invensys

NUCLEAR QUALIFIED PRODUCTS

TRICON V10 CONFORMANCE TO REGULATORY GUIDE 1.152

Document No.: NTX-SER-10-14

Revision: 0

Issue Date: July 11, 2010

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

The purpose of this document is to address the conformance of the Tricon V10 Programmable Logic Controller (PLC) to the guidance contained in NRC Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Reference 1).

The regulation at 10 CFR 50.55a(h) requires that protection systems for nuclear power plants meet the requirements of IEEE Std. 603-1991 (Reference 2) and the correction sheet dated January 30, 1995. With respect to the use of computers in safety systems, IEEE Std. 7-4.3.2-2003 (Reference 3) specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std. 603-1998, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std. 7-4.3.2-2003 evolved from IEEE Std. 7-4.3.2-1993 and reflects advances in digital technology. It also represents a continued effort by IEEE to support the specification, design, and implementation of computers in safety systems of nuclear power plants. In addition, IEEE Std. 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std. 603-1998.

Safety-Related instrumentation and control system designs based on the Tricon V10 make extensive use of advanced technology (i.e., equipment and design practices) relative to existing safety systems in the current operating fleet of U.S. nuclear reactors. Tricon V10 designs are functionally different from current designs, such as the use of microprocessors, modular redundancy, fiber optics, and different isolation techniques. For example, the Tricon V10 3008N main processor (MP) module contains two microprocessors, dual-port RAM (DPRAM), and a FPGA. One microprocessor executes the safety program, the other microprocessor handles all data transfer with I/O modules and Tricon Communications Modules (TCM). The two microprocessors exchange data through the DPRAM. The FPGA contains diagnostic logic. The Tricon V10 makes use of redundancy by having three redundant 3008N MP modules, hence "triple-modular-redundancy" that allows a 3-2-1 failure sequence. The FPGA on the 3008N MPs compare diagnostics to ensure failures on one module do not corrupt the safety function. Additional redundancy features include a triplicated I/O bus and triplicated communication bus (on the internal bus), and hot-spare I/O modules (i.e., dual-redundant I/O). Other advanced design features include fiber optic communications on the TCM with external devices and/or hosts. The Tricon V10 also has qualified safety-to-nonsafety isolation devices, such as the TCM and Remote Extender Modules (RXMs) that extend the internal I/O bus over distances exceeding the capabilities of copper cables.

The Tricon platform was not specifically designed for nuclear power plant applications. Though clause 5.4.2 of IEEE Std. 7-4.3.2-2003 provides general guidance for commercial-grade dedication, Invensys has generically qualified the Tricon V10 for safety-related applications in nuclear power plants in accordance with EPRI TR-107330 (Reference 4), which has been approved by the NRC as an acceptable approach for qualifying commercial PLCs for safety-related applications. Note that the Tricon V10 is a successor to the Tricon V9 system, which was also generically qualified under EPRI TR-107330, and approved by the NRC in safety evaluation

report (SER, Reference 5) dated December 12, 2001, for safety-related use in nuclear power plants.

Clause 5.9, "Control of Access," of IEEE Std. 7-4.3.2-2003 refers to the requirements in Clause 5.9 of IEEE Std. 603-1998, which states, "The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof." IEEE Std. 7-4.3.2-2003 does not provide any additional guidance for computer-based system equipment and software systems to address the IEEE-603-1998 access control requirements of Clause 5.9 or the independence requirements of Clause 5.6.3. Consequently, the NRC issued regulatory guidance concerning the security of the design and development phases of computer-based safety systems that was intended to address the criteria within these clauses[1]. The regulatory guidance clarified the staff's regulatory positions specifically concerned with the access controls and protective measures applied to the development of digital safety systems and with the ability of security features within the system to maintain system integrity and reliability in the event of inadvertent operator actions and undesirable behavior of connected equipment. The guidance was not intended to address the ability of those security features to thwart malicious cyber attacks. Rather, the requirements of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," specifies the requirements for licensees to develop cyber-security plans and programs to protect critical digital assets, including digital safety systems, from malicious cyber attacks, with RG 5.71, "Cyber Security Programs for Nuclear Facilities" (Reference 6), providing guidance to meet the requirements of 10 CFR 73.54.

In the context of RG 1.152, therefore, "Security" refers to protective actions taken against a predictable set of nonmalicious acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system.

1.1 Tricon V10 Conformance to Regulatory Guide 1.152

Based on the discussion in Section 1.0 and the definition of "security" found therein, the Tricon V10 conforms to the guidance in Regulatory Positions 2.1 through 2.5 contained in RG 1.152. The conformance table in Section 4.0, Regulatory Guide 1.152 Conformance Table, provides additional details on Tricon V10 conformance to Regulatory Positions 2.1 through 2.5. Furthermore, Invensys commits to maintain conformance to the Regulatory Positions with each new release of the Tricon, in accordance with the process described in NTX-SER-09-20, Invensys Triconex Safety Evaluation Report (SER) Maintenance Process (Reference **7**).

[1] The design requirements of 10 CFR Part 50, including the need for redundancy, diversity, and defense in depth, are based on the need to ensure reliable system functionality in the face of a wide range of nonmalicious failure modes up to and including the "design-basis accidents" described in each site's updated final safety analysis report (FSAR) and in the combined operating license and design certification applicants' FSARs. The regulations at 10 CFR Part 50 do not require licensees to include cyber-security-related features (hardware or software or both) in safety-related system designs (i.e., features intended to provide protection against malicious cyber attacks).

1.2 Scope

The remainder of this document provides the following information.

Section 2) An overview of the Tricon V10, including:

- Description of the Tricon V10 chassis configurations, including discussion of the Tricon system busses;
- Description of the Tricon V10 communications, including a summary of the compatible network protocols;

Section 3) Tricon V10 Security, including:

- Development environment security;
- Manufacturing environment security;
- Tricon V10 security features;

Section 4) The RG 1.152 conformance table; and

Section 5) References.

There are also two appendices that provide supplemental information relevant to the Tricon V10 conformance to RG1.152.

Appendix A discusses the Wurldtech testing of the Tricon V10 . It discusses the test configuration and summarizes the test results.

Appendix B discusses potential vulnerabilities of the Tricon V10 platform that are not mitigated by design. The information is generic to the Tricon V10 platform. Each identified potential vulnerability is accompanied by a possible mitigation method. However, when placed in the context of a specific plant configuration, additional mitigations may be required depending upon the plant's Cyber Security Plan developed to comply with 10 CFR 73.54 and conformance to RG 5.71, as explained in Section 1.0.

1.3 Abbreviations, Acronyms, and Definitions

ACK	Acknowledge (e.g., during network communication handshaking)
AI	Analog Input
AO	Analog Output
ASCII	American Standard Code for Information Interchange
ATWS	Anticipated Transient Without Scram
BTP	Branch Technical Position
CCF	Common-Cause Failure
CE	Conducted Emissions
CFR	Code of Federal Regulations
COM	Communication(s)
COMBUS	Communications Bus

CR	Contractor Report (e.g., NUREG/CR)
CRC	Cyclic Redundancy Check
D3	Diversity and Defense in Depth
DAS	Diverse Actuation System
DCS	Distributed Control System
DI	Digital Input
DI&C	Digital Instrumentation and Controls
DINT	Double Integer
DMA	Direct Memory Access
DO	Digital Output
DPRAM	Dual-Port Random Access Memory
EFT	Electrical Fast Transient
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
EQSR	Equipment Qualification Summary Report
ESD	Electrostatic Discharge
ESFAS	Engineering Safety Features Actuation System
ETA	External Termination Assembly
ETSX	Enhanced Tricon System Executive
EXP	Tricon Expansion Chassis
FAT	Factory Acceptance Test
FPGA	Field Programmable Gate Array
GATENB	Gate Enable (i.e,. in the standard Tricon function block Library)
GATDIS	Gate Disable (i.e,. in the standard Tricon function block Library)
GDC	General Design Criterion/Criteria
HFE	Human Factors Engineering
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IOCCOM	I/O Controller/Communications Controller
IP	Internet Protocol
ISG	Interim Staff Guidance
Kbps	Kilobits per second
KHz	Kilohertz
MHz	Megahertz
MIL-STD	Military Standard (e.g., MIL-STD-461E)
MP	3008N Main Processor
MTTF	Mean-Time-to-Failure
MVDU	Maintenance Video Display Unit
NAK	Negative Acknowledgement (e.g., during communication handshaking)
NGAID	Next-Generation I/O module – Analog Input/Differential
NGDO	Next-Generation I/O module – Digital Output
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant

NRC	U.S. Nuclear Regulatory Commission
NSB	Need Service Bit
NSIPM	Invensys Nuclear Systems Integration Program Manual
NUREG	Nuclear Regulatory
OSI	Open Systems Interconnect
OVD	Output Voter Diagnostics
OWL	One-Way Link
P2P	Peer-to-Peer
PFD	Probability of Failure on Demand
PLC	Programmable Logic Controller
PLM	Priority Logic Module
PPS	Plant Process Computer
RE	Radiated Emissions
RFI	Radio-Frequency Interference
RG	Regulatory Guide
RPS	Reactor Protection System
RTS	Reactor Trip System
RXM	Remote Expansion Chassis
SAP	System Application Protocol
SER	Safety Evaluation Report
SHMI	Safety(-related) Human Machine Interface
SVDU	Safety(-related) Video Display Unit
TCM	Tricon Communication Module
TCP	Transmission Control Protocol
TMR	Triple-Modular Redundant
TSAA	Tricon System Access Application
TR	Technical Report
TUT	Tricon Under Test
VAC	Volts – alternating current
VDC	Volts – direct current
VDU	Video Display Unit

2.0 OVERVIEW OF THE TRICON V10

The Tricon is a mature, flexible, robust, and fault tolerant controller and, as such, is ideally suited for critical control and safety-related applications in the hydrocarbon process industries, transportation – rail and transoceanic shipping, power generation, and now, with the endorsement of the NRC by SER (Reference 5), dated December 11, 2001, nuclear power and processing plants subject to NRC licensing. The Invensys Tricon V10 Equipment Qualification Summary Report (EQSR, Reference 8) demonstrates that the Tricon is sufficiently robust, and the quality of manufacturing hardware and operating software is acceptable for use in Nuclear Power Plant (NPP) and nuclear facility safety-related systems. Additional evidence of the high quality and reliability of the Tricon V10 is provided through operating experience of over 9000 units installed worldwide and over 500,000,000 hours of operation without failure upon demand.

Potential applications of the Tricon V10 in a nuclear facility include, but are not limited to:

Safety Systems	Systems Important to Safety
◆ Reactor Protection ◆ Reactor Trip Logic ◆ Safeguards Actuation ◆ Diesel Generator ◆ Heating Ventilation Air Conditioning ◆ Post-Accident Monitoring ◆ Items Relied on For Safety	◆ Saturation Margin Monitoring ◆ Reactor Vessel Level Indicating ◆ Inadequate Core Cooling ◆ Safety Parameter Display System ◆ Accident Mitigation System Actuation Circuit

While the Tricon V10 platform is qualified for safety-related applications, how it is applied has a major bearing on plant safety. Figure 1 illustrates one possible RPS and/or ESFAS configuration that demonstrates the flexibility of the Tricon V10 because of its many features. The figure is not proposed for any specific plant architecture, but is presented for discussion purposes of how the Tricon V10 may be applied in safety-related applications in compliance with regulatory requirements and endorsed industry standards.

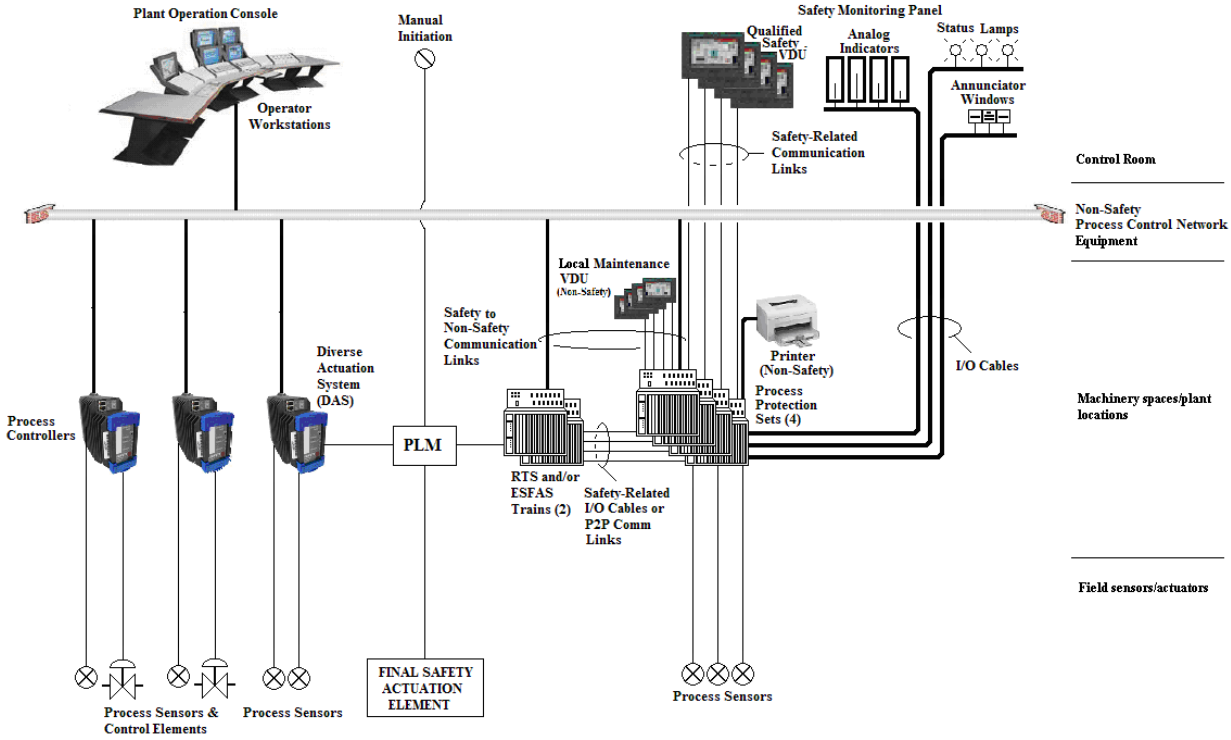


Figure 1. RPS/ESFAS Composite Architecture

As illustrated in Figure 1, a Distributed Control System (DCS) could be composed of Process Controllers and Operator Workstations communicating via a Process Control Network. Such a configuration could be installed in new plants and retrofitted into legacy plants. One or more Plant Operation Consoles support control room operator tasks of monitoring primary and secondary plant process parameters (pressures, temperatures, levels, flows, positions, etc.) and the manipulation of various final control elements (valves, motors, circuit breakers, etc.) The Operator Workstations present information in several formats including text, bar graphs, status indicators, graphics, and alarm windows. All components within the DCS are classified non-safety.

