in Appendix B.

4.1 Test Specimen Mounting

(a)

(a)

4.2 Test Specimen Power Supply Configuration

(a)

4.3 Wyle Instrumentation

Wyle Laboratories provided the test instrumentation required for applying and measuring the Class 1E to Non-1E isolation test voltages and currents given in Section 5.2 of this report. Wyle Test Procedure No. 46992-10 (Reference 8.13) and Test Report No. 41339-01 (Appendix A) provide a detailed identification and description of the Wyle test equipment and instrumentation used to perform Class 1E to Non-1E isolation testing.

4.4 Triconex Instrumentation

(a)

4.5 Instrument Calibration

All tests were performed using calibrated test instruments. Calibration certifications are held by Wyle Laboratories and Triconex. Appendices A and B document the calibration status of the test instrumentation used.

5.0 TEST PROCEDURE

Class 1E to Non-1E isolation testing was performed to the requirements of EPRI TR-107330 (Reference 8.6), which invokes IEEE Standard 384-1981 (Reference 8.7). The testing was performed on the communication module ports and relay output module identified in Section 2.0 of this report. The following sections describe the approach to satisfying the requirements of the referenced documents during Class 1E to Non-1E isolation testing of the Tricon Test Specimen. Reference 8.13 is the test procedure used by Wyle Laboratories to perform Class 1E to Non-1E isolation testing of the Tricon Test Specimen. The completed procedure used by Triconex to perform Class 1E to Non-1E isolation testing is included as Appendix B.

5.1 Test Method

EPRI TR-107330, Section 4.6.4, specifies that Class 1E to Non-1E electrical isolation testing of the PLC under qualification demonstrate that the isolation features conform to the instrumentation and control requirements for Class 1E to Non-1E connections given in IEEE 384-1981. Section 7.2.2.1 of IEEE 384 requires that (a) the isolation device prevents shorts, grounds and open circuits on the Non-1E side from degrading unacceptably 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.

(a)

(a)

As described in Section 2.0 of this report, 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 by Appendix B. The fiber optic cables are incapable of transmitting electrical faults from the remote RXM module to the primary RXM module (which would be installed in the safety related Tricon chassis), and therefore meet the item (a) and item (b) isolation requirements given above.

5.2 Test Levels

EPRI TR-107330, Section 4.6.4, requires that the PLC modules under qualification provide electrical isolation capability of at least 600 VAC and 250 VDC applied for 30 seconds. Per Section 7.2.2.1 of IEEE Standard 384, the highest voltage to which an isolation device Non-1E side is exposed shall determine the minimum voltage level that the device shall withstand across the Non-1E side terminals, and between the Non-1E terminals and ground.

(a)

5.3 Test Specimen Operation

EPRI TR-107330 does not include specific requirements for operation of the test PLC during Class 1E to Non-1E isolation testing. During Class 1E to Non-1E isolation testing, the

(a)

(a)

5.4 Test Specimen Performance Monitoring

Per EPRI TR-107330, Section 4.6.4, applying the specified levels of Class 1E to Non-1E isolation test voltage to relay output module points shall not disrupt the operation of any other modules in the Test Specimen, or cause disruption of the Test Specimen backplane signals.

(a)

(a)

5.5 Test Acceptance Criteria

The Class 1E to Non-1E isolation test acceptance criteria are as given below based on Appendix 6 of the Tricon Nuclear Qualification Program Master Test Plan (Reference 8.8), and EPRI TR-107330, Section 4.6.4 (Reference 8.6).

a.) 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.

b.) 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 the following:

i.) Application of the isolation test voltages to the specified module test points shall not result in damage to any other modules installed in the Tricon Test Specimen, including power supply modules, main processor modules, RXM modules, input/output modules and communication modules.

ii.) Application of the isolation test voltages to the specified module test points shall not result in disruption of the operation of any other modules in the Tricon Test

Specimen, including the ability to correctly acquire or receive input signals and generate or transmit output signals.

c.) 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. Faults or failures of redundant devices which occur during Class 1E to Non-1E isolation testing will be evaluated for effect on Test Specimen operation.

6.0 TEST RESULTS

This section summarizes the results of Class 1E to Non-1E isolation testing of the Tricon Test Specimen. This section also dispositions performance or data anomalies which were observed or recorded during testing.

6.1 Test Set-Up and Check-Out

Class 1E to Non-1E isolation testing was performed after EMI/RFI testing and Surge Withstand testing. The test set-up and check-out is documented by the System Set-Up and Check-Out Test Procedures for both EMI/RFI testing (Reference 8.10) and Surge Withstand testing (Reference 8.11). In addition, the Class 1E to Non-1E Isolation test procedure (Appendix B) includes a verification of system operation prior to testing (step 9.4). Results of the testing showed that the system was set-up and operating correctly.

6.2 Class 1E to Non-1E Isolation Testing

Class 1E to Non-1E isolation testing of the Tricon Test Specimen was performed in accordance with Triconex Test Procedure 7286-509, "Class 1E to Non-1E Isolation Test Procedure," and Wyle Test Procedure 46992-10, "Test Procedure for Electromagnetic Interference (EMI) Testing on a Tricon PLC System."

(a)

(a)

[redacted]

(a)

6.3 Communication Port Fault Testing

[redacted]

(a)

6.4 Test Anomalies

The following test anomaly was observed during Class 1E to Non-1E isolation testing:

(a) [redacted]

(a)

7.0 CONCLUSIONS

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 Class 1E to Non-1E 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.

3. The Class 1E to Non-1E isolation test results demonstrate that the Tricon PLC relay output module Model 3636R provides adequate electrical isolation per IEEE 384-1981 between the safety related portions of the Tricon and connected non-safety related field circuits. The testing demonstrated electrical isolation capability of the relay output points to applied voltages of 600 VAC (at 23.4 amps maximum) and 250 VDC (at 10 amps maximum).

4. 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 by Appendix B. 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.

8.0 REFERENCES

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

8.1 Triconex Document No. 7286-540, Nuclear Qualification of Tricon PLC System, Master Configuration List (MCL)

8.2 IEEE Standard 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

8.3 Triconex Document No. 7286-541, Nuclear Qualification of Tricon PLC System, System Description

8.4 Triconex Drawing No. 7286-102, Sheet 1, Rev. 1 and Sheet 2, Rev. 0, Generic Qualification System General Equipment Arrangement

8.5 Triconex Procedure No. 7286-504, Nuclear Qualification of Tricon PLC System, Prudency Test Procedure

8.6 EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Final Report dated December, 1996

8.7 IEEE Standard 384-1981, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits

8.8 Triconex Document No. 7286-500, Nuclear Qualification of Tricon PLC System, Master Test Plan

8.9 Triconex Report No. 7286-530, Nuclear Qualification of Tricon PLC System, Performance Proof Test Report

8.10 Triconex Report No. 7286-527, Nuclear Qualification of Tricon PLC System, EMI/RFI Test Report, Appendix B

8.11 Triconex Report No. 7286-528, Nuclear Qualification of Tricon PLC System, Surge Withstand Test Report, Appendix B

8.12 Triconex Procedure No. 7286-510, Nuclear Qualification of Tricon PLC System, EMI/RFI Test Procedure

8.13 Wyle Test Procedure No. 46992-10, Test Procedure for Electromagnetic Interference (EMI) Testing on a Tricon PLC System

9.0 ATTACHMENTS

Attachment 1: Example Plots of Tricon Test Specimen Normal Operating Performance Data

10.0 APPENDICES

Appendix A: Wyle Laboratories Test Report Number 41339-01, Electromagnetic Interference (EMI) Test Report on a Tricon PLC System

Appendix B: Completed Triconex Procedure No. 7286-509, Class 1E to Non-1E Isolation Test Procedure

(a)

ATTACHMENT 1
(Page 1 of 33)

pages 2-33 deleted in non-proprietary version

This attachment includes an example of the Tricon Test Specimen normal operating performance data,

TRICONEX

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

SURGE WITHSTAND TEST REPORT

Report No.: 7286-528

Revision 0

March 24, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Mitchell Albers	[signature]	Project Manager
Approvals:	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

Document Change History			
Revision	**Date**	**Change**	**Author**
0	03/24/00	Initial Issue	M. Albers

TABLE OF CONTENTS

1.0 PURPOSE

The purpose of this test report is to summarize the results of surge withstand testing of the Triconex Tricon PLC. This testing was performed in accordance with the requirements of Sections 4.6.2 and 6.3.5 of EPRI TR-107330 (Reference 8.1). The format of this report conforms to Section 8.3.(7) of IEEE Specification 323-1983 (Reference 8.2). Conclusions from the testing are provided in Section 7.0.

The following documents are included as appendices to this test report:

Appendix A: Wyle Laboratories Test Report Number 41339-01, "Electromagnetic Interference (EMI) Test Report on a Tricon PLC System." This report documents the activities of Wyle Laboratories personnel in performing surge withstand testing of the Tricon Test Specimen.

Appendix B: Completed Surge Withstand Test Run of Triconex Procedure No. 7286-502, "Set-Up and Check-Out Test Procedure". This completed procedure documents activities performed by Triconex and Wyle personnel in setting up the Tricon Test Specimen following a move of the test system midway through surge withstand testing.

Appendix C: Completed Triconex Procedure No. 7286-508, "Surge Withstand Test Procedure". This completed procedure documents activities of Triconex personnel in performing surge withstand testing of the Tricon Test Specimen, including performance monitoring during testing and evaluation of acceptable test results on completion of testing.

2.0 TEST OBJECTIVE

The objective of surge withstand testing is to demonstrate the suitability of the Triconex Tricon PLC for qualification as a safety-related device with respect to AC power line electrical surge withstand capability.

All of the Tricon Test Specimen components were subjected to surge withstand testing as required except for the 230 VAC Model 8312 chassis power supply module and the third party Lambda field power supply. Due to time constraints on testing encountered while at Wyle Laboratories, surge withstand testing of these components was not performed. Future testing to establish surge withstand capability of these components will be performed if justified by utility demand for the components. At present, Triconex will not offer the Model 8312 chassis power supply or Lambda field power supply as safety-related hardware under their 10 CFR 50, Appendix B program.

3.0 DESCRIPTION OF TEST SPECIMEN

The equipment tested consists of four Tricon PLC chassis populated with selected input, output, communication, chassis interface and chassis power supply modules. The tested equipment also includes external termination assemblies (ETA's) provided for connection of field wiring to the Tricon input and output modules. Triconex Drawing 7286-102 (Reference 8.3) shows the general arrangement and interconnection of the Tricon Test Specimen chassis. Project document 7286-541 (Reference 8.4) 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 8.5).

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 completed surge withstand test procedure (Appendix C) identifies the TSAP revision used during testing. The Master Configuration List identifies the revision level of all test specimen firmware.

4.0 TEST SET-UP AND INSTRUMENTATION

The following sections describe the set-up of the Tricon Test Specimen during surge withstand testing, and the instrumentation used to monitor the applied test conditions and the Tricon Test Specimen performance during and after testing. The initial system set-up is documented in Appendix C and Reference 8.13. Midway through surge withstand testing the test system was moved to a different location at Wyle Laboratories. Appendices B and C document set-up of the Tricon Test Specimen following the move. Specifications for test instrumentation supplied by Wyle Laboratories are included in Appendix A and Reference 8.14. Specifications for test instrumentation supplied by Triconex are included or referenced in Appendices B and C.

4.1 Test Specimen Mounting

EPRI TR-107330, Section 6.3.5.1 requires that during surge withstand testing, the test PLC be mounted on a non-metallic vertical surface at a height of at least six feet to the bottom of the PLC chassis, with no secondary enclosure. The PLC shall be connected to a ground bus located at the base of the mounting surface using the manufacturer's recommended grounding conductor. Grounding and shielding shall meet the requirements of IEEE 1050 (Reference 8.6) and EPRI TR-102323 (Reference 8.7).

(a)

(a)

4.2 Test Specimen Chassis and Module Configuration

Section 3.0 above describes the general arrangement of the Tricon Test Specimen which was maintained throughout all of the qualification testing. Chassis configurations for surge withstand testing are documented in the Master Configuration List. All of the Tricon Test

(a)

4.3 Test Specimen Power Supply Configuration

EPRI TR-107330 does not include specific requirements for configuration of the test PLC power supplies during surge withstand testing. The AC and DC power sources to the Tricon

Test Specimen chassis power supplies were set at nominal source voltage and frequency conditions during the surge withstand testing. Surge withstand testing was performed following EMI/RFI testing. The test system power distribution remained configured as described in Section 3.4 of Triconex Test Procedure 7286-510, "EMI/RFI Test Procedure" (Reference 8.8), except as temporarily modified by specific steps of the surge withstand test procedure.

4.4 Wyle Instrumentation

EPRI TR-107330, Section 4.6.2, requires that surge withstand testing be performed using industry standard ring wave and combination wave electrical surges. Section 6.4.4 requires that the applied surge withstand levels be checked for compliance with the industry standard specifications.

(a)

4.5 Triconex Instrumentation

After each surge withstand test, operation of the Tricon Test Specimen was monitored and

(a)

4.6 Instrument Calibration

All tests were performed using calibrated test instruments. Calibration certifications are held by Wyle Laboratories and Triconex. Appendices A through C document the calibration status of the test instrumentation used.

5.0 TEST PROCEDURE

Surge withstand testing was performed to the requirements of Sections 4.6.2 and 6.3.5 of EPRI TR-107330 (Reference 8.1). The TR invokes IEEE Standards IEEE C62.41-1991 (Reference 8.9) and C62.45-1987 (Reference 8.10).

The following sections describe the approach to satisfying the requirements of the referenced documents during surge withstand testing of the Tricon Test Specimen. Reference 8.14 is the test procedure used by Wyle Laboratories to perform surge withstand testing of the Tricon Test Specimen. The completed procedure used by Triconex to perform surge withstand testing is included as Appendix C.

5.1 Test Sequence

Figure 2 of the project Master Test Plan (Reference 8.11) shows the sequence of qualification testing performed on the Tricon Test Specimen. Surge withstand testing was performed following completion of the qualification tests which involve sequential exposure of the test specimen to aging factors. Accordingly, surge withstand testing was performed following completion of environmental testing, seismic testing and EMI/RFI testing.

5.2 Test Method

EPRI TR-107330, Section 6.3.5, requires that surge withstand testing of the PLC under qualification be conducted in accordance with IEEE Guide C62.45 (Reference 8.10). Section 4.6.2 of the TR requires that surge withstand testing be performed on both the AC power supply connections to the PLC and the signal and data communication lines to and from the PLC. IEEE C62.45 provides guidance on surge testing the AC power interfaces of equipment connected to low-voltage circuits. The guide does not address surge testing of connected signal and data communication lines. Surge testing of signal and data communication lines connected to industrial measurement and control equipment is addressed in IEC 801-5 (Reference 8.12). IEC 801-5 implements surge testing using wave forms described in IEEE C62.41.

Surge withstand testing of the Tricon Test Specimen was performed at Wyle Laboratories in

(a)

5.3 Test Levels

EPRI TR-107330, Section 4.6.2, requires that the PLC under qualification be tested for capability to withstand electrical surges with a characteristic of both the standard 0.5 Φs, 100 kHz ring wave and the standard 1.2/50 Φs, 8/20 Φs combination wave identified in IEEE Recommended Practice C62.41 (Reference 8.9). Per Section 4.6.2 of TR-107330, the surge withstand level shall comply with Section 9 of IEEE C62.41 for location "B" and "medium exposure", except the applied voltage shall be 3000 volts peak.

(a) Ring Wave Surge Withstand Testing. Ring wave surge withstand testing was performed in accordance with Triconex Procedure No. 7286-508 and Appendix L of Wyle Test Procedure No. 46992-10. These procedures implement ring wave surge

(a)

(b)

(c)

(a)

(a)

5.4 Test Specimen Operation

(a)

5.5 Test Specimen Performance Monitoring

EPRI TR-107330, Section 4.6.2, requires that the PLC under qualification continue to operate following application of the surge withstand test voltages. Applying the specified level of surge to the specified points:

- Shall not damage any other module or device in the PLC.

- Shall not cause a disruption of the PLC backplane signals that could result in a loss of the ability to generate a trip.

- Shall not cause a disruption of any other data acquisition signals that could result in a loss of the ability to generate a trip.

During surge withstand testing, Wyle Laboratories was responsible for generating and exposing the test system to the required surge test voltages. Triconex was responsible for monitoring operation of the test system and determining the withstand capability of the Tricon Test Specimen to the applied surge test voltages.

(a)

5.6 Test Acceptance Criteria

The surge withstand test acceptance criteria are as given below based on Appendix 6 of the Tricon Nuclear Qualification Program Master Test Plan (Reference 8.11), and EPRI TR-107330, Section 4.6.2 (Reference 8.1). As specified in Section 4.6.2, applying the surge test voltages specified in EPRI TR-107330 to the specified Tricon Test Specimen 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 data acquisition signals that could result in a loss of the ability to generate a trip.

Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) shall demonstrate satisfactory operation of the Tricon Test Specimen following application of the surge test voltage. The data evaluations shall demonstrate the following:

a) Application of the surge test voltages to the chassis power supply modules shall not result in damage to any other modules installed in the Tricon Test Specimen, including the main processor modules, the RXM modules, the input/output modules and the communication modules.

b) Application of the surge test voltages to the chassis power supply modules shall not result in permanent disruption of the operation of the Tricon Test Specimen, including the ability to correctly acquire input signals and generate output signals.

c) Application of the surge test voltages to an input/output module point shall not result in damage to any other modules installed in the Tricon Test Specimen, including the main processor modules, the RXM modules, other input/output modules and the communication modules.

d) Application of the surge test voltages to an input/output module point shall not result in permanent disruption of the operation of the Tricon Test Specimen, including the ability to correctly acquire the input signals associated with any other input module points, and to generate the output signals associated with any other output module points.

e) Application of the surge test voltages to a communication module port shall not result in damage to any other modules installed in the Tricon Test Specimen, including the main processor modules, the RXM modules, the input/output modules and other communication modules.

f) Application of the surge test voltages to a communication module port shall not result in permanent disruption of the operation of the Tricon Test Specimen, including the ability to correctly receive input signals to other communication module ports, and to transmit output signals to other communication module ports.

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.

6.0 TEST RESULTS

This section summarizes the results of surge withstand testing of the Tricon Test Specimen. This section also dispositions performance or data anomalies which were observed or recorded during surge withstand testing.

6.1 Set-Up and Check-Out Testing

(a)

(a)

6.2 Surge Withstand Testing

Surge withstand testing of the Tricon Test Specimen was performed in accordance with Triconex Test Procedure 7286-508, "Surge Withstand Test Procedure," and Wyle Test Procedure 46992-10, "Test Procedure for Electromagnetic Interference (EMI) Testing on a

(a)

6.3

(a)

6.4

6.5

(a)

6.6

Data collected after each surge withstand test was analyzed to demonstrate acceptable operation of the Test Specimen. Figures provided in Attachment 1 of this report show examples of the data plots which were analyzed for each surge withstand test to confirm acceptable performance of the Tricon Test Specimen following application of the surge voltage. Data trend verification sheets and data analysis results for each test are provided in the completed surge test procedure (Appendix C). Attachment 2 of this report provides a summary table of the surge withstand test results. The data analysis shows that the Tricon Test Specimen continued to operated in accordance with the test acceptance criteria given in Section 5.6 following application of the surge test voltages. Specifically:

a) Application of the surge test voltages to the chassis power supply modules did not result in damage to any other modules installed in the Tricon Test Specimen, including the main processor modules, the RXM modules, the input/output modules and the communication modules.

b) Application of the surge test voltages to the chassis power supply modules did not result in disruption of the operation of the Tricon Test Specimen, including the ability to correctly acquire input signals and generate output signals.

c) Application of the surge test voltages to the input/output module points did not result in damage to any other modules installed in the Tricon Test Specimen, including the main processor modules, the RXM modules, other input/output modules and the communication modules. In some tests of the digital output modules, the tested module experienced single or multiple point damage. These test results are discussed in Section 6.7 below.

d) Application of the surge test voltages to the input/output module points did not result in disruption of the operation of the Tricon Test Specimen, including the ability to correctly acquire the input signals associated with any other input module points, and to generate the output signals associated with any other output module points. In some tests of the digital output modules, the tested module experienced single or multiple point damage. These test results are discussed in Section 6.7 below.

e) Application of the surge test voltages to the communication module ports did not result in damage to any other modules installed in the Tricon Test Specimen, including the main processor modules, the RXM modules, the input/output modules and other communication modules.

f) Application of the surge test voltages to the communication module ports did not result in disruption of the operation of the Tricon Test Specimen, including the ability to correctly receive input signals to other communication module ports, and to transmit output signals to other communication module ports.

