invensys
TRICONEX®

TRICONEX PRODUCTS – INVENSYS PROCESS SYSTEMS

Project:	Tricon v10 NUCLEAR QUALIFICATION PROJECT

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

TRICON SYSTEM DESCRIPTION

Document No: 9600164-541

Revision 0

July 24, 2007

	Name	Signature	Title
Author:	Ravindar Baskaran	See ATTACHED	Responsible Engineer
Reviewer:	Hariprasad Parthasarathy	See ATTACHED	Independent Review Engineer
	Frank Kloer		Project Engineer
	George Hughes		Project Quality Assurance Engineer
Approvals:	Naresh Desai		Project Manager

invensys
TRICONEX

Project:	Tricon v10 NUCLEAR QUALIFICATION PROJECT

Tricon SYSTEM DESCRIPTION

Document No: 9600164-541

Revision 0

July 24, 2007

	Name	Signature	Title
Author:	Ravindar Baskaran		Responsible Engineer
Reviewer:	Hariprasad Parthasarathy		Independent Review Engineer
	Frank Kloer		Project Engineer
	George Hughes		Project Quality Assurance Engineer
Approvals:	Naresh Desai		Project Manager

Revision History

Revision	Date	Description	Author
0	24-July-2007	Initial Issue	Ravindar Baskaran

TABLE OF CONTENTS

1.0 PURPOSE

EPRI and a utility sponsored working group, using regulatory requirements, standards, guidelines, and expertise, has developed Electrical Power Research Institute (EPRI) Technical Report specification TR-107330 - titled "Generic Requirements Specification for Qualifying a Commercially Available Programmable Logic Controller (PLC) for Safety-Related Applications in Nuclear Power Plants" (Reference 4.1). The specification provides guidance on what is essential to qualify a commercially available PLC. It covers documentation, functional and qualification-testing requirements for use by utilities in developing their bid specifications for a PLC-based safety related application. The U.S. Nuclear Regulatory Commission (NRC) issued a Safety Evaluation Report (SER) on July 30, 1998, endorsing the methodology described in TR-107330.

The purpose of this document is to present an overview of Invensys Triconex Tricon TMR PLC product line in accordance with the requirements of EPRI TR-107330, Sections 8.1 through 8.5 and to provide a description of the test system in accordance with Section 8.8.

2.0 OBJECTIVE

The objective of this System Description is to convey to the reader an overview description of the:

1. Invensys Triconex Tricon TMR PLC and its basic operation
2. Invensys Triconex programming tools and documentation
3. Invensys Triconex equipment submitted for qualification
4. The platform configuration of the Tricon-Under-Test (TUT)

It is not intended to be exhaustive in its description, but help the reader to gain initial understanding of the Tricon design, operation, and methodology used for testing. This document also provides to the reader more detailed informational references. Discrepancies within Invensys Triconex reference information should be brought to the attention of Invensys Triconex for resolution by the technical staff.

3.0 SCOPE

The types of documentation required to support both generic qualification and application specific PLC usage are listed in the following subsections as specified in Section 8.0 of EPRI-TR-107330.

3.1 Equipment General Overview Document Requirements

Section 5 "*General Overview*" of this document describes in detail the product line of a generically qualified PLC as per EPRI TR-107330, Section 8.1.

The overview of the generically qualified Tricon TMR PLC product line includes:

A. Description of the Tricon TMR PLC platform structure.

B. Description of the types of interconnections between main and expansion/other types of I/O chassis.

C. Overview and selection guide of the modules available.

D. Overall capacity in terms of I/O and available processing speed.

E. Installation information as follows:

1. Any variations in mounting provided on Tricon PLC platform.
2. Information on torque values to set on any mounting screws.
3. Any requirements or limitations on the structure it can be mounted on, including space and clearance requirements
4. Any limitations on distances between the main chassis and expansion chassis.
5. Requirements and specifications for any user-supplied hardware required for mounting and connection to Tricon PLC (e.g., special connectors, screws, etc.).
6. Any special handling restrictions while mounting the Tricon PLC and installing modules.
7. Grounding and shielding requirements.

F. Handling and storage requirements in accordance with TR-107330, Sections 4.10.1 and 4.10.3.

G. A description of the self-diagnostics and redundancy features in Tricon PLC platform.

3.2 Equipment General Specification Requirements

Section 6 "*Tricon Equipment General Specification*" of this document details the general specification of the Tricon PLC and its modules used in the qualification program as per EPRI TR-107330, Section 8.2. This section of the document includes general specifications and all its references.

3.3 Operator's Manual Requirements

Section 7 "*Tricon Operator's Manual*" of this document details the information on the operation of the Tricon PLC as per EPRI TR-107330, Section 8.3.

3.4 Programmer's Manual Requirements

Section 8 of this document comprehensively covers the use of functions available in Tricon PLC processors as per EPRI TR-107330, Section 8.4. This section of the documents shall include:

A. A summary of the available functions with a brief description of each.

B. A detailed description of the usage of each function.

C. Examples of the application of complex function blocks.

D. Limitations on any of the functions (e.g., parameter ranges, number of functions of a particular type that can be used).

E. Methods for managing resource utilization (i.e., memory utilization, I/O mapping, scan time and overall response time estimating).

F. A user manual for the programming and debugging tools that is provided and, if applicable, for any programming terminal for the Tricon that is included for qualification.

G. Detailed information for the creation and testing of user-defined functions if this capability is provided.

H. Detailed description of the operation of any conditional execution statements (e.g., GOTO, SKIP, SUBROUTINES).

I. Description of the limitations of the application of dynamic functions (e.g., PID functions, Lead/Lag) and the relationship of their operation to scan time.

J. Detailed description of the interaction between the main processor, coprocessor modules, and I/O modules.

K. Detailed description of the interaction between the application program and any redundancy features included in the Tricon and any application layer activities and functions needed to support the redundancy.

L. Any software build procedures and software tools that are needed to apply the Tricon to a safety system configuration.

M. A description of the operation of the executive including flow control information.

N. A description of data and data base management, data handling, data definition, and configuration management features.

O. A description of the operation and use of the self-diagnostic features including the interface between the self-diagnostics and the application program.

P. A programming manual for any coprocessor included for qualification that covers the above items, as applicable to the function and design of the coprocessor.

3.5 Invensys Triconex Maintenance Manual Requirements

Section 9 of this document provides references to the maintenance manuals as specified in EPRI TR-107330, Section 8.5. This section shall include information needed for calibration, troubleshooting, and maintenance of the modules and the overall PLC.

3.6 Invensys Triconex System Description Requirements

Section 10 of this document includes description of the hardware and software used in the test specimen as a part of qualification program as specified in EPRI TR-107330, Section 8.8.

4.0 REFERENCES

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

4.2 TRICONEX Document No. 9600164-500, Master Test Plan

4.3 TRICONEX Document No. 9600164-540, Master Configuration List

4.4 TRICONEX Document No. 9600164-518, TSAP Software Design Description

4.5 TRICONEX Document No. 9600164-545, EQ Summary Report

4.6 TRICONEX Drawing No. 9600164-100 Tricon Under Test - General Arrangement

4.7 TRICONEX Drawing No. 9600164-102 Seismic Test Equipment Configuration Detail

4.8 TRICONEX Drawing No. 9600164-103 System Block Diagram

4.9 TRICONEX Drawing No. 9600164-200 Power Distribution Block Diagram

4.10 TRICONEX Drawing No. 9600164-201 Power Distribution Wiring Diagram

4.11 TRICONEX Drawing No. 9600164-202 Test Chassis #1 Power Distribution Wiring Diagram

4.12 TRICONEX Drawing No. 9600164-203 Test Chassis #2 Power Distribution Wiring Diagram

4.13 TRICONEX Drawing No. 9600164-204 Test Chassis #3 Power Distribution Wiring Diagram

4.14 TRICONEX Drawing No. 9600164-205 Test Chassis #4 Power Distribution Wiring Diagram

4.15 TRICONEX Drawing No. 9600164-206 Simulator Chassis #5 Power Dist. Wiring Diagram

4.16 TRICONEX Drawing No. 9600164-207 Simulator Chassis #6 Power Dist. Wiring Diagram

4.17 TRICONEX Drawing No. 9600164-300 Wiring Diagram General Notes

4.18 TRICONEX Document No. 9600164-700 Wiring Schedule

4.19 TRICONEX Drawing No. 9600164-600 to 614 Function Diagrams

4.20 Planning and Installation Guide for Tricon v9-v10 Systems, Part No. 97200077-002

4.21 Field Terminations Guide for Tricon v9-v10 Systems, Part No. 9700052-001

4.22 Technical Product Guide for Tricon v9-v10 Systems

4.23 Communication Guide for Tricon v9-v10 Systems, Part No. 9700088-001

4.24 Safety Considerations Guide for Tricon v9-v10 Systems, Part No. 9700097-003

4.25 Libraries Reference TriStation 1131, v4.1, Part No. 9700098-003

4.26 TRICONEX Document No. 9600164-545, Application Guide

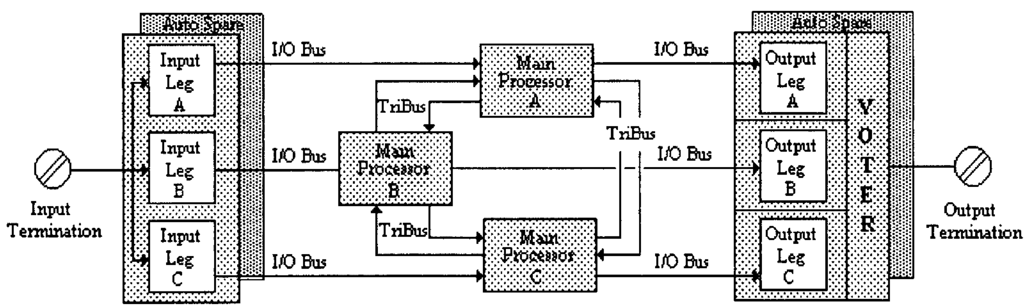
4.27 TRICONEX Document No. 9720107-002 Enhanced Diagnostic Monitor User's Guide, v2.0

5.0 GENERAL OVERVIEW

5.1 Equipment General Overview Document Requirements

The "Tricon Technical Product Guide" (Reference 4.22) and "Tricon Planning and Installation Guide" (Reference 4.20) provide detailed descriptions of the Tricon design and its operation. The following section is provided as an overview.