A small subset of plant process parameters are monitored and automatically manipulated by the RPS and ESFAS to halt the fission process and initiate cooling of the reactor during anticipated accident scenarios. Typically four independent Process Protection Sets (PPS), each composed of Tricon V10 components in separate cabinet(s), monitor critical plant process sensors. The Tricon V10 PLCs convert the signals to engineering units; test against specified setpoints (bistable function); and set/clear discrete memory variables depending on results of the test. Depending on the specific plant architecture, the discrete memory variables are passed to the other channel Tricon V10 PLCs, the Reactor Trip System (RTS), and the ESFAS. The passing of this data can be done via discrete I/O wiring, or high-speed, redundant Peer-to-Peer (P2P)

safety-related communication networks. The PPS and RTS (elements of the RPS) and ESFAS activate protective action upon receiving two or more signals from the four channels.

Maintaining the concept of Defense-in-Depth, the architecture also incorporates an automatic Diverse Actuation System (DAS) and supports manual initiation of protective actions. Since the DCS utilizes diverse digital technology and independent sensors to monitor the same critical parameters, one or more Process Controllers are dedicated to DAS functionality as shown in Figure 1. At their option, licensees may prefer other diverse technologies (diverse controller technology, Field Programmable Gate Arrays (FPGA), etc.) which are of satisfactory quality to serve the DAS function. Arbitration of the safety initiation via the Tricon, DAS, or operator manual action is accomplished via a Priority Logic Module[2] (PLM).

Critical process parameters are displayed in the control room at optional individual analog indicators, status lamps, and the setting of annunciator alarms. Each is controlled by Tricon output modules. In plants where the indicators, lamps and alarms are classified non-1E, those modules may be mounted in a remote Tricon chassis to provide physical separation and ensure electrical isolation.

The Tricon supports optional qualified Safety-Related Visual Display Units[3] (SVDU) or Safety-Related Human-Machine Interfaces (SHMI). Each SVDU executes read/write messages with Tricons via safety communication links. The SVDUs are configured and programmed to display the critical process parameters in the control room and allow the operator to manipulate various plant safety equipment.

The Tricon also supports optional non-safety Maintenance Visual Display Units (MVDU), which allow maintenance technicians to view plant variables and Tricon diagnostics during periodic functional surveillance testing. The MVDU enables maintenance technicians and engineering personnel to set and/or change addressable constants, setpoints, system parameters, and other programmable variables while the channel and protection loops are in bypass mode. In accordance with regulatory requirements and NRC staff guidance, administrative (procedural) and physical access controls would be used during these maintenance activities.

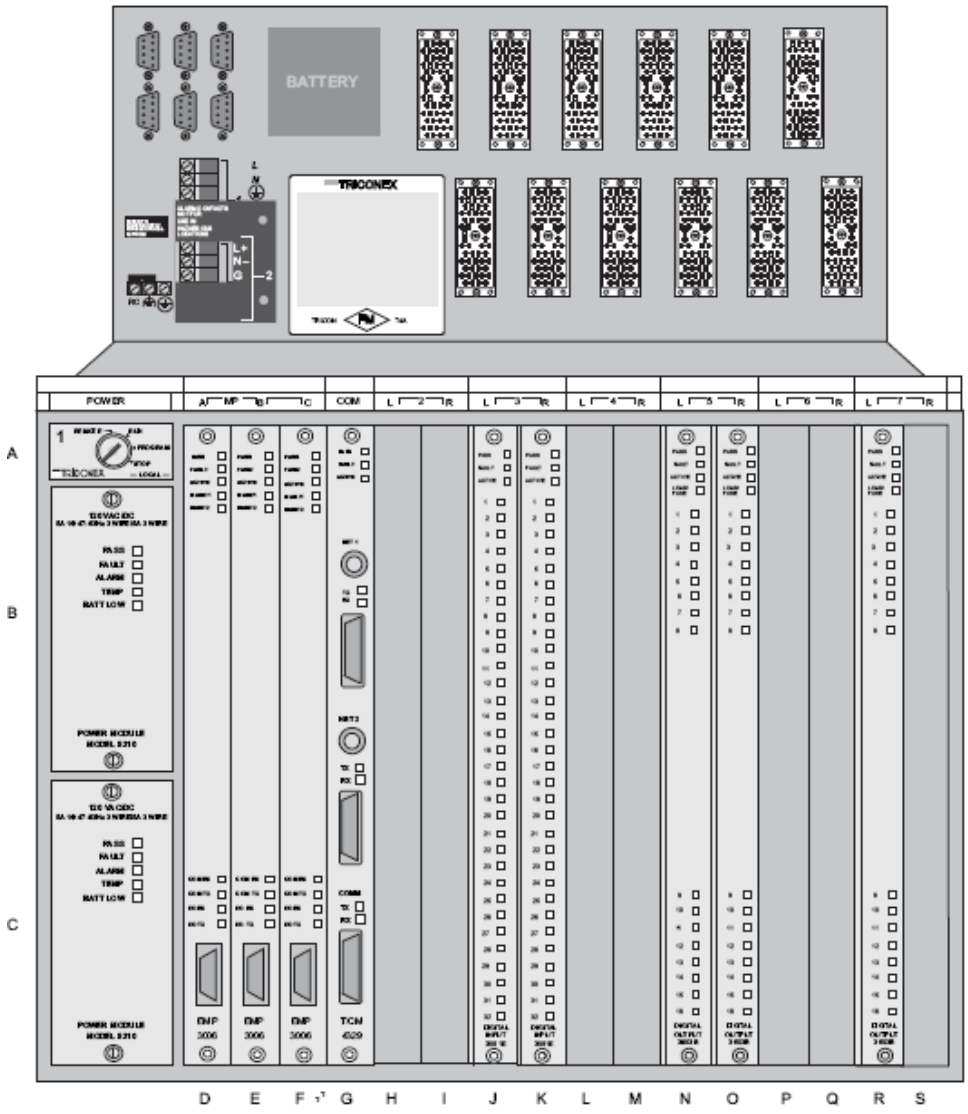
All Tricons support the broadcast of all critical parameters within memory, via optional non-safety communication links, to be displayed and logged at the Plant Operation Consoles and/or non-safety MVDUs.

2.1 TRICON CHASSIS CONFIGURATIONS

A Tricon system is composed of a Main Chassis and up to 14 Expansion (EXP) or Remote Expansion (RXM) Chassis. Two power supplies reside on the left side of all chassis, one above the other. In the Main Chassis (Figure 2), the three 3008N Main Processors (MPs) are located immediately to the right of the power supplies. The remainder of the chassis is divided into six logical slots for I/O and communication modules and one dedicated COM slot with no hot-spare

[2] The Priority Logic Module is not included in the V10 Tricon PLC safety evaluation.
[3] The Safety-Related Visual Display Unit is not included in the V10 Tricon PLC safety evaluation.

position. Each logical slot provides two physical spaces for modules, one for the active module and the other for its optional hot-spare module.



A	Keyswitch with Chassis Number
B, C	Redundant Power Modules
D, E, F	Three Main Processors
G	Tricon Communication Module (TCM) in COM Slot
H, I	Blank
J, K	Digital Input Module with Hot Spare
L, M	Blank
N, O	Digital Output Module with Hot Spare
P, Q	Blank
R	Digital Output Module with no Hot Spare
S	Blank

Figure 2. Tricon Main Chassis

The layout of an Expansion Chassis is similar to that of the Main Chassis, except that Expansion Chassis provide eight logical slots for I/O modules. (The spaces used by the MPs and the COM slot in the Main Chassis are now available for other purposes.) The Main and Expansion Chassis are interconnected by means of triplicated I/O Bus copper cables. Figure 3 shows the arrangement of the connectors on the chassis.

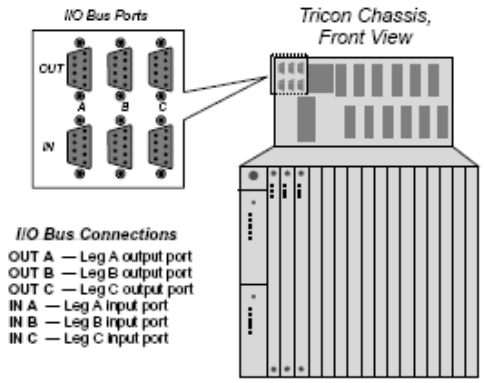


Figure 3. I/O Bus Ports

RXM Chassis are used for systems in which the total cable distance between the first chassis and the last chassis exceeds the distance that can be supported by copper. Each RXM Chassis houses a set of three RXM Modules in the same position as the Main Processors in the Main Chassis. Six remaining logical slots are available in an RXM Chassis and one blank (unused) slot. The first RXM chassis after the Main Chassis, also called the "primary" RXM, is connected to the Main Chassis with the triplicated I/O bus cables similar to the Expansion chassis. Subsequent RXM chassis, called the "remote" RXM, are connected to the primary RXM using three RXM 4200-series Modules.

The 4200 and 4201 RXM Modules convert the system I/O Bus to multi-mode fiber optic cable. No network communications are routed through the RXM Modules. As discussed in the EQSR, the 4200 and 4201 RXM Modules are qualified electrical isolation devices. The application software executed in the safety-related Main Chassis (i.e., the 3008N MPs mounted in the Main Chassis) would be developed and tested in accordance with NRC regulatory requirements for safety-related software. Furthermore, there are no I/O hardware or software failures that could occur in the non-safety remote RXM chassis that would prevent the safety function in the safety-related Main Chassis and primary RXM.

Figure 4 is an example arrangement of safety and non-safety Tricon chassis. The safety-related Tricon chassis include the Main, a primary RXM, and an Expansion chassis connected via the triplicated copper I/O bus cables. The primary RXM chassis connects non-safety remote RXM chassis using the 4200-series RXM modules (i.e., multi-mode fiber optic cables). All devices on

the fiber optic path between the primary and remote RXM chassis would be non-safety related components.

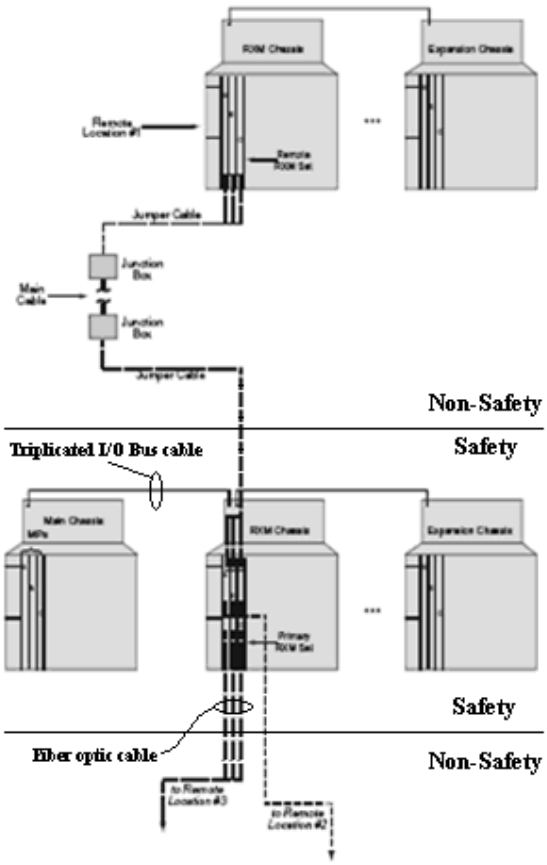


Figure 4. Safety-Related System with Non-Safety Remote Location

2.1.1 Tricon V10 System Bus Architecture

The Tricon V10 system is a triple-modular-redundant (TMR) programmable logic controller (PLC), comprising three legs, A, B, and C, from the input modules through the 3008N MP modules to the output modules[4], as shown in Figure 5, below. A separate 3008N MP module controls each leg of the Tricon, shown in the figure as "MP A", "MP B", and "MP C". The three 3008N MP modules communicate with each other via the Tribus. Tribus is a high-speed, fault-tolerant communication path between the MPs primarily used for voting.

A 3008N MP consists of two processor sections, the application processor section and the I/O and communications (IOCCOM) processor section. Each application processor communicates with its IOCCOM processor via a dual-port RAM (DPRAM). The application processor

[4]The TCM does not utilize a TMR architecture. The communication Gatekeepers control the communication processor access to the triplicated COMBUS. All messages from the TCM to the MPs are triplicated through the respective Gatekeeper circuits and sent separately to each 3008N MP.

executes the Tricon System Executive (ETSX) and the application program (developed using Tristation 1131 by the Application Engineer). The IOCCOM interfaces with the input and output (I/O) modules via the I/O Bus. The IOCCOM interfaces with the communication "Gatekeepers" on the Tricon Communications Modules (TCMs) via the Communications Bus (COMBUS).

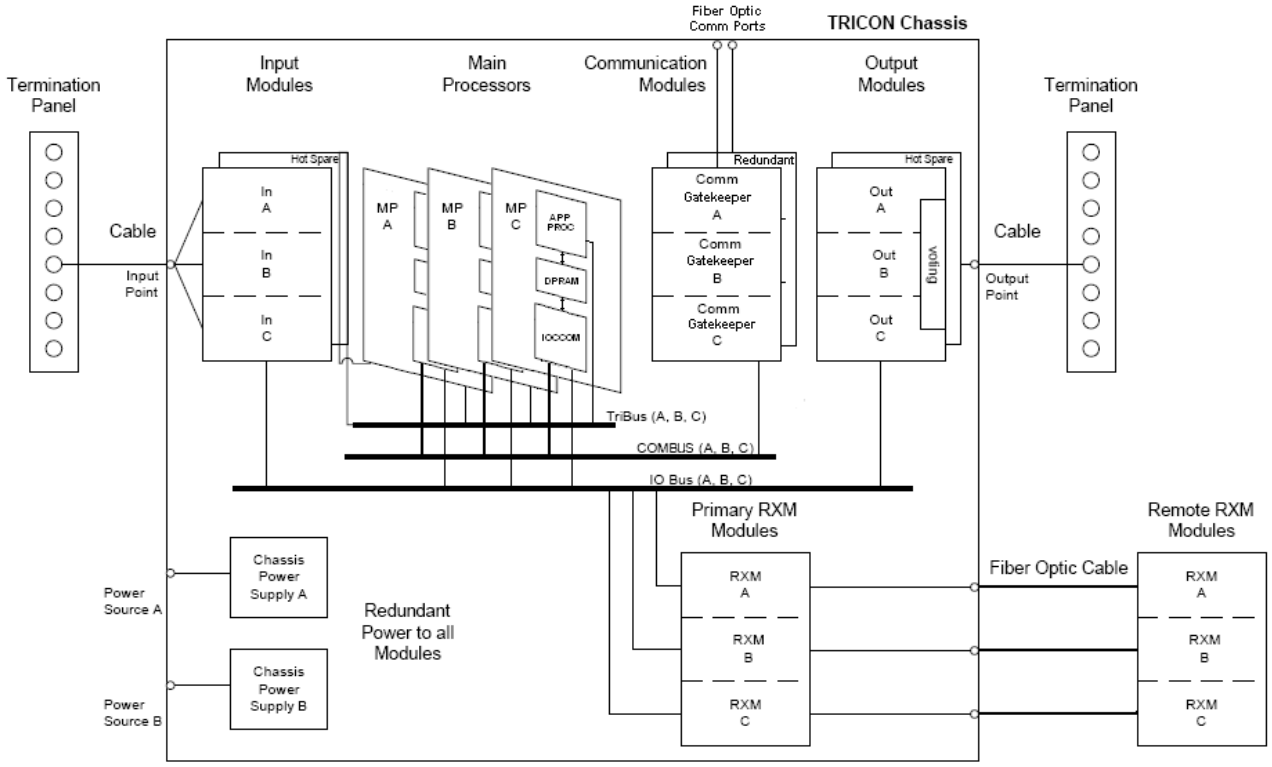


Figure 5. Simplified Block Diagram of the Tricon V10

Each MP operates in parallel with the other two MPs. The IOCCOM on each MP scans each I/O module installed in the system. As each Input Module is scanned, the new input data is transmitted to the application processor via the DPRAM and assembled into an input table for use in the executing application program. At the end of scan, the application processor transmits the output values to the IOCCOM via the DPRAM. The IOCCOM processor transmits the output data from the DPRAM to individual Output Modules in the system.