6.7

(a)

(a)

6.8

n

(a)

n

(a)

7.0 CONCLUSIONS

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. The following types of surge withstand tests were performed:

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

    The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List (Reference 8.5).

2. Attachment 2 of this report provides a summary table of the surge withstand tests performed on the Tricon Test Specimen including description of the applied ring waves and combination waves, identification of all tested Tricon components (chassis power supplies and I/O and communication modules), identification of all surge test points, and results (SAT or UNSAT) of each surge test. The summary results show that in all cases the Tricon Test Specimen continued to operate in accordance with the test acceptance criteria given in EPRI TR-107330, Section 4.6.2 following application of the surge test voltages.

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

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

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

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

4. The Model 3603E digital output module and associated Model 9661-910 ETA exhibited vulnerability (permanent damage) to applied surge voltages. The Model 3603T digital output module and associated Model 9661-910 (revised) ETA are revised versions of the Model 3603E module and ETA. These revised components were demonstrated through testing performed as part of the Tricon Nuclear Qualification effort to have acceptable surge withstand capability (i.e., no demonstrated vulnerability). By evaluation (Reference 8.15) it is determined that the design modifications incorporated in the Model 3603T module and ETA do not affect the environmental, seismic and EMI/RFI test results obtained for the Model 3603E module and ETA. Therefore, the Model 3603T digital output module and Model 9661-910 (revised) ETA

are considered equivalent replacements for the Model 3603E digital output module and Model 9661-910 ETA.

5. Due to time constraints on testing encountered while at Wyle Laboratories, surge withstand testing was not performed on the 230 VAC Model 8312 chassis power supply modules and the third party Lambda field power supply. At present, Triconex will not offer the Model 8312 chassis power supply or Lambda field power supply as safety-related hardware under their 10 CFR 50, Appendix B program.

8.0 REFERENCES

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

8.1 EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Final Report dated December, 1996

8.2 IEEE Standard 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

8.3 Triconex Drawing No. 7286-102, Sheet 1, Rev. 1 and Sheet 2, Rev. 0, Generic Qualification System General Equipment Arrangement

8.4 Triconex Document No. 7286-541, Nuclear Qualification of Tricon PLC System, System Description

8.5 Triconex Document No. 7286-540, Nuclear Qualification of Tricon PLC System, Master Configuration List (MCL)

8.6 IEEE Standard 1050-1989, Guide for Instrumentation and Control Equipment Grounding in Generating Stations

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

8.8 Triconex Document No. 7286-510, Nuclear Qualification of Tricon PLC System, EMI/RFI Test Procedure

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

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

8.11 Triconex Document No. 7286-500, Nuclear Qualification of Tricon PLC System, Master Test Plan

8.12 IEC Standard 801-5, Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment, January 1990

8.13 Triconex Report No. 7286-527, Nuclear Qualification of Tricon PLC System, EMI/RFI Test Report, Appendix B

8.14 Wyle Test Procedure No. 46992-10, Test Procedure for Electromagnetic Interference (EMI) Testing on a Tricon PLC System

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

9.0 ATTACHMENTS

Attachment 1: Example Plots of Tricon Test Specimen Normal Operating Performance Data

Attachment 2: Summary of Surge Withstand Test Results

10.0 APPENDICES

Appendix A: Wyle Laboratories Test Report Number 41339-01, Electromagnetic Interference (EMI) Test Report on a Tricon PLC System

Appendix B: Completed Surge Withstand Test Run of Triconex Procedure No. 7286-502, System Set-Up and Check-Out Procedure

Appendix C: Completed Triconex Procedure No. 7286-508, Surge Withstand Test Procedure

(a)

ATTACHMENT 1

(Page 1 of 31)

pages 2-31 deleted from non-proprietary version

This attachment includes an example of the Tricon Test Specimen normal operating performance data.

(a)

ATTACHMENT 2

(Page 1 of 2)

page 2 deleted from non-proprietary version

Summary of Surge Withstand Test Results

TRICONEX

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

EMI/RFI TEST REPORT

Report No.: 7286-527

Revision 0

May 16, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Mitchell Albers	[signature]	Project Manager
Approvals:	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

Document Change History

Revision	Date	Change	Author
0	05/12/00	Initial Issue	M. Albers

TABLE OF CONTENTS

1.0 PURPOSE

The purpose of this test report is to summarize the results of Electromagnetic Interference/Radio Frequency Interference (EMI/RFI) testing of the Triconex Tricon PLC. This testing was performed in accordance with the requirements of Sections 4.3.7 and 6.3.2 of EPRI TR-107330 (Reference 8.1). The format of this report conforms to Section 8.3.(7) of IEEE Specification 323-1983 (Reference 8.2). Conclusions from the testing are provided in Section 7.0.

The following documents are included as appendices to this test report:

Appendix A: Wyle Laboratories Test Procedure Number 46992-10, Test Procedure for Electromagnetic Interference (EMI) Testing on a Tricon PLC System. This procedure provides instruction for Tricon Test Specimen EMIRFI test activities performed by Wyle personnel.

Appendix B: Completed Pre-EMI/RFI Test Run of Triconex Procedure No. 7286-502, "Set-Up and Check-Out Test Procedure". This completed procedure documents activities performed by Triconex and Wyle personnel in setting up the Tricon Test Specimen for EMI/RFI testing and verifying proper system operation prior to testing.

Appendix C: Wyle Laboratories Test Report Number 41339-2, "Electromagnetic Interference (EMI) Test Report on a Tricon PLC System." This report documents the activities of Wyle Laboratories personnel in performing EMI/RFI testing of the Tricon Test Specimen.

Appendix D: Completed Triconex Procedure No. 7286-510, "EMI/RFI Test Procedure". This completed procedure documents activities of Triconex personnel in performing EMI/RFI testing of the Tricon Test Specimen, including performance monitoring during testing and evaluation of acceptable test results on completion of testing.

2.0 TEST OBJECTIVE

The objective of EMI/RFI testing is to demonstrate the suitability of the Triconex Tricon PLC for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility withstand capability.

All of the Tricon Test Specimen components were subjected to EMI/RFI testing as required except for the 230 VAC Model 8312 chassis power supply module and the third party Lambda field power

(a)

(a)

3.0 DESCRIPTION OF TEST SPECIMEN

The equipment tested consists of four Tricon PLC chassis populated with selected input, output, communication, chassis interface and chassis power supply modules. The tested equipment also includes external termination assemblies (ETA's) provided for connection of field wiring to the Tricon input and output modules. Triconex Drawing 7286-102 (Reference 8.3) shows the general arrangement and interconnection of the Tricon Test Specimen chassis. Project document 7286-541 (Reference 8.4) 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 8.5).

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 completed EMI/RFI test procedure (Appendix D) identifies the TSAP revision used during testing. The Master Configuration List identifies the revision level of all test specimen firmware.

4.0 TEST SET-UP AND INSTRUMENTATION

The following sections describe the set-up of the Tricon Test Specimen during EMI/RFI testing, and the instrumentation used to monitor the applied test conditions and the Tricon Test Specimen performance during and after testing. The system set-up is documented in Appendix B. Specifications for test instrumentation supplied by Wyle Laboratories are included in Appendix C. Specifications for test instrumentation supplied by Triconex are included or referenced in Appendices B and D.

4.1 Test Specimen Mounting

(a)

(a)

4.2 Test Specimen Chassis and Module Configuration

Section 3.0 above describes the general arrangement of the Tricon Test Specimen which was maintained throughout all of the qualification testing. Chassis configurations for EMI/RFI testing are documented in the Master Configuration List.

4.3 Test Specimen Power Supply Configuration

(a)

(a)

(a)

4.4 Wyle Instrumentation

EPRI TR-107330, Section 6.4.4, requires measurement of the test levels of EMI/RFI where the PLC under qualification meets performance requirements.

Wyle Laboratories provided the test instrumentation required for generating, monitoring and recording the emitted and applied levels of EMI/RFI during testing. Wyle Test Procedure No. 46992-10 (Appendix A) and Test Report No. 41339-2 (Appendix C) include a detailed identification and description of the Wyle test equipment and instrumentation used to perform EMI/RFI testing.

4.5 Triconex Instrumentation

(a)

4.6 Instrument Calibration

All tests were performed using calibrated test instruments. Calibration certifications are held by Wyle Laboratories and Triconex. Appendices B, C and D document the calibration status of the test instrumentation used.

5.0 TEST PROCEDURE

EMI/RFI testing was performed to the requirements of Sections 4.3.7 and 6.3.2 of EPRI TR-107330 (Reference 8.1). The TR invokes test methods and test levels described in EPRI TR-102323-R1 (Reference 8.7), and MIL-STD-461D (Reference 8.8), MIL-STD-462D (Reference 8.9), and IEC 801-4 (Reference 8.10).

The following sections describe the approach to satisfying the requirements of the referenced documents for EMI/RFI testing of the Tricon Test Specimen. Appendix A is the test procedure used by Wyle Laboratories to perform EMI/RFI testing of the Tricon Test Specimen. The completed procedure used by Triconex to perform EMI/RFI testing is included as Appendix D.

5.1 Test Sequence

Figure 2 of the project Master Test Plan (Reference 8.11) shows the sequence of qualification testing performed on the Tricon Test Specimen. EMI/RFI testing was performed following completion of the qualification tests which involve sequential exposure of the test specimen to aging factors. Accordingly, EMI/RFI testing was performed following completion of environmental and seismic testing, and prior to surge withstand and Class1E to Non-1E isolation testing.

5.2 Test Method

EPRI TR-107330, Section 4.3.7, requires that the PLC under qualification be tested for EMI/RFI susceptibility and emissions in accordance with the requirements of EPRI TR-102323-R1 (Reference 8.7). The EMI/RFI susceptibility testing shall include both radiated and conducted susceptibility testing per Appendix B of EPRI TR-102323-R1. The EMI/RFI emissions testing shall include both radiated and conducted emissions testing per Section 7 of EPRI TR-102323-R1.

EMI/RFI testing of the Tricon Test Specimen was performed at Wyle Laboratories in Huntsville, Alabama. The testing was performed in accordance with Wyle Test Procedure No. 46992-10, "Test Procedure for Electromagnetic Interference (EMI) Testing on a Tricon PLC System," (Appendix A). This procedure implements EMI/RFI testing in accordance with the test method requirements specified in EPRI TR-107330 and TR-102323-R1.

5.3 Test Levels

(a)

(a)

(a)

5.4 Test Specimen Operation

(a)

5.5 Test Specimen Performance Monitoring

EPRI TR-107330, Section 4.3.7, requires that the PLC under qualification withstand the EMI/RFI levels given in EPRI TR-102323-R1. Specifically, when subjected to the EMI/RFI test levels, the PLC modules shall perform as follows:

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

(a)

5.6 Test Acceptance Criteria

(a)

The EMI/RFI test acceptance criteria are as given below based on Appendix 7 of the Tricon Nuclear Qualification Program Master Test Plan (Reference 8.11), and EPRI TR-107330, Section 4.3.7 (Reference 8.1).

a) The Tricon Test Specimen shall meet allowable equipment emission limits as specified in EPRI TR-102323-R1 for the following MIL-STD-462D Test Methods:

CE101 – Conducted Emissions, 30 Hz to 50 kHz (Figure 7-1)
CE102 – Conducted Emissions, 50 kHz to 400 MHz (Figure 7-2)
RE101 – Radiated Emissions, 30 Hz to 100 kHz (Figure 7-3)
RE102 – Radiated Emissions, 10 kHz to 1 GHz (Figure 7-4)

b) The Tricon Test Specimen and Lambda field power supply shall operate as intended during and after application of the EMI/RFI test levels specified in EPRI TR-102323 for the following MIL-STD-462D and IEC Test Methods:

CS101 – Conducted Susceptibility, Audio Frequency, 30 Hz to 50 kHz
CS114 – Conducted Susceptibility, High Frequency, 50 kHz to 400 MHz
RS101 – Radiated Susceptibility, Magnetic Field, 30 Hz to 100 kHz
RS103 – Radiated Susceptibility, Electric Field, 10 kHz to 1 GHz
801-4 – Conducted Susceptibility, EFT Burst, 2.5 to 5 kHz, 3 Hz Burst Rep. Rate

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:

i.) The main processors and coprocessors shall continue to function.
ii.) The transfer of I/O data shall not be interrupted.
iii.) The emissions shall not cause the discrete I/O to change state.

iv.) Analog I/O levels shall not vary more than 3%.

6.0 TEST RESULTS

This section summarizes the results of EMI/RFI testing of the Tricon Test Specimen. The discussion of test results also includes disposition of performance or data anomalies which were observed or recorded during EMI/RFI testing.

6.1 Set-Up and Check-Out Testing

(a)

The check-out test results also demonstrated that the reconfigured test system was operating correctly with no indicated hardware faults or failures.

6.2 Radiated Magnetic Field Emissions from 30 Hz to 100 kHz (RE101)

(a)

The recorded magnetic field emissions data for the Tricon PLC are included in Wyle Laboratories Test Report No. 41339-2 (Appendix C). The data show that the Tricon PLC fully complies with the allowable equipment emissions level shown in Figure 7-3 of EPRI TR-102323-R1 (Reference 8.7).

6.3

6.4

n

(a)

6.5

(a)

6.6

(a)

6.7

(a)

(a)

6.8

(a)

(a)

6.9 High Frequency Conducted Susceptibility from 50 kHz to 400 MHz (CS114)

The susceptibility of the Tricon PLC to conducted EMI was tested over the frequency range of 50 kHz to 400 MHz. The test was conducted in accordance with the methodology defined

(a)

6.9.1

6.9.2

(a)

6.9.3

(a)

(a)

6.9.4

(a)

(a)

6.9.5

TRICONEX

Document:	7286-527	Title:	EMI/RFI TEST REPORT		
Revision:	0	Page:	28 of 44	Date:	05/12/00

(a)

(a)

(a)

(a)

6.9.6

(a)

(a)

6.9.7

(a)

(a)

6.9.8

(a)

6.10

(a)

6.11

7.0 CONCLUSIONS

7.1 Test Methodology

The following EMI/RFI tests were performed on the Tricon Test Specimen:

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

(a)

7.2 Emissions Testing

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

2. The Tricon Test Specimen does not fully comply with the allowable equipment emissions levels defined in Section 7 of EPRI TR-102323-R1 for the following emissions tests:

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

   Sections 6.3, 6.4 and 6.5, and Appendix C of this report provide a detailed description of the non-compliances in emissions which were measured during each of the tests listed above.

   An understanding of the electromagnetic emissions from a device is necessary to minimize the potential for the device to adversely affect the operation of other equipment that is physically located near the device, shares common electrical connections with it, or has wires or cables routed in close proximity to it. Therefore, prior to installing the Tricon PLC in a nuclear safety-related or non-safety related application, an evaluation of the device emission levels should be made to determine whether the emission levels are acceptable for the planned application, or if mitigating actions would be required. The Tricon PLC EMI/RFI emissions testing documented in this report provides the data required to perform such an evaluation. The Tricon PLC was tested without the benefit of a secondary enclosure, additional cable and wire shielding, or installed power line filtering. Mitigating actions to address the non-compliances in measured emission levels would likely incorporate these common in-plant installation features.

7.3 Susceptibility Testing

1. The Tricon PLC system successfully passed all of the EMI/RFI susceptibility tests listed in Section 7.1, subject to the two test level exceptions described in Section 7.1. The main processors and coprocessors continued to function correctly throughout testing. The transfer of input and output data was not interrupted. There were no interruptions or inconsistencies in the operation of the system or the software.

2. The Tricon Test Specimen input, output and communication modules fully comply with the as-tested radiated magnetic field (RS101) susceptibility thresholds shown in Figure 2-1 of Attachment 2 of this report. There were no interruptions in the transfer of input, output and communication data. There were no spurious changes in state of the

discrete inputs and outputs. The analog input and output levels did not vary by more than ±3% of the expected levels.

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

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

   Sections 6.7, 6.8, 6.9 and 6.10, and Appendix C of this report provide a detailed description of the module susceptibilities which were measured during each of the tests listed above, and the results of threshold testing which was performed. Module

(a)

An understanding of the electromagnetic susceptibility of a device is necessary to ensure that its operation will not be adversely affected by EMI/RFI levels already present or permitted in the area where the device will be located. Therefore, prior to installing the Tricon PLC in a nuclear safety-related application, an evaluation of the input, output and communication module susceptibilities should be performed. An evaluation of the module susceptibilities should also be performed for non-safety related applications if there is a potential for the PLC to impact plant reliability and availability. The Tricon PLC EMI/RFI susceptibility testing documented in this report provides the data required to perform such an evaluation.

To address the impact of the Tricon PLC input, output and communication module EMI/RFI susceptibilities for a specific plant application, one or more of the followi approaches may be pursued:

(a)

(a)

4. Table 6-1 in Attachment 6 of this report provides a summary table of the EMI/RFI susceptibility test results (Pass, Fail or Inconclusive) for each module installed in the Tricon Test Specimen. The purpose of the table is to identify a set of modules which demonstrated acceptable susceptibility performance at similar test levels. The CS114

(a)

7.4 Post-EMI/RFI Operability and Prudency Testing

The Operability and Prudency tests run at the completion of all qualification testing demonstrates acceptable system performance following EMI/RFI testing. Triconex Report No. 7286-530, Performance Proof Test Report (Reference 8.12), provides a detailed summary and comparison of all test results obtained from performance of the Operability and Prudency tests throughout the Tricon Qualification Effort.