Tricon, a Triple Modular Redundant (TMR) Programmable Logic Controller (PLC) is triple redundant from input point to output point. This design feature of the Tricon eliminates single point of failure within the system, which can prevent it from executing its application program. It detects and corrects such failures on-line, without interruption of the process under control. It will recover from such failures when the faulty 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 channel operation, it will operate in dual and single processor modes, depending on the fault encountered. This 3-2-1 operational mode stabilizes operations by providing the user the option of continued process operation or controlled shutdown.



Triplicated Architecture of the Tricon PLC

Figure 1

Figure 1 shows the triplicated architecture of a Tricon controller. At the heart of the system are three identical main processor modules (MP's). Each MP is designed around a thirty-two-bit microprocessor and multiple eight-bit microprocessors used as I/O control managers. The operating system, run time diagnostics and fault analyzer for the MP is fully contained in read-only memory (ROM) on each module. The MP's communicate with one another through a patented, high speed, bi-directional serial channel called TriBUS. Each spawns an I/O channel for communicating with the triplicated I/O modules, which may be added to the system. Each MP has an independent clock circuit and selection mechanism, which enables all three MP's to synchronize their operations periodically to allow voting of data and exchange of diagnostic information.

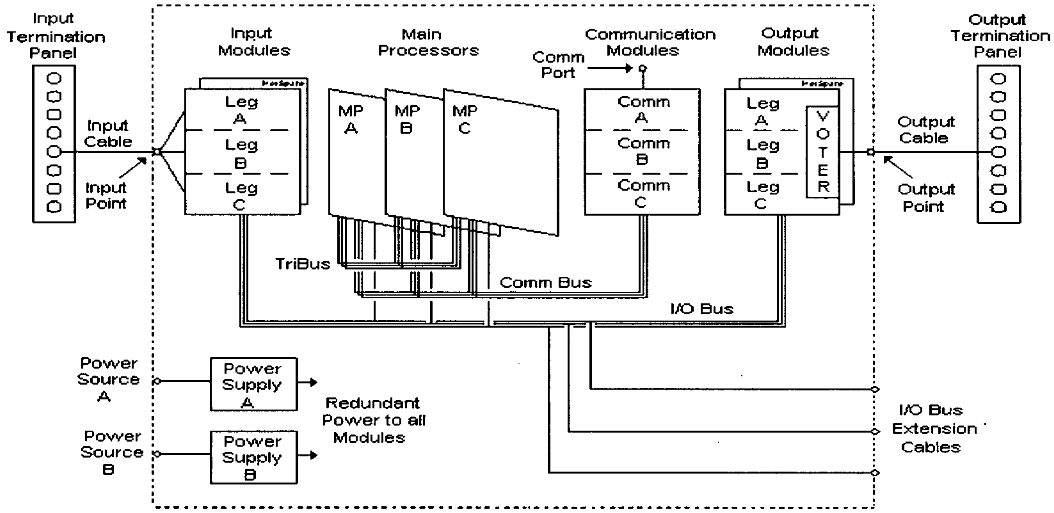
When a fault is detected on a main processor module, it is voted out and processing continues through the remaining two MP's. When the faulty main processor is replaced, it runs a self-diagnostic to determine basic Health State and then begins the process of "re-education" whereby the control program is transferred from one of the working units.

The I/O bus carries the states of inputs to the main processors from the three legs of the input/output 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 and sent to the MP's through a dual port RAM interface. All data is then voted and corrected over the TriBUS and the control algorithm is invoked. After the MP's complete the control algorithm, data is sent out to the output modules where it is voted again at the final output point through a unique patented power output voter circuit. All output points have integral loopback, which is used to determine whether the programmed value is in fact achieved through the output stage.

If an I/O module leg fails to function, an alarm is raised to the MP's which check to determine if a "hot standby" unit is installed next to the faulty module. If so, and that module is itself deemed healthy by the MP's, 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 unabated. The user plugs a replacement unit into the system in the position reserved for a "hot replacement." This position is the same one in which the hot standby unit would reside. When the MP's detect the presence of the hot replacement module, they initiate local Health State diagnostics and if the module is healthy, automatically switch over to the new module. The faulty module may then be removed and returned to the factory for analysis and repair.

5.2 Types of Interconnection Between Tricon Main And Expansion I/O Chassis

The Tricon supports three types of chassis: Main Chassis, Local Expansion Chassis and Remote Expansion Chassis. The Main Chassis supports the three Main Processors, optional Communications and I/O modules. Figure 2 is a block diagram of a Main Chassis depicting the electrical and data interfaces to chassis components.



TRICON Main Chassis
Figure 2

The Main Chassis houses two redundant power supplies, which provide power for all modules within the chassis. Modules housed within the Main Chassis are the three independent Main Processors (MP), a communication module (for example TCM) and, at the option of the user, six I/O or additional Communication Modules (single or hot standby).

As shown in the diagram, the power supplies can receive power from independent sources and supply unregulated voltage and current to independent, redundant power buses within the chassis. Each MP, Communication and I/O module has independent voltage regulators to support the electronic components on the module.

Field sensor wiring is terminated at passive, external termination panels (ETP). The termination panels also support field sensors excitation/power with connections to single or dual redundant field power supplies depending on the type of field device.

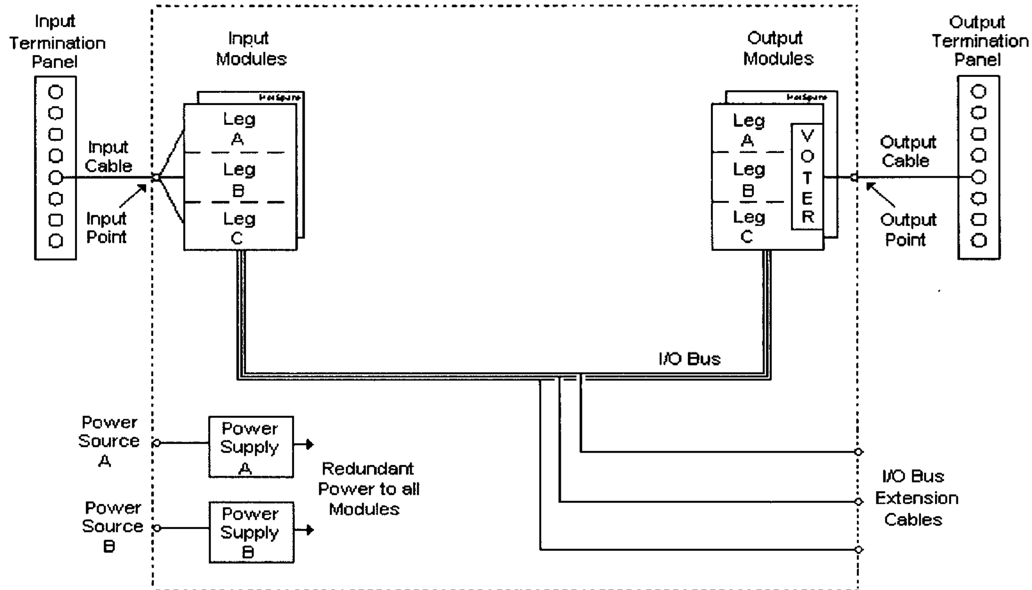
Field signals are coupled to the input module via a Invensys TRICONEX supplied, pre-fabricated, multi-conductor cable from the termination panel to a connector on the chassis backplane, which in turn is connected to the input module. Cable lengths may be ordered in lengths up to 90 feet (27.4 meters).

Each input point on the module is distributed to three independent "legs", each with dedicated signal conditioning networks that filter and convert field level voltage/current to data level voltage. When polled by the MP a communication microprocessor, mounted in each leg, acquires the data and serially transmits it to its respective MP via the triplicated I/O Bus. Each MP exchanges the input data tables via the triplicated TriBUS, votes the data (pre-computation) and computes the application program logic. The logic results are then serially transmitted to the respective "legs" of the output module where the signal is converted and voted again (post-computation) prior to being transmitted to the field device via output terminations.

The passive (fuses excepted) output termination panels are connected to the output module via a Invensys TRICONEX supplied, pre-fabricated, multi-conductor cable from the termination panel to a connector on the chassis backplane which in turn is connected to the output module. Cable lengths may be ordered with lengths up to 90 feet (27.4 meters).

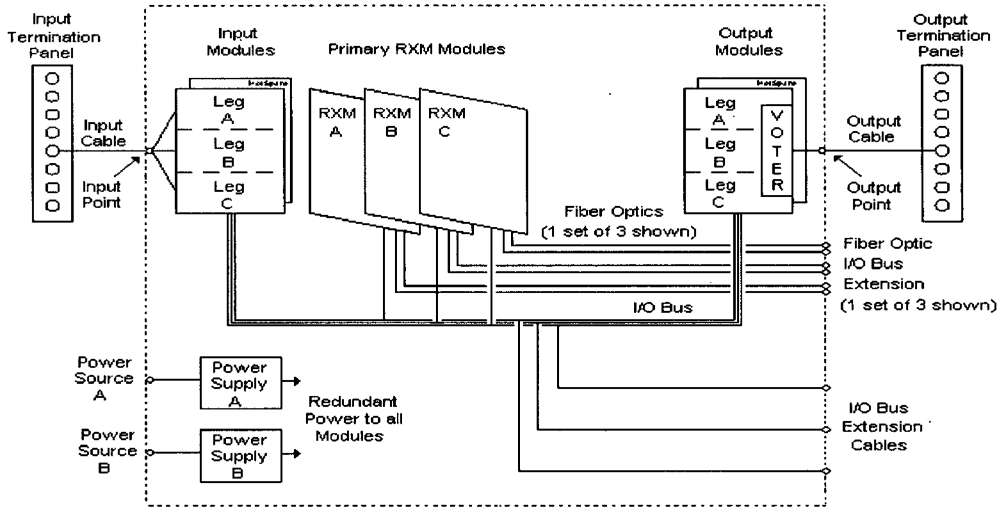
Communication Modules are also supported in the Main Chassis to allow secure exchange of data with a variety of host devices. While data is exchanged via the triplicated communication bus, the communication module is not fully triplicated. Data exchanged with the host device is via single media. The Main Chassis supports redundant communication modules and redundant media should the user classify the data to be process critical.