In general, I/O data processing takes priority over the communication messages to/from TCMs. Thus, the transmittal of I/O output data has priority over routine scanning of all I/O modules and TCM(s).

Tribus. The Tribus is a three-channel parallel-to-serial/serial-to-parallel interface with a DMA controller, hardware loop-back fault detection, Cyclic Redundancy Checks, and MP-to-MP

electrical isolation. Tribus is an internal system bus used by the MPs to transfer process data, application data, status, etc. The Tribus is inaccessible to the Application Engineer during development of project-specific application programs. Therefore, no changes can be made to the Tribus during normal operations.

The complete input data in each MP is transferred to its neighbors for "voting" by the application processors. If a disagreement is discovered, the value found in two out of three tables prevails, and the third table is corrected accordingly. One-time differences, which result from sample timing variations, are distinguished from a pattern of differing data. Each MP maintains a history of corrections and faults. Any disparity is noted for future reference by the ETSX Fault Analyzer routines.

The application program is executed in parallel on each 3008N MP by the application processor using the voted and corrected input values. The application program generates a set of output values based upon the input values as determined by the application program. The application processor transmits the output values to the IOCCOM via the DPRAM. The application processor votes the output values via Tribus to detect faults.

I/O Bus. The I/O Bus is the low-level RS485[5] serial protocol operating at 375 Kbps. The I/O Bus is set up in a master-slave (or primary-secondary node) arrangement between the IOCCOM and I/O modules.

The application processor (ETSX) sends commands/output to the I/O modules by storing the command message in the DPRAM. The IOCCOM detects, verifies, processes, and passes the pending commands/output to the I/O modules. The IOCCOM processor separates the output data corresponding to individual Output Modules in the system. Upon receiving the responses/input from I/O modules, the IOCCOM verifies, processes, and passes the responses/input to the DPRAM. The application processor (ETSX) then uses the responses/input for further processing and analysis.

Each IOCCOM communicates with the Tricon I/O modules via one channel of the triplicated I/O bus using a serial Master - Slave protocol where the IOCCOM “master” polls the I/O module leg “slave”. The interactions between the IOCCOM and a given I/O module leg are single-threaded, which means a response to a given request must be received or timed out before the next request is issued. An I/O module leg responds only to IOCCOM requests that are sent to it. Legs on a spare I/O module only “listen” to IOCCOM requests to and responses from the active I/O module.

Configurations may require more I/O modules than a single Main chassis can handle, which would require an EXP chassis. This configuration would utilize a copper cable to extend the I/O Bus to the EXP chassis (see Figure 3). Other configurations may require a chassis at a remote location that exceeds distances supported by copper. In this case a primary-remote RXM chassis configuration would be used (see Figure 4). The primary RXM chassis would be connected locally to the Main chassis via copper cables. For the remote RXM chassis, the triplicated I/O

[5] The RS485 standard defines the electrical (i.e., physical layer) characteristics of drivers and receivers for use in balanced digital multipoint systems.

Bus is converted to multi-mode fiber optic cable with RXM 4200-series Modules. Furthermore, the 4200-series RXM Modules extend only the I/O Bus. Network communications are not transmitted via the multi-mode fiber optic cable. The fiber optic connections on the RXM modules provide immunity against electrostatic and electromagnetic interference.

The I/O Bus is a system bus that utilizes a low-level, serial master-slave protocol that does not involve network communications. If I/O modules or RXM chassis are added without using TriStation 1131 and performing a download to the 3008N MPs in the Main chassis, the newly inserted I/O module or the RXM chassis would be inoperative with no degradation on the system as designed. The I/O module and RXM would never reach an ACTIVE state, and the 3008N MPs will ignore the new I/O module and/or RXM chassis. Because the I/O Bus is strictly an internal bus between the IOCCOM and I/O modules, external hosts cannot affect the I/O Bus (i.e., attach to the bus). Therefore, in the context of "security" as defined in Section 1.0, undesirable behavior of connected equipment would not affect the I/O Bus. However, there are adverse affects from inadvertent operator actions that arise from direct physical access to the Tricon (e.g., withdrawing the wrong I/O module during maintenance activities). Potential vulnerabilities that are not mitigated by design are addressed in Appendix B.

COMBUS. Each IOCCOM communicates with the TCMs via one channel of the triplicated RS485 COMBUS. The IOCCOM sends and receives data from the TCMs via the RS485 COMBUS in a similar fashion to the I/O Bus. Like the I/O Bus, the COMBUS is also an internal bus. Before a new TCM is inserted into the system, the system must first be configured in the application by Tristation and downloaded. Otherwise the new TCM would never reach the ACTIVE state, and the 3008N MPs will ignore the new module.

Unlike the I/O Bus, system errors and faults notwithstanding, the data transmitted over the communications link (including the COMBUS) can be affected during normal operations. Therefore, TCM functionality is discussed in additional detail in the overall discussion of Tricon communications. Conformance of the Tricon communications features to RG 1.152 is treated in the remainder of this document. Potential vulnerabilities as a result of inadvertent operator actions and undesirable behavior of connected equipment that defeat the Tricon V10 design are addressed in Appendix B.

2.2 TRICON V10 COMMUNICATIONS

The flexibility of the Tricon allows for various system architectures to transmit data, safety-related and non-safety-related. For nuclear applications, the Tricon Communication Module (TCM) is the only communications module qualified by Invensys for the V10 Tricon as the functional and electrical isolator. The TCM handles all network communications so that communications errors and TCM malfunctions will not interfere with the execution of the safety function by the TMR Main Processor modules as documented in the Invensys Failure Modes and Effects and Criticality Analysis (FMECA, Reference 9). Electrical isolation is provided by multi-mode fiber optic cable connections on the TCM, and isolation tests of the TCM serial communication ports demonstrate adequate electrical isolation between the safety-related portions of the Tricon V10 and connected non-safety related communication circuits.

Qualification testing of the TCM is documented in the EQSR. Invensys document 9700077-013, Planning and Installation Guide, (Reference 20) provides a detailed discussion of the TCM hardware.

Several communications protocols are supported by the TCM, including:

(1) Triconex System Access Application (TSAA) protocol. The TSAA protocol allows client/server communication between a Triconex controller and an external host device. In addition, the TSAA protocol can also be used to write custom programs for accessing Tricon data points.

(2) MODBUS and MODBUS TCP. MODBUS is an industry-standard master/slave protocol that is traditionally used for energy management, transfer line control, pipeline monitoring, and other industrial processes. A Tricon controller with a TCM can operate as a MODBUS master or slave. A DCS typically acts as the master while the Tricon controller acts as a slave. The master can also be an operator workstation or other device that is programmed to support MODBUS devices. The ability to be a master or slave is available on each port, including serial ports. The MODBUS serial ports have been qualified as Class 1E-to-non1E electrical isolation devices, as explained in the EQSR. The TCM can also be configured for use as a MODBUS master or slave for communication over TCP, using the MODBUS TCP variant of the protocol.

(3) Time Synchronization. The Time Synchronization protocol allows networks of Tricon controllers to be synchronized with each other, and optionally, with external devices. Tricon controllers on a network are typically synchronized with the master node (the controller with the lowest node number). If desired, the master node can accept time adjustments from an external device, such as a DCS, so that the external device time prevails for all Tricon controllers on the network. Triconex Time Synchronization can be used with external devices that use TSAA or the MODBUS protocol. If networked controllers are collecting event data for system maintenance and shutdown analysis, Triconex Time Synchronization must be used to ensure accurate time-stamping of events.

(4) Network Printing. A Tricon controller can send brief ASCII text messages to a printer by means of a print server connected to an Ethernet port on the TCM. These messages are typically used for alarms, status, and maintenance. The printing devices compatible with a Tricon controller include an HP JetDirect-compatible print server and a networked printer through a router or hub.

(5) Peer-to-Peer (P2P). The Triconex proprietary P2P protocol allows multiple Triconex controllers in a closed network to exchange safety-critical data. The controllers exchange data by using SEND and RECEIVE function blocks in their TriStation 1131 applications. The controllers can synchronize their time with the master node or with an external device, such as a DCS.

(6) Safety Application Protocol (SAP). The Tricon controller uses the proprietary SAP to communicate safety-critical data with safety-related video display units (VDUs). The SAP is an application layer protocol designed to provide secure communications and detect and

protect against a variety of communication threats. These threats include, but are not limited to, corrupted messages, out-of-sequence message, delayed messages, etc.

The SAP and P2P protocols, supported by Invensys for safety-related communications, provide end-to-end message integrity protection. The extra protection provided by the TCM is not credited in the safety analysis, but adds to the overall communication link reliability.

Various communication architectures are possible with a Tricon controller utilizing a qualified TCM. Some examples are described in the following sections. The Tricon V10 has several built-in security features that mitigate the consequences of inadvertent operator actions and undesirable behavior of connected equipment. The features will be configured to satisfy site-specific security performance requirements in accordance with the Licensee's regulatory commitments.

2.2.1 Safety-to-Safety Communications

Typical safety-to-safety architectures will involve connections between safety-related Tricons or between Tricons, qualified safety-related VDUs (SVDUs), and other safety-related devices. In the context of Figure 1, the connection between safety-related Tricons is shown by the "Safety-Related I/O Cables or P2P Comm Links" between the RTS/ESFAS trains and Plant Protection Sets. Safety-related I/O cables (i.e., digital outputs hardwired to digital inputs) do not require communication protocols. P2P connections would involve interconnected TCM modules on separate Tricon controllers, either between divisions/channels, or between redundant Tricon controllers in a single division. Such P2P connections would be point-to-point connections over an isolated network. The TCM module provides two network ports that support the P2P protocol. Invensys recommends the use of redundant TCM modules to assure availability of safety-critical communications.

For connections with qualified safety-related VDUs (SVDUs), the SAP would be utilized. The configuration could be one or more Tricons connected to one or more SVDUs, based on the customer requirements. Because the SAP ensures end-to-end integrity of the safety-critical messages, no credit is taken for the TCM protections. However, it is expected that devices on the SVDU network (e.g., network switches) would be of requisite quality for the application.

2.2.2 Safety-to-Nonsafety Communications

Interactions between safety and non-safety systems, such as plant process computers (PPCs), distributed control systems (DCSs), control room operator VDUs, etc., are supported by the Tricon TCM for normal operations. There may also be configurations in which non-safety Maintenance Visual Display Units (MVDU) are necessary to view plant variables and Tricon diagnostics during periodic functional surveillance testing. The MVDU would enable maintenance technicians and engineering personnel, in accordance with site-specific administrative (procedural) and physical-access controls, to set and/or change addressable constants, setpoints, system parameters, and other programmable variables while the channel and protection loops are in bypass mode. Additionally, Tricon controllers support the broadcast of

all critical parameters within memory via non-safety communication links for display and logging at the Plant Operation Consoles and/or non-safety MVDUs.

Figure 6 presents a generic configuration to support maintenance personnel and control room operators. All of the data pathways shown would be transmitting non-safety-related data. None of the pathways would be used during accidents, nor would failures of any of the devices adversely impact the safety function of the safety-related Tricon controllers.

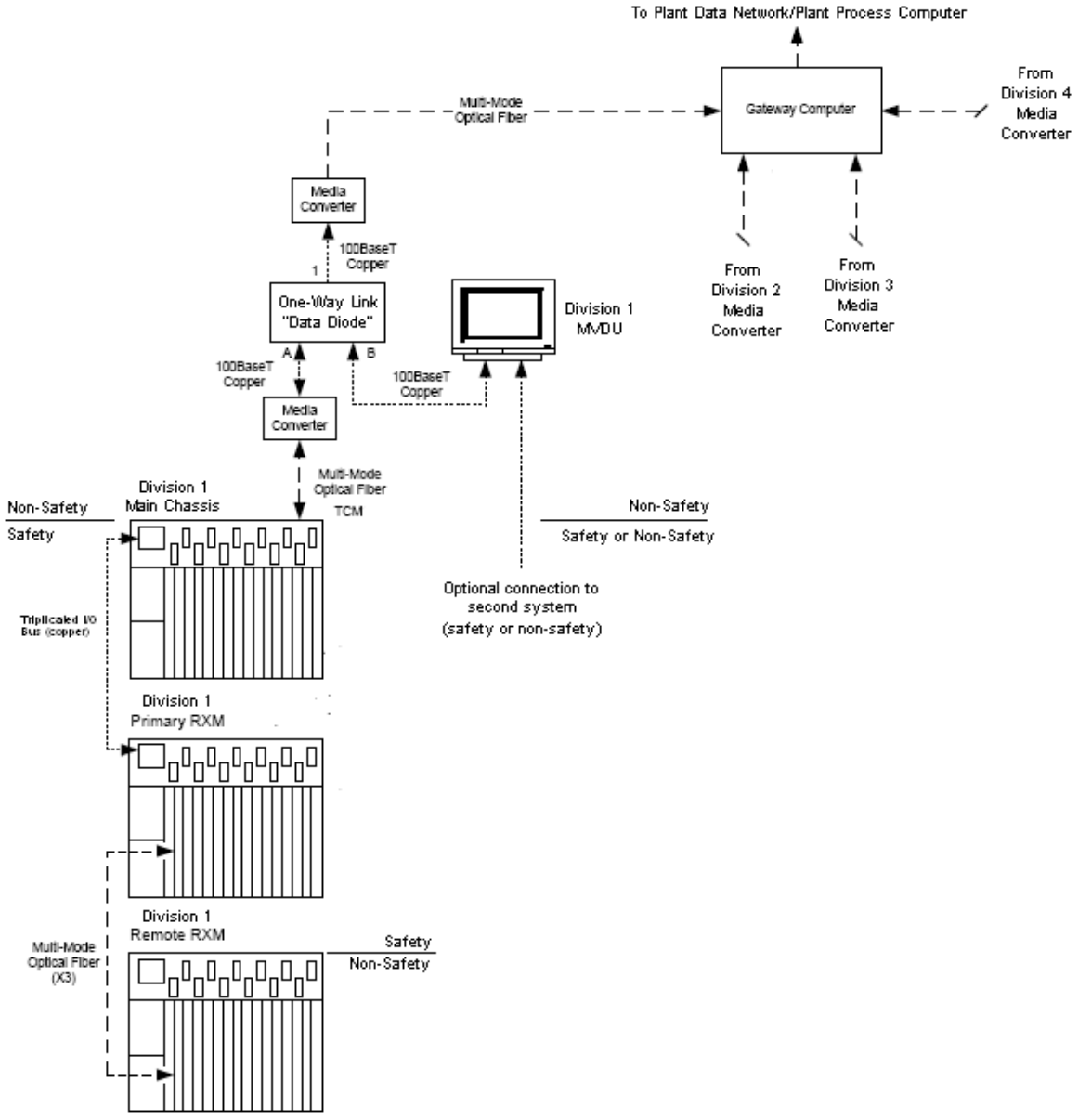


Figure 6. Safety-to-Nonsafety with MVDU and One-Way Link(s)

The essential feature of this configuration is the device to protect the data link between the safety-related Tricon controller and the Gateway computer. One example of an approved device is the one-way link (OWL) device "Aggregator Tap" (model number PA-CU) from NetOptics that was previously reviewed and accepted by NRC (Reference 10) as a communications isolation device for safety-related applications. The NetOptics device would allow bidirectional data flow between the safety-related Tricon and the non-safety MVDU for data display, scheduled maintenance, and troubleshooting. It is expected that there would be site-specific administrative (procedural) and physical-access controls over such activities. Under normal plant conditions the MVDU would periodically poll the safety-related Tricon (i.e., data "read" requests) using one of the approved protocols, such as TSAA or MODBUS. The data response from the Tricon would be copied by the NetOptics device onto port "1" as a one-way only transmission to the Gateway computer, which could be a data collector or a workstation that serves various plant functions.