8.0 REFERENCES

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

8.1 EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Final Report dated December, 1996

8.2 IEEE Standard 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

8.3 Triconex Drawing No. 7286-102, Sheet 1, Rev. 1 and Sheet 2, Rev. 0, Generic Qualification System General Equipment Arrangement

8.4 Triconex Document No. 7286-541, Nuclear Qualification of Tricon PLC System, System Description

8.5 Triconex Document No. 7286-540, Nuclear Qualification of Tricon PLC System, Master Configuration List (MCL)

8.6 IEEE Standard 1050-1989, Guide for Instrumentation and Control Equipment Grounding in Generating Stations

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

8.8 Military Standard MIL-STD-461D, dated January 1993, Electromagnetic Emission and Susceptibility Requirements for Control of Electromagnetic Interference

8.9 Military Standard MIL-STD-462D, dated January 1993, Measurement of Electromagnetic Interference Characteristics

8.10 International Electrotechnical Commission (IEC) Standard 801-4, dated 1991, Electrical Fast Transient/Burst Requirements

8.11 Triconex Document No. 7286-500, Nuclear Qualification of Tricon PLC System, Master Test Plan

8.12 Triconex Report No. 7286-530, Nuclear Qualification of Tricon PLC System, Performance Proof Test Report

9.0 ATTACHMENTS

Attachment 1: Example Plots of Tricon Test Specimen Normal Operating Performance Data

Attachment 2: RS101 Radiated Susceptibility Test, Plot of Comparison of Actual Test Levels to As-Required Test Levels

Attachment 3: RS103 Radiated Susceptibility Test, Plots of Data Evaluations and Module Susceptibility Thresholds

Attachment 4: CS114 Conducted Susceptibility Test, Summary Table of Module Susceptibilities

Attachment 5: CS114 Conducted Susceptibility Test, Composite Susceptibility Threshold Plots

Attachment 6: Summary Table of EMI/RFI Susceptibility Test Results

10.0 APPENDICES

Appendix A: Wyle Laboratories Test Procedure Number 46992-10, Test Procedure for Electromagnetic Interference (EMI) Testing on a Tricon PLC System

Appendix B: Completed Pre-EMI/RFI Test Run of Triconex Procedure No. 7286-502, System Set-Up and Check-Out Procedure

Appendix C: Wyle Laboratories Test Report Number 41339-2, Electromagnetic Interference (EMI) Test Report on a Tricon PLC System

Appendix D: Completed Triconex Procedure No. 7286-510, EMI/RFI Test Procedure

TRICONEX

Document:	7286-527	Title:	EMI/RFI TEST REPORT		
Revision:	0	Page:	Attachment 1	Date:	05/12/00

(a)

ATTACHMENT 1

(Page 1 of 30)

pages 2-30 deleted from non-proprietary version

This attachment includes an example of the Test Specimen normal operating performance data, which was

(a)

page 2 deleted from non-proprietary version

ATTACHMENT 2
(Page 1 of 2)

RS101 Radiated Susceptibility Test

Figure 2-1: Comparison of Actual Test Levels to As-Required Test Levels

ATTACHMENT 3
(Page 1 of 6)

(a)

pages 2-6 deleted from non-proprietary version

RS103 Radiated Susceptibility Test

Figure 3-1: Evaluation of Analog Input Module Model 3703E Performance

Figure 3-2: Established Susceptibility Threshold Plot for RTD Input Module Model 3700A

Figure 3-3: Established Susceptibility Threshold Plot for Thermocouple Input Module Model 3706A

Figure 3-4: Established Susceptibility Threshold Plot for Thermocouple Input Module Model 3708E

Figure 3-5: Established Susceptibility Threshold Plot for Analog Output Module Model 3805E

(a)

ATTACHMENT 4
(Page 1 of 12)

pages 2-12 deleted from non-proprietary version

CS114 Conducted Susceptibility Test

Table 4-1: Summary of Module Susceptibilities

TRICONEX

Document:	7286-527	Title:	EMI/RFI TEST REPORT		
Revision:	0	Page:	Attachment 5	Date:	05/12/00

(a)

ATTACHMENT 5
(Page 1 of 12)

pages 2-12 deleted from non-proprietary version

CS114 Conducted Susceptibility Test, Composite Susceptibility Threshold Plots

Figure 5-1: Susceptibility Threshold Plot for Communication Module Models 4329 and 4119A

Figure 5-2: Susceptibility Threshold Plot for ACM Communication Module Model 4609

Figure 5-3: Susceptibility Threshold Plot for RTD Input Module Model 3700A

Figure 5-4: Susceptibility Threshold Plot for 4 to 20 mA Analog Input Module Model 3703E

Figure 5-5: Susceptibility Threshold Plot for Thermocouple Input Module Model 3706A

Figure 5-6: Susceptibility Threshold Plot for Thermocouple Input Module Model 3708E

Figure 5-7: Susceptibility Threshold Plot for 24 VDC Digital Input Module Model 3503E

Figure 5-8: Susceptibility Threshold Plot for:

120 VDC Digital Output Module Model 3604E
48 VDC Digital Output Module Model 3607E
115 VAC Digital Output Module Model 3601E
115 VAC Digital Output Module Model 3611E
48 VDC Digital Input Module Model 3502E
120 VAC Relay Output Module Model 3636R
24 VDC Digital Input Module Model 3504E
115 VAC Digital Input Module Model 3501E

Figure 5-9: Susceptibility Threshold Plot for 24 VDC Digital Output Module Model 3624 and 0 to 10 V Analog Input Module Model 3701

Figure 5-10: Susceptibility Threshold Plot for 120 VDC Digital Output Module Model 3623 and 24 VDC Digital Input Module Model 3505E

Figure 5-11: Susceptibility Threshold Plot for 120 VDC Digital Output Module Model 3603E

ATTACHMENT 6
(Page 1 of 2)

(a)

page 2 deleted from non-proprietary version

EMI/RFI Susceptibility Test Results

Table 6-1: Summary Table of EMI/RFI Susceptibility Test Results

TRICONEX

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

SEISMIC TEST REPORT

Report No.: 7286-526

Revision 0

February 25, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Randolph Trench	[signature]	Engineer
Approvals:	Mitchell Albers	[signature]	Project Manager
	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

Document Change History			
Revision	**Date**	**Change**	**Author**
0	02/25/00	Initial Issue	R. Trench

TABLE OF CONTENTS

1.0 PURPOSE

The purpose of this test report is to summarize the results of seismic testing of the Triconex Tricon PLC to meet the requirements of EPRI TR-107330 (Reference 8.6). The format of this report conforms to Section 8.3.(7) of IEEE Specification 323-1983 (Reference 8.2). Conclusions from the testing are provided in Section 7.0, including the seismic withstand response spectrum determined from the testing. This response spectrum will also be included in the Final Summary Report Application Guide.

The following documents are included as appendices to this test report:

Appendix A: Wyle Laboratories Test Report Number 41339-1. This report documents the activities of Wyle Laboratories personnel in performing seismic testing of the Tricon Test Specimen.

Appendix B: Completed Pre-Seismic Run of Triconex Procedure No. 7286-502, "System Set-Up and Check-Out Procedure". This completed procedure documents activities performed by Triconex and Wyle personnel in setting up the Tricon Test Specimen for seismic testing and verifying proper system operation prior to testing.

Appendix C: Completed Triconex Procedure No. 7286-507, "Seismic Test Procedure". This completed procedure documents the activities performed by Triconex personnel in performing seismic testing of the Tricon Test Specimen, including performance monitoring during testing and evaluation of acceptable test results on completion of testing.

Appendix D: Completed Post-Seismic Run of Triconex Procedure No. 7286-503, "Operability Test Procedure". This completed procedure documents the performance and results of post-seismic operability testing of the Tricon Test Specimen, including evaluation of acceptable test results.

Appendix E: Completed Post-Seismic Run of Triconex Procedure No. 7286-504, "Prudency Test Procedure". This completed procedure documents the performance and results of post-seismic prudency testing of the Tricon Test Specimen, including evaluation of acceptable test results.

2.0 TEST OBJECTIVE

The objective of seismic testing is to demonstrate the suitability of the Triconex Tricon PLC for qualification as a Category 1 seismic device based on seismic withstand type testing performed on the Tricon Test Specimen. The testing also demonstrates similar suitability of a third party field power supply (a included in the tested equipment. (b)

3.0 DESCRIPTION OF TEST SPECIMEN

The equipment tested consists of four Tricon PLC chassis populated with selected input, output, communication, chassis interface and chassis power supply modules. The tested equipment also includes external termination assemblies (ETA's) provided for connection of field wiring to the Tricon input and output modules, and two third party field power supplies. Triconex Drawing 7286-102 (Reference 8.4) shows the general arrangement and interconnection of the Tricon Test Specimen chassis. Project document 7286-541 (Reference 8.3) 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 8.1).

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 completed Seismic Test procedure (Appendix C) identifies the TSAP revision used during seismic testing. The Master Configuration List identifies the revision level of all test specimen firmware.

4.0 TEST SET-UP AND INSTRUMENTATION

The following sections describe the set-up of the Tricon Test Specimen and field power supplies during seismic testing, and the instrumentation used to monitor the applied seismic test conditions and the Tricon Test Specimen and field power supply performance during and after testing. The system set-up is documented in Appendix B. Specifications for test instrumentation supplied by Wyle Laboratories are included in Appendix A. Specifications for test instrumentation supplied by Triconex are included in Appendices B, C, D and E.

4.1 Test Specimen Mounting

Seismic testing was performed on the Triaxial Seismic Simulator Table at Wyle Laboratories in Huntsville, Alabama. The Tricon Test Specimen and third party field power supplies were mounted to the seismic test table in accordance with mounting details provided on Triconex Drawing No. 7286-101, "Generic Qualification System Equipment Mounting Details," (Reference 8.5). A copy of this drawing is included as Attachment 1 to this report. 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 assembly (ETA) mounting plates, and manufacturer supplied field power supply mounting plates.

Each Tricon Test Specimen chassis was installed in a separate simulated 19" rack mount section, which was then rigidly fastened to the seismic test table. The ETA's were mounted

(a)

[redacted]

(a)

Each simulated rack mount section was installed on the Wyle seismic table such that its horizontal axes were collinear with the horizontal shake axes of the table. All fastener torque values indicated on Triconex Drawing 7286-101 were verified by Wyle personnel prior to (or following) testing using calibrated hand tools. Torque verifications are documented in Appendices A and C of this test report.

4.2 Test Specimen Chassis and Module Configuration

(a)

[redacted] configurations for seismic testing are documented in the project Master Configuration List.

4.3 Test Specimen Power Supply Configuration

EPRI TR-107330, Section 6.3.4.2, requires that seismic testing be performed with the power sources to the test PLC power supply modules set to operate at the following minimum AC and DC source voltages and frequencies given in Section 4.6.1.1 of the EPRI TR:

(a) Power supply modules fed from AC sources shall remain operable at a minimum source voltage of 90 VAC and a minimum source frequency of 57 Hz.

(b) Power supply modules fed from DC sources shall remain operable at a minimum source voltage of 20.4 VDC.

During seismic testing, the AC and DC power sources to the Tricon Test Specimen chassis power supplies were set as follows:

(a)

(a) [redacted]

(b)

(c)

(a)

4.4 Wyle Instrumentation

Instrumentation supplied by Wyle Laboratories for seismic testing included control and response accelerometers with associated signal conditioning and data recording hardware,

(a)

4.5 Triconex Instrumentation

During seismic testing, operation of the Tricon Test Specimen was monitored and recorded

(a)

similar detailed information on the various signal simulation and measurement instruments used during post-seismic Operability and Prudency testing.

4.6 Instrument Calibration

All tests were performed using calibrated test instruments. Calibration certifications are held by Wyle Laboratories and Triconex. Appendices A through E document the calibration status of the test instrumentation used.

5.0 TEST PROCEDURE

Seismic testing was performed to the requirements of EPRI TR-107330 (Reference 8.6), which invokes IEEE Standard 344-1987 (Reference 8.7). The following sections describe the approach to satisfying the requirements of the referenced documents during seismic testing of the Tricon Test Specimen. The test procedure used by Wyle Laboratories to perform seismic testing of the Tricon Test Specimen is included in the Wyle Seismic Test Report, Appendix A. The completed procedures used by Triconex to perform seismic testing are included as Appendices B and C. The completed procedures used by Triconex to perform post-seismic Operability and Prudency testing are included as Appendices D and E.

5.1 Test Sequence

Figure 2 of the project Master Test Plan (Reference 8.8) shows the sequence of qualification testing performed on the Tricon Test Specimen. In accordance with requirements for sequential exposure of the test specimen to various aging factors, seismic testing was performed after environmental testing.

5.2 Test Method

Seismic testing was performed to the requirements of IEEE 344-1987 and included the following tests:

(a)

(a)

(b)

[redacted]

(a)

5.3 Test Levels

EPRI TR-107330, Section 4.3.9, requires that the test PLC meet its performance requirements during and following the application of 5 OBE's and one SSE to the levels shown in Figure 4-5 of TR-107330. The maximum SSE and OBE levels shown in Figure 4-5 are 14 g's and 9.8 g's respectively, based on 5% damping.

Seismic testing of the Tricon Test Specimen and field power supplies was performed using [redacted] documented in the Final Summary Report Application Guide prepared as part of the qualification effort. *(a)*

5.4 Test Specimen Operation

EPRI TR-107330, Section 6.3.4.2, requires that the test PLC be powered with its TSAP operating during seismic testing, 1/2 of its solid-state discrete outputs shall be ON and loaded to their rated current, 1/2 of its relay outputs shall be ON, and 1/2 of its relay outputs shall be 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. *(a)*

[redacted]

[redacted]

(a)

5.5 Test Specimen Performance Monitoring

EPRI TR-107330, Section 4.3.9, requires that the test PLC operate as intended during and following the application of an SSE, that all connections and parts remain intact and in-place, and that relay output contacts not chatter.

During seismic testing, operation of the Tricon Test Specimen was monitored and recorded [redacted] figures which show the normal performance of the data points which were monitored during seismic testing (during and after each OBE and SSE). The data was monitored for deviations or trends from the normal performance shown in the figures. (a)

During seismic testing, the output of the Lambda field power supply was monitored by a [redacted]

(a)

5.6 Test Acceptance Criteria

The seismic test acceptance criteria are as given below. These criteria were developed based on EPRI TR-107330, Section 4.3.9 (Reference 8.6), and Appendix 5 of the Tricon Nuclear Qualification Program Master Test Plan (Reference 8.8).

(a) 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.

(b) 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.

(c) The operation of the Model 3636R electromechanical relay output module installed in the Tricon Test Specimen shall be monitored during application of the OBE and SSE vibrations. The relay contacts shall be demonstrated to change state from energized to de-energized and de-energized to energized in accordance with execution of the application program running in the Tricon Test Specimen during testing. Any spurious change of state of the relay contacts shall not exceed 2 milliseconds in duration for both energized and de-energized contact states.

(d) The Tricon Test Specimen shall pass the Operability Test, as implemented by Reference 8.9, following completion of the seismic testing.

6.0 TEST RESULTS

This section summarizes the results of seismic testing of the Tricon Test Specimen and field power supplies. This section also dispositions performance or data anomalies which were observed or recorded during seismic testing.

6.1 Pre-Seismic Test Set-Up and Check-Out Testing

This testing directs set-up of the Tricon Test Specimen and field power supplies for seismic testing and verification of proper system operation prior to testing. Results of the testing are documented in the completed System Set-Up and Check-Out Test Procedure (7286-502)

(a)

6.2 Seismic Testing

(a)

Seismic testing of the Tricon Test Specimen was performed in accordance with Triconex Test Procedure 7286-507, “Seismic Test Procedure”, and Wyle Test Procedure 46992-20, “Test Procedure for Environmental and Seismic Testing of a Four Chassis Tricon Industrial

(a)

Appendix C includes the completed Triconex Seismic Test Procedure. Appendix A includes the Wyle Seismic Test Procedure. Results of the testing are summarized below.

6.3 Resonance Search Tests

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

Response accelerometer output data provided in Appendix A shows the following results from the resonance search testing:

(a)

(a)

(b)

(c)

(a)

These test results are used in the evaluation of the OBE and SSE test results as described in the next section.

6.4 OBE and SSE Seismic Tests

6.4.1 **Test Response Spectrum Description.** EPRI TR-107330, Section 4.3.9 requires the SSE test to be preceded by five OBE tests. Each OBE required response spectrum (RRS) has a peak acceleration of 9.8 g's at 5% damping. The SSE RRS has a peak acceleration of 14 g's at 5% damping. The TR-107330 OBE and SSE RRS's are shown in Figure 6-1 of this report.

(a)

(a)

6.4.2

(a)

[redacted]

(a)

6.5 Test Specimen Performance Monitoring

The Tricon Test Specimen and field power supply performance were monitored at the start

[redacted]

(a)

6.6 Test Specimen Condition Monitoring

(a)

6.7 Post-Seismic Operability and Prudency Tests

EPRI TR-107330, Section 6.3.4.3, requires post-seismic Operability Testing to assess the impact of exposure to the OBE and SSE vibrations on the operability of the Tricon Test Specimen. Appendix D documents performance of the post-seismic Operability Test, and provides analysis of the test data and test results. A post-seismic Prudency Test was also performed as part of the Tricon Qualification Project. Appendix E documents performance of the post-seismic Prudency Test, and provides analysis of the test data and test results. The

(a)

6.8

(b)

(a)

(c)

(d)

(a)

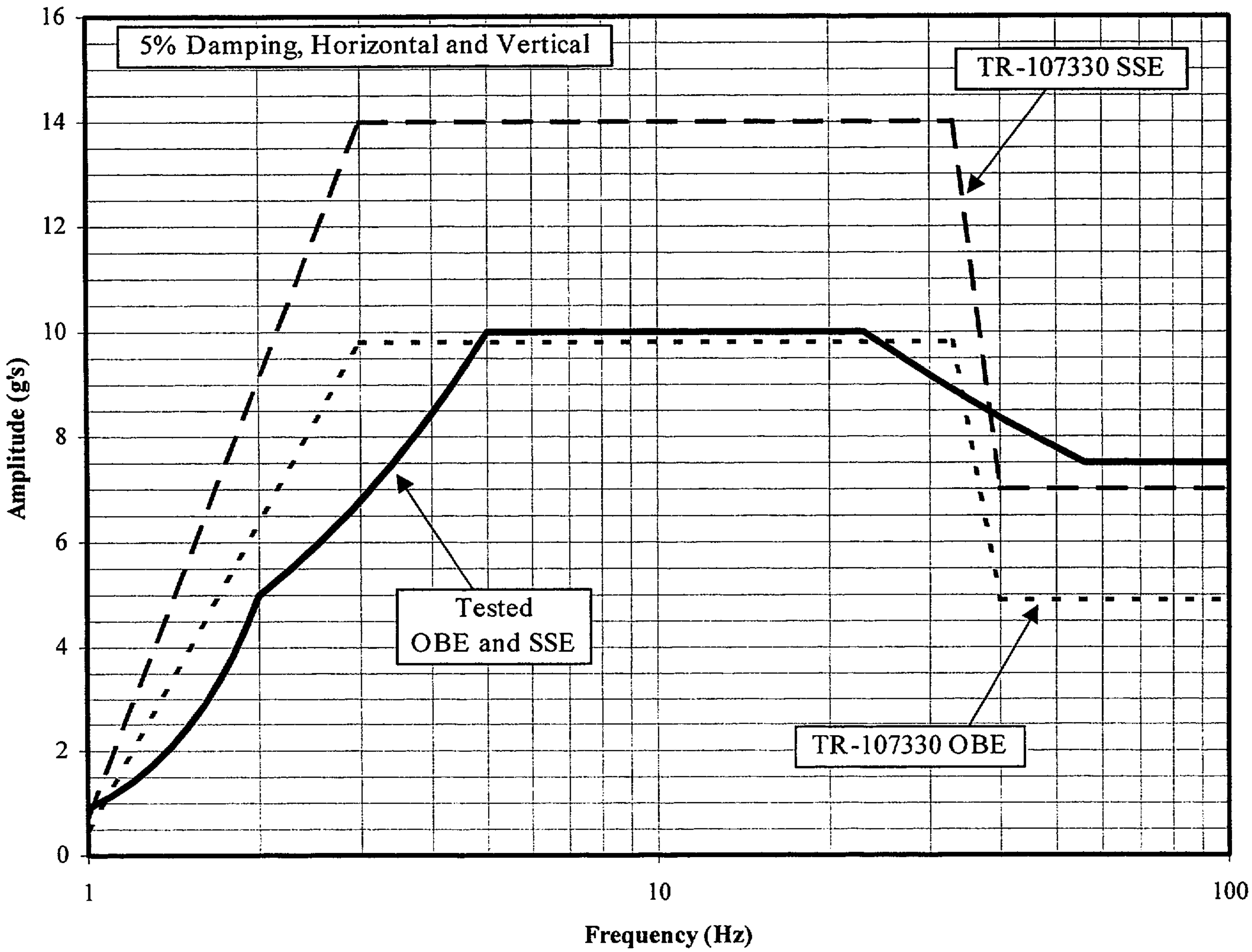


Figure 6-1. Comparison of Seismic Test Levels to EPRI TR-107330 Requirements

7.0 CONCLUSIONS

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 is suitable for qualification as a Category 1 seismic device. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List (Reference 8.1).

4. The seismic test results demonstrate that the Lambd[redacted] (b) supply is suitable for qualification as a Category 1 seismic device.

5. 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 7-1. The figure is based on a damping value of 5% used in the data analysis.

6. The seismic test results demonstrate that the equipment mounting configurations shown in Triconex Drawing No. 7286-101 (included as Attachment 1 of this report) are adequate to support seismic qualification of the Tricon PLC and the Lambda [redacted] (b)

7. The seismic test results demonstrate that the mounting configuration used for the [redacted] (b) (b) [redacted]ipply does not support qualification of the power supply to the same seismic withstand response spectrum as the Tricon PLC. Seismic testing at reduced levels was not performed to establish a lower withstand response spectrum for the [redacted] (b) ower supply.