Should the application require I/O in excess of the capacity of a Main Chassis, a Local Expansion Chassis may be integrated into the system by extending the I/O Bus via installing triplicated I/O Bus Cables as shown in Figure 2.



TRICON Local Expansion Chassis
Figure 3

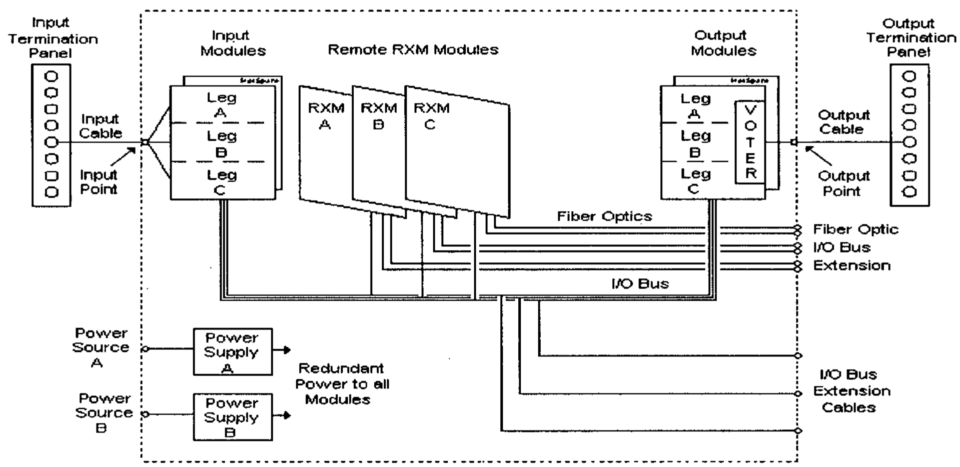
Figure 3 is a block diagram of a Tricon Local Expansion Chassis. As with the Main Chassis, the Local Expansion Chassis houses two redundant power supplies that provide power for all modules within the chassis. The Local Expansion Chassis supports eight I/O modules (single or hot standby).



TRICON Primary Remote Expansion Chassis

Figure 4

Figure 4 is a block diagram of a Tricon Remote Expansion Chassis with Primary RXM Modules that are the electrical interface between the I/O Bus and fiber optic media. The Tricon Main Chassis supports up to three Primary Remote Expansion Chassis, each connected through an extended I/O Bus. Each Primary Remote Expansion Chassis supports three separate Remote Expansion Chassis with Remote RXM Modules, providing a maximum of nine remote locations per Tricon system, each a distance of up to 2 kilometers from the Main Chassis. Two redundant power supplies and six I/O modules may be housed in a local RXM Chassis.



TRICON Remote Extension Chassis

Figure 5

Figure 5 is a block diagram of a Tricon Remote Expansion Chassis with Remote RXM Modules that are the electrical interface between the I/O Bus and fiber optic media at the remote location. Each Remote Expansion Chassis supports multiple local (to the remote chassis) Expansion Chassis through I/O Bus extension. Two redundant power supplies and six I/O modules may be housed in a remote RXM Chassis.

As with all I/O Bus communications, Remote Expansion Chassis communication rate is 375 Kbaud. The use of point-to-point fiber optic media and modems eliminate ground loops and provide exceptional immunity against electrostatic and electromagnetic interference, and serve as Class 1E to non-1E isolators.

The reader should consult The Tricon Technical Product Guide (Reference 4.22) and the Tricon Planning and Installation Guide (Reference 4.20) for detailed information on the interconnections of the different types of chassis.

5.3 Tricon Overview and Selection Guide of the Modules Available

The Tricon supports a wide variety of I/O and communication modules. Specifications and features are listed in the Tricon Planning and Installation Guide (Reference 4.20). While all Tricon modules comply with International Standards, not all modules have been validated to those standards listed in TR-107330 during nuclear qualification testing. Table 1 lists those modules included in the Master Test Plan (Reference 4.2) and submitted for qualification testing. Results of testing and the final qualification status of the modules in the Tricon-Under-Test (TUT) are described in the Final Summary Report.

5.3.1 Tricon Chassis (8110, 8111, 8112)

The Tricon chassis is designed for rack-or panel-mount. Physical size of a chassis is 19 in wide, 22.75 in height, x 17.75 in depth. Each chassis has a unique I/O bus address supporting up to 15 chassis in a Tricon system. Each module within a chassis has an address defined by its location or slot.

The Main Chassis houses the three Main Processors, Communication Modules and up to six I/O modules. It has a four-position keyswitch that controls the entire Tricon system. Switch settings are RUN, PROGRAM, STOP and REMOTE.

Expansion Chassis provide housing and support for up to eight I/O module slots. The first Expansion Chassis also supports Communication Modules.

A RXM Chassis is used in place of an Expansion Chassis to set up remote locations up to twelve (12) kilometers (7.5 miles) away from the local chassis cluster. Each RXM Chassis houses either Primary or Remote Fiber Optically connected RXM Sets and up to six I/O modules.

The Primary Fiber Optic RXM (4200) set consists of three modules that provide active repeater support for the triplicated RS-485 I/O communication bus. An additional RXM Chassis containing a Remote Fiber Optic RXM module (4201) set must be used at each remote location. Each primary set supports up to three remote locations. Expansion Chassis may be connected to the RS-485 I/O expansion bus ports of a RXM Chassis.

5.3.2 Power Modules (8310, 8311, 8312)

Each chassis is supported by two independent Power Modules. Under normal circumstances, both Power Modules are active, and each contributes power to the Tricon chassis. Either Power Module is capable of running the Tricon for an indefinite length of time. If one of the Power Modules, or its supporting power line fails, the second module will increase its output to maintain power for the Tricon. The Power Module can be hot-replaced. A Power Module may be removed for repair from the Tricon Chassis, and replaced without shutting down the Tricon.

5.3.3 Main Processors (3008)

The Tricon Main Chassis houses the three Main Processor (MP) modules, each serving one leg of the controller. The MPs are located adjacent to the Power Modules in the Tricon Main Chassis. Each processor independently communicates with its I/O subsystem and executes the user-written control program. The three MPs compare data and the control program at regular intervals.

Each Main Processor operates autonomously with no shared clocks, power regulators, or circuitry. A 32-bit microprocessor serves as the primary processor with another 32-bit microprocessor managing I/O and communication subsystems. A high-speed proprietary bus system called TRIBUS on each Main Processor handles inter-processor communications. A direct memory access controller manages the synchronization, transfer and data correction independent of user applications or executive software.

5.3.4 Communication Modules (4352A)

The Tricon Communication Module (TCM) is an optional module for the Tricon controller, which supports multiple message protocols and physical media types. Ports on the TCM can communicate with TriStation, other Tricon or Trident controllers, Ethernet devices, and Modbus master and slave devices. The TCM functionally replaces the older generation communication modules (Enhanced Intelligent Communication Module and Network Communication Module).

The Tricon controller supports two logical slots of TCM, which means there can be a maximum of four TCMs in a system. Each TCM operate independently. Each TCM can be connected to a separate network, or they can be used in a redundant configuration.

A TCM provides four optically isolated RS-232/RS-485 serial ports, which are TriStation configurable for point-to-point or multi-point serial connections. Transmission rates up to 115.2 kilobits per second per port can be selected.

The TCM provides two Fiber Ethernet ports for connection to multimode 62.5/125 um fiber cables. NET 1 and NET 2 are 100BaseFL connectors, which can operate at 100 megabits per second. Additionally TCM with two RJ45 Ethernet ports for connection to twisted pair copper cables are also available. For more details about communication modules refer to the Tricon Communication Guide for V9 – V10 Systems (Reference 4.23).

5.3.5 Analog Input Modules (3721, 3701, 3703E)

The Tricon supports a variety of Analog Input Modules (AI). All AI modules have three independent input legs. Each input leg receives variable voltage signals from each point, converts the signals to digital values, and transmits the values to the three Main Processors on demand. One value is then selected using a mid-value selection algorithm for use in computing the application. Sensing of each input point is performed in a manner that prevents a single failure on one leg from affecting another leg.

The 3703E Analog Input Module provides a +6 percent over-range measurement capability. If an open input occurs or the voltage goes out of range, the Main Processors receive the integer value +32,767 for upscale or -32,767 for downscale. The 3721 Analog Input Module integrated with signal conditioners accepts RTD inputs.

Each AI 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 contacts. The FAULT indicator points to a leg fault, not a module failure. The module is guaranteed to operate properly in the presence of a single fault and may continue to operate properly with some multiple faults.

AI modules support hot spare functionality, which allows on-line replacement of a faulty module or continuous backup to an active module. Analog input modules require a separate field termination assembly with a cable interface to the Tricon backplane. Each module is mechanically keyed to prevent improper installation in a configured chassis.

5.3.6 Thermocouple Input Modules (3708E)

Like any other Tricon input modules, the Enhanced Isolated T/C module has three independent input legs. Each input leg receives variable voltage signals from each point, performs thermocouple linearization and cold-junction compensation, and converts the result to degrees Celsius and Fahrenheit. Each leg then transmits 16-bit signed integers representing 0.125 degrees per count to the three Main Processors on demand. To ensure correct data for every scan, a value is selected using a mid-value selection algorithm.