A firewall could also be used to protect the link. One supplier has developed a device to be compatible with the V10 Tricon TCM specifically[6], but standard firewalls could also be used. Because the TCM is a qualified Class 1E to Non-1E isolation device, the safety-function would not be compromised if the firewall on the non-safety data link were to fail. The use of a firewall with safety-related architectures will be considered on a case-by-case basis.

The Tricon design offers several layers of defense against communication failures. The data messages are verified in terms of format and content at multiple points in the communication path. The TCM itself provides functional and electrical isolation, and it is a reliable design that offers an extra layer of protection. There is reasonable assurance that there would be no failures of the MVDU that will impact the safety function performed by the safety-related Tricon.

A potential variation on the configuration in Figure 6 would be a MVDU with the capability to connect to multiple subnets. This is shown as an optional connection into the MVDU from a second system, either safety or non-safety. One example of this use would be the case of a diverse back-up for a reactor protection system division, such as a system based on field-programmable gate array technology. Both the primary safety-related Tricon and the diverse back-up could connect into a single MVDU for a given safety-related division.

The access control list is configured on the Tricon to limit access to safety-related Tricon controllers. The Tricon will ignore data transmissions from IP addresses not programmed in the access control list. In the event that network data packets from, for this example, the diverse back-up reach the safety-related Tricon, the design features described above provide reasonable assurance that the safety function will not be adversely impacted. Though not shown in the figure, Invensys recommends the use of an OWL device on the second input to the MVDU to ensure maximum security against communications threats.

[6] Tofino Firewall, an in-line line firewall requiring minimal configuration that would not require extensive development and testing of complex rule sets that would have to be done with standard firewalls. The concept is called "plug and protect". This device is not within the scope of the V10 Tricon safety evaluation.

2.2.3 Hybrid Safety and Nonsafety Networks

The Tricon design is flexible enough to support hybrid networks containing both safety and non-safety devices. However, the Invensys V10 Tricon Application Guide (Appendix B to the EQSR), clearly states that safety-related and non-safety-related communications should not be combined on a single TCM to meet the requirements of the V10 Tricon nuclear qualification. Therefore any configuration in conflict with Invensys guidance would be the responsibility of the licensee/applicant.

3.0 TRICON V10 SECURITY

Regulatory guidance addresses design of computer-based systems, both system hardware and software, such that they are secure from vulnerabilities that could impact the reliability of the system. In the context of RG 1.152, "vulnerabilities" are considered to be:

1) Deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the safety system that may degrade the reliability, integrity or functionality of the safety system during operations; or
2) Inability of the system to sustain the safety function in the presence of undesired behavior of connected systems.

Based on the regulatory guidance, computer security includes the protection of digital computer-based systems throughout the development lifecycle of the system to prevent unauthorized, unintended, and unsafe modifications to the system. In addition, consideration of hardware should include physical access control, modems, connectivity to external networks, data links, and open ports.

Regulatory Guide 1.152 uses the Waterfall lifecycle model as a framework for the computer security guidance. The framework of both the (Tricon platform) engineering development and nuclear system integration processes are based on a lifecycle model similar to that used in RG 1.152. The framework waterfall lifecycle phases from RG 1.152 correlate with the analogous phases from the Invensys Engineering Department Manual (EDM, Reference 11) and the Invensys Nuclear Systems Integration Program Manual, NTX-SER-09-21, (NSIPM, Reference 12) as follows:

Table 1. Invensys Lifecycles

<table>
<tr><th>RG 1.152</th><th>EDM</th><th>NSIPM</th></tr>
<tr><td>Concepts</td><td rowspan="2">Requirements</td><td>Acquisition and Planning</td></tr>
<tr><td>Requirements</td><td>Requirements</td></tr>
<tr><td>Design</td><td>Design</td><td>Design</td></tr>
<tr><td>Implementation</td><td>Implementation</td><td>Implementation</td></tr>
<tr><td>Test</td><td rowspan="2">Verification
Validation</td><td>Test</td></tr>
<tr><td>Installation, Checkout, and Acceptance Testing</td><td rowspan="4">Delivery

(Invensys support is determined on a project-by-project basis per project contract.)</td></tr>
<tr><td>Operation</td><td rowspan="2">Active</td></tr>
<tr><td>Maintenance</td></tr>
<tr><td>Retirement</td><td>Retirement</td></tr>
</table>

It is important to note the differences in the above lifecycle models. The regulatory guidance addresses computer security from conceptual design through operation and maintenance to retirement. As a supplier of digital safety systems, Invensys necessarily requires two lifecycle models. One is for the design development of the Tricon platform, which is described in the Invensys EDM. This lifecycle maps to the Waterfall closely due to the fact that Invensys must support the numerous and varied Tricon customers through the entire life of the platform. The focus is thus on maintaining the engineering design basis of the Tricon platform, rather than on domain-specific issues (e.g., nuclear industry). The second lifecycle model is applied to nuclear safety-related system integration projects when working with nuclear Licensees on site-specific upgrades using the Tricon platform, which is described in the NSIPM. Neither the EDM nor the NSIPM cover the Operation, Maintenance, and Retirement lifecycle phases. The exception would be if Invensys has been contracted to provide a service-level agreement (such as extended warranty, or service agreements involving Tricon firmware upgrades) to a Licensee. Project-specific procedures, most likely under the umbrella of the Licensee's site Quality Assurance program, would necessarily be developed to stay within the Tricon V10 licensing and qualification envelope. Therefore, based on the structure of the regulatory guidance in RG1.152, the approach to describing conformance in this document is to address the two facets of the guidance: 1) development environment and platform issues, and 2) Licensee/nuclear system integration project issues.

1) In conformance with RG 1.152, Invensys has taken measures to protect safety systems during development from inadvertent actions that may result in unintended consequences to the system. Invensys computer security controls include the protection of both physical and logical access to the engineering development data (engineering documents, quality records, etc.), nuclear integration project data and Tricon V10 equipment, and any other relevant Tricon V10 (e.g., corrective action reports, bug fixes, security test reports) data. Security controls are provided to prevent unauthorized changes via network connections during engineering development and nuclear system integration projects.

   Furthermore, security controls have been designed into the Tricon V10 to protect against inadvertent operator actions and unintended operation of connected equipment. Invensys EDM procedures also provide assurance that the Tricon V10 does not have undocumented codes (e.g., backdoor coding) and unwanted functions that could adversely impact system reliability. Further discussion is provided in the following sections.

2) 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," specifies the requirements for licensees to develop cyber-security plans and programs to protect critical digital assets, including digital safety systems, from malicious cyber attacks, with RG 5.71, "Cyber Security Programs for Nuclear Facilities" (Reference 6), providing guidance to meet the requirements of 10 CFR 73.54. It is expected that site-specific security requirements will flowdown to Invensys via the procurement process. Invensys will work with the Licensee to establish security performance requirements for the Tricon V10 safety system, building upon the built-in security features. The Invensys NSIPM requires that these security requirements have traceability through system integration testing (typical Invensys scope of supply). This requirement is met, in part, through code reviews

and walkthroughs of the site-specific Tricon V10 application software to prevent undocumented codes (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely impact the reliable operation of the digital system. If within Invensys scope of supply, Invensys will assist the Licensee with installing and maintaining the Tricon V10 safety-related systems in accordance with the station administrative procedures and the licensee's security program (in accordance with the requirements of 10 CFR 73.54).

With regard to Tricon V10 system architectures that involve plant data communication, Invensys will analyze the architecture to determine whether the security controls built into the Tricon V10 provide adequate assurance that there is no electronic path by which a person can make unauthorized changes to plant safety systems or display erroneous plant status information to the operators. Invensys will make appropriate recommendations to mitigate security vulnerabilities, consistent with the Licensee's cyber security plan.

The remainder of this section discusses the security controls over the Invensys development environment, and the security features built into the Tricon V10.

3.1 Tricon V10 Development Environment Security

Security controls in place for software development environments include network firewall protection, server and workstation anti-virus protection, password-based access control, administrative restrictions on write permissions, and control of source code versions and protection of record versions in a source-code repository described in Section 3.1.1.3. The ability to embed an access backdoor or malicious code in system or application software would require not only access but also expert knowledge of the programming conventions and tools to avoid immediate detection through erratic behavior or design measures (e.g., comparison of code against checksums during initialization, failed execution of undefined or erroneous code, or rejection of communication messages based on format nonconformance). In-house measures at the Irvine facility to ensure the fidelity of software include manual code reviews and version control using the source-code repository. The observed platform capabilities and control of the development environment address RG 1.152, Regulatory Position 2 for the Tricon V10 software.

Application specific reviews of security can address system-level security considerations (e.g., confirmation of secure communications pathways with external systems or Licensee-specific administrative procedures related to platform configuration to ensure control over software download activities). Invensys will work with Licensees to ensure such controls are in place to maintain traceability to the Tricon V10 safety evaluation requirements and the Licensee's site cyber security plan.

3.1.1 Access Control

Tricon platform development and U.S. domestic safety-related nuclear system integration projects are performed primarily at the Invensys facility in Irvine, California. This includes

Tricon platform maintenance releases (e.g., product upgrades), commercial grade dedication for nuclear applications, and nuclear system integration testing (both safety and non-safety).

Facilities at Webster, Texas, and Foxboro, Massachusetts, provide engineering support to the Irvine facility on certain nuclear system integration projects. In these cases, the safety-related nuclear procedures at the Irvine facility govern the project activities regardless of geographic location. For Tricon V10 safety-related nuclear system integration projects specifically, the NSIPM (Reference 12) will govern U.S. domestic nuclear safety related system integration project activities.

3.1.1.1 Physical Access

Irvine Facilities management maintains physical access controls over the Irvine facility and, indirectly, critical network servers. The facility manager issues both access security cards and photo ID badges for full time employees. Part-time and contract employees, and visitors all require special badges to wear. All security access cards are issued with associated security access documentation.

The access to the Irvine network servers is controlled by the Invensys Global Information Services (GIS) department, which serves a traditional information technology role for Invensys. The local GIS personnel are allowed to enter the room in which the network servers are located, as well as personnel responsible for maintaining the Irvine facility (e.g., lighting, electrical, heating and cooling).

Additional information on actions upon employee separation is provided in Section 3.1.2.2.

3.1.1.2 Network Access

Before 2003, there was a local remote access server that was controlled by the local IT department. After 2003, network access came under control of the corporate GIS department. Invensys is a global company, thus employees worldwide have access to the corporate network. Network access is partitioned based on work responsibilities. For example, access to Irvine network servers holding nuclear data is limited to Invensys personnel that require it, such as nuclear system integration project team members.

3.1.1.3 Code-Level Access

Invensys uses Rational Synergy tool for integrated configuration management of Tricon V10 platform software. All personnel that are authorized access to Synergy have read-access to the code. Synergy applies role-based access controls, with the “developer” role allowed to add and/or modify code. However, code changes are not integrated until a formal build is done. Invensys engineering procedures for software configuration change control define the Tricon V10 software configuration and change process.

3.1.2 Personnel Security

3.1.2.1 Background Checks

In North America, Canada, and Mexico Invensys conducts background checks on all new hires. The check includes the following:

US Standard Package
- Social Security Trace
- County Criminal Felony & Misdemeanor – 7 years; addresses as revealed by the SSN trace
- Federal Criminal – per district
- Motor Vehicle – current state of residency
- Education Highest Degree
- Employment History – up to 7 years, and two previous employers
- National Criminal Database Search
- Professional Reference Check (1)
- Credit Check (if required for position)

Canadian Standard Package
- County Criminal Felony & Misdemeanor (1)
- Employment Report (2)
- Professional Reference Check (1)
- MVR
- Credit Check (if required for position)

Mexico Standard Package (Reynosa)
- Employment History – up to three previous employers
- Infonavit (national housing agency) – cross verification of previous employers
- Education History (diplomas, certifications)
- Birth and Marriage Certificate Verification
- Verification of Registration Document CURP
- Verification of RFC (tax ID#)
- Medical Examination
- Drug Test

3.1.2.2 Employee Separation

On separation and/or termination of an employee, the picture ID badge and security badge are returned, the terminated employee is removed from the security system and access to the corporate network is disabled. In those cases when the badges are not returned, the account is monitored for a period of time after separation/termination.

3.1.3 Source Control Systems

Control over Tricon platform source code has been upgraded over the years. Several systems have been used, including Revision Control System (1985 – 2000), Polytron Version Control System (2000 – 2006), and the latest configuration management tool Rational Synergy.

3.1.3.1 Revision Control System, 1985 – 2000

The Revision Control System (RCS) was first released in 1982 as freeware. It is now part of the GNU Project but its maintenance was stopped with the last version 5.7 released in 1995. RCS is a software implementation of revision control that automates the storing, retrieval, logging, identification, and merging of revisions. Revisions are stored with the aid of the *diff* utility.

The access to the code was controlled by account authorization to the network (Orion) server. This server was controlled by what is today GIS and the System Architect for the Tricon platform in the Engineering Department.