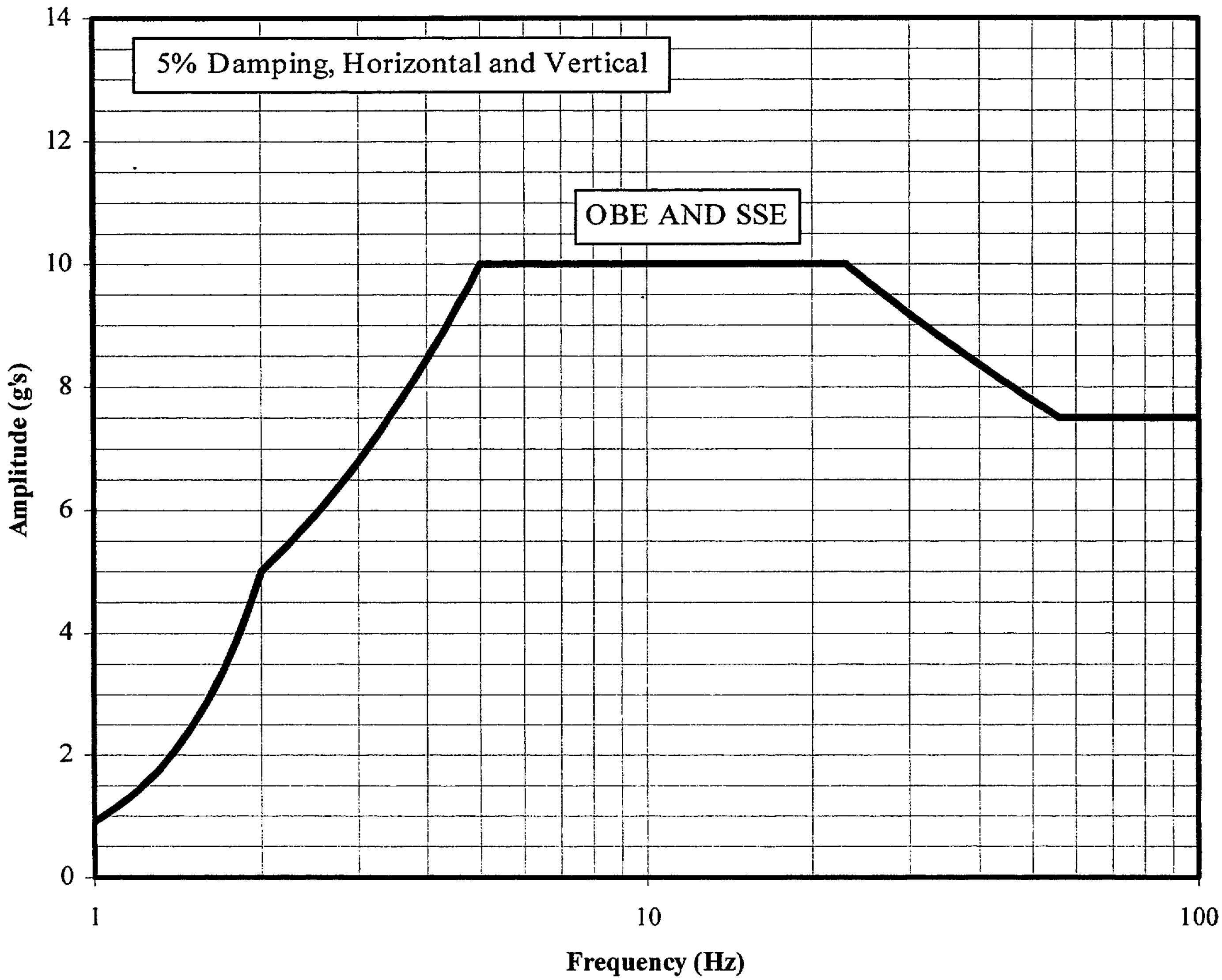


Figure 7-1. Seismic Withstand Response Spectrum

8.0 REFERENCES

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

8.1 Triconex Document No. 7286-540, Nuclear Qualification of Tricon PLC System, Master Configuration List (MCL)

8.2 IEEE Standard 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

8.3 Triconex Document No. 7286-541, Nuclear Qualification of Tricon PLC System, System Description

8.4 Triconex Drawing No. 7286-102, Sheet 1, Rev. 1 and Sheet 2, Rev. 0, Generic Qualification System General Equipment Arrangement

8.5 Triconex Drawing No. 7286-101, Sheet 1, Rev. 2 and Sheet 2, Rev. 1, Generic Qualification System Equipment Mounting Details

8.6 EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Final Report dated December, 1996

8.7 IEEE Standard 344-1987, Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

8.8 Triconex Document No. 7286-500, Nuclear Qualification of Tricon PLC System, Master Test Plan

8.9 Triconex Procedure No. 7286-503, Rev. 2, Nuclear Qualification of Tricon PLC System, Operability Test Procedure

9.0 ATTACHMENTS

Attachment 1: Triconex Drawing No. 7286-101, Sheet 1, Rev. 2 and Sheet 2, Rev. 1, Generic Qualification System Equipment Mounting Details (2 pages)

Attachment 2: Example Plots of Tricon Test Specimen Normal Operating Performance Data

10.0 APPENDICES

Appendix A: Wyle Laboratories Test Report Number 41339-1, Environmental Stress Test and Seismic Simulation Test Program on a Four Chassis Industrial Controller

Appendix B: Completed Pre-Seismic Run of Triconex Procedure No. 7286-502, System Set-Up and Check-Out Procedure

Appendix C: Completed Triconex Procedure No. 7286-507, Seismic Test Procedure

Appendix D: Completed Post-Seismic Run of Triconex Procedure No. 7286-503, Operability Test Procedure

Appendix E: Completed Post-Seismic Run of Triconex Procedure No. 7286-504, Prudency Test Procedure

ATTACHMENT 1

(a)

(Page 1 of 3)

pages 2, 3, deleted from non-proprietary version

Page 2: Triconex Drawing No. 7286-101, Sheet 1, Rev. 2, Generic Qualification System Equipment Mounting Details

Page 3: Triconex Drawing No. 7286-101, Sheet 2, Rev. 1, Generic Qualification System Equipment Mounting Details

(a)

ATTACHMENT 2

(Page 1 of 37)

pages 2-37 deleted from non-proprietary version

This attachment includes an example of the Tricon Test Specimen normal operating performance data [redacted]

TRICONEX

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

ENVIRONMENTAL TEST REPORT

Report No.: 7286-525

Revision 0

March 16, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Randolph Trench	[signature]	Engineer
Approvals:	Mitchell Albers	[signature]	Project Manager
	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

TRICONEX

Document Change History			
Revision	Date	Change	Author
0	03/16/00	Initial Issue	R. Trench

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

Section

10.0 APPENDICES (continued)

1.0 PURPOSE

The purpose of this test report is to summarize the results of environmental testing of the Triconex Tricon PLC to meet the requirements of EPRI TR-107330 (Reference 8.6), Section 6.3.3. The format of this report conforms to Section 8.3.(7) of IEEE Specification 323-1983 (Reference 8.2). Conclusions from the testing are provided in Section 7.0.

The following documents are included as appendices to this test report:

Appendix A: Wyle Laboratories Test Report Number 41339-1. This report documents the activities of Wyle Laboratories personnel in performing environmental testing of the Tricon Test Specimen.

Appendix B: Completed Pre-Environmental Test Run of Triconex Procedure No. 7286-502, "System Set-Up and Check-Out Procedure". This completed procedure documents activities performed by Triconex and Wyle personnel in setting up the Tricon Test Specimen for environmental testing and verifying proper system operation prior to testing.

Appendix C: Completed Triconex Procedure No. 7286-506, "Environmental Test Procedure". This completed procedure documents the activities of Triconex personnel in performing environmental testing of the Tricon Test Specimen, including performance monitoring during testing and evaluation of acceptable test results on completion of testing.

Appendix D: Completed Environmental-High Temperature Run of Triconex Procedure No. 7286-503, "Operability Test Procedure". This completed procedure documents the performance and results of operability testing of the Tricon Test Specimen during the high temperature phase of environmental testing. The completed procedure includes evaluation of acceptable test results.

Appendix E: Completed Environmental-High Temperature Run of Triconex Procedure No. 7286-504, "Prudency Test Procedure". This completed procedure documents the performance and results of prudency testing of the Tricon Test Specimen during the high temperature phase of environmental testing. The completed procedure includes evaluation of acceptable test results.

Appendix F: Completed Environmental-Low Temperature Run of Triconex Procedure No. 7286-503, "Operability Test Procedure". This completed procedure documents the performance and results of operability testing of the Tricon Test Specimen during the low temperature phase of environmental testing. The completed procedure includes evaluation of acceptable test results.

Appendix G: Completed Environmental-Ambient Temperature Run of Triconex Procedure No. 7286-503, "Operability Test Procedure". This completed procedure documents the performance and results of operability testing of the Tricon Test Specimen during the final ambient temperature phase of environmental testing. The completed procedure includes evaluation of acceptable test results.

2.0 TEST OBJECTIVE

The objective of environmental testing is to demonstrate that the Triconex Tricon PLC will not experience failures due to abnormal service conditions of temperature and humidity. Environmental testing also demonstrates similar performance of a third party field power supply (a Lambda [illegible] ncluded in the tested equipment.

(b)

3.0 DESCRIPTION OF TEST SPECIMEN

The equipment tested consists of four Tricon PLC chassis populated with selected input, output, communication, chassis interface and chassis power supply modules. The tested equipment also includes external termination assemblies (ETA's) provided for connection of field wiring to the Tricon input and output modules, and a Lambda field power supply. Triconex Drawing 7286-102 (Reference 8.11) shows the general arrangement and interconnection of the Tricon Test Specimen chassis. Project document 7286-541 (Reference 8.3) 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 8.1).

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 completed Environmental Test procedure (Appendix C) identifies the TSAP revision used during this testing. The Master Configuration List identifies the revision level of all test specimen firmware.

4.0 TEST SET-UP AND INSTRUMENTATION

The following sections describe the set-up of the Tricon Test Specimen and Lambda field power supply during environmental testing, and the instrumentation used to monitor the applied environmental test conditions and the Tricon Test Specimen and Lambda field power supply performance during testing. The system set-up is documented in Appendix B. Specifications for test instrumentation supplied by Wyle Laboratories are included in Appendix A. Specifications for test instrumentation supplied by Triconex are included in Appendices B through G.

4.1 Test Specimen Mounting

EPRI TR-107330, Section 6.3.3.1 requires that the test PLC be mounted on a simple structure that does not enclose the test specimen chassis. No additional cooling fans shall be included in the test chamber.

The Tricon Test Specimen and Lambda field power supply were installed in the Wyle Laboratories environmental test chamber in Huntsville, Alabama. The tested equipment was

(a)

No additional cooling fans were included in the test chamber. All other test system equipment was located outside the environmental test chamber.

4.2 Test Specimen Chassis and Module Configuration

Section 3.0 above describes the general arrangement of the Tricon Test Specimen which was maintained throughout all of the qualification testing. Chassis configurations for environmental testing are documented in the project Master Configuration List. EPRI TR-107330, Section 6.2.1.1 requires that the modules be arranged to simulate the maximum expected temperature rise across the chassis for any reasonable arrangement of modules

(a)

4.3 Test Specimen Power Supply Configuration

EPRI TR-107330, Section 6.3.3, requires that environmental testing be performed with the PLC power supply sources set to values that maximize heat dissipation in the test PLC. During environmental testing, the AC and DC power sources to the Tricon Test Specimen chassis power supply modules were set as follows:

(a)

4.4 Wyle Instrumentation

Instrumentation supplied by Wyle Laboratories for environmental testing included temperature and relative humidity measurement devices. The test chamber ambient temperature and relative humidity were recorded throughout the duration of the environmental test on a dual-pen circular chart recorder. Chamber humidity was monitored and recorded using the wet bulb/dry bulb method. In accordance with EPRI TR-107330, Section 6.3.3.1 (for PLC's that use natural circulation cooling), air temperature was monitored and recorded at the bottom of each Tricon Test Specimen chassis. Air temperature was also monitored and recorded at the Lambda field power supply.

4.5 Triconex Instrumentation

During environmental testing, operation of the Tricon Test Specimen was monitored and

(a)

4.6 Instrument Calibration

All tests were performed using calibrated test instruments. Calibration certifications are held by Wyle Laboratories and Triconex. Appendices A through G document the calibration status of the test instrumentation used.

5.0 TEST PROCEDURE

Environmental testing of the Tricon Test Specimen and Lambda field power supply was performed to the specific requirements of EPRI TR-107330, Sections 4.3.6 and 6.3.3, and the general requirements of IEEE 381-1977, "Standard Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations," (Reference 8.7). The following sections describe the approach to satisfying the requirements of the referenced documents during environmental testing of the Tricon Test Specimen. The test procedure used by Wyle Laboratories to perform environmental testing of the Tricon Test Specimen is included in the Wyle Environmental Test Report, Appendix A. The completed procedures used by Triconex to perform environmental testing are included as Appendices B and C. The completed procedures used by Triconex to perform Operability and Prudency testing during environmental testing are included as Appendices D through G.

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. Triconex Report No. 7286-533 (Reference 8.5) provides an evaluation of the withstand capability of the Tricon PLC to a radiation exposure of 1000 rads. The evaluation concludes that an exposure of 1000 rads will not prevent the Tricon PLC from performing its safety-related function.

5.1 Test Sequence

Figure 2 of the project Master Test Plan (Reference 8.8) shows the sequence of qualification testing performed on the Tricon Test Specimen. In accordance with requirements for

(b)

5.2 Test Method

Environmental testing of the Tricon Test Specimen and Lambda field power supply was performed using the Wyle Laboratories environmental test chamber. Inside the test chamber, the equipment was subjected to abnormal environmental conditions which simulate minimum and maximum extremes of temperature and air moisture content that could be experienced by the equipment during and after an accident condition in a nuclear power plant. The abnormal environmental conditions were applied to the Tricon Test Specimen in accordance with a time varying profile which included ramp-ups, ramp-downs and hold periods of temperature and humidity, eventually returning to ambient conditions. In accordance with TR-107330 and IEEE-381, Test Specimen performance was monitored throughout the test period, and detailed operability tests were performed after each hold period at high temperature, low temperature and return to ambient temperature.

5.3 Test Levels

EPRI TR-107330, Section 4.3.6.2, requires that the generic PLC meet its performance requirements over abnormal environmental conditions of 40°F to 120°F and 10% to 95% relative humidity (non-condensing). EPRI TR-107330, Section 4.3.6.3, requires that the test PLC operate for the environmental (temperature and humidity) withstand profile given in Figure 4-4 of the TR. The profile includes a beginning ramp-up period (unspecified in duration) from ambient to 140°F and 90% relative humidity (non-condensing). These conditions are held for 48 hours minimum, after which the Operability and Prudency tests are run. Conditions are then ramped down over a four hour minimum period to 40°F and

5% relative humidity. These conditions are held for 8 hours minimum, after which a second Operability test is run. Conditions are then ramped up over a four hour minimum period to ambient temperature and relative humidity. The equipment is stabilized at ambient conditions, after which a final Operability test is run. Section 6.3.3 of TR-107330 requires that environmental testing be performed with margins of 5°F and 5% applied to the temperature and humidity values given above.

The three sections of the EPRI TR described above present inconsistent maximum and minimum conditions of temperature and humidity for environmental testing. Based on discussions with the EPRI Working Group (B. Sotos), the EPRI TR-107330 Figure 4-4 profile was specified for environmental testing of the Tricon PLC with maximum temperature and relative humidity conditions of 140°F and 95%, and minimum temperature and relative humidity conditions of 35°F and 5%. These conditions include the required test margin of 5°F and 5% relative humidity, and consider the Tricon hardware temperature rating of 140°F.

Figure 7-1 of this report shows the environmental test profile which was achieved in the Wyle Laboratories environmental test chamber.

5.4 Test Specimen Operation

EPRI TR-107330, Section 6.3.3, requires that the test PLC 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.

(a)

5.5 Test Specimen Performance Monitoring

(a)

EPRI TR-107330, Section 4.3.6.3, requires that the test PLC operate as intended during and following exposure to the temperature and humidity profile given in Figure 4-4 of TR-107330.

(a)

5.6 Test Acceptance Criteria

The environmental test acceptance criteria are as given below. These criteria were developed based on EPRI TR-107330, Section 4.3.6 and Appendix 4 of the Tricon Nuclear Qualification Program Master Test Plan (Reference 8.8).

(a) The Tricon Test Specimen shall operate as intended during and after exposure to abnormal environmental test conditions. Evaluation of normal operating performance data (inputs, outputs and diagnostic indicators) collected during testing shall demonstrate operation as intended.

(b) The Tricon Test Specimen shall pass the Operability Test, as implemented by Reference 8.9, at the following times during and after the environmental test:

- Following at least 48 hours of operation at 140°F and 95% relative humidity (non-condensing).
- Following at least 8 hours of operation at 35°F and 5% relative humidity.

- Upon completion of the environmental test and after 2 hours minimum stabilization time at ambient conditions.

(c) The Tricon Test Specimen shall pass the Prudency Test, as implemented by Reference 8.6, following at least 48 hours of operation at 140°F and 95% relative humidity.

6.0 TEST RESULTS

This section summarizes the results of environmental testing of the Tricon Test Specimen and Lambda field power supply. This section also dispositions performance or data anomalies which were observed or recorded during the testing.

6.1 Pre-Environmental Test Set-Up and Check-Out Testing

This testing directs set-up of the Tricon Test Specimen and Lambda field power supply for environmental testing and verification of proper system operation prior to testing. Results of the testing are documented in the completed Pre-Environmental Test System Set-Up and Check-Out Test Procedure (No. 7286-502) included as Appendix B. Results of the testing showed that the system was set-up and operating correctly.

6.2 Environmental Testing

Environmental testing of the Tricon Test Specimen was performed in accordance with Triconex Test Procedure 7286-506, "Environmental Test Procedure," (Reference 8.4), and Wyle Test Procedure 46992-20, "Test Procedure for Environmental and Seismic Testing of a Four Chassis Tricon Industrial Controller," (included as an attachment to Appendix A).

The Environmental Test sequence is outlined below:

- Test Specimen and Lambda field power supply installation in the Wyle Laboratories environmental test chamber, and stabilization at ambient temperature and relative humidity conditions.

(a)

(a)

Figure 7-1 shows the above Environmental Test sequence. The test sequence and conditions shown in Figure 7-1 satisfy the sequence and conditions required by Figure 4-4 of EPRI TR-107330 with the following exception:

(a)

6.3 Test Specimen Performance Monitoring

During environmental testing, the Tricon Test Specimen was operating in accordance with execution of the Test Specimen Application Program (TSAP). The Test Specimen performance was monitored continually throughout the test period (except during Operability and Prudency test periods). This included recording of all monitored input and

(a)

The periodic data reviews show that the Tricon Test Specimen operated as intended throughout environmental testing. The completed data sheets record a number of module diagnostic messages which were indicated at the Tristation Console during testing. Attachment 2 of this report provides a tabular summary of the diagnostic messages recorded during testing, including which modules were indicated, identification of the diagnostic, when the diagnostic was received during testing, and when the diagnostic was cleared (or the module replaced) during testing. Section 6.5 provides an evaluation and disposition of each diagnostic received during testing. The evaluations conclude that not all diagnostics were indications of Test Specimen hardware faults, and that any actual hardware faults did not affect the expected operation of the Tricon, which is consistent with the fault tolerant design of the Tricon PLC.

(a)

6.4 Environmental Test Operability and Prudency Tests

EPRI TR-107330, Section 5.5, requires Operability and Prudency testing during environmental testing to assess the impact of exposure to the abnormal environmental conditions on the operability of the Tricon Test Specimen. In accordance with TR-107330, Operability and Prudency testing was performed at the following times:

- After the high temperature hold period (Operability and Prudency)
- After the low temperature hold period (Operability only)
- After return to ambient temperature (Operability only).

Appendices D through G document performance of Operability and Prudency tests at these times, and provide analyses of the test data and test results. Review of the test results shows

(a)

6.5 Test Anomalies

The following operational or performance anomalies were observed during environmental testing:

(a)

(a)

(a)

(a)

(a)

f

n

e

e

e

(a)

7.0 CONCLUSIONS

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 and Triconex field experience, 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 Triconex Tricon PLC will not experience failures due to abnormal service conditions of temperature and humidity. The specific Tricon hardware which was tested (chassis, power supplies, modules, external termination assemblies and interconnecting cabling) is identified in the project Master Configuration List (Reference 8.1).