The T/C module can be configured for various thermocouple types and engineering units and can be selected between Celsius and Fahrenheit. TriStation also programs the Isolated Thermocouple Module (3708E) for upscale or downscale burnout detection as required. If a thermocouple burnout occurs, or if the thermocouple input voltage is out of range, the Main Processors receive the integer value +32,767 for upscale burnout detection or -32,767 for downscale.

Triplicated temperature transducers residing on the field termination module support cold-junction compensation. Each leg of a thermocouple module performs auto-calibration and reference-junction compensation every five seconds using internal-precision voltage references.

Sensing of each thermocouple input is performed in a manner, which prevents a single failure on one leg from affecting another leg. Each module performs complete ongoing diagnostics on each leg.

Thermocouple modules support the hot spare feature, which allows on-line replacement of a faulty module or continuous backup to an active module. Like all I/O modules, thermocouple modules require a cable interface to a remotely located external termination panel. Each module is mechanically keyed to prevent improper installation in a configured chassis.

5.3.7 Analog Output Module (3805E)

The Analog Output (AO) module receives output signals from the Main Processors on each of three legs. Each set of data is voted, and a healthy leg is selected to drive the eight 4-20 mA outputs. The AO module monitors its own current outputs (as input voltages) and maintains an internal voltage reference that provides self-calibration and module health information. The output over-range capability of the module is +6 percent.

Each leg on the AO module has a current loopback circuit, which verifies the accuracy and presence of analog signals independently of load presence or leg selection. A non-selected leg cannot drive an analog signal to the field. A LOAD indicator is set to ON if the module cannot drive current to one or more outputs because of an open loop.

The AO module provides for redundant loop power sources with individual indicators, PWR1 and PWR2, set to ON when loop power is present. External loop power supplies are provided for each application. Each module requires up to 1 ampere @ 24-42.5 volts.

Each module sustains complete, ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the FAULT indicator, which in turn activates the chassis alarm contact. The FAULT indicator points to a leg fault, not a module failure. The module is guaranteed to operate properly in the presence of a single fault and may continue to operate properly with certain kinds of multiple faults.

AO modules support hot spare functionality, which allows on-line replacement of a faulty module or continuous backup to an active module. Like all I/O modules, AO modules require a cable interface to a remotely located external termination panel. Each module is mechanically keyed to prevent improper installation in a configured chassis.

5.3.8 Digital Input Modules (3501E, 3502E, 3503E)

The Tricon supports a variety of Digital Input Modules (DI). Each DI module has three independent legs, which process all data input to the module. A microprocessor on each leg scans each input point, compiles data, and transmits it to the Main Processors upon demand.

Then input data is voted at the Main Processors just prior to processing to ensure the highest integrity.

All DI modules sustain 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 contact. The FAULT indicator points to a leg fault, not a module failure. The module is guaranteed to operate properly in the presence of a single fault and may continue to operate properly with certain kinds of multiple faults.

TMR Digital Input Modules with Self-Test (3502E, 3503E) continuously verify the ability of the Tricon to detect the transition of a normally energized circuit to the OFF state.

All DI modules support hot spare functionality, which allows on-line replacement of a faulty module or continuous backup to an active module.

Like all I/O modules, DI modules require a cable interface to a remotely located external termination panel. Each module is mechanically keyed to prevent improper installation in a configured chassis.

5.3.9 Pulse Input Module (3511)

The Pulse Input (PI) Module provides eight, very sensitive, high-frequency inputs. It is used with non-amplified magnetic speed sensors common on rotating equipment such as turbines or compressors. The module senses voltage transitions from magnetic transducer input devices. The transitions are accumulated during a selected window of time (rate measurement), and the resulting count is used to generate a frequency or RPM which is transmitted to the Main Processors. The pulse count is measured to 1/2 microsecond resolution.

The PI module has three isolated input legs. Each input leg independently processes all data input to the module and passes the data to the Main Processors, where it is voted just prior to processing to ensure the highest integrity.

Each PI module provides ongoing diagnostics on each leg. Failure of any diagnostic on any leg activates the module's FAULT indicator, which in turn activates the chassis alarm contact. The FAULT indicator points to a leg fault, not a module failure. The module is guaranteed to operate properly in the presence of a single fault and may continue to operate properly with certain kinds of multiple faults.

The PI module supports hot spare functionality and requires a cable interface to a remotely located external termination panel. Each Pulse Input module is mechanically keyed to prevent improper installation in a configured chassis.

5.3.10 Digital Output Modules (3601E, 3603E/T, 3607E, 3623, 3625)

The Tricon supports a variety of Digital Output (DO) Modules. Every TMR DO module houses the circuitry for three identical, isolated legs. Each leg includes an I/O micro-processor, which receives its output table from the I/O communication processor on its corresponding Main Processor. All of the DO modules use special quadruplicated output circuitry, which votes on the individual output signals just before they are applied to the load. This voter circuitry is based on two parallel paths which pass power if the drivers for Legs A and B, or Legs B and C, or Legs A and C command them to close—in other words, 2-out-of-3 drivers voted ON. The quadruplicated output circuitry provides multiple redundancies for all critical signal paths, ensuring safety and maximum availability.

Each type of DO module executes a particular type of Output Voter Diagnostic (OVD) for every point. In general, during OVD execution the commanded state of each point is momentarily reversed on one of the output drivers, one after another. Loop-back sensing on the module allows each microprocessor to read the output value for the point to determine whether a latent fault exists within the output circuit. For devices that cannot tolerate a signal transition of any length, OVD on both AC and DC voltage digital output modules may be disabled.

The Supervised Digital Output Modules (3623, 3625) provide both voltage and current loopback sensing, allowing complete fault coverage for both energized-to-trip and de-energized-to-trip conditions. In addition, a supervised DO module verifies the presence of the field load by doing continuous circuit-continuity checks. The module annunciates any loss of field load.

A DC voltage DO module (3603E/T, 3625, 3607E) is specifically designed to control devices, which hold points in one state for long periods of time. The OVD strategy for a DC voltage digital output module ensures full fault coverage even if the commanded state of the points never changes. On this type of module, the output signal transition normally occurs during OVD execution, but is designed to be less than 2.0 milliseconds (500 microseconds is typical) and is transparent to most field devices.

On the AC voltage DO module (3601E), a faulty switch identified by the OVD process will cause the output signal to transition to the opposite state for a maximum of half an AC cycle. This transition may not be transparent to all field devices. Once a fault is detected, the module discontinues further iterations of OVD. Each point on an AC voltage DO module requires periodic cycling to both the ON and OFF states to ensure 100% fault coverage.

All DO modules support hot sparing for on-line replacement of a faulty module or continuous backup to an active module. Each module is mechanically keyed to prevent improper installation in a configured chassis.

Like all I/O modules, DO modules require a cable interface to a remotely located external termination panel. DO modules are designed to source the current to field devices. Field power must be wired to each output point on a field termination module.

5.3.11 Relay Output Module (3636T)

The Relay Output (RO) Module is a non-triplicated module for use on points which are not compatible with "high-side" solid-state output switches: An example is interfacing with annunciator panels. The RO module receives output signals from the Main Processors on each of three legs. The three sets of signals are then voted, and the voted data is used to drive the 32 individual relays. Each output has a loopback sensing circuit, which verifies the operation of each relay switch independently of the presence of a load. Ongoing diagnostics test the operational status of the RO module, which is not intended for switching of field loads.

The RO module supports hot sparing for on-line replacement of a faulty module or continuous backup to an active module. Each module is mechanically keyed to prevent improper installation in a configured chassis.

Like all I/O modules, RO modules require a cable interface to a remotely located external termination panel. Field power must be wired to each output point on a field termination module.

5.3.12 Seismic Balance Module (8107)

The Seismic Balance Module (SBM) is a weighted module, approximately the weight of a DO module, but having no active components mounted on the module. It is not mechanically keyed, so it may be inserted into any empty slot.

5.4 Tricon Capacity

5.4.1 Tricon I/O Capacity

A Tricon system is composed of a single Main Chassis and up to 14 Expansion or Remote Expansion Chassis. The Main Chassis has six slots, which can house a combination of I/O and Communication Modules. An Expansion Chassis can house 8 I/O Modules and a Remote Expansion Chassis can house 6 I/O Modules.

The maximum number of I/O modules in a Tricon system is 118, which is a physical limitation. The MP operating system I/O allocation limitations allow up to 2048 Digital Input points, 2048 Digital Output points, 1024 Analog Input points, 512 Analog Output points, and 80 Pulse Input points.

5.4.2 Tricon Processing Speed Capacity

Tricon scan time is function of the number of chassis, number and type of I/O modules, functions used within an application program and its length. The Tricon supports scan times between 10 msec. and 450 msec. Typical scan times are less than 100 msec.

5.5 Tricon Installation

Chapter 3 of the Tricon Planning and Installation Guide (Reference 4.20) provides detailed installation information. The Tricon may be mounted using Invensys TRICONEX provided chassis mounting brackets at the rear, front or both for maximum support. (The TUT was seismically qualified utilizing both front and rear brackets). For safety related installations four (4) mounting brackets are required. Each bracket is attached to an appropriate seismic rated structure using four, stainless steel, 10-32UNF screws, washers and nuts. Each is tightened to a

x.

torque of 31 in-lbs. Captive screws at the top and bottom of each Tricon module are tightened to 12, +/- 2 in-lbs. The structure should be designed to support the weight and moments of the Tricon during postulated seismic events. Multiple chassis may be mounted within a single enclosure. When there is more than one chassis within an enclosure, Invensys TRICONEX recommends a minimum of 1.75 inches vertical clearance for cable access and 5.25 inches between top, bottom and side panels for convection cooling.