3.1.3.2 Polytron Version Control System, 2000 – 2006

The Polytron Version Control System (PVCS) is a software package originally published by Polytron in 1985 for revision control of files, in particular source code files. PVCS follows the "locking" approach to concurrency control. However, PVCS can also be configured to support several users simultaneously attempting to edit the file; in this case the second commiter (chronologically speaking) will have a branch created so that both modifications, instead of conflicting, will appear as parallel histories for the same file.

The access to the code under the Polytron Version Control System configuration management was restricted to engineers in the Engineering Department. The restrictions were based on who was authorized to access data on the network (Orion) server. Personnel allowed access included people based in Irvine as well as in the offshore development center.

3.1.3.3 Rational Synergy, 2006 – Present

The Rational Synergy environment provides a logical change-based workflow (beneficial to performing code fixes and enhancements), aids in identification and resolution of integration problems, facilitates a configuration management process that detects whether or not software builds have complete and consistent sets of changes, and provides comprehensive traceability and impact analysis capabilities.

The Synergy system administrator controls the access to code under Synergy configuration management. Synergy is used for build management and only source code changes that have been reviewed will be included in a build.

3.1.4 Revision Control/Code Changes

Invensys personnel assigned the “developer” role in Synergy can add and modify Tricon V10 code. During a build for a system, changes to the source code are reviewed. Invensys software development guidelines define the code-review process. In the process of a release of a product, a change impact analysis is performed during which the new source base is compared to the last source base. Any changes have to be documented and justified.

3.2 Tricon V10 Manufacturing Environment Security

Security controls in place for the manufacturing environment includes network firewall protection, server and workstation anti-virus protection, password-based access control, administrative restrictions on write permissions, control of test procedures and test code versions, and protection of record versions in the Agile repository. (Agile is used as the system of record for Tricon product lifecycle information, beginning at conception/planning, through design, source, build, test, and maintenance, to retirement.) The ability to embed an access backdoor or malicious code in system or application software during the manufacturing process would require not only access but also expert knowledge of the testing conventions and tools to avoid immediate detection through test procedures that would cause erratic behavior (e.g., comparison of code against checksums during initialization, failed execution of undefined or erroneous code during testing).

For nuclear systems, integration testing is done at the Irvine facility to maintain control over the manufacturing environment to assure conformance with applicable regulatory guidance (e.g., RG 1.152) and compliance to customer requirements.

3.2.1 Controlling Firmware in Manufacturing

3.2.1.1 R&D Control

All firmware/software is controlled and released into Agile, which is the R&D document control program. In addition to the firmware/software, Agile also contains corresponding documents called the Software Requirements Definition (SRD) and the Software Control Specification. The SRD summarizes the software configuration, major features, enhancements, and minimum acceptable levels for hardware and software. The Software Control specification contains instructions in the uses of identified data files for the programming of production devices, as well as checksum and build number information.

3.2.1.2 Programmable Components

The process for programming of components in Reynosa is described in Work Aid 112 PLD Programming Process. Test Engineering takes the files from Agile and creates a Jobmaster file. This file brings together all the information required to properly identify, program, and then verify the programmed parts. Jobmaster memory locations that are undefined by the source code are manually filled per the SRD. The Jobmaster verification process ensures that all memory locations in the integrated circuit (IC) are correct. WA112 Identifies the location on the network where Reynosa has “read only” access to the Jobmaster files. Reynosa loads the Jobmaster files into the programmer and verifies the checksum against the documentation in Agile. Parts are then programmed. If this is the first time the file is being used, it will be in a pilot folder and will require a first Article test before it is moved into the active folder. For firmware loaded into the Unit Under Test (UUT) at functional test, the files are copied from Agile directly onto the test computer. Interim messages are monitored to ensure the proper loading of the firmware.

3.2.1.3 System Test and Verification

During System Test all firmware is checked for correct Meta numbers per the configuration called out in the configuration database (SHAFT, described in Section 3.2.2.1). This is verified via an electronic dump of the Tricon system firmware. The information is again checked a second time in the final inspection process.

3.2.2 Tools Used to Control the Process

3.2.2.1 System Hierarchy Automated File Transfer (SHAFT)

SHAFT is a program that is used to configure the system. It contains all the rules that must be followed to assemble a proper system. It also contains the appropriate Meta and Check Sum data for whatever version of product is being configured. As each chassis is configured with modules, the serial numbers of the modules are scanned into SHAFT. An updated sheet is then attached to each chassis with the following information: the version of the system, the modules requested by the customer, the location of each module, the serial numbers, hardware revisions and Meta numbers for all programmed parts.

3.2.2.2 MDS/POT

The process is controlled and monitored by an in-house developed program known as the "Manufacturing Data System" (MDS) program. This database utilizes programs that generate test yield data, repair data, and a Production Order Tag (POT) Report. The POT contains a custom router for the module, as well as a complete history of who did what, when it was done, and the results of each test.

3.2.2.3 Process Changes

Invensys utilizes statistical process control (SPC) methods in its manufacturing process for commercial systems. SPC methods facilitate efficiency gains by allowing reduced test times or removal of certain tests. However, nuclear modules are excluded from any of these changes to ensure consistent and repeatable test results, and to ensure traceability to nuclear requirements through the generation of auditable quality records.

3.2.3 Controlling PCB/Module Test Process

3.2.3.1 Functional Test

The first step in the test process is functional test. Functional test verifies board level integrity. Each PCB has a test procedure that describes how to test that board. Test procedures are approved through change control board (CCB) and controlled in Agile. Agile is used to determine the latest revision of the test procedure. In older-generation test fixtures the revision of the software is defined in the test procedure. In the current generation the revision of the software is defined in Agile. The Irvine Test Engineer copies the files from Agile to the network and the test equipment pulls it from there or confirms that the latest versions are running prior to each run of the test. The current generation of validated test equipment is all automated so that

the equipment determines the pass/fail status rather than the operator. The Test Equipment, rather than the operator automatically does the entry of the pass/fail status into MDS. At the end of the test for nuclear 1E boards only, a report is run which details the values of the critical characteristics that were tested and records the actual readings.

3.2.3.2 Burn In

The reporting of the Burn In test results is also fully automated. The test software determines the pass/fail status of the modules and will only allow for a pass status if the module has been in Burn In for the minimum required time. The system will then enter the pass status or the fail status along with the appropriate error message into the MDS data base.

3.2.3.3 System Test

After a system is configured to the customer's requirements, all of the modules are then scanned into the system by serial number. A system-level test is then performed in accordance with Test Procedure 9600051-001. A check list is provided that requires the technician to sign off on each test conducted. In addition, if it is a nuclear 1E system the test procedure requires recording of critical characteristics. At the end of the test the technician will do a dump of the firmware that provides a printout that lists each module, its serial number, its location, and the Meta numbers for all programmed parts. The technician will then verify that the Meta numbers and versions match the configuration document generated by the SHAFT tool. The printout is then placed in the documentation package that accompanies the system. Manufacturing never ships with application software installed. Virus Scan is run daily on all workstations used to execute test programs.

3.2.3.4 Final Inspection

At the final inspection station the inspector will scan in the system number and run a POT checker program. This program will verify that every module in the system has a properly completed POT report. The inspector will also, at this time, compare the firmware dump printout from System Test with the Firmware information on the configuration document. The documentation package with the check lists signed off will then be given to the Test Engineer for a final review and signature. After final inspection is completed, a request is made to the Test Engineering Manager to assemble and review the documentation package for the system. This package includes the POT report for each module and a maintenance-and-test equipment (M&TE) report for each module. Each M&TE report identifies the calibrated equipment and the Test Procedure/Revision used for that module. Upon completion of the review, the documentation package is signed by the Test Engineering Manager.

3.3 Tricon V10 Security Features

Security is part of the Invensys design considerations for operation, and was considered as part of the Tricon V10 system and TriStation 1131 (TS1131) designs. While the design considerations are not labeled as "Security" and predate current NRC security guidance in RG 1.152 (Reference 1), the several aspects of the Tricon V10 design are intended to protect and reduce the vulnerability of the fielded Tricon V10 systems themselves.

During the design of the Tricon V10 and TS1131 software, peer reviews were performed on documents, logic, tests, and other electronic documents to ensure that the contents are complete, logical, correct, and also that the Tricon and TS1131 designs include only the required functionality. This eliminates the possibility of inadvertent or malicious injection of faults and failures into the system and application program logic.

The Tricon V10 features are verified and validated during system development, and qualification testing. During the design life of the Tricon V10 it may be necessary to issue feature updates, etc. Such Tricon V10 modifications will be assessed against regulatory guidance in RG 1.152 to ensure traceability and continued conformance to the Tricon V10 licensing basis – see Invensys document NTX-SER-09-20, Invensys Triconex Safety Evaluation Report (SER) Maintenance Process (Reference 7) for a description of the process that will be used by Invensys to maintain traceability.

For nuclear system integration projects, the NSIPM (Reference 12) governs Tricon V10 applications, including verification and validation activities, factory acceptance testing, etc. There may also be supplemental Licensee-specific project requirements. Security features built into Tricon V10 Licensee applications will be verified and validated in accordance with project requirements, including factory acceptance testing and site acceptance testing, if within Invensys scope of supply.

3.3.1 Physical Security

The following sections discuss features of the Tricon that protect against single failures and mitigate unintended operator actions. The features protect against failure of a single module, removing the wrong module during maintenance, prevent unauthorized or unintended application code changes, and ensure a controlled firmware upgrade process for Tricon V10 modules. These features are generic to the Tricon V10, and taken in combination with Licensee procedures at site, they are expected to mitigate a majority of failures, whether hardware or human.

3.3.1.1 Tricon redundancy

- Triple-modular redundant 3008N MPs have a 3-2-1 fail sequence. Therefore, pulling an active MP module will not cause system shutdown, but will cause a system alarm.
- Hot-spare I/O modules allow fail-over from active I/O module to hot spare.
- Pulling a hot-standby module does not affect the system, but will cause an alarm.

3.3.1.2 Maintenance/Debug front-panel ports

- 3008N MP and TCM have physical ports on front panels for debug and firmware upgrades.
- Ports are not activated during run-time.
- The application must first be halted before initiating the firmware update.
- Firmware upgrades require specialized tools; these tools are not provided or sold to customers.

3.3.1.3 Tricon Keyswitch

The Tricon Main Chassis has a keyswitch that sets the system operating mode:

RUN – Normal operating mode for the Tricon. This mode provides read-only capability to externally connected systems, including TS1131. Normally the keyswitch is set to this position and the key is removed and stored in a secure location.

REMOTE – Same as RUN mode, except TS1131, Modbus masters, and external hosts have the capability to write to the application (control) program variables. This applies only to application program variables that have been configured as read/write during design time.

PROGRAM – Allows for control of the Tricon system using an externally connected PC running TS1131. This mode is necessary to download application programs.

STOP – Stops application program execution.

The keyswitch is implemented by a three-gang, four-position switch. Each of the gangs is connected to one of the 3008N MPs. The values are read by each of the 3008N MPs as a two-bit value:

Position	Value	
	decimal	**binary**
STOP	0	00
PROGRAM	1	01
RUN	2	10
REMOTE	3	11

The keyswitch position is voted between the three 3008N MPs and the voted value is used to perform keyswitch functions. The application has access to the voted keyswitch position and performs any required action on change of the position of the keyswitch. For example, the application could turn on an enunciator if the keyswitch position is changed.

The keyswitch design mitigates any single hardware fault. If one of the gangs on the switch or one of the keyswitch inputs to a 3008N MP goes bad, it only affects the 3008N MP attached to the failed gang/input. The other two 3008N MPs will continue to receive good input values and vote out the 3008N MP with the bad input. This protects against any single fault in the physical keyswitch or on the 3008N MP.

3.3.2 Software/Firmware Security

The following sections discuss Tricon V10 features that ensure system software and firmware integrity during development and maintenance (e.g., firmware upgrades). These features are generic to the Tricon V10, and taken in combination with administrative procedure, such as coding guidelines, the Invensys NSIPM (Reference 12), and Licensee site procedural controls,

these software/firmware security features are expected to mitigate a majority of failures, whether hardware or human.

3.3.2.1 TS1131 Application Program Protection

TriStation (TS) 1131 Developer's Workbench is an engineering software tool for developing, testing, and documenting safety-critical and process-control applications that execute on Tricon controllers. TS1131 was included in the NRC safety evaluation of Tricon V9, as documented in the SER (Reference 5). After installing TS1131 on a workstation or laptop, Invensys provides the capability to verify proper installation of TS1131 as part of the installation package. Invensys recommends that proper installation be verified prior to developing and/or downloading safety-related application programs. The installation check ensures the TS1131 engineering tool and associated files are not corrupted. Furthermore, if TS1131 is installed on a maintenance laptop, Invensys recommends that it have ECC memory.

The TS1131 application programs are identified by a ".PT2" extension, and the application programs are referred to as "PT2 files." TS1131 projects must always be run from a local drive. Projects may be saved to a network drive for backup purposes, but the project must be copied to a local drive before it can be opened in TS1131. Application programs (PT2 files) are protected with a CRC32 calculation. Any non-TS1131 modification to the PT2 file corrupts the CRC and will not be recognized when subsequently opened in TS1131.

When downloading a PT2 file to the Tricon V10 controller, the TS1131 workstation must be connected to the controller at the TCM. The target system version specified in the PT2 file must be the same as the system version of the Tricon controller being modified, otherwise the TS1131 workstation cannot connect to the controller.

3.3.2.2 TS1131 role-based access

TS1131 provides security controls configurable to satisfy project needs, particularly with regard to limiting access to important project data files. At a minimum, each new TriStation 1131 project is created with a user name and password. Depending upon the version of TS1131 being used, when configuring the TS1131 project, the application engineer can select one of two security settings that define the type of authentication used to identify users upon login:

- Standard Security – uses a simple user name and password scheme. This is standard for TS1131 V4.6 and older, and the default setting for V4.7.
- Enhanced Security – TS1131 V4.7 has an optional security setting that adds another layer of protection against unauthorized access by requiring Windows domain user authentication.

Regardless of the security setting, every TS1131 operation is assigned a default security level and each user is assigned a security level that defines what operations a user can perform. User privileges are based on the security level assigned to the user, from the highest level (01) to the lowest level (10). Each level of security includes default settings for the operation privileges allowed for that level. For example, the Manager Level (03) includes privileges for operations associated with managing a TS1131 project. In addition, higher security levels inherit the

privileges of lower levels. For example, if a particular TS1131 operation is set to level 04, users with level 01, 02, and 03 privileges also have access to that operation. The multiple levels of access control help prevent unauthorized access to TriStation 1131.

Only users assigned to levels 01, 02, or 03 can access the security controls for controller and TS1131 operations. Therefore, only users with access level 01, 02, or 03 can change security level privileges. Before application development begins, a user account can be created for each project member who will be working with the project to ensure unauthorized users do not access the project file. Also, the number of Level 01 users can be limited based on project needs.