(b)

5. The environmental test results demonstrate that the Lambda [redacted] power supply will not experience failures due to abnormal service conditions of temperature and humidity.

6. The temperature and humidity profile applied during environmental qualification testing of the Tricon PLC and Lambda field power supply is shown in Figure 7-1.

8.0 REFERENCES

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

8.1 Triconex Document No. 7286-540, Nuclear Qualification of Tricon PLC System, Master Configuration List (MCL)

8.2 IEEE Standard 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

8.3 Triconex Document No. 7286-541, Nuclear Qualification of Tricon PLC System, System Description

8.4 Triconex Procedure No. 7286-506, Rev. 0, Nuclear Qualification of Tricon PLC System, Environmental Test Procedure

8.5 Triconex Report No. 7286-533, Nuclear Qualification of Tricon PLC System, Radiation Hardness Evaluation

8.6 EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Final Report dated December, 1996

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

8.8 Triconex Document No. 7286-500, Nuclear Qualification of Tricon PLC System, Master Test Plan

8.9 Triconex Procedure No. 7286-503, Rev. 2, Nuclear Qualification of Tricon PLC System, Operability Test Procedure

8.10 Triconex Procedure No. 7286-504, Rev. 2, Nuclear Qualification of Tricon PLC System, Prudency Test Procedure

8.11 Triconex Drawing No. 7286-102, Sheet 1, Rev. 1 and Sheet 2, Rev.0, Generic Qualification System General Equipment Arrangement

9.0 ATTACHMENTS

Attachment 1: Example Plots of Tricon Test Specimen Normal Operating Performance Data

Attachment 2: Summary of Module Diagnostic Messages Recorded During Environmental Testing

10.0 APPENDICES

Appendix A: Wyle Laboratories Test Report Number 41339-1, Environmental Stress Test and Seismic Simulation Test Program on a Four Chassis Industrial Controller

Appendix B: Completed Pre-Environmental Test Run of Triconex Procedure No. 7286-502, System Set-Up and Check-Out Procedure

Appendix C: Completed Triconex Procedure No. 7286-506, Environmental Test Procedure

Appendix D: Completed Environmental-High Temperature Run of Triconex Procedure No. 7286-503, Operability Test Procedure

Appendix E: Completed Environmental-High Temperature Run of Triconex Procedure No. 7286-504, Prudency Test Procedure

Appendix F: Completed Environmental-Low Temperature Run of Triconex Procedure No. 7286-503, Operability Test Procedure

Appendix G: Completed Environmental-Ambient Temperature Run of Triconex Procedure No. 7286-503, Operability Test Procedure

TRICONEX

Document:	7286-525	Title:	ENVIRONMENTAL TEST REPORT		
Revision:	0	Page:	Attachment 1	Date:	03/16/00

(a)

ATTACHMENT 1

(Page 1 of 30)

(pages 2-30 deleted in non-proprietary version)

This attachment includes an example of the Tricon Test Specimen normal operating performance data which was monitored during environmental testing. The data was automatically recorded during testing by

(a)

ATTACHMENT 2

(Page 1 of 2)

Summary of Module Diagnostic Messages Recorded During Environmental Testing

SUMMARY OF MODULE DIAGNOSTIC MESSAGES RECORDED DURING ENVIRONMENTAL TESTING

TRICONEX

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

PRE-QUALIFICATION TEST REPORT

Document No.: 7286-524

Revision 0

June 9, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Troy Martel	Troy Martel	Triconex Project Director
Reviewer	Keith Adams	Keith D. Adams	Engineer
Approvals:	Mitchell Albers	Mitchell Albers	Project Manager
	Aad Faber	Aad Faber 6/16/2000	Director, Product Assurance

Document Change History			
Revision	**Date**	**Change**	**Author**
0	06/09/00	Initial issue.	Troy Martel

TABLE OF CONTENTS

1.0 PURPOSE

The purpose of this test report is to summarize the results of the Pre-qualification testing of the Triconex Tricon PLC to meet the requirements of EPRI TR-107330 (Reference 8.6). The format of this report conforms to Section 8.3.(7) of IEEE Specification 323-1983 (Reference 8.2). Conclusions from the testing are provided in Section 7.0.

The following documents are included as appendices to this test report:

Appendix A: Completed Initial Test Run of Triconex Procedure 7286-502, "Set-Up & Check-Out Test Procedure." This completed procedure documents activities performed by Triconex personnel in setting up the Tricon Test Specimen for Pre-qualification testing and verifying proper system operation prior to testing.

Appendix B: Completed Initial Test Run of Triconex Procedure 7286-503, "Operability Test Procedure." This completed procedure documents the performance and results of the initial Operability testing of the Tricon Test Specimen including evaluation of acceptable test results.

Appendix C: Completed Initial Test Run of Triconex Procedure 7286-504, "Prudency Test Procedure." This completed procedure documents the performance and results of the initial Prudency testing of the Tricon Test Specimen including evaluation of acceptable test results.

2.0 TEST OBJECTIVE

The Pre-qualification Test Plan is described in the Appendix 3 of the Master Test Plan (Reference 8.5). The basic objectives of the pre-qualification testing are to 1) confirm that the test specimen is properly configured, assembled and operational, 2) provide baseline performance data for comparison with data obtained during and after qualification tests, and 3) prove out the test procedures. Operability testing demonstrates the basic functionality of the Tricon in accordance with its published specifications. Prudency testing demonstrates the ability of the Tricon to perform under highly dynamic conditions.

3.0 DESCRIPTION OF TEST SPECIMEN

The equipment tested consists of four Tricon PLC chassis populated with selected input, output, communication, chassis interface, and chassis power supply modules. The tested equipment also includes external termination assemblies (ETAs) provided for connection of field wiring to the Tricon input and output modules, and a Lambda field power supply.

Triconex Drawing 7286-102 (Reference 8.4) shows the general arrangement and interconnection of the Tricon Test Specimen chassis. Project document 7286-541, System Description (Reference 8.3) 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 8.1).

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 completed Operability and Prudency Test Procedures (Appendices B and C) identify the TSAP revision used during pre-qualification testing. The Master Configuration List identifies the revision level of all test specimen firmware.

4.0 TEST SET-UP AND INSTRUMENTATION

The following sections describe the set-up of the Tricon Test Specimen and Lambda field power supply during Pre-Qualification testing, and the simulation and measuring instrumentation used during testing. The system set-up is documented in Appendix A. Results of the initial Operability and Prudency tests are documented in Appendices B and C. Specifications for test instrumentation are included in Appendices A, B, and C. In addition, Attachment 1 provides a summary list of the calibrated test equipment used in the qualification test program.

4.1 Test Specimen Mounting

Pre-qualification testing was performed at the Triconex Irvine, California facility. The

(a)

4.2 Test Specimen Chassis and Module Configuration

Section 3.0 above describes the general arrangement of the Tricon Test Specimen which was maintained throughout Pre-qualification testing. Drawing 7286-102 (Reference 8.4) shows the configuration of modules installed in each of the four chassis. Specific modules under test were identified by serial number in the Master Configuration List.

4.3 Test Specimen Power Supply Configuration

(a)

4.4 Test Instrumentation

(a)

4.5 Instrument Calibration

All tests were performed using calibrated test instruments. Calibration certificates are held by Triconex. Appendices A, B, and C document the calibration status of the test equipment used. A summary list of calibrated test equipment is provided in Attachment 1.

5.0 TEST PROCEDURE

Pre-qualification testing was performed in accordance with the requirements of Sections 5.0 and 6.4.3 of EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications (Reference 8.6) and as described in Appendix 3 of the Master Test Plan (Reference 8.5). The testing was performed at the Triconex Irvine, California facility after completion of assembly of the Test Specimen. This section describes the procedures used to conduct Pre-qualification testing of the Tricon Test Specimen.

(b)

5.1 Test Sequence

Figure 2 of the project Master Test Plan (Reference 8.5) shows the sequence of testing performed on the Tricon Test Specimen. During the Pre-qualification phase, the Set-Up and Check-Out test was performed initially to confirm proper assembly. As

(a)

5.2 Test Method

Pre-qualification testing was conducted in accordance with the following test procedures:

<u>Set-Up and Check-out Test Procedure 7286-502</u>
This procedure verifies the proper assembly and configuration of the test system and confirms the proper functioning of the test system.

(a)

5.3 Test Levels

(a)

Operability and Prudency testing involves exposing the Tricon Test Specimen to various normal and abnormal conditions of input/output operation and source power. EPRI TR-107330 section 5.3 describes the specific criteria to be met for Operability tests. The Operability test included power quality testing as specified in EPRI TR-107330, section 6.4.3. Prudency Test Criteria are defined in EPRI TR-107330, section 5.4. The test procedures (Appendices B and C) provide a detailed description of the conditions simulated during the Operability and Prudency tests.

5.4 Test Specimen Operation

(a)

5.5 Test Specimen Performance Monitoring

Operability and Prudency testing required monitoring numerous aspects of performance of the Tricon Test Specimen and Lambda field power supply under (a)

5.6 Test Acceptance Criteria

The completed Pre-qualification (initial) Operability and Prudency Test procedures (Appendices B and C) include detailed acceptance criteria in Section 4.0 of each test procedure. These acceptance criteria were developed from the applicable sections of EPRI TR-107330 and from Triconex product specifications for the Tricon PLC. Section 6 of this report summarizes the test results and identifies where the applicable test acceptance criteria were met or not met. A detailed evaluation of the measured test data to the applicable test acceptance criteria is presented in the Performance Proof Test Report (Reference 8.12) for all Operability and Prudency tests. The data analyses

(a)

6.0 TEST RESULTS

This section discusses the results of the Pre-qualification testing of the Tricon Test Specimen and the Lambda field power supply. The testing involved Initial runs of the Set-up and Check-Out Test Procedure (Reference 8.7), the Operability Test Procedure (Reference 8.8), and the Prudency Test Procedure (Reference 8.9). Completed test results are included as Appendices A, B, and C. A complete analysis of Operability and Prudency test data taken throughout the qualification testing, including comparisons to the initial test data, is provided in the Performance Proof Test Report (Reference 8.12). This section also provides a discussion of performance and data anomalies observed during the Operability and Prudency testing.

(a)

6.1

6.2

6.3

(a)

6.4

(a)

6.5

6.6

(a)

(c)

(d)

(e)

7.0 CONCLUSIONS

Pre-qualification test objectives discussed in section 2.0 were met. The test specimen and test procedures were exercised during Pre-qualification testing to identify set-up or documentation problems. Discrepancies or inconsistencies in test documentation were identified and resolved, as appropriate, with revisions to test procedures, drawings, and the TSAP application program.

Baseline performance data was obtained during Operability and Prudency Testing. Operability testing demonstrated the basic functionality of the Tricon in accordance with its published specifications. Prudency testing demonstrated the ability of the Tricon to perform under highly dynamic conditions. Test Anomalies (noted above) were documented and evaluated for effect on the Test Specimen qualification status. Data collected was utilized in subsequent evaluation of Test Specimen performance throughout the qualification testing (Reference 8.12, Performance Proof Test Report).

As noted in Test Anomaly 6.6.d, there was one failure to meet test procedure acceptance criteria. Power interruption hold-up time capability for the Lambda field power supply was not met. A more complete discussion of the pre-qualification Test Anomalies is contained in the Performance Proof Test Report (Reference 8.12) which summarizes all Operability and Prudency Tests conducted during Pre-qualification and Qualification testing.

8.0 REFERENCES

(Note: Unless indicated, applicable revision levels of all Triconex documents, procedures, and drawings are per the current revision of the Master Configuration List, Triconex document 7286-540).

8.1 Triconex Document No. 7286-540, Nuclear Qualification of Tricon PLC System, Master Configuration List.

8.2 IEEE Standard 323-1983, Standard for Qualifying 1E Equipment for Nuclear Power Generating Stations.

8.3 Triconex Document No. 7286-541, Nuclear Qualification of Tricon PLC System, System Description.

8.4 Triconex Drawing No. 7286-102, Sheet 1, Rev. 1 and Sheet 2, Rev. 0, Generic Qualification System General Equipment Arrangement.

8.5 Triconex Document No. 7286-500, Nuclear Qualification of Tricon PLC System, Master Test Plan.

8.6 EPRI TR-107330, Generic Requirements for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Final Report dated December, 1996.

8.7 Triconex Document No. 7286-502, Nuclear Qualification of Tricon PLC System, Set-up and Check-out Test Procedure.

8.8 Triconex Document No. 7286-503, Nuclear Qualification of Tricon PLC System, Operability Test Procedure.

8.9 Triconex Document No. 7286-504, Nuclear Qualification of Tricon PLC System, Prudency Test Procedure.

8.10 Triconex Document No. 7286-513, Nuclear Qualification of Tricon PLC System, TSAP Validation Test Procedure.

8.11 Triconex Document No. 7286-535, Nuclear Qualification of Tricon PLC System, TSAP V & V Report.

8.12 Triconex Document No. 7286-530, Nuclear Qualification of Tricon PLC System, Performance Proof Test Report.

9.0 ATTACHMENTS

Attachment 1: Calibrated Test Equipment List

Attachment 2: Special Test Data, 24 VDC Chassis Power Supply Over-range Test per EPRI TR-107330, Section 4.6.1.1.C.

10.0 APPENDICES

Appendix A: Completed Initial Run of Triconex Procedure No. 7286-502, System Set-up and Check-out Test Procedure

Appendix B: Completed Initial Run of Triconex Procedure No. 7286-503 Operability Test Procedure

Appendix C: Completed Initial Run of Triconex Procedure No. 7286-504, Prudency Test Procedure

Attachment 1
(Page 1 of 1)

(a)

Attachment 2
(Page 1 of 3)

Special Test Data
24VDC Chassis Power Supply Over-range Test
per EPRI TR-107330, Section 4.6.1.1.C

(a)

Attachment 2

(Page 2 of 3)

Attachment 2
(Page 3 of 3)

(a)

TRICONEX

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

SOFTWARE QUALIFICATION REPORT

Document No: 7286-535

Revision 1

July 14, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

See Appendix A for proprietary designation

	Name	Signature	Title
Author:	David Herrell	[signature]	Nuclear Quality Engineer
Approvals:	Mitch Albers	[signature]	Project Manager
	Troy Martel	[signature]	Triconex Project Director
	Aad Faber	[signature]	Director, Product Assurance

TRICONEX

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

SOFTWARE QUALIFICATION REPORT

Document No: 7286-535

Revision 1

July 14, 2000

QUALITY ASSURANCE DOCUMENT

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

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

Document Change History			
Rev.	**Date**	**Change**	**Author**
0	June 26, 2000	Initial document issue.	D. Herrell
1	July 14, 2000	Incorporate Triconex comments	D. Herrell
1	August 1, 2000	Issued amended pages 38 and 39	D. Herrell

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the evaluation of the Triconex software and firmware, which comprises the TRICON Programmable Logic Controller (PLC), and TriStation 1131 Developer's Workbench. This evaluation is based on two main elements: the software development process, including Verification and Validation, and the design integrity of the system. Evaluation of the Triconex software development is based on the guidance provided in BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." Evaluation of the system design integrity is based on the requirements established in IEEE Standard 7-4.3.2 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations."

The design of the TRICON PLC has evolved into a mature product over more than 15 years. The software quality assurance program has also evolved and improved significantly over this period. The current process meets the intent of the requirements established by BTP HICB-14. The TriStation 1131 Developer's Workbench, used for engineering support and programming of the TRICON has been developed over the last 7 years, under a process compatible with the intent of BTP HICB-14.

The evaluation uncovered strengths in the development process, including the quality of the final product, design partitioning, product testing, error diagnosis and reporting, and change and configuration control. However, weaknesses were uncovered in maintenance of documentation of design bases and in documentation of review, or verification, of those documents. These weaknesses are adequately compensated for by reviews provided by a classically independent external agency (TÜV Rheinland) and in the quality of the work performed by the Triconex design and validation staff. Proof of the quality of their work is demonstrated in such statistics as 100 million operating hours, in safety critical functions, without a single failure to take a required protective action. These strengths and weaknesses are discussed and evaluated in this report and its appendix.

With the incorporation of the application guidelines provided in this report, the Triconex TRICON PLC and the TriStation 1131 software tools required for programming are acceptable for use in any safety related or high criticality application for nuclear power plants. The specific versions of the software and firmware considered in this qualification are provided in the Master Configuration List, Triconex Report 7286-540.

As long as Triconex uses their current development processes, or provides audited improvements, new versions of this software will be developed under a process which has been evaluated and accepted as compliant with the requirements established in 10CFR50 Appendix B. Therefore, these new versions would also be acceptable for use.

2. INTRODUCTION

This report, which has been prepared in support of the TRICON nuclear qualification program, documents the basis for qualification of the software used in the TRICON version 9.3.1 system. This software includes the embedded real time operating system with its associated communication and input/output modules, and the PC-based system configuration software, TriStation 1131 Developer's Workstation, Version 2.0, Service Pack 3.

The approach used to develop the software qualification is based on the guidance provided in EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." EPRI TR-107330 states that qualification of software is to be performed using the guidance provided in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Essentially, the approach involved evaluating the processes, procedures, and practices used to develop the software, assessing the history of the software itself and its associated documentation and operating experience, and analyzing the software architecture.

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). The approach allows the qualifier to compensate for shortcomings in the design, quality assurance, and verification and validation of the software by taking compensatory actions, including evaluating operating experience and performing "black box" testing.

2.1. Differences Between EPRI TR-107330 and TRICON Qualification

EPRI TR-107330 provides requirements for functional evaluations and tests. There are two significant differences between the approach used in this qualification effort and the EPRI requirements. In each case, the differences result from a careful technical evaluation, and do not result from issues of schedule, budget, or cost. These differences, and the technical reasons for their acceptability, are defined in this section.

Application Software Objects Acceptance (ASOA) Testing

TR-107330 requires an Application Software Objects Acceptance test. This test is designed to verify that the software functions available for use in application programs have been adequately tested and perform as specified in the design basis documents. EPRI TR-107330 defines this as a mandatory test, without any regard or credit for the vendor's internal programs or other previous testing.

However, independent testing was performed by the external certifying agency, Technischer Überwachungs-Verein (TÜV) Rheinland. The TÜV Rheinland testing was evaluated against the requirements established in EPRI TR-107330. Since the TÜV testing was performed independently and since the testing exceeded the requirements of EPRI TR-107330, it was determined that performing the ASOA test would provide no additional value or useful data for the qualification effort. Accordingly, the ASOA test was not performed. The TÜV Rheinland testing is further described in Section 5.2 and Appendix A.

Use of TriStation 1131 and TriStation MSW

The qualification testing used the Test Specimen Application Program (TSAP) during all tests. This program was generated with the TriStation Multi-System Workstation (MSW) development tool. This report provides an evaluation, contained in Section 7.3, of operational differences between the TriStation MSW and TriStation 1131 tools.

At the time the TSAP was initially developed, TriStation MSW was the most mature application development tool available. However, the MSW software is only available in a DOS-based environment. The more recently developed TriStation 1131 is designed for a Windows NT environment. TriStation 1131 is now a mature product, with a documented design basis and improved functionality. Since TriStation 1131 provides beneficial improvements and more commercial longevity, the justification for qualification of application development software focuses on TriStation 1131 and not on TriStation MSW.

2.2. Report Structure

This report contains the evaluation of the TRICON firmware and the TriStation 1131 Developer's Workbench software. The report is structured to protect the Triconex proprietary materials required to support this evaluation. The proprietary materials, including the detailed architectural and process evaluations, are contained in Appendix A. An architectural overview is provided to support the conclusions and application guidance provided in this report.

Appendix A contains the detailed evaluation of the firmware and software against the requirements established in BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." Appendix A also contains part of an evaluation of design integrity based on the requirements established in IEEE Standard 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations."