Each Tricon chassis should be properly grounded to an Earth Ground Bus Bar as shown in Tricon Planning and Installation Guide (Reference 4.20). The Tricon's internal signal ground is allowed to float with respect to the safety ground. Each Tricon Power Module is equipped with an internal RC network to limit the potential voltage differences between the signal ground and safety ground. The signal ground and safety ground should be connected at the same point.

On analog termination panels, connections are provided for field wiring shields. Invensys TRICONEX recommends connecting one end of the shield at the field device. If this is not practical, an external shield bus bar should be installed which is connected to earth ground.

5.6 Tricon Handling And Storage Requirements

As indicated in the Tricon Planning and Installation Guide (Reference 4.20), and in compliance with Sections 4.10.1 – 4.10.3 of TR-107330, Tricon components should be stored within factory provided containers, in a controlled environment between –40 to 75 degrees C and a relative humidity of 5% to 95%, non-condensing.

5.7 Tricon Self Diagnostics And Redundant Feature

The Tricon is a fault tolerant controller. As such, it is designed to run continuous diagnostics to detect and mask or override faults. Diagnostic results are available to host devices via communication modules and alarm contacts on the Main Chassis. The alarm contacts on Main Chassis Power Modules are asserted when:

1. The system configuration does not match the control-program configuration
2. A Digital Output (DO) Module experiences a LOAD/FUSE error
3. A module is missing somewhere in the system
4. A Main Processor, I/O or Communication module in the Main Chassis fails
5. An I/O or Communication module in an Expansion Chassis fails
6. A Main Processor detects a system fault
7. The inter-chassis I/O bus cables are incorrectly installed—for example, the cable for Leg-A is accidentally connected to Leg-B
8. A Power Module fails
9. Primary power to a Power Module is lost
10. A Power Module has a Low Battery or Over Temperature warning

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 errant module is hot-replaced or operated in a fault-tolerant manner until hot replacement is completed.

Main Processor diagnostics do the following:

1. Verify fixed-program memory
2. Verify the static portion of RAM
3. Test all basic processor instructions and operating modes
4. Test all basic floating-point processor instructions
5. Verify the shared memory interface with each I/O communication processor and communication leg
6. Verify handshake signals and interrupt signals between the CPU, each I/O communication processor and communication leg
7. Check each I/O communication processor and communication leg microprocessor, ROM, shared memory access and loopback of RS-485 transceivers
8. Verify the TriClock interface
9. Verify the TRIBUS interface

All I/O modules sustain 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. The FAULT indicator points to a leg fault, not a module failure. The module is designed to operate properly in the presence of a single fault and may continue to operate properly with some multiple faults.

TMR Digital Input Modules with Self-Test continuously verify the ability of the Tricon to detect the transition of a normally energized circuit to the OFF state. TMR High-Density Digital Input Modules continuously verify the ability of the Tricon to detect transitions to the opposite state.

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

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

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

The results of all diagnostic tests are available to a host device via each installed communication module. Individual diagnostic flags are asserted upon any module fault within any chassis, DO load fuse or output voter fault, printer fault, math error, scan time overrun, Tricon keyswitch out of position, host communication error, program change, and I/O point disabled.

The Tricon Planning and Installation Guide (Reference 4.20) provide descriptions of the Main Processor (MP) and I/O modules diagnostics.

6.0 TRICON EQUIPMENT GENERAL SPECIFICATION

The Tricon Technical Product Guide (Reference 4.22) and Tricon Planning and Installation Guide (Reference 4.20) provide details of system and individual model specifications for speed, accuracy, I/O capacity (stated above), general environmental conditions, etc. The Final Summary Report (Reference 4.5) and Application Guide (Reference 4.27) provides the 1E qualification envelope specifications including environmental parameters, seismic withstand, EMI/RFI capability, surge withstand capability, 1E to non 1E isolation capability, and other characteristics which were verified during the test program.

7.0 TRICON OPERATOR'S MANUAL

The Tricon Planning and Installation Guide (Reference 4.20) provides detailed information on the operation of the Tricon, including each module status indicator, special procedures that should be used for operation of the Tricon, and the use of any switches or control that are part of a Tricon module. The guide includes a description of the fault tolerant operation of the Tricon and its use of redundancy features.

8.0 TRICON PROGRAMMING MANUAL

The following information is excerpted from the TriStation 1131 User's Manual (Reference 4.25) and the Tricon Planning and Installation Guide (Reference 4.20) and is not intended to be an exhaustive resource. The reader should reference Invensys TRICONEX provided documentation listed in Section 4 "Reference" for complete details.

The Tricon is configured and programmed using TriStation 1131. TriStation TS1131 is a Windows based programmer's tool for developing, testing, and documenting Tricon applications. TriStation 1131 Developers Workbench supports three languages that fully comply with IEC 1131-3 International Standard on Programming Languages for Programming Controllers as reflected in the guidelines documented in the IEC 65A Type 3 Report. TS1131 is also compliant with NUREG/CR-6463 "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems." The three languages are: Ladder Diagrams (LD); Structured Text (ST); and Function Block Diagram (FBD).

LD is the traditional PLC language, which is a graphically oriented language that uses a standard set of symbols to represent relay ladder logic. Elements in LD are primarily contacts and coils connected by links. Links transfer Boolean data between LD symbols. This flow is consistent with the power flow characteristics of relay logic. Functions and Function Blocks may be used in LD diagrams.

ST is a general purpose, high-level programming language, similar to PASCAL, or C. ST is particularly useful for complex arithmetic calculations, and can be used to implement complicated procedures that are not easily expressed in the graphical languages, LD or FBD.

FBD is a graphical oriented language that corresponds to block or circuit diagrams. The elements used in this language appear as blocks wired together to form circuits. The "wires" communicate binary or other types of data between the FBD elements.

TS1131 also supports the Cause and Effect Matrix Programming Language Editor (CEMPLE), an automated implementation of the traditional Cause and Effect Matrix (CEM) methodology, used specifically to develop safety shutdown applications. CEMPLE provides a two-dimension matrix with Cause Rows and Effect Columns. Once a CEM is defined, CEMPLE automatically generates an FBD program, which implements the safety shutdown application.

8.1 TriStation 1131 Developers Workbench Functions

As defined by IEC 1131-3, the code within the PLC is called a Project. Projects are composed of one or more Programs. Each Program is composed of one or more Function and Function Blocks. Function Blocks are composed of one or more Functions. Programs are the highest-level logic element within a TS1131 project. Programs can invoke functions or Function blocks, but cannot invoke other Programs.

A Function is a logic element that yields exactly one result. Functions have no retentive memory capabilities; therefore, output values do not persist from one evaluation of the function to the next.

A Function Block is logic element that yields one or more values and is generally used to perform repetitive operations. Function Blocks have memory capabilities and therefore, variables persist from one evaluation of the function block to the next, allowing values calculated for one evaluation to be used in the next. For more details about description of function and function blocks refer TriStation 1131 Libraries Reference (Reference 4.25).

8.2 TriStation 1131 Functions

TriStation 1131 supports a rich set of Functions and Function Blocks in three libraries. The Standard Library of Functions is defined by the IEC-1131 standard, which includes Boolean logic (AND, OR, NOT), bit manipulation, data conversion, arithmetic functions, and comparisons. The Tricon Library Functions include higher-level functions as specified by Invensys TRICONEX customers, which include process control functions (PID, Lead/Lag, etc.), Fire and Gas functions. The Tricon Library Functions include Sequence of Events, System Health Status, and Communications Functions (Peer-to-Peer, MODBUS, and Printer). Should the project require a function not supplied in these libraries, TS1131 supports the development of user specified

Functions and Function Blocks under stringent data type and compilation controls. For more details about description of functions and function blocks refer TriStation 1131 Libraries Reference (Reference 4.25).

8.3 TriStation 1131 Example – Process Control Program

Figure 6 is an example of a single TS1131 program using the Function Block Diagram Language. A PID function block and Lead Lag function block are used to demonstrate the process control functionality. The output from the PID function block is passed to the Lead Lag function block, which passes its output to the PID variables.

As is shown in Figure 6, FBD is a graphical programming language similar to ISA Function Diagrams. The programmer selects and sets Functions and Function Blocks on the page, and draws connecting "wires" to form a functional network. Functions and Function Blocks resources may be selected from the Standard Functions Library (as defined by IEC 1131-3), the Tricon Functions Library (process control functions provided by Invensys TRICONEX), or from a Project Specific Library of functions (developed by the customer).