Whether Standard or Enhanced Security, if an existing TS1131 project was created by a user with restricted or administrator-level rights in Windows, other users must have the same access rights to open that project. Windows security file access rules apply to all TriStation project files. A user must have read/write access to a TS1131 project, and the folder it is located in, to be able to open the project. Access to a project documents can be further restricted by settings on the documents and operating parameters.

Additional security controls when Enhanced Security is selected:

1) Windows passwords will be used. As a result, password rules will be enforced at the Windows domain/Active Directory level. When Enhanced Security is enabled, all TriStation 1131 passwords are protected from unauthorized read or copy access because they are stored and protected by Windows security mechanisms.
2) The number of login attempts is determined by the Windows domain setting. For example, if the Windows domain setting is limited to three login attempts, after three unsuccessful attempts to log into the project, the account will be locked.
3) TS1131 keeps a log of all user login attempts, whether they are successful or not. The log can be used to identify any unauthorized user attempting to access the TS1131 project. The log is also a useful troubleshooting tool to solve login problems. Note that Windows "Guest" accounts will be unable to view the Windows System Events Log.

3.3.2.3 Firmware upgrades

Firmware upgrades utilize Field Replaceable Software (FRS) files. A FRS file contains the image for updating a module's firmware. Firmware updates require that the module must first be removed from the chassis. Additional security controls over the firmware upgrade process:

- Before starting the download process, firmware update utility checks the module's hardware revision level to verify that it is compatible with the firmware version in the selected FRS.
- If the selected firmware version for upgrade is incompatible with the module being upgraded, an error message is generated and the firmware download is prevented to protect against downloading the wrong firmware to the module.

- A firmware download is made up of multiple sections (or images). By default, if a section in the FRS file is the same version as that in the module, the section will not be downloaded.
- The firmware download cannot be stopped once the update process has begun.
- There is no harm in downloading the same firmware more than once.
- Once the firmware is installed, the installation is verified prior to reinstallation of the module into the Tricon chassis.

3.3.3 Communications Security

Depending on the specific plant architecture, Tricon controllers could receive read-only communication requests from the Plant Process Computer, the Plant Control Network or Distributed Control System (DCS), Safety-Related Video Display Units (SVDUs), and/or Maintenance VDUs (MVDUs). The criticality of the request (safety or non-safety) will determine which communication protocol and TCM port(s) are utilized, as well as the network architecture. For example, safety-critical communications between a Tricon and SVDU always require the Safety Application Protocol (SAP), but plant-specific requirements (e.g, diversity and defense in depth analysis) may require redundant TCMs to meet the safety-critical mission. Another example is if the plant DCS utilizes a data historian, then such a connection would utilize MODBUS TCP or the TSAA protocol. See Section 2.2 for discussion of the communication protocols compatible with the Tricon V10.

In terms of the communication pathway, as shown in Figure 7 below, multiple layers of defense are designed into the Tricon, including the hardware, the software, and the Triconex communication protocols themselves.

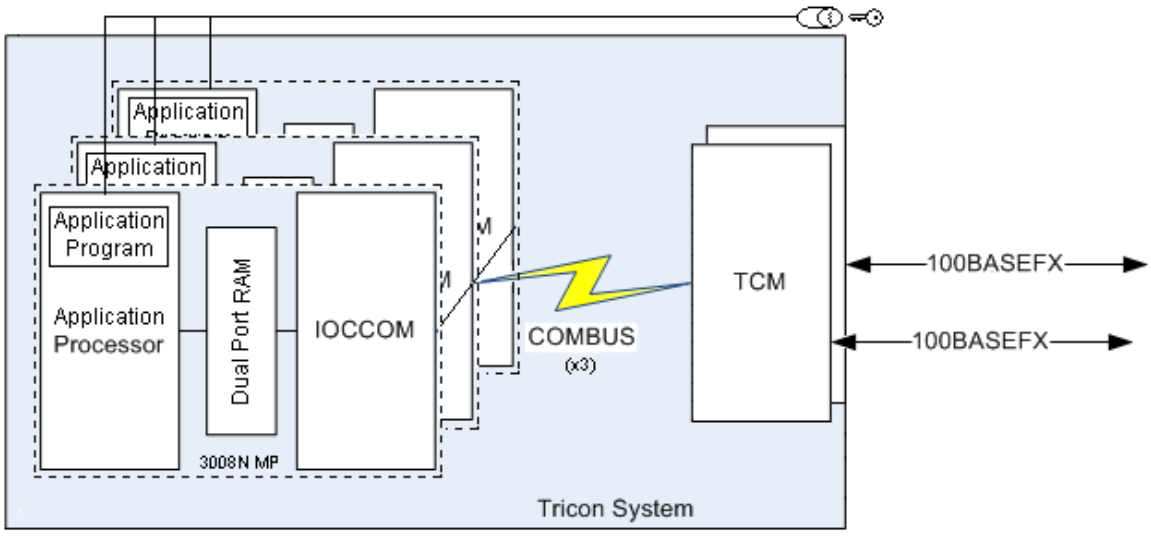


Figure 7. Tricon V10 Pathway for Network Communications

The communication path comprises the multi-mode fiber optic cable, the TCM, the triplicated Communication Bus (COMBUS), and the triple-modular-redundant (TMR) 3008N MPs, which themselves contain the IOCCOM processor, dual-port RAM (DPRAM), and the embedded application processor that executes the control program.

3.3.3.1 Tricon Communication Module

The TCM provides functional isolation by handling all the communications with external devices, and it has been qualified under the Invensys Appendix B program for nuclear safety-related applications. The fiber optic cable prevents propagation of electrical faults into the safety processors. The open-standard communication protocol TCP is "connection-oriented" and thus contributes to the overall reliability of the communication link through the use of Cyclic Redundancy Checks (CRCs). Operating experience with the TCM demonstrates its reliability and that it fails no more often than any other Tricon module. Testing has demonstrated that it will protect the safety core from network storms and other communication failures. Upon total loss of all TCMs, the safety core will continue to function. Furthermore, the Tricon has been tested by Wurldtech and it has been shown to be resilient against the communication faults listed in ISG-04 (see Invensys response to Staff Position 12 in document NTX-SER-09-10, Reference 13). Appendix A discusses Wurldtech testing of the Tricon V10.

3.3.3.2 Communication Bus

The COMBUS is a triplicated, internal communications bus utilizing a master-slave protocol with the TCM configured as the slave. The COMBUS uses a CRC for integrity checks.

3.3.3.3 IOCCOM Processor

Each 3008N MP module contains an IOCCOM processor to handle the data exchange between the embedded application processor and either the I/O modules or the TCM. The IOCCOM processor is scan based, and does not utilize interrupts. Separate queues are provided in the IOCCOM for I/O bus (not shown in the figure) and COM messages, applying checks on both the link-level formatting and CRCs. To ensure adequate execution time for safety-related I/O, the IOCCOM executes COM messages only while waiting for I/O responses.

3.3.3.4 Dual-Port RAM

The application processor and IOCCOM exchange data through the DPRAM. The application processor has higher priority, but the design guarantees that the interface is equally shared – neither processor can starve the other processor accessing the DPRAM. The application processor assigns highest priority to executing the safety function, and messaging is rate-limited. It is also important to note that the three 3008N MPs first vote on the message before acting on any message from the TCM.

3.3.3.5 TCM Configuration and Access Control Lists

During application software development the application engineer will configure the Tricon IP addresses as required by the system architecture. In addition to the multiple layers of CRC and message checking on the internal busses, the Tricon rejects messages from unknown source IP addresses. Also during application development the TCM can be configured to limit access to

the Tricon data points using access control lists based on IP addresses. For each IP address or group of IP addresses, the access level, the protocols the client can use to access the TCM, and the network ports the client can use to access the TCM can all be set by the application engineer.

3.3.3.6 End-to-End Communication Link Integrity

Another layer of protection is provided by the communication protocols at the Application Layer of the OSI protocol stack. The Peer-to-Peer (P2P) protocol and the Safety Application Protocol (SAP) ensure end-to-end integrity of safety-critical messages. System architectures requiring data transfer between safety-related Tricon controllers would use the P2P protocol over an isolated, point-to-point network. Architectures requiring safety-critical data exchange between a Tricon and a SVDU(s) would utilize the SAP. Both protocols have been developed in accordance with Invensys quality and engineering procedures and thus are of requisite quality for use in nuclear safety-related applications. The P2P protocol was introduced in Tricon V8 and was approved by the NRC for safety-related use as part of the V9 Tricon Safety Evaluation.

For all communication links between safety-related equipment, P2P and SAP have complete responsibility for ensuring the end-to-end integrity of the communication link, and thus are independent of both the TCM(s) and IOCCOM when determining message integrity. Certain integrity features are built into the protocols, such as message acknowledgement and negative acknowledgement (ACK/NAK). However, other features will be the responsibility of the application engineer to build into the application program, such as periodic message transmission intervals based on the needs of the specific safety process. Invensys provides guidance on proper application code design of communication links, such as that contained in the "Safety Considerations Guide for v9-v10 Systems" (Safety Considerations Guide, Reference 14) for implementing safety-related P2P communication networks. The Invensys NSIPM governs safety-related application software development and verification and validation. Security performance requirements will be appropriately designed, verified, and validated in accordance with the NSIPM to ensure conformance to the guidance in RG1.152.

4.0 REGULATORY GUIDE 1.152 CONFORMANCE TABLE

The following compares NRC Regulatory Guide (RG) 1.152 (Reference 1) staff regulatory positions and Invensys compliance and comments in a point by point matrix. The table below is intended to describe the conformance of the Tricon V10 PLC (or "platform") to RG 1.152, Regulatory Positions 2.1 through 2.5, to support the NRC safety evaluation. The NRC safety evaluation of the Tricon V10 platform is generic, and thus is not specific to any particular configuration. At various points RG 1.152 makes references to "licensee" and "developer" when describing the security-related activities that should be performed during the safety-related system lifecycle. Therefore, not every activity in RG 1.152 applies to the Tricon V10 platform safety evaluation. Activities particular to a given licensee configuration are identified in the table.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
1.0 Functional and Design Requirements		
Conformance with the requirements of IEEE Std. 7-4.3.2-2003 is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants.	N/A	Conformance to the referenced IEEE standard is outside the scope of this document, which is focused on security of the Tricon V10 PLC.
2.0 Security		
This regulatory position uses the lifecycle phases of the waterfall model only as a framework for describing specific digital safety system security guidance.	N/A	Information Only. Invensys uses a lifecycle model for both development and application projects (see below).

<table>
<tr><th>REGULATORY POSITION</th><th>DEVIATION
N/A = Not Applicable
CO = Conform
DE = Deviation</th><th>INVENSYS CONFORMANCE & COMMENTS</th></tr>
<tr><td>The digital safety system development process should identify and mitigate potential security vulnerabilities in each phase of the digital safety system lifecycle.</td><td>CO</td><td>Appropriate security controls are in place in each phase of the respective lifecycles.</td></tr>
<tr><td>The framework for the waterfall lifecycle model consists of the following phases:

(1) concepts,
(2) requirements,
(3) design,
(4) implementation,
(5) test,
(6) installation, checkout, and acceptance testing,
(7) operation,
(8) maintenance, and
(9) retirement.</td><td>DE</td><td>The framework of both the (Tricon platform) engineering development and nuclear system integration processes are based on a waterfall lifecycle approach similar to that used in RG 1.152. The framework waterfall lifecycle phases from RG 1.152 correlate with the analogous phases from the Invensys Engineering Department Manual (EDM, Reference 11) and the Invensys Nuclear Systems Integration Program Manual, NTX-SER-09-21, (NSIPM, Reference 12) as follows:
<table>
<tr><th>RG 1.152</th><th>EDM</th><th>NSIPM</th></tr>
<tr><td>Concepts</td><td rowspan="2">Requirements</td><td>Acquisition and Planning</td></tr>
<tr><td>Requirements</td><td>Requirements</td></tr>
<tr><td>Design</td><td>Design</td><td>Design</td></tr>
<tr><td>Implementation</td><td>Implementation</td><td>Implementation</td></tr>
<tr><td>Test</td><td rowspan="2">Verification
Validation</td><td>Test</td></tr>
<tr><td>Installation, Checkout, and Acceptance Testing</td><td rowspan="4">Delivery

(Invensys support is determined on a project-by-project basis per project contract.)</td></tr>
<tr><td>Operation</td><td rowspan="2">Active</td></tr>
<tr><td>Maintenance</td></tr>
<tr><td>Retirement</td><td>Retirement</td></tr>
</table>
</td></tr>
</table>

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
		For internal engineering development projects, where Invensys is involved in the total lifecycle, all lifecycle phases are addressed as shown in the EDM column. The NSIPM describes the requirements for IOM nuclear system integration project activities conducted at IOM facilities. A system integration project is defined as any project that incorporates standard Tricon products into a fully operational integrated system in accordance with customer-specified requirements. The NSIPM specifically governs the implementation of safety-related nuclear system integration projects. Accordingly, the software implemented under the NSIPM is assigned the highest Software Integrity Level (SIL), i.e., SIL4. For applications projects where systems are delivered to plant licensees, Invensys involvement in the last four phases of the RG 1.152 lifecycle (installation, operation, maintenance, and retirement) will be consistent with project contract provisions as shown in the NSIPM column of the above table.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
The NRC will evaluate the security controls applied to safety system development through the test phase and any security design features intended to ensure reliable system operation included in a submittal as part of its review of a license amendment request, design certification, or combined operating license application. Security controls applied to the latter phases of the lifecycle that occur at a licensee's site (i.e., site installation, operation, maintenance, and retirement) are not part of the 10 CFR 50.55(a) licensing process and fall under the purview of other licensee programs. Regulatory Positions 2.1 - 2.5 describe digital safety system security guidance for the design and development phases of the lifecycle and are applicable to the review of license amendment requests, design certification, and combined operating license applications. The guidance is specifically intended to ensure reliable operation of digital safety systems.	N/A	Information Only

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
2.1 Concepts Phase		
In the concepts phase, the licensee and developer should identify safety system security capabilities that should be implemented. A licensee should describe these security design features as part of its application.	CO	Security, as defined in Section 1.0, "Introduction[7]," is an important design consideration for the Tricon system and TriStation 1131 (TS1131). Since the time of the NRC safety evaluation of the Tricon V9, RG1.152 has been revised to address security of safety-related systems. Tricon version releases previous to and around the time of the revised regulatory guidance do not specifically identify all the pertinent design considerations as "security." Subsequent Tricon releases may generally identify "security" design considerations in the planning documents. The Tricon design includes security features intended to protect the Tricon V10 system, Invensys proprietary information (and thus the system design), and the computing systems inside Invensys design organizations from unauthorized access and modification. The features include: 1) Tricon keyswitch – The triplicated 3008N MP modules vote on the position of the keyswitch to determine, among other things, whether downloads from the TriStation 1131 are allowed. With the keyswitch in "RUN" mode, downloads from TS1131 are rejected. 2) Runtime memory check – The application (or "control") program is downloaded into flash memory on the 3008N MPs. During runtime, the control program is transferred to and executed from RAM. Periodically the control program in RAM is compared to the control

[7] Section 1.0 definition: "'Security' in the context of Regulatory Guide 1.152, refers to protective actions taken against a predictable set of nonmalicious acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system."