Application guidelines were developed while evaluating the software. These guidelines are intended to assure that plant-specific systems are implemented in a way that reduces, to the maximum extent possible, the likelihood of errors due to application of the TRICON. These guidelines have been incorporated into the Application Guideline Section of the Qualification Summary Report, Triconex Report Number 7286-545.

The TÜV Rheinland evaluation of the TRICON and TriStation 1131 resulted in the restrictions and requirements for safety critical programs defined in Triconex documentation. During evaluation of the TRICON and TriStation 1131 for nuclear safety related use, the TÜV requirements were evaluated and modified for application to USNRC nuclear safety related requirements. These restrictions and requirements are also included in the Application Guidelines.

3. ARCHITECTURE OVERVIEW

In order to evaluate design integrity, it is necessary to understand the TRICON architecture. This section of the report provides a brief description of the TRICON system and its operation. The intent is to describe the important functionality of the system and the relationship between the hardware and software.

3.1. System Overview

The TRICON, a Triple Modular Redundant (TMR) digital controller, is triple redundant from input terminal to output terminal, as shown in Figure 1. The TMR architecture is intended to allow continued system operation in the presence of any single point of failure within the system. Most, but not all, of the TMR capabilities are provided through Software Implemented Fault Tolerance (SIFT) features. There are Hardware Implemented Fault Tolerance (HIFT) features for decreased microprocessor loading and increased reliability.

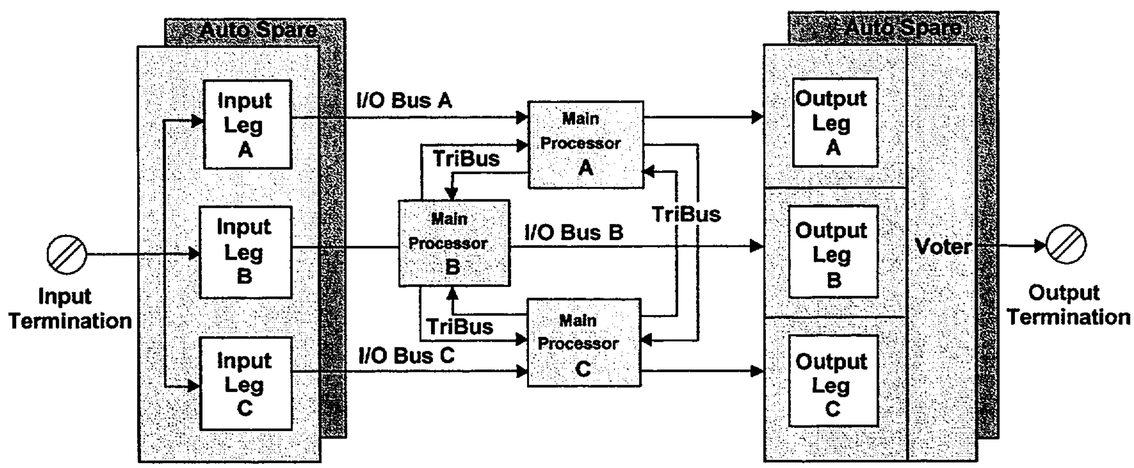


Figure 1. TRICON Triple Modular Redundant Architecture

The TRICON is designed for harsh environments. The electronics use many CMOS components, allowing the system function in up to 60°C environments without cooling fans. Each system consists of one or more rack or panel mounted chassis. Each chassis is powered by two independent, redundant power supplies, each capable of providing the full power requirements of the chassis. Thus, the system can withstand a power supply failure without interruption.

The TMR architecture, shown in Figure 1, is also intended to allow the TRICON to detect and correct individual faults on-line, without interruption of the process under control. It will recover from such faults when the affected module is replaced; thus returning to fully triplicated status. It provides for on-line, hot replacement of any module, under power while the system is running, with no impact to the operation of the control application. In addition to its triplicated operation, it will operate in dual and single modes, depending on the failure encountered. This 3-2-1 operational mode stabilizes operations by providing the user the option of continued process operation or controlled shutdown.

Figure 1 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. These circuits communicate independently with the three main processor modules. The TRICON chassis includes provisions for a spare module, logically paired with a single input or output module. These spare modules are hot swapped into the system by removing the other module. Standard firmware is resident on the main processor modules for all three microprocessors as well as on the input and output modules and other communication modules.

3.2. Main Processor Modules

Each Main Processor (MP)is designed around a thirty-two bit microprocessor (the National Semiconductor 32GX32) and two auxiliary 8-bit microprocessors used for communication. One of the auxiliary microprocessors interfaces with the eight bit microprocessors used on the input and output modules. The other auxiliary microprocessor interfaces with the eight bit microprocessors used for communication with external computing systems. The operating system, run-time library, and fault analysis for the MP is fully contained in read-only memory (ROM) on each module. The MPs communicate with one another through a proprietary, high speed, voting, bi-directional serial channel called TriBUS. Each MP has an I/O channel for communicating with the triplicated I/O modules. Each MP has an independent clock circuit and selection mechanism that enables all three MPs to synchronize their operations periodically to allow voting of data and exchange of diagnostic information.

When a fault is detected on a main processor module, it is annunciated and voted out, and processing continues through the remaining two MPs. When the faulty main processor is replaced, it runs a self-diagnostic to determine its basic health. When the self-diagnostic successfully completes, the MP then begins the process of "re-education," where the control program is transferred from each of the working units into the returning MP. All three Main Processors then resynchronize data and voting, and the replacement processor is allowed back in service. During program loading, the application program is loaded into a single MP. A second MP is manually enabled and automatically re-educated. Once the second MP is active, the third, final MP is manually enabled and automatically re-educated.

The system firmware resident on the MP is designed in a modular manner. Three sets of dedicated function microprocessor firmware exist on the Main Processor. The main 32-bit microprocessor has the TSX operating environment firmware. The two additional microprocessors (the I/O and communication interfaces) each have their own firmware.

The main microprocessor firmware provides the intelligence to implement the extensive built-in self-diagnostics and triple redundancy functions.

The application program interfaces only with the main 32-bit microprocessor. The main microprocessor is configured with the application program from TriStation 1131. Some configuration data is provided to the I/O and communication microprocessors on the main processor board. A limited amount of communication module configuration data is passed from the main microprocessor to communication modules. All other microprocessors perform their dedicated functions based on fixed firmware programming.

3.3. I/O Modules

Each I/O module consists of three identical and independent circuits, all contained on a single printed circuit assembly. Input data is sampled continuously, in some modules compared and/or voted, and sent to the MPs. Each of the triplicated I/O busses 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. The control algorithm is invoked only on known good data.

After the MPs complete the control algorithm, data is sent out to the output modules. The output modules vote on the data again at the final output point. Each solid state discrete output uses a unique, patented, power output voter circuit. Analog outputs use a switching arrangement tying the three legs of digital to analog converters to a single point. Outputs from the MPs are provided to the I/O bus microprocessors through dual port RAM. The I/O bus microprocessors then transfer that data to the triplicated microprocessors on the output modules. The output modules then set the output hardware appropriately on each of the triplicated sections and vote on the appropriate state and/or verify correct operation.

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 itself 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 into 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 faulty module is then removed and returned to the factory for repair.

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

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

3.4. Communication Modules

The interconnection between Main Processors and Communication Modules is shown in Figure 2. There are similarities as well as significant differences between the design of communication modules and the input/output 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 MPs.

Unlike the I/O modules, the three communication bus interfaces are merged into a single microprocessor. In the ACM, that microprocessor votes on the communication messages from the three MPs and transfers only one of them to an attached external system. In the EICM and NCM modules, the most recent information is used without voting. For two-way communications, messages received from the attached external system are triplicated and provided to the three MPs.

The communication paths to external systems have appropriate levels of Cyclic Redundancy Checks (CRC), handshaking, and other protocol-based features. These features are supported in hardware and firmware. There is core functionality common to the communication modules. The firmware and hardware are customized to support the intended external protocols.

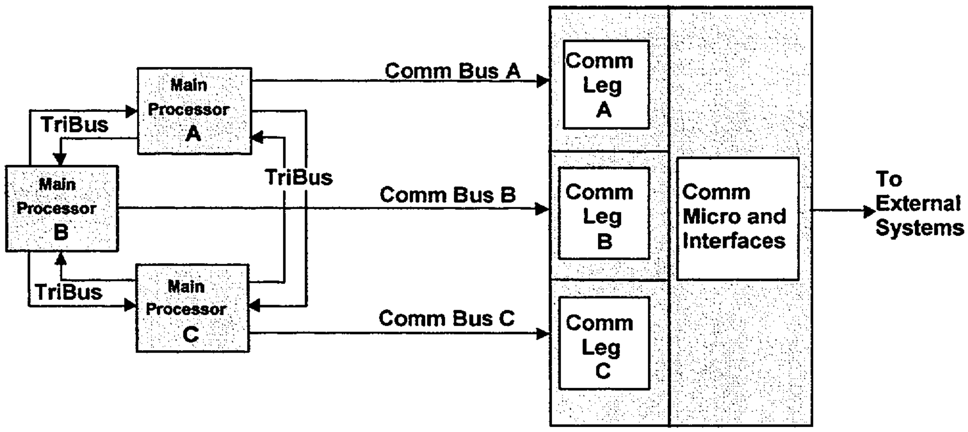


Figure 2. TRICON External Communication Architecture

3.5. TriStation 1131 Software

One of the supported external protocols is communication with the external application programming and diagnostics tool. Application programming is generated and diagnostics are performed using the TriStation 1131 Developer's Workbench. The TriStation 1131 software provides three IEC 61131-3 compliant languages, including Structured Text, Function Block Diagrams, and Ladder Diagrams, as well as a Triconex-defined Cause and Effect Matrix language, called CEMPLE. The TriStation 1131 software implements a Graphical User Interface comprising language editors, compilers, linkers, emulation, communication, and diagnostic capabilities for the TRICON. While the TRICON is performing safety critical functions, the TriStation 1131 PC would not normally be connected.

The TriStation 1131 software is the tool for developing an application program tailored to its field use and downloading that application to the TRICON PLC. This software platform is an IBM compatible PC, operating in a Windows NT environment. The software is constructed using current Microsoft Visual C++ and graphical user interface design techniques appropriate to Microsoft Foundation Classes.

4. QUALIFICATION APPROACH AND CRITERIA

With an understanding of the platform and its architecture established in the earlier sections of this report, the basis for review can be established and findings discussed.

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 this section.

4.1. Regulations and Industry Standards

The SRP contains specific requirements for the digital aspects of instrumentation and control equipment. These requirements are contained in:

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

4.2. IEEE Standard 7-4.3.2

IEEE Standard 7-4.3.2 is primarily for the development of new computer systems and provides requirements for a complete system life cycle. Section 5.3.2 of this standard recognizes the need to qualify existing commercial computers, with Annex D discussing some aspects of commercial grade dedication. This standard does not go into any detail on the acceptance of pre-developed software, although the standard states that, after acceptance, future changes shall follow the IEEE Standard 7-4.3.2 requirements.

The principal thrust of IEEE Standard 7-4.3.2 is to address requirements for sufficient design integrity. Since the final proof of any Software Quality Assurance program is the quality of the final product, the TRICON and TriStation 1131 Developer's Workbench were evaluated to the design integrity requirements specified in this IEEE Standard. Detailed results from this evaluation are provided in the proprietary Critical Digital Review, Appendix A.

4.3. BTP HICB-18 and BTP HICB-14

An essential issue for acceptability is a defined, controlled development process. The requirements specified in IEEE Std 1012-1986 provide an approach that is acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 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.

While the Triconex process does not exactly comply with IEEE Standard 1012, significant common elements exist in both programs. This evaluation considers common elements, missing elements, and means of compensating for the missing elements and data. This evaluation is based on the guidance provided in the SRP.

Referring to SRP Section 7.1, paragraph II, "Supplemental Guidance for Digital Computer-Based Safety Systems", item 2.b discusses the use of existing PLCs as a means of implementing safety related instrumentation and controls. Per this item, "BTP HICB-18 describes an acceptable process for applying the recommendations of this section to PLC implementations."

BTP HICB-18 is based on review of licensee submittals and the analysis of PLC related issues documented in NUREG/CR-6090. The acceptance criteria of BTP HICB-18 discuss six areas of review. These are:

1. PLC hardware
2. Embedded and operating system software
3. Application software
4. Application software development tools
5. Real-time performance and testing
6. Program change configuration control

Of these six areas, four (items 2, 3, 4, and parts of 6) are within the scope of verification and validation (V&V) documentation and software quality processes. These areas will be addressed in further detail. Of these four, three (items 2, 4, and 6) are classified as pre-developed software. That is, the Triconex PLC hardware and software system was not originally developed within the scope of a 10CFR50 Appendix B QA Program.

Certain areas of the PLC platform clearly map the base platform of the TRICON and the TriStation 1131 Developer's Workbench into the requirements established in BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." The platform and the application tools are clearly software written on a computer. The Critical Digital Review, attached as Appendix A to this report, provides a complete analysis of the PLC and the workstation tool for compliance with the requirements established in BTP HICB-14. The attributes provided in BTP HICB-14 are a means of evaluating the concerns associated with digital I&C systems.

As expressed in SRP Appendix 7.0A, the use of digital I&C systems presents the concern that minor errors in design and implementation can cause digital devices 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. One of the protection means against common-mode software failures is also accomplished by an emphasis on the quality 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.

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-6421, 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

This review establishes that there are sufficient documents, as well as sufficiently mature product, to accept the TRICON PLC and TriStation 1131 as acceptable for nuclear safety related use. This acceptance is based on certain compensatory actions and evaluations defined in the proprietary appendix to this report.

4.4. Software Qualification Approach and Criteria

Table 1 summarizes the critical characteristics of digital devices being evaluated for safety critical applications. The acceptance criteria used to qualify the TRICON and TriStation 1131 software and the methods used to evaluate compliance with these criteria are described in Table 1. Table 1 is based on Tables 4-1 and 4-2 of EPRI TR-106439. The criteria shown were selected based on guidance from the USNRC Standard Review Plan and associated Branch Technical Positions, IEEE Standard 7-4.3.2, EPRI reports on qualification of software for safety related use, and USNRC NUREG/CR-6421.

In selecting these criteria, specific criteria relating to performance, hardware, and physical characteristics of the product were not included. These criteria are evaluated in other parts of the qualification program.

Table 1. Software Qualification Criteria

Critical Characteristics	Acceptance Criteria	Methods Used for Verification
Built-in quality through structured and controlled quality assurance processes for: design, testing, manufacturing, error tracking.	QA Program complying with recognized standards and addressing key elements of organization, design control and verification, document control, and record keeping. QA Program certifications via external audits.	Review past and current vendor QA Program against relevant standards (e.g., 10 CFR 50, Appendix B). Evaluate history of QA Program documentation, as it relates to the early development of the system.
	Evidence that the QA Program was applied in the development of the system.	Review completed documentation for compliance with QA Program requirements.

Table 1. Software Qualification Criteria

Critical Characteristics	Acceptance Criteria	Methods Used for Verification
Built-in quality through application of a suitable system design and development process	A system development process is followed which includes: • A life cycle development model consistent with industry standards • Documented design requirements • Requirements traceability • Documented V&V plans • Validation tests and documented reports	Review vendor procedures and practices for system/software development, documentation of requirements, traceability, V&V, and testing for compliance with BTP HICB-14. Evaluate evolution of development practices. Assess extent of software verification activities (e.g., design reviews) and validation, challenge, and failure testing.
	Evidence that the development process was applied to the system.	Review software design documentation for compliance with requirements.
Configuration control and traceability of software, firmware, and errors.	A formal configuration control program is in place which includes: • Documented procedures • Baseline maintenance • Change control • Firmware control during manufacture and servicing • Control of development tools • Error reporting	Review configuration control program requirements against appropriate standards (including BTP HICB-14 and Regulatory Guide 1.169) and verify actual implementation of requirements. Assess vendor history for control of changes and notification of changes (e.g., after servicing). Assess maintainability of basis for qualification. Verify the prioritization of discrepancy reports and the authority of the change control board.

Table 1. Software Qualification Criteria

Critical Characteristics	Acceptance Criteria	Methods Used for Verification
Problem reporting	Vendor has established error reporting procedures that provide comprehensive tracking of problems. Vendor has established procedures for communicating potential problems to users, including compliance with 10 CFR 21.	Review error reporting and tracking procedures, including coverage of potential problems. Review problem notification procedures. Assess track record of prioritizing and correcting problems that have been identified.
Reliability and dependability	Documented product operating history shows product stability, reliability, and freedom from critical software errors.	Review operating experience and determine number of systems in service, how long they have been in service, and associated error reports.
Quality of design	Design and implementation of software includes essential elements of real time system quality: • Simplicity • Determinism of program execution and data flow • Internal consistency • Limited unneeded features with minimal impact on required functionality • Error handling capabilities	Review software design documentation and its implementation in code against the requirements established in IEEE Standard 7-4.3.2.

Table 1. Software Qualification Criteria

Critical Characteristics	Acceptance Criteria	Methods Used for Verification
Fault management and diagnostics	Continuous built-in self-testing is provided that will detect as a minimum: • Memory failures • Internal communication failures (between modules) • Processor halt • Redundant processor failures • Internal fuse failures • Power supply failures Alarms or other indications of failure are provided. Testability features will support periodic surveillance testing for nuclear safety systems. Potential failure modes, particularly those that would affect nuclear safety system functions, have been identified and adequately addressed.	Review PLC design, system architecture, and operating system. Identify important failure modes and effects, and verify that self-test features (e.g., watchdog timers) will detect these failures. Assess the impact of failure on PLC operation, particularly with respect to typical safety system functions. Include evaluation of abnormal conditions and events. Review vendor's failure analysis and testing. Review product operating history to verify the absence of critical failures.

The approach used to evaluate these critical characteristics employs the Critical Digital Review (CDR) methodology defined in EPRI TR-106439 and EPRI TR-107339. The CDR focused on the following areas:

- The procedures, processes, and practices used to develop, test, and maintain the software, including evaluating the history of these practices.
- The history of the software itself, including its evolution over time, and its current design basis documentation.
- The design of the software, including detailed analysis of the documentation, code, and test procedures.

The results of these evaluations were then used to assess the overall quality of the TRICON software with respect to the level of quality expected for nuclear safety related systems. As shortcomings were found, compensatory actions were developed. The results from these compensatory measures are included in Appendix A. The following items correspond to Table 1 and reflect conclusions developed and explained throughout the report and its appendix.

Process Controls and Software Quality Assurance

- This report concludes that the software reviewed was developed under a commercial quality assurance program. Triconex initial quality assurance program was based on NQA-1. Since the Triconex quality assurance program has matured with the product, the quality of design basis documentation improves commensurate with the program. Minor inconsistencies were found between upper level and lower tier implementing procedures, which are being addressed by Triconex.

- Triconex development practices have been shown to be deficient in maintenance and documentation of review of design basis documents. The quality assurance program has improved since the beginning of the TRICON development effort. Currently, the program will produce documentation, verification, and validation as expected for an IEC-61508 compliant program.

- One weakness in the system is the quality and completeness of the design basis documentation. These documents tend to represent the initial configuration, and tend not to be updated as changes, upgrades, and enhancements are installed. However, the code quality is not adversely impacted by incomplete design basis documents. Triconex design engineers seem to document the areas where designs will be difficult or complicated. These areas do compare favorably with the code that implements those difficult or complicated design areas. Areas where coding is simple or routine usually have little to no documentation.

Configuration Control

- Triconex has always had a formal configuration control, change control, and error tracking system. Software and documents, once placed under configuration control, are retrievable. Changes are controlled. Errors, once entered into the automated error tracking system, are retrievable, changes are controlled, appropriate resolutions are generated, and all data is available. Errors may, after review for risk of implementation, be held for future implementation, released for immediate resolution, or indefinitely postponed. Included in the configuration control system is a complete listing of each system and module, by serial number, defining where the module is, when it was installed, and any repairs at Triconex.

Error Tracking and Reporting

- The Triconex problem reporting and tracking system is designed to provide traceability of an error from inception and entry through resolution and final validation.

Reliability and Dependability

- A review of operating history has been performed. Over 100 million system operational hours can be documented with no failures to take a required protective action. This data is presented in Section 8.4 of this report. Since the modules are expensive and since existing customers do not perform module repairs, Triconex can maintain records and service histories to the module level.