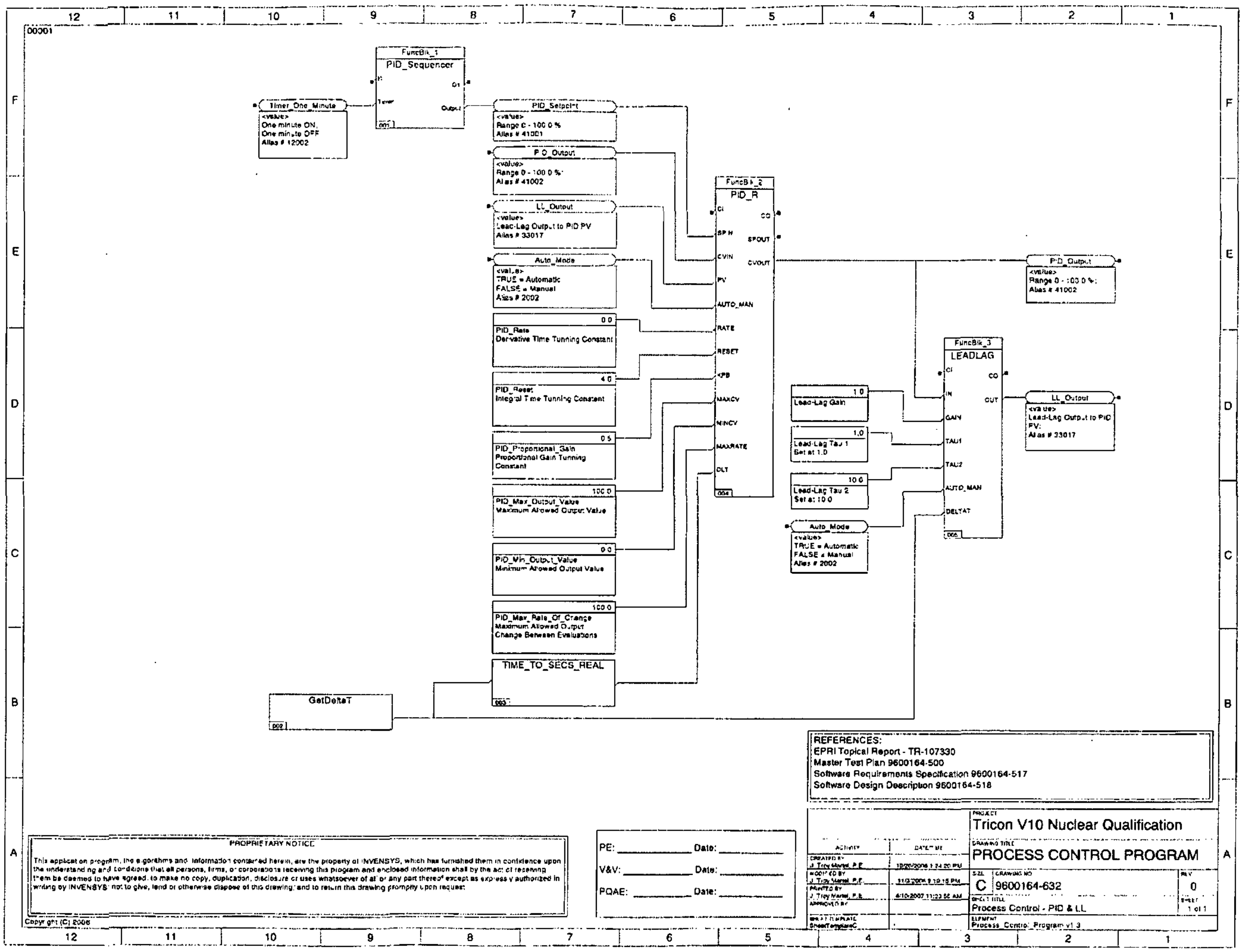


Figure 6 – Process Control Program

8.4 TriStation 1131 Limitations

The Tricon supports up to 4Mb memory for a single TS1131 project. Each TS1131 project supports up to 250 Programs composed of Functions and Function Blocks. Each function or function blocks support up to 400 variables. A single program may contain up to 2000 variables (input, output, and local variables).

8.5 TriStation 1131 Resource Allocation Features

TS1131 automatically allocates resources based on system configuration and program size. TS1131 also offers a rich set of features to monitor and re-allocate Tricon resources if the programmer desires. The Hardware Allocation node of the configuration tree supports monitoring chassis power usage, and chassis and module configuration. The Memory Allocation node supports changing memory allocation for memory, input and output points if desired.

8.6 TriStation 1131 Program Emulation Features

TS1131 supports all Tricon functionality requirements. No other terminal or software is required. TS1131 supports hardware and software configuration, programming, program and data base documentation and program emulation. The Emulation Control Panel supports functional testing of the program prior to downloading into the Tricon. Inputs may be simulated and program operation may be observed in single triggered scan or continuous scan in TS1131 on the programmer's PC.

8.7 TriStation 1131 User Created Functions

TS1131 provides a rich set of tools to allow the programmer to develop unique functions in a safe programming environment. Function Blocks written in Structured Text must conform to good programming practices of variable name and type declaration prior to the body of the function. Format of each statement must confirm to TS1131 discipline. The TS1131 Build command will first save the function, check for data types, naming convention, and code structure prior to compiling the function. Only if there are no errors will compilation complete. Compile errors are counted and displayed in the Message Bar. Selecting the error message directs the editor to the problem statement.

8.8 TriStation 1131 Flow of Control Statements

Invensys TRICONEX believes user directed Flow of Control statements are hazardous within safety related software; therefore, none is supported by TS1131. TS1131 does not support GOTO (forward or backward), SKIP, JUMP, SUBROUTINES, USER DEFINED INTERUPTS, etc. or any function that would alter project flow from beginning to end.

8.9 TriStation 1131 Dynamic Functions

TS1131 dynamic functions (PID, LEADLAG, LOOPDETR) are executed each scan, but their outputs are updated only on programmer specified Function Evaluation time. Therefore, dynamic functions have minimal effect on project scan time.

8.10 Tricon Module Interaction

Voltage and current signals received at input module termination panels are conducted via multi-conductor cables to input modules. Signals are immediately distributed to the three independent module legs where the field signal is conditioned to word or bit logic levels, and serially transmitted to the respective Main Processor on request. Each MP re-transmits the input data to its up-stream and down-stream neighbor. Each MP votes the data received from its input module leg with that received from neighboring MPs, using a 2 out of 3 (2-o-o-3) algorithm for discrete inputs and a mid-value selection algorithm for analog signals. Each MP uses the voted signal in computing the application program (project). Each MP serially transmits the results of the application program to the respective output module leg, where the signal is again voted using quad-voter hardware for discrete outputs and round robin with feed back hardware for analog outputs.

Each MP exchanges all aliased data (Tag Names) with the respective legs of all communication modules, each scan. Data is exchanged with the host via serial or 802.3 communication ports of the communication module.

8.11 Tricon Redundancy

The Tricon is designed and functions as a fault-tolerant controller, using independent triplicated circuitry. This triple modular redundancy is inherent to the system and requires no system or application programming by the user. Extensive system diagnostics are employed to detect errors and set system flags and alarms. Diagnostic indicators on each module are illuminated should a fault occur. The internal flags and alarms are also available to the host device for logging and/or display at the plant operator's console.

8.12 Tricon Safety System Configuration

The Tricon hardware and software is specifically designed for safety-related and critical control applications within the industrial environment. No special system or application programming, software tools, special build or compile procedures are required for safety-related or critical control applications.

8.13 Tricon Executive Software

A Tricon utilizes two fundamental software architectures representing two basic software sets. The main set (ETSX and IO/COM) is executed on a Main Processor providing primary control for the Tricon. The second set is the software executed on each I/O and Communication Modules. Figure X shows the overview of the Tricon software architecture.

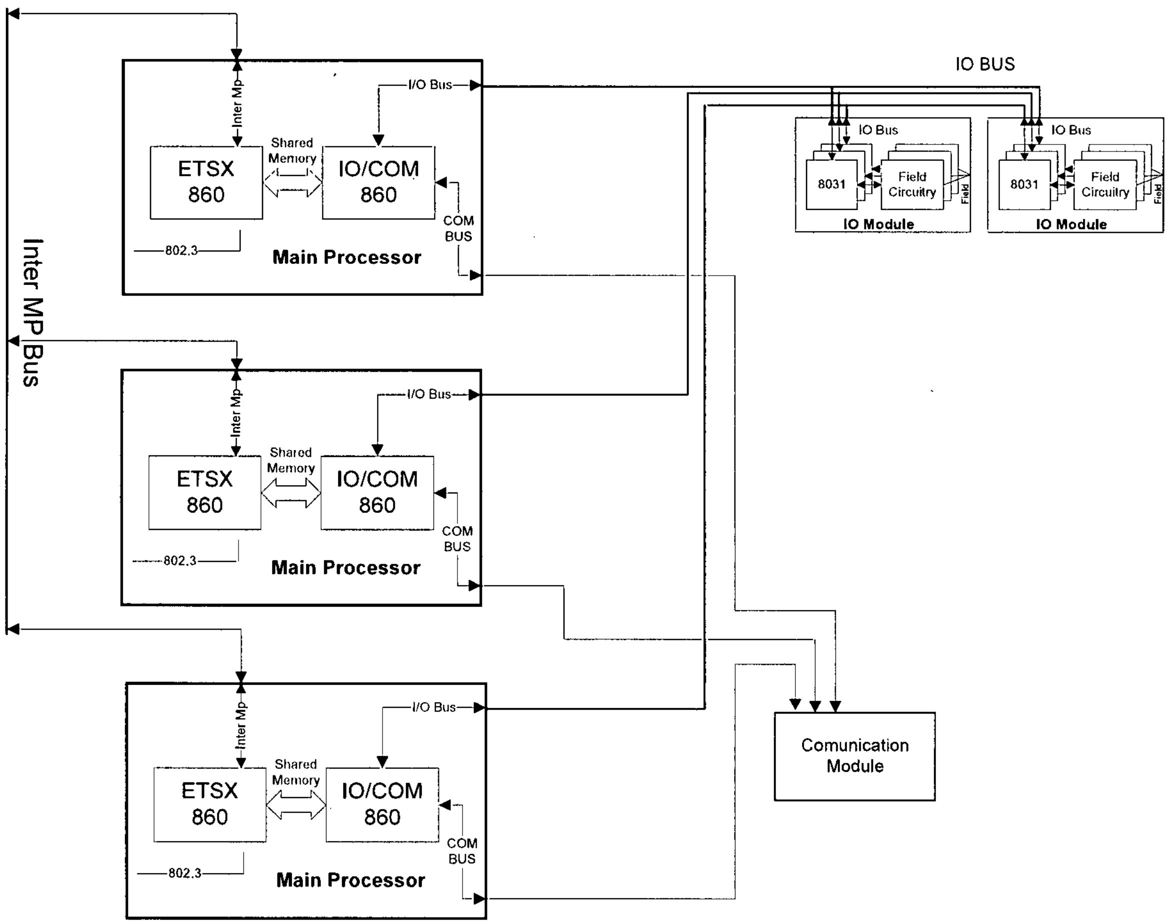


Figure 7 - Tricon System Software

The Tricon System Executive (ETSX) is the firmware that runs on the Main Processor along with the IOCCOM firmware. The main function of ETSX is to provide an execution environment for the TS 1131 Application (Control Program).