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
		program (i.e., the downloaded application program) in flash memory to ensure system integrity. 3) Role-based access – The TS1131 programming tool provides up to ten levels of password protection. Access to TS1131 functionality can then be based on the user's job responsibility, e.g., System Engineer versus Maintenance Technician. 4) Communication integrity checking – End-to-end integrity of the communications is ensured through the use of cyclic redundancy checks (CRCs) on the 3008N MPs (i.e., IOCCOM, DPRAM, and the Application Processor). For communication data links utilizing P2P and/or SAP in the fielded system, the application program logic that interfaces with the data link is defined and interpreted in the safety-related 3008N MP, which adds another layer of security. 5) Access control lists – The TCM can be configured to restrict access based on IP addresses. 6) Read/Write access control – The TCM can be configured to restrict access by external devices to read-only operations. With regard to plant-specific safety-related applications of the Tricon V10, the necessary security controls will be identified during the Concept phase of any plant-specific safety-related implementation of the Tricon V10. The security controls could be a combination of the above Tricon V10 security features, plus any controls required by the Licensee's site Cyber Security Plan developed in compliance with 10 CFR 73.54. Examples of additional site security controls are administrative controls over the Tricon keyswitch,

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
		alarmed cabinet doors in which the controller is mounted, and application coding logic to control the communication data links. Any security controls included in the Tricon V10 application code would be developed in accordance with the Invensys NSIPM (Reference 12). The security features required for the plant-specific application would be appropriately described in the Licensee's application submittal.
The licensee and developer should perform a security assessment to identify the system's potential susceptibility to security vulnerabilities against the effects of inadvertent access and undesirable behavior from connected systems over the course of the system's lifecycle that could degrade the system's reliable operation. This assessment should identify the potential operational security vulnerabilities of the digital safety system and the vulnerabilities to the system's development lifecycle phases. The results of the analysis should be used to establish security requirements for the system's design (hardware and software) and protective measures for the development environment.	CO	Invensys currently has security controls in place for safety-related nuclear systems produced at the Irvine facility. These controls provide assurance that the Tricon V10 platform code and plant-specific application code are protected from unauthorized access and modification. The existing security controls include: 1) Physical access controls to the building. 2) Corporate policy on appropriate use of email and network resources. 3) Local policy on the use of computer resources and removable media on nuclear system integration projects and equipment. 4) Network access controls. Access to network resources is based upon job responsibility, therefore R&D engineers, for example, do not have access to the Manufacturing network resources. Also, only engineers involved in nuclear system integration projects have access to nuclear projects folders. Furthermore, Irvine employees have limited access to network resources at other Invensys locations that is also based upon work responsibilities. 5) Managed Virtual Private Networks. Access is granted after special request. Several methods for VPN access are used, such as secure

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
		tokens. 6) Managed firewalls and DMZs partition the network using current best practices to isolate the corporate network from the outside; Wireless access points for "Guest" accounts are outside the firewall. 7) Network server and workstation virus scanning. 8) Controls over Tricon V10 source code and build process. Since 1985, Invensys has used source control systems to control access to the Tricon platform code. The source control system has been upgraded through the years, and today Invensys uses Synergy. Engineers who are authorized access to Synergy can read the code, but only a subset has write access to change code. Even then, the modified code will not be integrated until a formal build is completed. 9) Controls over the Tricon manufacturing process. The Tricon manufacturing process is described in Section 3.2. The security assessment will also take into consideration the development lifecycle for the plant-specific Tricon application software. As discussed previously, the Invensys NSIPM (Reference 12) defines the safety-related application software development lifecycle. However, it is recognized that Licensee requirements may dictate additional security controls during the Invensys development lifecycle that will be appropriately incorporated to assure security of the application code while under the control of Invensys project team members.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
The licensee should not implement remote access to the safety system.	DE	The Tricon V10 system allows for and supports bi-directional communications with external devices and hosts. The Tricon V10 has been tested and certified by third-parties that communications errors, including unexpected operation of connected equipment, will not corrupt the safety function of the Triple Modular Redundant (TMR) 3008N MPs. At the application level, the safety system architecture would be dependent upon Licensee requirements. There are certain cases that require safety-nonsafety communications. Interim Staff Guidance DI&C-ISG-04 (Reference 16) provides guidance on communications between safety and non-safety systems. ISG-04 allows bi-directional communications as long as certain provisions are included in the system design. Invensys document NTX-SER-09-10, "Tricon Applications In Nuclear Reactor Protection Systems – Compliance With NRC Interim Guidance ISG-2 & ISG-4," (Reference 13) describes the Tricon V10 conformance to ISG-04. In the context of Licensee-specific requirements, Invensys will work with the Licensee on the security assessment of the plant-specific design to mitigate any hazards that could potentially affect the safety function to assure conformance to ISG-04.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
For the purposes of this guidance, remote access is defined to be the ability to access a computer, node, or network resource that performs a safety function or that can impact the safety function from a computer or node that is located in an area with less physical security (e.g., outside the protected area) than the safety system. Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and nonsafety digital systems.	N/A	Information Only. See Invensys document NTX-SER-09-10 (Reference 13) for additional information on Tricon V10 conformance to ISG-04 (Reference 16).
2.2 Requirements Phase		
2.2.1 System Features		
The licensee and developer should define the security functional performance requirements and system configuration; interfaces external to the system; and the requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and	CO	For the Tricon platform, Tricon V9.6 System Requirements Specification, Invensys document 9100038-001, and Main Processor Functional Specification, Invensys document 7100222-001, contain references to security requirements. These are Tricon release versions prior to the Tricon V10 that is currently being reviewed by NRC staff. Security has long been a design consideration in the life of the Triconex Tricon platform. The built-in security features are described above, in response to Regulatory Position 2.1. The Tricon V10 has been tested and certified by third-party organizations as being robust against communications failures such that the safety functions of the TMR 3008N MPs are not affected.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
execution, and maintenance.		For plant-specific safety-related applications, Invensys will work with the Licensee to define the security performance requirements. Invensys document 9600164-545, Equipment Qualification Summary Report (EQSR), summarizes the results of the Tricon V10 Qualification Project. The EQSR Appendix B, Application Guide, (Reference 8) provides supplemental requirements for applying the Tricon V10 in nuclear power plant safety-related systems in a manner to remain within the environmental qualification (EQ) envelope. The supplemental requirements address EQ issues, as well as communications with external devices and hosts using the TCM, application software design guidance for handling I/O errors and communications errors, and application software design guidance for using the TCM for safety-related communications between Tricon controllers and between a Tricon controller and a safety-related video display unit. Conforming to the Application Guide design guidance provides reasonable assurance that safety-related implementations of the Tricon V10 will be protected against single failures, inadvertent operator actions, and undesirable behavior of connected systems. Licensee requirements for human factors engineering and plant-specific configurations to support the lifecycle phases beyond those indicated in RG 1.152 will be addressed in the plant-specific requirements specification.
The security requirements intended to ensure reliable system operation should be part of the overall system requirements. Therefore, the verification and validation process of the overall system should ensure	CO	On the basis of the staff's review of Invensys documents, the staff determined that the software development and life cycle planning for the Tricon V9 system was adequate for software intended for safety-related use in nuclear power plants (Tricon V9 SER, Reference 5). Invensys continues to implement the software development process approved by the NRC, with

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
the correctness, completeness, accuracy, testability, and consistency of the system security requirements.		enhancements (see Invensys document NTX-SER-09-05, Differences between the TRICON V9.5.3 System and the TRICON V10.2.1 System, Reference 17). With regard to the Invensys verification and validation process, the staff determined that, for the Tricon V9 platform, Invensys did not follow the verification and validation process shown in IEEE Std. 1012. Instead, Invensys used a similar (but not identical) process that included verification and validation. The staff reviewed the process to determine its adequacy to produce software that is intended for safety-related use in nuclear power plants. The Invensys procedures, such as Quality Procedures Manual (QPM, Reference 18) and Engineering Department Manual (EDM, Reference 11), provided the basis for the verification and validation of the Tricon V9 system software. In addition, third-party reviews were conducted (by MPR Associates, ProDesCon, and TÜV- Rheinland). Based upon the staff's review, the staff had confidence that the verification and validation activities related to the Tricon V9 system software were adequate. The staff, therefore, concluded that the Tricon V9 system verification and validation activities were acceptable for software that is intended for safety-related use in nuclear power plants. It should be noted, however, that in the Tricon V9 SER (Reference 5) the staff required that any future version of the Tricon V9 system would require an equivalent level of independent V&V in order to be considered acceptable for safety-related use in nuclear power plants. For every subsequent release of the Tricon system, whether maintenance releases of the Tricon V9 or the updated Tricon V10, Invensys continues to obtain certification from TÜV-Rheinland for the Tricon platform.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
		The security features identified previously have been specified, tested, and verified in accordance with the NRC-approved software development process, as well as certified by TÜV-Rheinland. In addition, the Tricon V10 has been certified by Wurldtech to Achilles Level 1. The testing demonstrates that the Tricon V10 safety function is not adversely impacted by communication failures, including undesirable operation of connected systems. For plant-specific configurations utilizing the Tricon V10, the development process for safety-related application software will be governed by the IOM NSIPM (Reference 12). The Invensys NSIPM describes the requirements for IOM safety-related nuclear system integration project activities conducted at IOM facilities, including requirements for independent verification and validation. Invensys will work with the Licensee to identify security performance requirements, and, in accordance with the IOM NSIPM and any additional Licensee-specific security requirements (e.g., based upon the site-specific Cyber Security Plan), such security requirements will be identified appropriately in the project V&V plan.
Requirements specifying the use of predeveloped software and systems (e.g., reused software and commercial off-the-shelf (COTS) systems) should address the reliability of the safety system (e.g., by using predeveloped software functions that have been tested and are supported by operating	CO	The Tricon V10 communication module (TCM) utilizes a third-party operating system that is considered as predeveloped software. The Critical Digital Review (Reference 19) assessed the impact on reliability of the safety system and found it to be acceptable. IOM QA has recently performed additional surveillance of the WindRiver quality program and specifically the VxWorks operating system relative to control of the critical characteristic of "operability". The results of this review determined that adequate controls and operating history exist to support the dedication of

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
experience).		the TCM for safety-related applications. An important design consideration of the Tricon V10 is that communication failures do not adversely affect the safety function of the TMR 3008N MPs. The TCM has been certified by TÜV, which demonstrates that the TCM meets applicable functional safety-requirements. Wurldtech has certified the TCM to Achilles Level 1, which demonstrates that the TCM is robust against communication failures. Operating experience with the TCM furthermore indicates that the TCM satisfies the reliability requirements for the Tricon V10 system. The combination of testing, the results of the IOM surveillance of WindRiver VxWorks and an evaluation of the software's operating history, and TCM operating experience form the basis for use as a basic component. Plant-specific configurations could require predeveloped software for interfacing to the Tricon V10, e.g., safety-related software for operator consoles. In this case, IOM will work with the Licensee to identify the security performance requirements to ensure that the third-party software is of requisite quality to minimize adverse impact on safety system reliability (e.g., predeveloped software that has been adequately tested and of sufficient, demonstrable operating experience in the same or similar nuclear applications.)

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
2.2.2 Development Activities		
During the development of requirements, measures should be taken to ensure that the requirements development processes and documentation are secure such that the system does not contain undocumented code (e.g., backdoor coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system.	CO	As explained in the previous Invensys response to Regulatory Position 2.1, security controls are in place at the Irvine facility to prevent unauthorized access and modification of nuclear systems and related data. These include: 1) Network and physical access controls preventing unauthorized access to Tricon platform and nuclear system integration project data. 2) Software design reviews involving structural walk-through of overall Tricon v10 design and individual module design. In accordance with EDM 40.50, all requirements must be traceable from the system specification to the design, thus accounting for hidden functions. 3) Controls over Tricon V10 source code and build process. Since 1985, Invensys has used source control systems to control access to the Tricon platform code. The source control system has been upgraded through the years, and today Invensys uses Synergy. Engineers who are authorized access to Synergy can read the code, but only a subset has write access to change code. Even then, the modified code will not be integrated until a formal build is completed. 4) Controls over the Tricon manufacturing process. The Tricon manufacturing process is described in Section 3.2. 5) Application program code walk-through to ensure traceability to Licensee requirements specifications.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
2.3 Design Phase		
2.3.1 System Features		
The safety system security requirements identified in the system requirements specification should be translated into specific design configuration items in the system design description.	CO	As explained in Invensys response to Regulatory Position 2.1, since the time of the NRC safety evaluation of the Tricon V9 platform, RG1.152 has been revised to address security of safety-related systems. Tricon version releases previous to and around the time of the revised regulatory guidance do not specifically identify all the pertinent design considerations as "security." Subsequent Tricon releases generally identify "security" design considerations. Regardless of being specifically identified as "security" or not, all security-related design considerations have been translated into design configuration items in the various Tricon system design descriptions. One example of this is the TCM software design specification, document number 6200152-004, TCOM Software Design Specification with regard to Access Control Lists. For plant-specific configurations utilizing the Tricon V10, the development process for safety-related application software will be controlled under the Invensys NSIPM (Reference 12). The NSIPM describes the requirements for IOM safety-related nuclear system integration project activities conducted at IOM facilities, including translation of requirements into design configuration items. Invensys will work with the Licensee to identify applicable Tricon V10 security performance requirements that should be incorporated, and, in accordance with the NSIPM, provide traceability of these requirements into the plant-specific application software design.