Quality of Design

- An evaluation of the overall system design, and designs for the Main Processor (MP) as well as several of the input, output, and communication modules, demonstrates that the designs exhibit the essential elements of real time system quality defined in IEEE Standard 7-4.3.2. The Main Processor contains less than 45,000 lines of "C" code, including support for triple modular redundancy, fault tolerance, and diagnostics.

- Even as a general purpose device, the system has been designed with modularity and simplicity as guiding principles. As a completely modular system, only those functions that are required are installed. Only those library functions that are used are loaded.

- Both from an analysis and from testing during this evaluation, the system has been shown to exhibit determinism in both program execution and in data flow.

Failure Management and Diagnostics

- Diagnostics and failure management are among the most complex issues in a triple modular redundant environment. Recovery from detected errors is not a simple, straightforward issue. However, the TRICON provides an application program with a programming environment that does not force the application engineer to develop diagnostics or determine appropriate courses of action for internal system failures. The TRICON provides internal diagnostics and failure management for the application. The application software can determine if errors exist and can be used to provide information and annunciation of those failures to a plant operator. The diagnostic and failure management capabilities of the TRICON are appropriate and provide an acceptable basis on which to build a safety system.

5. PROCESS EVALUATION

The TRICON software was initially developed 15 years ago, evolving into the present day configuration. Within this time frame, the product has matured to incorporate design enhancements. When the TRICON operating system and support software 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 evolution and history of the processes, practices, and procedures used to control the development of this software are summarized in this section. A more detailed description and evaluation of the development process is provided in Appendix A.

5.1. Qualify Assurance and Software Development Process

The basic software developed for the TRICON and TriStation MSW originated over 15 years ago. The development process demonstrates administrative and program controls which have evolved over time, becoming formally documented in departmental procedures.

The Triconex Quality Assurance Manual was first issued in June of 1986. The model for the QA program was ANSI/ASME NQA-1 and was prepared in the 18 criteria format. The intent of ANSI/ASME NQA-1 is to provide the nuclear industry with a standard for a Quality Assurance program that will meet the requirements of 10CFR50 Appendix B.

The Triconex Engineering Design Manual (EDM), first issued in 1986, formalized common practices with the following key procedures:

- EDM 20.00, Configuration Management
- EDM 40.10, Design Specification Software Format
- EDM 40.51, Software Coding Practices

In 1991, the TRICON Version 6.2.3 received TÜV Rheinland certification for use as Class 5 safety equipment. As a result of the TÜV certification, new procedures were added and existing procedures reinforced to formalize the software development and configuration control process actually practiced in 1992. IEEE standards and other software development references available at that time were used as guides. New software development procedures included:

- EDM 24.00, Software Configuration and Control Procedure (based on IEEE Standard 1042)

- EDM 40.10, Design Specification Software Format (based on IEEE Standards 830 and 1016)
- EDM 40.50, Software Development Guidelines (based on IEEE Standard 1012)
- EDM 40.51, Software Coding Practices

ASME NQA -1-1994 Subpart 2.7 addresses a software life cycle that is based on the model similar to IEEE 1012-1998, "IEEE Standard for Software Verification and Validation Plans." It should be noted that these standards allow for alternate approaches and flexibility depending on the nature and complexity of the software. This is consistent with the BTP HICB-14 which also acknowledges alternate approaches. In Table 2, a comparison of the major elements of the Triconex life cycle development process to NQA 1-1994 / IEEE 1012 is shown to illustrate similarities.

Table 2. Software Product Development Cycle

Triconex Development Phase	NQA-1-1994 / IEEE 1012
Initial: Marketing requirements System specification Engineering project plan System Test Plan	***Concept***: Statement of need etc.
Requirements: Software requirements specification Engineering project plan (updated as needed) Software test specification	***Requirements***: Establish functionality requirements V & V plan
Design: Software design spec Software test specification (updated as needed)	***Design***: Develop design bases
Coding: Write source code Software design spec (for incremental changes) Software test specification (updated as needed) Preliminary user documents	***Implementation***: Put design into programming language Software verification
Test: Unit test to check execution against requirements Release media out of source code control system	***Testing***: Validation of code
Quality Assurance: Production release for testing Quality assurance validation testing Approved production release Software Release Description	***Installation and Checkout:*** Execution of tests for installation Approval of the software
Operation and Maintenance: Minor releases for enhancements Minor releases for corrections Error notices	***Operation and Maintenance:*** Corrective Predictive Adaptive

Table 2. Software Product Development Cycle

Triconex Development Phase	NQA-1-1994 / IEEE 1012
N/A	***Retirement***: Software product support is terminated

With a worldwide market, Triconex adopted the more universally accepted ISO 9001 QA program in September 1994. The most significant change at this time was the transfer of responsibility for validation testing to the independent Quality Assurance department. The software engineering and quality assurance procedures were revised in January 1995 to support the revised validation testing responsibility. The key Quality Assurance responsibilities related to validation testing are to:

- Develop the Validation Test Plan encompassing functional tests of all modules
- Perform I/O Fault Insertion Testing for any new modules
- Perform integrated System Testing to verify not only correct operation of the changes but also continued correct operation of the remainder of the system and complete backward compatibility through regression testing
- Assure correct operation of the programming tools, such as TriStation 1131, after any modifications

The QA program was updated in March of 1998 to be in full compliance with 10CFR50 Appendix B as well as ISO 9001-1994. The current QA program and departmental procedures satisfy the following:

- ISO 9001-1994
- 10CFR50 Appendix B
- TÜV Certification for DIN V VDE 19250, resp. DIN V VDE 0801 Class 6

5.2. TÜV Certification

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 to meet standard DIN V VDE 19250, resp. DIN

V VDE 0801 requirements for safety equipment, class 5 (Test Report 945/EL 366/91).

Each new version has been tested by TÜV Rheinland, with Version 9.3 being certified in February of 1998 to class 5 and class 6 of the DIN standard (Test Report 945/EZ 102/98). The testing preformed by TÜV Rheinland examines both the hardware and the software. Both the system software (TSX and associated communication and I/O support modules) and the application development tools software (TriStation MSW 3.1 and 1131) are reviewed and tested with each new version.

The three aspects of software review and testing by TÜV Rheinland are:

- Software analysis
- Software test
- Software and integration (software/hardware) test

Software Analysis

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 function is sufficiently described in each module specification. From the specification, the source code is examined to ensure that the source code implements the specification.

Another element of the TÜV Rheinland analysis is the evaluation of 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 that Triconex uses.

Software Test

The original TriStation MSW software (the application tools software) TÜV Rheinland testing consisted of three parts.

- User Program – The translation from the user program (ladder logic) to the final code for the Main Processors in the TRICON was checked. This was accomplished by disassembling the code the TriStation MSW software produced and then downloading the reassembled code to the TRICON using a TÜV program.

- User Interface – The programs developed for the hardware tests were used to validate the functionality of the ladder logic.

- Negative Testing – All the error message conditions (except Out of Space) were simulated and verified that the correct messages were produced.

TRICON software testing consisted of the following:

- Internal Fault Routines – Procedures such as the watchdog routines, CPU test, etc. were checked by watching the normal execution of these routines and by forcing execution of the routines by injecting faults.

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

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

Software and Integration Testing

The function and purpose of the PLC is processing information based on instructions provided from the user application program. In addition, the PLC must have the ability to allow communication with the outside world and have the ability to detect and process hardware problems. These tests are designed to verify the interface between the PLC software and PLC hardware.

- Application Program – TÜV Rheinland tested the ability to process the user application program with the TriStation MSW software.

- System Test – The main processor operating system software (TSX) is tested by Triconex's Functional Verification procedure, which is intended to simulate a system environment. TÜV Rheinland performed selected portions of this procedure; particularly dealing with external inputs to the TRICON in addition to the TÜV Rheinland I/O malfunction test.

5.3. Configuration Control

The TRICON contains several firmware sets, on several modules. A TRICON version is defined on a formally released, configuration controlled Software Release Definition. These documents define the unique compilation and linkage definition Meta 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 before the release is announced. Unannounced releases can not be shipped to anyone other than TÜV Rheinland for testing.

It is important to recognize that this qualification effort evaluates and accepts the TRICON Version 9.3.1 and TriStation 1131 Version 2.0 as products acceptable for use in nuclear safety related applications. The CDR provides the evaluation of the Triconex quality assurance program and determines that it is sufficient to maintain qualification of future software versions. This qualification does not create a "golden version" of the TRICON PLC and TriStation 1131 Developer's Workstation, with unchanging versions and hardware fixed in time from this qualification.

Instead, this report accepts the quality of the Triconex procedures and the TRICON and the corporate capability to maintain system quality. With a functional Quality Assurance program and acceptable software quality assurance procedures, the current version is acceptable for nuclear safety related use. Thus, there are no issues with accepting a firmware enhancement in the ACM module, thus upgrading the TRICON to Version 9.4. With that upgrade, TriStation 1131 Version 2.0 is required. This report concludes that TRICON Version 9.4 or later and TriStation 1131 Version 2.0 or later are acceptable for use in a nuclear safety related application.

A base TRICON PLC and TriStation 1131 Developer's Workbench provides an acceptable platform on which applications can be built for safety related service. This qualification effort used a synthetic application program, built under the Triconex Application Engineering Quality Assurance program, for testing.

6. SYSTEM HISTORY

The TRICON and the TriStation 1131 software are not new products. As mature products, they provide proven technology for safety related use. The TRICON and the TriStation 1131 are mature, evolutionary products, grown and enhanced through a continuous process of hardware, software, and firmware improvement. New versions reflect hardware or software improvements or corrections, not new directions. This development process is reflected in Figure 3.

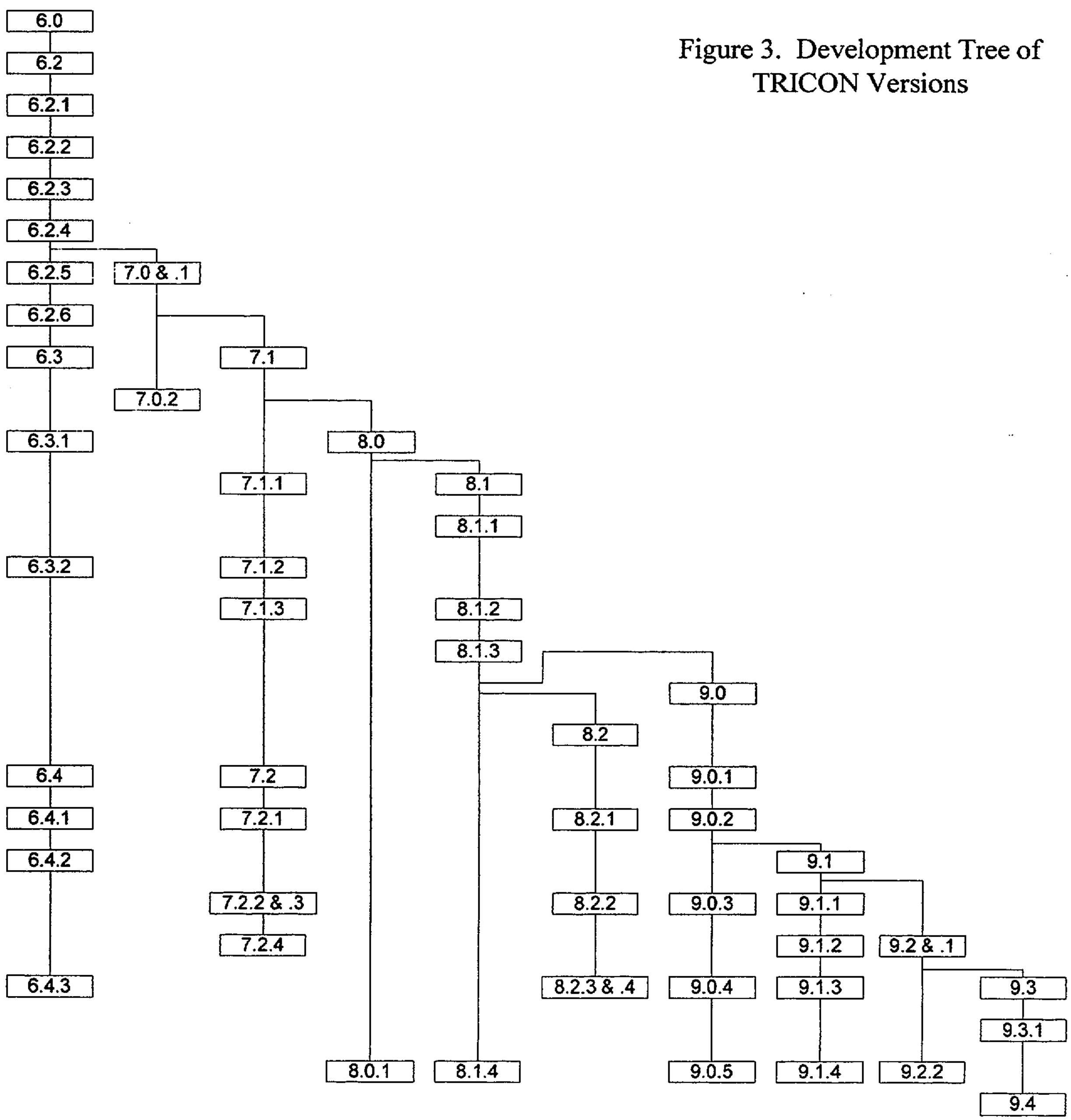


Figure 3. Development Tree of TRICON Versions

TRICON release 6.2.3, released in 1991, is the first version to be certified by TÜV Rheinland for safety critical use. Figure 3 started at version 6.0 to illustrate the development to version 6.2.3, which is credited as the first version to have independent verification and validation from the classically independent certification agency, TÜV Rheinland.

In order to trace the development of the TRICON from that certification, the Product Release Notices and Software Release Definitions for the releases since version 6.0 were reviewed. All Product Alert Notices for the entire system were reviewed. The Product Alert Notices are the Triconex commercial equivalent to the nuclear Part 21 notification process.

The version tree, provided as Figure 3, attempts to graphically summarize the resulting data. Time advances down the page. To provide some concept of the amount of time, version 6.2.3 was released in 1991. Version 9.3.1 was released in April 1998. Version 9.4 was released in February 1999. Since the table was created, version 9.5 has been released and is the current version that would be purchased and installed.

Versions are numbered with a numbering system that provides the major, minor, and maintenance version data. Major versions on the figure are 6.0, 7.0, 8.0, and 9.0. Major releases require extensive hardware and/or software changes to upgrade. As an example, major 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. Thus, an upgrade to version 9 would have required major hardware and field termination changes.

Minor releases and maintenance releases require less effort to install. For these releases, software and/or firmware changes may be required. The minimum supported hardware, software, and firmware levels are defined in the Product Release Notice. These releases normally result from error corrections or product capability enhancements. Just because releases occur in a vertical line across the figure does not require or imply that there are errors common to the released versions. There are releases where the only commonality is the rough time of the release.

There is no fixed requirement to upgrade to the next release. As reflected in the table, Triconex continues to provide maintenance releases to older firmware versions. For instance, common issues in multiple versions were corrected with the version 6.4.3, 8.2.3, 9.0.4, 9.1.3, and 9.3 releases. Triconex maintains support and availability of the products and related support services for a period of 10 years after Triconex has discontinued inclusion of such products on its standard Price List. While no new functionality will be provided for the older versions, the error detection, correction, and upgrade processes are performed across all active versions.

7. DESIGN INTEGRITY

There is a great deal of guidance in the industry for evaluating the design integrity of newly developed systems. This guidance has been applied to this evaluation. However, one of the strongest proofs of design integrity is system operation. A sound history is available only for mature products and only if the manufacturer can keep extensive records. The TRICON hardware is sufficiently expensive that repairs are made to modules, rather than replacement. Thus, Triconex has extensive records of module failure mechanisms and can determine whether any given TRICON module is still being used.

One of the simplest measures of design integrity is evidenced in the fact that there have been no failures to take appropriate protective actions in more than 100 million operating hours. There are several possibilities for converting the 1E+8 system operating hours to failures per operating hour. The basic difficulty with such a conversion is that there are no failures during this period. If a statistically valid number of failures had occurred, one could divide the failure count by 1E+8 and determine a valid measured Mean Time Between Failures (MTBF). Since no failures exist, a different approach is required. Assuming that a failure occurs in the next hour, the MTBF would be 1E+8 hours. Other approaches assume that decimation of one or two orders of magnitude can yield a valid MTBF. That approach provides an MTBF of 1E+6 to 1E+7 hours. For either case, the targeted reliability for IEC 61508 or IEEE Standard 1012-1998 Software Integrity Level (SIL) 3 or 4 is met.

Further evaluations of architectural features to enhance or demonstrate design integrity are provided below.

7.1. TSX and Main Processor

All versions of the TRICON dispatch application programs the same way, using the same construct. The compiled application programs are downloaded to the TRICON from a TriStation 1131 Developer's Workbench. In order to minimize the resource requirements in the TRICON, the applications are translated into native machine code for the National Semiconductor 32GX32 microprocessors. Each of up to 250 program instances possible in the TRICON is downloaded to the MP battery-backed static RAM (SRAM). The program downloads include the necessary function and function block library entries necessary for each program segment. Thus, any possible library function errors are correctable by linking the program instances with new copies of the libraries.

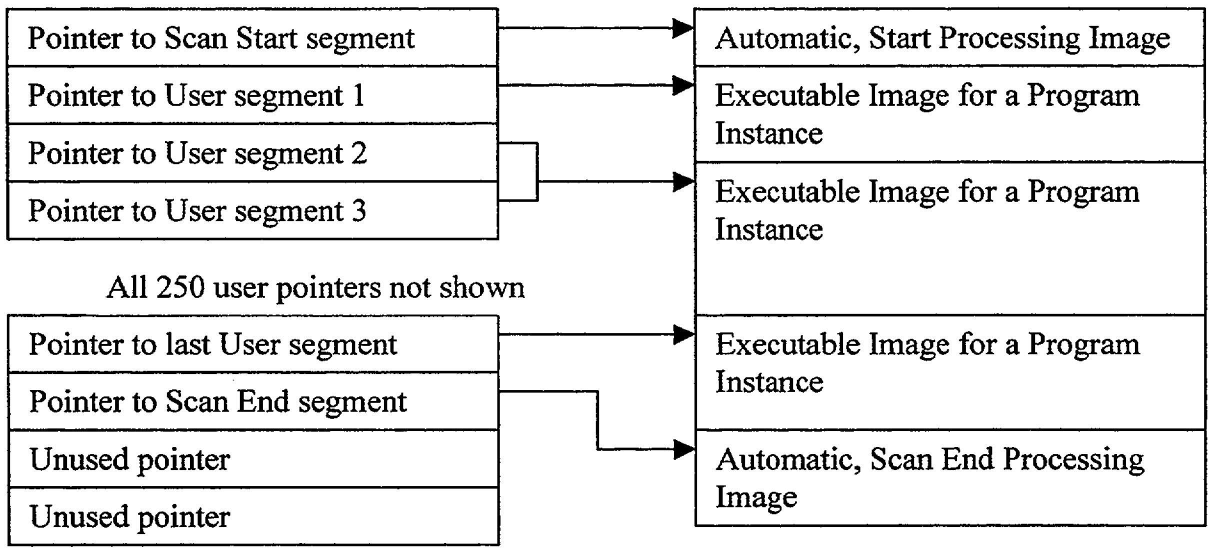


Figure 4. Program Vector Table

The program vector table is the interface between the TSX operating system and the application programs. Each slot contains a pointer to a program instance. Each instance thus operates as an independent function, called by the operating system. When the straight line programming comprising each program completes, the function returns to the TSX operating system. Each slot is dispatched in turn. The first slot in the Program Vector Table is automatically and transparently reserved for the functions associated with starting a scan. After the last program instance, the last slot in the Program Vector Table is automatically and transparently reserved for the function associated with completing a scan.

For the TriStation MSW, each program slot contains a pointer to a single relay ladder segment. For the TriStation 1131, each program slot contains a pointer to a single instance of a program. During normal program execution, the TSX operating system dispatch functions use the Program Vector Table with no differences between programs generated by either the TriStation MSW or TriStation 1131.