ETSX is concurrently running on the three Main Processors in the Tricon System. These Processors are kept in real time synchronization by a combination of the Tritime, hardware and software. ETSX uses this real time synchronization to rendezvous all three of the Main Processors at the maximum scan rate. Once the rendezvous occurs, ETSX transfers information between the three Main Processors. ETSX then decides what functions that need to be done during this scan. These include updating memory, running a control program, etc.

The ETSX firmware executes the Control Program generated by the user and down loaded from TRISTATION. The Control Program uses Digital and Analog IOCCOM Inputs and sends outputs to the IOCCOM and COMM boards. ETSX controls timing and synchronization between the three MPs, voting of input data and system data, detection and analysis of I/O faults and internal faults, and communication with TS 1131 and the diagnostic port.

ETSX is divided into three tasks: Scan task, Communication Task, and Background Task.

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

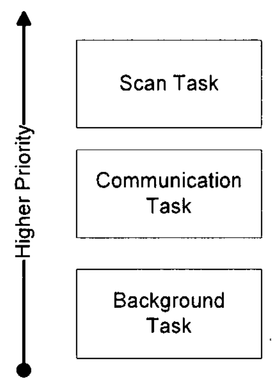


Figure 8 - ETSX tasks and priorities

The Scan task performs the following steps:

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

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

1. Process Messages from IOC/COM.
2. Process Messages from COMMUNICATION MODULES.

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

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

Figure A shows the overview of the EMP Diagnostics subsystem.

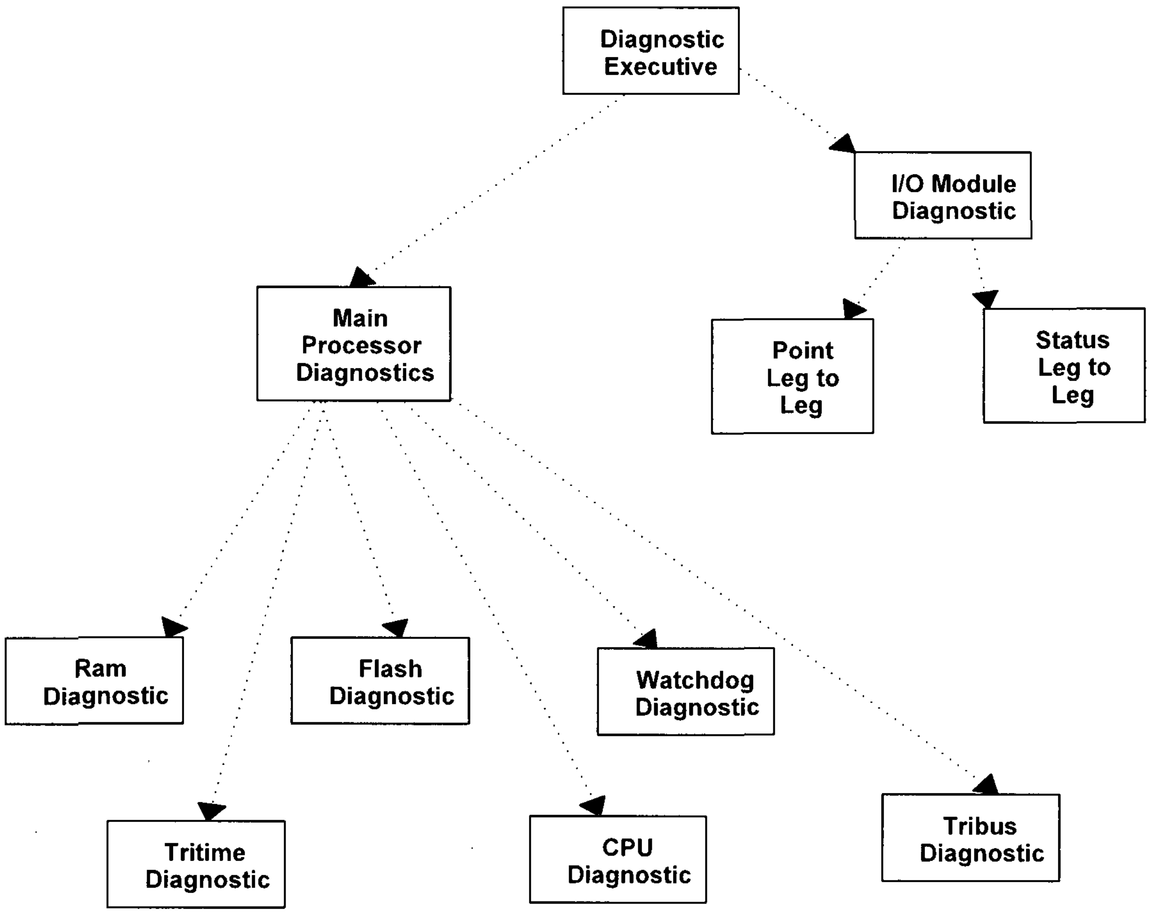


Figure 9 - EMP Diagnostics subsystem

The I/O module software (second set of software) is executed on each leg of an I/O module. This software is divided into core functions that are common to all I/O modules and functions that are specific to individual I/O modules. Core functions include runtime diagnostics (checksum verification of I/O module EPROM memory and shared RAM, Watch Dog timer testing, testing for "stuck" discrete inputs, output power detect testing, etc.) and I/O bus messaging.

8.14 TriStation 1131 Data Base Management

The user, utilizing the TriStation 1131 Workbench, develops TRICON application programs. Application programs are written using one of the supported language editors and are usually a graphical representation at the user level. TS1131 manages the database of I/O and memory points (tag name, data type, and description), Tricon configuration management, and performs the following task:

1. Develop programs, functions, function blocks, and data types
2. Configure the I/O modules and points for each Tricon chassis
3. Manage security and password protection of each project and program
4. Print application program logic, hardware configuration, and variable lists
5. Verify application program logic via emulation at the workstation.
6. Download and verify projects (programs) to the Tricon.

Each I/O and memory point has a rich set of properties including: tag name, data type, address, alias, group assignment, and description, which is managed by TriStation 1131.

8.15 Tricon Diagnostics

The Tricon performs two extensive types of diagnostics: initialization (Power Up) diagnostics and run-time (Scan Level) diagnostics. Initialization diagnostics are run on every module after power is first applied. Run-time diagnostics run continually on modules that have passed the initialization tests.

Faults detected are classified into five categories:

1. Hard Fault - The failed leg will no longer respond to the EMP. The other legs of the module that have not experienced a fault continue to operate normally. On enhanced boards, the non-failed legs will report with a "Minor Error" the inactivity of the failed leg and any error code the leg stored in shared memory.
2. Fatal Fault - The failed leg will report the error to the EMP on the next poll message from ETSX. Six bytes of additional information are included in the poll response message. The failed leg will no longer drive outputs. Inputs are defaulted to zero or the configured upscale or downscale values.
3. Major Fault - This category of faults includes Dual-Port RAM failures and failures that do not effect the proper operation of the board. Diagnostics that would affect inputs or output are suspended. The error is reported to the EMP in the same as a Fatal Fault.
4. Minor Fault - This category of faults is reported to EMP for logging purposes only. Minor errors are generated when errors are detected but they haven't reached the catastrophic level.

5. Information - This category of faults is reported to EMP for logging purposes only.

Initialization diagnostics are run immediately after power is applied to the system or the module is installed in the backplane. There are several different tests that are executed sequentially, some of them multiple times. I/O modules are not permitted to communicate with the system until initialization diagnostics have been successfully completed. When the I/O module successfully completes the initialization diagnostics, it enters the "Executive Loop" where it is allowed to respond to system messages on the I/O Bus. If a fault is detected by one of the initialization diagnostics or if one of the module legs is unable to perform the tests, the leg's watch-dog timer is allowed to expire. The failed leg goes to a benign state, with the Fault LED illuminated, and disabled from communicating on the bus.

Run-time diagnostics run continually while the system is in operation. Diagnostics segments are alternately scheduled with the modules main program. The next diagnostic segment in sequence is executed with the next program cycle. Run-time diagnostics are scheduled in one of three ways:

1. Background diagnostics are continuously scheduled.
2. Leg dependent diagnostics are run one leg at a time. Execution is controlled by a token that is passed between the legs.
3. Event driven diagnostics are initiated by a clock timer or a specific system event.

When a Hard, Fatal or Major fault is detected, it is annunciated by illuminating a FAULT LED on the face of the faulty module and expressing alarm contacts on the chassis, and by setting internal flags, which are aliased. The flags may be used within the application program if desired and they may be monitored by one or more host devices for operator awareness and/or logging.

System variables indicate the health status of the Tricon system, individual chassis, and the modules in each chassis. System variables are available to the application program and external hosts.

9.0 TRICON PLANNING AND INSTALLATION GUIDE

The Planning and Installation Guide (Reference 4.20) provides details of Tricon System planning, installation and maintenance.

- Chapter 1 describes the main features, system configuration, and theory of operation.
- Chapter 2 describes the Tricon system components (Chassis, power supplies, EMP module, Communication modules, I/O modules, etc.).
- Chapter 3 describes the installation and maintenance instructions and guidelines. It includes system installation, chassis and module installation, controller grounding, maintenance and module replacement.
- Chapter 4 describes fault and alarm indicators for the Tricon system, EMP, I/O and communication modules.
- Appendices provide additional installation and maintenance information

10.0 TRICON TEST SPECIMEN DOCUMENTATION

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, fulfills the major portion of the requirements for qualifying the equipment.

Section 6.2 (PLC System Test Configuration) of EPRI TR-107330 describes requirements for configuring and programming a representative sample of the selected PLC. The sample, identified as the Qualification Test Specimen, consists of a selection of standard hardware and software that supports the qualification testing requirements of EPRI TR-107330. The PLC modules, ancillary equipment, communication paths, and interfaces are tested with hardware, software and diagnostics representative of those intended for actual operation.