As discussed earlier, the TriStation 1131 Developer's Workbench translates the various languages into native mode executable machine code. Intermediate steps are performed in the translation, and evaluated in Appendix A. The Cause and Effect Matrix, Ladder Diagrams, and Function Block Diagrams are translated into Structured Text. The Structure Text is translated into an emulated code. The emulated code can then be translated into assembly language for the Main Processor. This is then assembled and linked with native mode code libraries to generate a program. Up to this point, all work can and should 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 intermediate language 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.

Programs and translated code are protected by 32-bit Cyclic 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.

Even a 32-bit CRC can fail to indicate bit changes in memory. However, the bit changes must be carefully crafted and must occur in all three MPs almost simultaneously. Normally, bit changes that result in the same CRC result in code that behaves erratically, which usually results in faulting the affected MP. Bit changes that do not occur in all three MPs almost simultaneously will result in the voting diagnostics faulting one or more MPs, since the 2 megabyte SRAM in which the configuration is stored is also voted for correctness.

Once the program download is complete, the user may and should request a comparison between the content of the TRICON and the data stored in the TriStation. Proprietary details of that comparison process are provided in the CDR. However, there is sufficient comparison between the stored and re-calculated TRICON data 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.

There are no issues with Y2K and the TRICON or TriStation. The TRICON uses a 64-bit integer date offset, in millisecond resolution, which removes the 32-bit integer, in seconds resolution, 2038 overflow problem present in earlier versions. An unsigned 32 bit date field in non-compliant products usually starts at 1/1/1970, counts seconds, and rolls back to zero around August of 2038. The TRICON uses a 64 bit date/time offset, counting milliseconds, which provides a unique, linear, increasing date/time offset for several millennia.

7.2. Input, Output, and Communication Modules

The firmware used in these modules exhibits the recommendations from various NRC guidance on high criticality software. The firmware is simple. The firmware does not use an operating system. The firmware performs a few functions and only those functions necessary for the operation of the board and the board's diagnostics. There is no dead code on the modules. Other evaluations performed, documented in the Appendix A, demonstrate that the dedicated function input, output, and communications module firmware is robustly designed to be used in high safety criticality applications.

7.3. TriStation 1131 and MSW

Triconex used the language and functions in IEC Standard 61131-3 as the technical design basis for the TriStation 1131 programming languages. The IEC standard defines the design basis and operation of most of the functions in the PLC. Additional Triconex documentation defines the operation of the TRICON specific functions, required to interface with diagnostics and TRICON implementation specific features. The operation of these functions has been exhaustively verified and validated by TÜV Rheinland. This independent agency has certified the TRICON since 1991.

The independent verification and validation performed by TÜV Rheinland was evaluated as part of the qualification effort. The automated testing performed on the system by Triconex and TÜV Rheinland appears to satisfy the intent of EPRI TR-107330. The same testing program and test data cases are used at both TÜV Rheinland and Triconex.

The automated testing program was initially defined by Triconex. The program has been extended based on comments from TÜV Rheinland. As part of the qualification effort, Triconex evaluated the test case coverage and found it included almost all the functions. Those functions that can be exercised in an automated test were added to the test suite, based on the Triconex evaluation of test case coverage. Some functions can only be tested completely with manual tests, which are also included in the Triconex test program. The test cases validate operation at the numeric limits of integer and floating point mathematical functions.

The testing validates that a series of TRICON programs compile, fail to compile, run correctly, or produce defined error conditions. The testing has a set of predefined failure conditions that are validated to occur. Testing validates not only correct operation but correct identification of deliberately introduced errors. The testing system automatically downloads successful compilations into a TRICON and executes them. The pass/fail results of the program operation are returned to the PC used to automate this testing, evaluated for expected results, and stored. This process can continue for over two weeks, if all tests are performed.

The TS1131 Validation Test Coverage document, Triconex 9600066-001, revision 1, defines automated test suites containing 31,846 compiler tests, 3,218 standard library tests, and 37 TRICON library tests. There are additional manual tests performed for timing and error detection. Thus, more than 35,101 separate, distinct automated test cases exist, with additional manual tests. It should be pointed out that most of the test cases are collections of individual tests. For example, one of the test cases contains in excess of 1,600 individual tests. Triconex personnel have not counted the individual tests in most of the test cases. Further proprietary data is contained in the CDR.

TriStation 1131 provides a secure, password protected environment, with a Windows NT look and feel, in which development is performed. Offline capabilities are provided for support of configuration control and documentation of changes.

The more modern interface provided in TriStation 1131 should minimize inadvertent errors that might be made during program development and modification. From a human factors view, the TriStation 1131 tool is far superior to the older DOS-based TriStation MSW in minimizing human error. The TriStation 1131 tool also provides a common application language, familiar to most users of programmable logic controllers.

The TriStation 1131 tool provides additional functionality while connected to a TRICON over that provided in the older DOS-based tool. This additional functionality provides capabilities for verifying that the content of the PLC is the same as those on the PC from which the download occurred. The vulnerability associated with building programs in a SIL 0 environment for SIL 3 and 4 applications has been minimized.

The version of TriStation 1131 addressed in this report is Version 2.0, Service Pack 3. The Triconex Product Release Notice associated with TRICON Version 9.3.1 is TriStation 1131 Version 1.1. While Version 2.0 has not been formally validated for use with TRICON 9.3.1, evaluation shows that the only significant differences are the inclusion of the high current analog output module (which is not included in the qualification) and a change to the ACM communication module firmware. The TSX operating environment did not change. Desirable enhancements and software corrections were made in Version 2.0. These included the Cause and Effect Matrix Editor and internal corrections.

The TriStation 1131 software runs in a Windows NT environment on a standard PC. Triconex recognized that a SIL 0 environment, like Windows NT, is not acceptable for use in a safety system. However, the TRICON is acceptable for SIL 3 or 4 processing. Failure analyses have been performed and the TriStation 1131 workstation software has been written to attempt to detect the random bit errors and other transient faults possible in a PC environment. The designed in software coping mechanisms reduce the possible degradations that might occur for software developed in a SIL 0 environment that implements a SIL 4 process.

The SIL 0 problem is common to all digital devices that use a commercial operating system and/or development environment to compile and link code. The Triconex TriStation 1131 software attempts to address the development problem by inclusion of 32-bit CRCs on critical program elements and by careful design. The design features include saving a copy of the CRC locally and concurrently while sending the CRC protected code to the TRICON.

The older TriStation MSW software operates in a DOS environment. This report evaluated TriStation MSW as part of the nuclear qualification and found that compensatory actions are required for its use in a nuclear safety related environment. While the program has been in use for several years, historical evidence coupled with extensive system testing is not sufficient for acceptance. Since design basis, verification, and validation documentation does not exist for TriStation MSW, compensatory actions are required for its use.

This compensatory action would include use of a Triconex tool to disassemble the executable image, interspersing the assembly language code into the appropriate relay ladder logic diagrams. The application engineer would then read the assembly language code and verify that the translation from relay ladder logic to assembly language was correct. This compensatory action is viewed as an excessive burden for nuclear safety related applications. Thus, TriStation MSW is not recommended for nuclear use.

While the TRICON is actively performing its safety related function, there are no significant differences between operation of programs developed under TriStation 1131 and TriStation MSW. Both use the Program Vector Table, described in Section 7.1 of this report, to dispatch functions. A minor difference is that TriStation MSW creates an entry in the Program Vector Table for each relay ladder segment, while TriStation 1131 creates an entry in this table for each program instance. The TRICON dispatches the functionality in the same manner, starting at the beginning of the table, and working through to the end. The results are the same. Since the TRICON successfully dispatched functions throughout qualification testing, it does not matter whether the functions were generated by TriStation 1131 or TriStation MSW.

This report recommends the use of the TriStation 1131 tool over TriStation MSW for the following reasons:

- The product is documented.
- The product operates in a language more familiar to utility engineers.
- The language used is an international standard.
- Triconex actively participates in the development of the IEC 61131-3 standard.
- Operation under code generated by the modern tool does not affect the qualification.
- TriStation 1131 will be supported and continue to be enhanced by Triconex. TriStation MSW will not.

Based on these reasons, TriStation 1131 is appropriate for use in a nuclear environment.

7.4. Application Software

The actual application programming for the TRICON is plant specific and is not evaluated as part of this report. However, the TriStation 1131 tools provide language features and functionality in keeping with the recommendations of USNRC guidance documents, such as NUREG/CR-6463, Rev. 1, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems."

Application software is developed from Structured Text, Ladder Diagrams, Function Blocks or Cause and Effect Matrices, using the TriStation 1131 software. This software is loaded into the MPs using the TriStation 1131 software. The application software provides the functionality defined by the code and implements the desired monitoring and controls defined by the programmer for the specific nuclear safety application.

The TriStation 1131 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 integrate TriStation 1131 generated applications into their existing software control and configuration management processes. Various programmatic requirements are provided in Appendix B, Applications Guidelines, Triconex Report Number 7286-545.

In addition to the support features offered by the TriStation 1131, the standardized language features will aid in development of safety critical functions. TriStation 1131 does not provide the complete implementation of all features in IEC 61131-3. The functions that are not offered are viewed as inappropriate for safety critical functions. Triconex is actively working on an IEC 61131 subcommittee to define a standard function subset of 61131-3 for safety critical applications. The existing TriStation 1131 function subset does not allow such constructs as looping and GOTO that could inadvertently result in infinite program flow loops or at least in non-deterministic execution timing. This reduces the chance of bad programming constructs creating unexpected system hangs, further reducing the chance of system failures as well as software common cause failures.

8. CONCLUSIONS

The evaluation of software quality assurance and design integrity demonstrates that the TRICON is acceptable for use in nuclear safety related applications. The TRICON provides an acceptable means to implement high availability, high reliability systems in an easily configured, commercially available, system. The TRICON is acceptable for use in systems such as Reactor Trip or Protection Systems, Engineered Safety Feature Systems, Safe Shutdown Systems, Information and Interlock Systems Important to Safety, and other safety critical control system applications. Other conclusions relating to the critical characteristics presented in Section 4.4 are presented in this section.

Detailed evaluations performed as part of the Critical Digital Review are provided in Appendix A. The important conclusions are provided in this section.

8.1. Process Controls and Software Quality Assurance

- The first revision of the Triconex QA Manual, dated 6/30/86, was developed based on the requirements of NQA-1, and specifies controls which essentially comply with the requirements of 10 CFR 50, Appendix B. The documentation for software development practices has 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. Based on this history, it is concluded that, from the earliest versions, the TRICON software has been developed in a controlled and structured environment, using industrial procedures that continue to improve.

- The TRICON and TriStation 1131 are not Legacy Software. Starting at TRICON release 6.2.3, Triconex established a contract with an external, independent certification agency (TÜV Rheinland) to perform code review and testing for the product. TÜV assisted Triconex in establishing safety coding standards, which have been maintained and extended since. The TriStation 1131 software was developed under these standards. TRICON software changes since then have been documented and controlled. Based on the independent review performed by TÜV Rheinland, this report provides objective evidence in Appendix A supporting a conclusion that that the TRICON, after release 6.2.3, and TriStation 1131 have been developed and maintained under a controlled process. Further, this process is substantially compliant with BTP HICB-14 and current industry standards

- Version 9.3.1 of the TRICON software was extensively reviewed as part of the qualification effort. 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.

- The software quality assurance program generally is strong; its weakest link is in documenting peer review (verification) activities. This weakness is adequately compensated for by reviews provided by classically independent external agencies and in the quality of the work performed by Triconex design and validation staff. Significant improvement has been made since the initial TRICON development. Triconex has committed to compliance to IEC-61508. Additional improvement in documentation of verification activities is being implemented. Current procedures and practices comply with those provided in IEEE Standard 7-4.3.2.

8.2. Configuration Control

- Triconex has always had formal configuration and change control systems. Software and documents, once placed under configuration control, are retrievable and changes are controlled. Included in the configuration control system is a complete listing of each system and module, by serial number, defining where the module is, when it was installed, and any repairs at Triconex.

8.3. Error Tracking and Reporting

- Triconex has always had formal error tracking and recording systems. These systems are 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.

8.4. Reliability and Dependability

- There is a large base of experience with the TRICON system and its associated software. Triconex has an ongoing relationship with each customer. Knowledge is maintained about the system configuration and any customer concerns for those systems.

  The operating experience with these systems demonstrates that the software is highly reliable. This operating experience is based on data sampled in early 1999 and provided in Table 3. Of the 812 Version 9 systems, 354 are Version 9.3.1. Assuming that just the Version 7, 8, and 9 systems remained in service and that no new systems were sold (which combine to a conservative evaluation), then these 1892 systems, operating 24 hours a day, 7 days a week, for the last year and a quarter added more than 20 million additional hours to the total provided in Table 3. Thus, there have been no failures to take the appropriate protective action in more than 100 million operating hours.

Table 3. TRICON System Cumulative Operating Hours, Early 1999

Version	No. Systems	Operating Hours
5	104	9,110,401
6	696	39,514,945
7	646	24,699,181
8	434	10,154,372
9	812	7,072,640
	Total	90,551,539

- Supplementary testing performed as part of the nuclear qualification effort provided further confidence in the quality and reliability of the TRICON software. This supplementary testing included seismic, temperature, humidity, and electromagnetic compatibility. These tests impose significant challenges to the software-based system. Throughout these tests, a Test Specimen Application Program (TSAP) operated, ensuring that the system continued to operate in the presence of these challenges.

- There is no single action that can be taken to mitigate software common cause failure. However, there are many aspects to the TRICON that make software common cause failure less likely. The system is mature and widely used. The installed base has been operated for over a 100 million hours with no failures to take a required protective safety action. The system has been subjected to verification and validation by an independent group. Since common cause failure is not caused by random faults, the capability of the system to find and vote out single faults is not applicable. The assumption is that the failures would occur simultaneously in all TRICON PLCs. For a typical protection system, particularly in older units, none of the programs in the TRICON PLCs is likely to be identical, since many differences exist in sensor inputs to the divisions. All of these features and functions, taken as a group, tend to indicate that software common cause failure is unlikely to occur.

8.5. Quality of Design

- The design of the hardware and software evidences modularity, design partitioning, the concepts of information hiding which are now defined as object oriented programming, logical partitioning of functions between software and hardware, and other key evidence of a logical, thorough, well-designed system. During the evaluation, the samples of coding that were reviewed were logical, simple, well thought out, and commented. The code has been reviewed, line by line, by TÜV Rheinland and their coding standards for safety critical coding have been incorporated. The design and coding comply with the precepts established in guidance documents such as NUREG/CR-6463, Rev. 1, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems."

- The Triconex Design Engineering staff exhibits the safety conscious, safety critical attitudes that are consistent with those expected from nuclear industry personnel. Several engineers reiterated that the culture at Triconex is that the equipment must be designed as if it was going to be installed in a hydrocarbon processing facility beside one's own home. Risk and failures are unacceptable.

- The Triconex Design Engineering staff also demonstrates the ideas now codified in the Software Engineering Institute's Personal Software Process. Their successful processes are documented in the procedures, and are based on the actual activities and principles used by individual engineers at Triconex. The Triconex software design and development procedures are reflections of the methods used by the engineering staff. The procedures are updated to reflect the evolutionary improvements made by the engineering staff, over and above the requirements reflected in previous design and development procedures. Process improvements are driven by staff belief, not established by management decree. Thus, the intent of the quality assurance program is embodied in work product, since the staff using the procedures believe that the methods and processes used are appropriate and necessary to produce safe, high quality products.

- The TRICON has a validated formula for calculating minimum and maximum cycle times, based on program and hardware complexity. Allowances are included, which are necessary for proper operation of the internal diagnostics.

The proposed program and hardware configuration shall be evaluated against plant and system specific minimum design basis time response requirements to determine if the TRICON is acceptable for use in the intended system.

8.6. Fault Management and Diagnostics

- The design of the software includes features to detect and mitigate system failures. 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 provided comply with the requirements established in BTP HICB-17, "Guidance on Self-Test and Surveillance Test Provisions." The diagnostics are integrated into the base TRICON and require no special programming. In addition, data is made available to the application program concerning program operation, results of arithmetic operations, and other internal faults, consistent with the requirements of BTP HICB-17. The application program shall be designed to provide appropriate error recovery and annunciation of such faults. Use of several of the diagnostic data inputs are mandated in the application guidelines in this report.

- The diagnostics are not excessively complex. The diagnostics provide proven fault coverage, based on validated automated fault injection testing. Triconex performs automated tests that verify correct system behavior, fault detection, and the check for detection of the expected fault.

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

9. REFERENCES

The extensive list of proprietary Triconex documentation used in the development of this report is contained in the Critical Digital Review, provided as Appendix A to the proprietary version of this report.

9.1. Regulatory Documents

Regulatory Guide 1.152; Criteria for Digital Computers in Safety Systems of Nuclear Power Plants, Revision 1, January 1996

Regulatory Guide 1.168; Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

Regulatory Guide 1.169; Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

Regulatory Guide 1.170; Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

Regulatory Guide 1.171; Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

Regulatory Guide 1.172; Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

Regulatory Guide 1.173; Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

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

NUREG/CR-6083; Reviewing Real-Time Performance of Nuclear Reactor Safety Systems; May 28, 1993

NUREG/CR-6090; The Programmable Logic Controller and Its Application in Nuclear Reactor Systems; June 30, 1993

NUREG/CR-6101; Software Reliability and Safety in Nuclear Reactor Protection Systems; June 11, 1993

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

NUREG/CR-6303; Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems; December 1994

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

9.2. Industry Standards and Guides

ANSI/ASME NQA-1-1994; Quality Assurance Program Requirements for Nuclear Facilities Applications

IEEE Std 7-4.3.2-1993; IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

IEEE Std 730-1989; IEEE Standard for Software Quality Assurance Plans

IEEE Std 730.1-1989; IEEE Guide for Software Quality Assurance Planning

IEEE Std 828-1990; IEEE Standard for Software Configuration Management Plans

IEEE Std 829-1983; IEEE Standard for Software Test Documentation

IEEE Std 930-1993; IEEE Recommended Practice for Software Requirements Specification

IEEE Std 1008-1987; IEEE Standard for Software Unit Testing

ANSI/IEEE Std 1012-1998; IEEE Standard for Software Verification and Validation Plans

ANSI/IEEE Std 1016-1987; IEEE Recommended Practice for Software Design Descriptions

IEEE Std 1016.1-1993; IEEE Guide to Software Design Descriptions

IEEE Std 1028-1988; IEEE Standard for Software Reviews and Audits

ANSI/IEEE Std 1042-1987; IEEE Guide to Software Configuration Management

ANSI/IEEE Std 1058.1-1987; IEEE Standard for Software Project Management Plans

IEEE Std 1059-1993; IEEE Guide for Software Verification and Validation Plans

IEEE Std 1074-1995; IEEE Standard for Developing Software Life Cycle Processes

ISO 9000-3:1991; Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software

ISO 9001:1994(E); Quality systems – Model for quality assurance in design, development, production, installation and service

9.3. Other

EPRI TR-102348; Guideline on Licensing Digital Upgrades; December 1993

EPRI TR-103291-Volume 1; Handbook for Verification and Validation of Digital Systems, Volume I: Summary; December 1994

EPRI TR-103291-Volume 2; Handbook for Verification and Validation of Digital Systems, Volume II: Case Histories; December 1994

EPRI TR-103291-Volume 3; Handbook for Verification and Validation of Digital Systems, Volume III: Topical Reviews; December 1994

EPRI TR-106439; Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications; October 1996

EPRI TR-107330; Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants; December 1996; with the April 24, 1998 revisions and the July 30, 1998 USNRC Safety Evaluation

Appendix A

Critical Digital Review

of the Triconex

TRICON PLC

and TriStation 1131 Developer's Workbench

APPENDIX A, THE CRITICAL DIGITAL REVIEW

IS CONSIDERED PROPRIETARY IN ITS ENTIRETY

(a,b,e)

The Critical Digital Review

is not included in this

Non-Proprietary Version of

The Software Qualification Report.

The Critical Digital Review is

Provided only in the Proprietary Version of

The Software Qualification Report