Invensys TRICONEX Tricon PLC system is provided as a representative sample for the Qualification Test Specimen. This system is defined in Appendix 1 of the Master Test Plan (Reference 4.2) and is consistent with the technical requirements of EPRI specification TR-107330. In general, the setup consists of a standard Tricon PLC system configured with a selection of modules needed to encompass a variety of applications.

System Architecture drawings, wiring diagrams, and other diagrams were developed to define the configuration of the Tricon-Under-Test (TUT). Test plans and procedures provided specific details on hardware mounting and interfaces used in the qualification testing. A Test Specimen Application Program (TSAP) was developed and integrated with the equipment. Detailed configuration information such as serial numbers, software versions, etc. is included in the Master Configuration List (MCL). The MCL (Reference 4.3) also captured all hardware and software configuration information.

10.1 PLC System Test Configuration Requirements

As required by EPRI TR-107330 the test specimen configuration, test specimen design, test specimen application program development, and any supporting test fixture design were in compliance with the applicable requirements of Sections 7.3 (10CFR21 Compliance), 7.7 (Configuration Management), 7.8 (Problem Reporting/Tracking), and 8.6 (Qualification Documentation). The requirements of Section 8.11 (System Software/Hardware Configuration Documentation) were applied to all hardware and software, including all software tools and supporting software.

10.1.1 Test Specimen Hardware Configuration Requirements

The hardware configuration used was developed and documented in compliance with the Quality Assurance Measures and Acceptance Criteria as stated in EPRI TR-107330 Section 6.5 and Section 8.6.3. The test specimen included the following items listed below and deviations from the stated requirements are captured in theEQ Summary Report (Reference 4.5).

A. The Tricon-Under-Test (TUT) was populated with the modules needed to encompass the requirements of EPRI TR-107330 Sections 4.3 (Hardware) and any hardware related requirements in Sections 4.4 (Software/Firmware), 4.5 (Human/Machine Interface), and 4.9 (Other). Some particular modules were configured, to provide different capabilities (e.g., Two NGAI modules were used to measure normal voltage inputs and RTD inputs, respectively). Hence, sufficient modules were used to cover the configurations needed to meet the referenced requirements. A Type K thermocouple module was also tested as a part of this qualification project.

B. Modules in the TUT were setup to support Operability Test and Prudency Test requirements. Further inputs and outputs from the Simulator Tricons (Chassis-5 & Chassis-6) were also configured as an aid to Operability and Prudency Test.

C. The Tricon Communication Module was selected to meet the requirements of EPRI TR-107330 Sections 4.3 (Hardware) and any hardware related requirements in Sections 4.4 (Software/Firmware), 4.5 (Human/Machine Interface), and 4.9 (Other). Although permitted by Sections 4.3.2 and 4.3.3 of EPRI TR-107330, no additional external devices were used to meet the requirements of Sections 4.6.2 (Surge Withstand Capability) and 4.6.4. (Class 1E/Non-1E Isolation). The modules used in the TUT were capable of handling the Surge and Class 1E/Non-1E Isolation requirements.

D. One main chassis, two remote expansion chassis and one expansion chassis were selected to meet the requirements of EPRI TR-107330 Section 4.2.1 (General Functional Requirements). The connections between the main chassis and the expansion chassis used typical application cable lengths. Chassis to chassis signal loading caused by connecting the number of chassis needed to meet the requirements of Section 4.2.1 (General Functional Requirements) were simulated.

E. Due to Tricon System Architecture, additional load resistors could not be placed. Refer to the EQ Summary Report (Reference 4.5) for more details about the exception.

F. Chassis-3 of the TUT was fully loaded with each logical slot filled. Spare module slots were populated with module blanks. Refer to the EQ Summary Report (Reference 4.5) for more details. All empty slots in Chassis-1 and Chassis-4 were loaded with Seismic Balance Modules (SBM), each of which approximate the weight of a Digital Output Module.

G. Chassis-1 and Chassis-2 of the TUT were connected using the IO/COMM Bus Extension Cable. Similarly, Chassis-3 and Chassis-4 of the TUT were connected using the I/O Bus Extension Cable. Chassis-2 and Chassis-3 of the TUT were connected using fiber optic cables. All Tricon modules are field replaceable modules consisting of an electronic assembly housed in a metal spine. Signals from the field are easily connected to an electrically passive printed circuit board called an External Termination Panel (ETP). The ETP and its associated cable pass input signals from the field directly to an input module or pass output signals from the output modules to the field wiring. The ETP cables are connected to a 56 Pin Connector at the top of the Tricon Controller. This arrangement permits the removal or replacement of I/O modules without disturbing the field wiring.

H. Fiber Optic Cables between the Chassis-2 and Chassis-3, IO/COMM Bus cables between Chassis-1 and Chassis-2, IO Bus Cables between Chassis-3 and Chassis-4 and power supplies required to implement redundancy were installed in the TUT.

I. Tricon modules in the simulator Tricon and other M&TE required to support operability and prudency testing per EPRI TR-107330 Sections 5.3 (Operability Test) and 5.4 (Prudency Testing) were used. The modules in the Simulator Tricon were not a part of the TUT and were not subjected to any testing or configuration control.

J. One power supply of the redundant pair in each TUT chassis was a 115Vac supply to accommodate power quality testing.

K. All power requirements for the TUT were provided by individual external power supplies (PS-1 to PS-6). To accommodate power frequency changes, power to the 230Vac chassis power supplies was provided through a step-up transformer. Refer to Power distribution drawings 9600164-202 to 9600164-207 for more details about the external power supplies.

L. The model 9764-310 termination panel (4-7T) was populated with Analog Devices signal conditioners. The conditioners were qualified as part of the TUT in order to accommodate RTD and mV inputs.

M. The TUT utilized "loop-back" wiring in order to simplify the test system configuration. The basis was that looping analog or discrete outputs back to analog or discrete inputs would eliminate the need for input simulators for those input points, and would reduce the amount of wiring that had to be connected from the test specimen to the extended test system (the input simulators and the data acquisition and control systems).

10.1.2 Test Specimen Application Program Requirements

Test Specimen Application Program (TSAP) were developed using the applicable portions of Section 8.6 (Qualification Documentation) and Section 7 (Quality assurance) and its subsections of EPRI TR-107330. For more details about TSAP design, refer TSAP Software Design Description (Reference 4.4).

10.2 Tricon Qualification Test Specimen Hardware

Shown in Figures 10A and 10B is a block diagram of the TUT provided in the test suite. The TUT was comprised of a four chassis system, housing modules submitted for qualification testing. The TUT program (Test Specimen Application Program - TSAP), composed of a set of networks and algorithms typically used to simulate all I/O requirements as stated in EPRI TR-107330, was running continuously.

Two other Tricon Systems (See Figures 110A and 10B) served as a simulator to emulate I/O in real time. The Simulator Tricon running the Simulator Application Program (Sim-1 & SIM-2) provided outputs for the connection of the inputs to the TUT. A unique set of data was transmitted continuously between the TUT and Simulator Tricon using the peer-to-peer capabilities of the TCM. Similarly, a unique set of data was transmitted continuously between the TUT and the Simulator Tricon using the Modbus serial interface capabilities of the TCM Serial Ports.

a, b

10.2.1 Tricon-Under-Test Description

Details of the TUT configuration and mounting are described in the Master Configuration List (Reference 4.3) and General Equipment Arrangement Drawing 9600164-100 (Reference 4.6).

a, b

Three different chassis, three different Power Modules, two different RXM sets, four communication modules and seventeen different I/O modules were included in the TUT system. Modules were positioned within each chassis to maximize stress during environmental, seismic and electrical testing. The use of Seismic Balance Modules in each open slot of the Main Chassis and the Expansion Chassis maximizes chassis weight. All I/O modules were connected to their respective termination panels as indicated in the Master Configuration List.

a, b

a, b

10.2.2 Simulation Tricon

Details of Two Simulation Tricon configuration and mounting are shown on General Arrangement drawing 9600164-100 (Reference 4.6). The two Simulators were mounted on a freestanding 19" relay frame. Simulator-1 in Chassis-5 housed two Power Modules, three Main Processors, two TCM, one Relay Output Module and a 4-20 mA Analog Output Module. Simulator-2 in Chassis-6 housed two Power Modules and two TCM.

a, b

a, b

Table 1 – Tricon Under Test Equipment

a, b

Table 2 – Manual Input Devices

a, b

a, b

a, b

Table 3 – TUT and Simulator I/O Configuration

EPRI Section
4.3.2.3.1
4.3.2.1.4
5.4.A 3&4
6.4.3
6.3.3
6.4.3
6.3.3
5.4.A 3&4
5.4.A 3&4 and 6.4.3
6.3.3
5.4.A 1&2
5.3 B
5.4.A 1&2
5.4 A&B
5.4.A 1&2 and 6.4.3
5.4 A 1&2
6.3.3
5.4 A&B
5.4.A 1&2 and 6.4.3
5.4 A 1&2
6.3.3
5.4.A 1&2 and 6.3.4.2
6.3.3
6.3.4.2
6.3.3
5.3B & 6.2.2.B.5
5.3G & 6.2.2.B.7
6.3.3
6.3.4.2
5.3G & 6.2.2.B.7

EPRI Section
5.3B & 6.2.2.B.5
5.3B
6.3.4.2
5.3G & 6.2.2.B.7
5.3B & 6.2.2.B.5
5.4.A 3&4
5.4.A&B
5.4.A 3&4
5.4.A&B
5.4.A 3&4
5.4.A&B
5.4.A&B
5.4.A 3&4
5.4.A&B
5.4.A 3&4
5.4.A&B
5.4.A 3&4
5.4.A&B
5.4.A 3&4
4.3.2.1.3
5.4.A&B
5.4.A 3&4
5.3.B
5.3.K
5.3.B
5.4.A&B