<table>
<tr><th>REGULATORY POSITION</th><th>DEVIATION
N/A = Not Applicable
CO = Conform
DE = Deviation</th><th>INVENSYS CONFORMANCE & COMMENTS</th></tr>
<tr><td>The safety system security design configuration items intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items that incorporate predeveloped software into the safety system should address the security vulnerabilities of the safety system.</td><td>CO</td><td>The Tricon V10 security design configuration items described in Invensys response to Regulatory Position 2.1 address the three items as follows:
<table><tr><th>Concern</th><th>Design Configuration Item</th></tr><tr><td>1) Physical and logical access</td><td>Tricon keyswitch, Role-based access controls</td></tr><tr><td>2) Use of safety system services</td><td>Tricon keyswitch, Role-based access controls</td></tr><tr><td>3) Data communication with other systems</td><td>End-to-end communication message integrity checks, TCM access control list</td></tr></table>An important design consideration of the Tricon V10 is that communication failures do not adversely affect the safety function of the TMR 3008N MPs. Third-party testing by Wurldtech has certified the TCM to Achilles Level 1, which demonstrates that the TCM is robust against communication failures and undesirable operation of connected equipment. Invensys document NTX-SER-09-10 (Reference 13) describes the Tricon V10 conformance to ISG-04, Staff Position 12, regarding communication faults and how they are mitigated.</td></tr>
<tr><td>Physical and logical access control features should be based on the results of the security assessment performed in the concepts phase of the lifecycle. The results of this assessment may identify the need for more complex access control</td><td>CO</td><td>The necessary security controls will be based on the results of the security assessment performed during the Concept phase of the plant-specific safety-related implementation of the Tricon V10. The security controls could be a combination of the Tricon V10 security features described previously, plus any controls required by the Licensee’s site Cyber Security Plan developed by the Licensee to comply with 10 CFR 73.54. These additional security controls could be key and/or smart card readers, or</td></tr>
</table>

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
measures, such as a combination of knowledge (e.g., password), property (e.g., key and smart card), or personal features (e.g., fingerprints), rather than just a password.		biometrics systems that would supplement the built-in Tricon V10 security features. The additional security features required for the plant-specific application would be appropriately described in the Licensee's application submittal.
2.3.2 Development Activities		
The developer should delineate the standards and procedures that will conform with applicable design controls to ensure that the system design products (hardware and software) do not contain undocumented code (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely impact the reliable operation of the digital safety system.	CO	The staff determined that the software development and life cycle planning for the Tricon V9 system was adequate for software intended for safety-related use in nuclear power plants. Invensys continues to implement the software development process approved by the NRC, with enhancements (see Invensys document NTX-SER-09-05, Reference 17). The development process for the Tricon V10 system is controlled by the Invensys QPM (Reference 18) and EDM (Reference 11). Engineering development of future releases of Tricon technology will be governed by these two Invensys manuals, because they have been reviewed and approved by NRC previously. In addition, future releases of the Tricon platform will be reviewed against the criteria in RG 1.152 to ensure continued conformance to the security-related regulatory guidance. For plant-specific configurations utilizing the Tricon V10, the development process for safety-related application software will be governed by the IOM NSIPM (Reference 12). The Licensee's site Cyber Security Plan developed in compliance with 10 CFR 73.54 may require additional security controls beyond either the NSIPM procedures or built-in Tricon V10 security features. If the Licensee requires additional standards beyond NRC-

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
		approved and -endorsed guidance, and/or procedures beyond the Invensys QPM, EDM, and NSIPM, as appropriate, then that will be part of the plant-specific safety evaluation.
2.4 Implementation Phase		
In the system (integrated hardware and software) implementation phase, the system design is transformed into code, database structures, and related machine executable representations. The implementation activity addresses hardware configuration and setup, software coding and testing, and communication configuration and setup (including the incorporation of reused software and COTS products).	N/A	Information Only

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
2.4.1 System Features		
The developer should ensure that the transformation of the security design configuration items from the system design specification are correct, accurate, and complete.	CO	See Invensys responses to Regulatory Positions 2.1 and 2.3.1 regarding "security" requirements and design configuration items, respectively. All of the Tricon V10 security-related design configuration items have been correctly, accurately, and completely translated during this phase of the Tricon V10 platform life cycle. For plant-specific configurations utilizing the Tricon V10, the development process for safety-related application software will be controlled under the IOM NSIPM (Reference 12). The Invensys NSIPM describes the requirements for IOM safety-related nuclear system integration project activities conducted at IOM facilities, including translation of design configuration items into application code, database structures, and machine executable representations. Invensys will work with the Licensee to identify applicable Tricon V10 security performance requirements that should be incorporated, and, in accordance with the IOM NSIPM, provide traceability of these requirements into the plant-specific implementation of the application software.
2.4.2 Development Activities		
The developer should implement security procedures and standards to minimize and mitigate any tampering with the developed system. The developer's standards	CO	As explained in Invensys response to Regulatory Position 2.2.2, Invensys has security controls over physical and network access to Tricon platform source code and build process, and nuclear system integration project data. These controls provide protection against unauthorized access and modification of any software and firmware under Invensys control.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
and procedures should include testing, (such as scanning), as appropriate, to address undocumented codes or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave outside of the system requirements or in an unreliable manner.		The development process for the Tricon V10 system is controlled by the Invensys QPM (Reference 18) and EDM (Reference 11). Coding practices for the Tricon platform code are governed by several documents: 1) C Coding Standards, Invensys document number 9200000-002; 2) C Coding Conventions for Safety Software, Invensys document number 9200000-014; and 3) Laguna VHDL Coding Standards, Invensys document 9200000-004. Engineering development of future releases of Tricon technology will be governed by the above Invensys process documents. In addition, future releases of the Tricon platform will be reviewed against the criteria in RG 1.152 to ensure continued conformance to the security-related regulatory guidance. For plant-specific configurations utilizing the Tricon V10, the development process for safety-related application software will be governed by the IOM NSIPM (Reference 12). In addition to the NSIPM, the Nuclear Delivery Programming Guide, Invensys document 9600380-001, provides guidance on Tricon V10 application programming for nuclear system integration projects. The Licensee's site Cyber Security Plan developed in compliance with 10 CFR 73.54 may require additional security controls beyond either the NSIPM procedures or built-in Tricon V10 security features. If the Licensee requires additional standards beyond NRC-approved and -endorsed guidance, and/or procedures beyond the Invensys QPM, EDM, NSIPM, and Invensys coding standards, then the adequacy of the additional standards

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
		and procedures will be addressed during the plant-specific safety evaluation. Any test methods beyond standard Invensys V&V practices, such as system scanning of the integrated system, will be Licensee specific, and thus will also be addressed during the plant-specific safety evaluation.
The developer should account for hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system. These functions should be removed or (as a minimum) addressed (e.g., as part of the failure modes and affects analysis of the application code) to prevent any unauthorized access or impact the reliability of the safety system.	CO	The TMR architecture of the Tricon V10 comprises three 3008N main processor modules to provide protection of the safety function against any single failure. If any failure occurs that results in the execution of unused functions may result in watchdog time-out or the affected 3008N MP would be voted out by the other two. EDM 40.50 defines the software code review process. The software design review includes structural walk-through of overall design as well as individual module design. All requirements must be traceable from the system specification to the design, thus accounting for hidden functions. The critical characteristic of the TCM is to provide a highly available communication path between the 3008N MP and external devices and/or hosts. Surveillance of the supplier's operating experience database indicates there have been no failures that affect the critical characteristics of the TCM operating system. This would include unused functions. Furthermore, the design features of the Tricon V10 combined with Invensys operating experience with the TCM demonstrates there have been no failures of the TCM that prevent the safety function of the 3008N MP.

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
COTS systems are likely to be proprietary and generally unavailable for review. In addition, a reliable method may not exist for use in determining security vulnerabilities for operating systems (e.g., operating system suppliers often do not provide access to the source code for operating systems and callable code libraries).	N/A	Information Only
In such cases, unless the application developer can modify such systems, the security development activity should ensure that the features within the system do not compromise the required security functions of the system in such a manner that the reliability of the safety system would be degraded.	CO	All firmware and TS1131 software is implemented and tested by Invensys personnel, with the exception of the WindRiver VxWorks software in the TCM. TÜV certification and Wurldtech testing (i.e., Achilles Level 1 certification) of the Tricon V10 PLC provide objective evidence that failure of the TCM or communication errors do not interfere with safety function of the TMR 3008N MPs. Invensys has qualified the TCM for safety-related use in nuclear facilities. Licensee-specific applications would not normally require modification of the predeveloped software (i.e., WindRiver software). Rather, standard configuration items would be configured using the TS1131 engineering tool. The configuration items would be specified and implemented in accordance with the Invensys NSIPM (Reference 12).

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
2.5 Test Phase		
The objective of testing security functions is to ensure that the system security requirements are validated by the execution of integration, system, and acceptance tests where practical and necessary. Testing includes system hardware configuration (including all connectivity to other systems, including external systems), software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing.	N/A	Information Only
2.5.1 System Features		
The security requirements and configuration items intended to ensure reliable system operation are part of the validation of the overall system requirements and design configuration items. Therefore, security design configuration items are just one element of the overall system validation.	N/A	Information Only

REGULATORY POSITION	DEVIATION N/A = Not Applicable CO = Conform DE = Deviation	INVENSYS CONFORMANCE & COMMENTS
Each system security feature should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access and/or the effects of undesirable behavior of connected systems and does not reduce the reliability of system's safety functions.	CO	Invensys procedures in the EDM (Reference 11) require validation of the traceability of all system requirements through design and testing. To maintain compliance with the staff's conclusion in the Tricon V9 SER (Reference 5), every subsequent release of the Tricon system, whether maintenance releases of the Tricon V9 or the updated Tricon V10, Invensys continues to obtain independent verification and validation through certification from TÜV-Rheinland for the Tricon platform. In addition, Invensys obtains Wurldtech certification as objective evidence that communication failures and undesirable operation of connected equipment will not adversely impact the safety function of the TMR 3008N MPs.
2.5.2 Development Activities		
The developer should configure and enable the designed security features correctly. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features.	CO	For plant-specific configurations utilizing the Tricon V10, the test-phase activities for safety-related application software will be controlled under the Invensys NSIPM (Reference 12). The NSIPM describes the requirements for Invensys safety-related nuclear system integration project activities conducted at Invensys facilities, including testing and V&V. Invensys will work with the Licensee to identify applicable plant-specific security performance requirements that should be incorporated into the Tricon V10 system, and, in accordance with the NSIPM, provide traceability of these requirements through testing and V&V of plant-specific application software.

5.0 REFERENCES

1) Regulatory Guide 1.152, Rev. 2 "Criteria For Use Of Computers In Safety Systems Of Nuclear Power Plants."

2) IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

3) IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

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

5) United States Nuclear Regulatory Commission Letter to Troy Martel (Triconex Corporation), "Review of Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1", December 2001.

6) Regulatory Guide 5.71, Rev. 0, "Cyber Security Programs for Nuclear Facilities," January 2010.

7) NTX-SER-09-20, Invensys Triconex Safety Evaluation Report (SER) Maintenance Process, Revision 1, April 2010.

8) 9600164-545, Tricon V10 Equipment Qualification Summary Report, Rev. 2 (October 2008).

9) 9100089-001, Tricon V9/10 Failure Modes and Effects Analysis with Criticality Analysis," Version 1.0, July 2006.

10) United States Nuclear Regulatory Commission Letter to Mr. Dave Baxter, "Oconee Nuclear Station Units 1, 2, and 3, Issuance of Amendments Regarding Acceptance of the Reactor Protective System and Engineered Safeguards Protective System (RPS/ESPS) Digital Upgrade, January 2010.

11) Invensys Engineering Department Manual.

12) NTX-SER-09-21, Nuclear System Integration Program Manual, Revision 1, June 2010.

13) NTX-SER-09-10, "Tricon Applications In Nuclear Reactor Protection Systems – Compliance With NRC Interim Guidance ISG-2 & ISG-4," Revision 1, April 2010.

14) 9720097-007, Safety Considerations Guide for v9-v10 Systems, September 2009

15) United States Nuclear Regulatory Commission Memorandum, "Status Of Revision To Regulatory Guide 1.152, 'Criteria For Digital Computers In Safety Systems of Nuclear Power Plants,'" March 9, 2010, Adams Accession Number ML100670348.

16) United States Nuclear Regulatory Commission Digital Instrumentation and Controls Task Working Group #4, Rev. 1, "Highly-Integrated Control Rooms—Communications Issues (HICRc)."

17) NTX-SER-09-05, Differences between the TRICON V9.5.3 System and the TRICON V10.2.1 System, Revision 2, April 2010.

18) Invensys Quality Procedures Manual.

19) 9600164-539, Rev. 1, Critical Digital Review, August 2009.

20) 9700077-013, Planning and Installation Guide for Tricon v9–v10 Systems, September 2009.

APPENDIX A

Wurldtech Testing of the Tricon V10

1.0 INTRODUCTION/SUMMARY

The Tricon Communication Module (TCM) implements an access control list feature such that the Tricon accepts messages only from those IP addresses that are specified in the access list. Messages from nodes not defined in the access list are discarded.

The access list allows the user to specify access permissions for external devices/clients to access data in the Tricon V10 according to the following criteria:

1) IP address;
2) Read Access, Read/Write Access, or No Access;
3) Allowed protocols (TSAA or TriStation); and
4) TCM physical interface (Net 1 or Net 2).

Security testing of the Tricon V10 TCM was performed using the Wurldtech Achilles Satellite test system and was awarded Achilles Level 1 certification.

2.0 ACHILLES TEST SYSTEM DESCRIPTION

The Tricon V10 was tested with the Wurldtech Achilles Satellite test system against Achilles Level 1 criteria. The purpose of the testing was to independently confirm the robustness of the Tricon system against network communication errors.

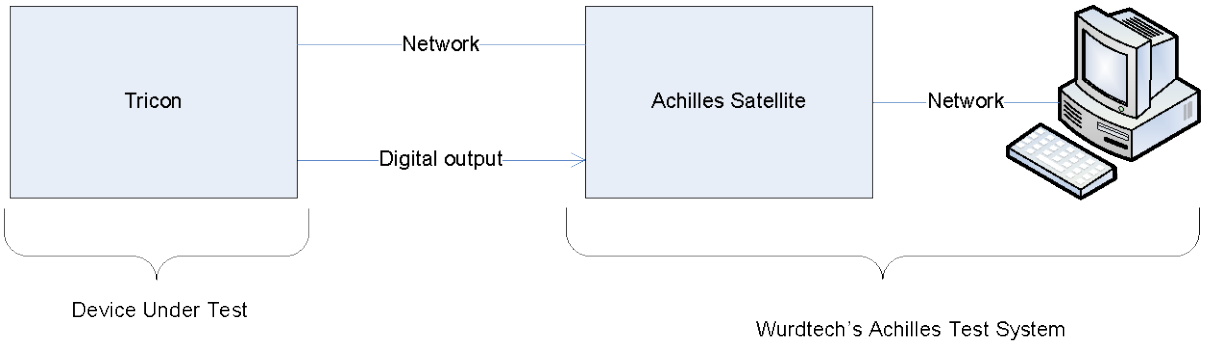


Figure A-1. Test bench for Wurldtech Achilles Certification

The test bench consisted of a Tricon chassis with the TCM connected to the Wurldtech Achilles Satellite test system, as shown in Figure A-1. The Tricon was connected to the test system with a network interface and a digital output (DO) module. The Tricon under test generated a one-second pulse (500 ms on, 500 ms off) at the digital output.

The test bench monitored the health of the Tricon at both the network interface and the DO module. The test bench measured the periodic cycle length of the digital signal as one indicator of Tricon health. The other measure of Tricon health was determined by monitoring the network stack using ICMP and ARP network packets. The test bench periodically sent ICMP echo

requests and ARP requests and monitored the network connection for ICMP echo responses and ARP responses.

The Achilles Satellite tests are designed to verify network stack compliance to protocol standards. The protocols tested include: Ethernet, ARP, IP, ICMP, TCP, and UDP. Passing the suite of Achilles Level 1 tests confirms that the network protocol stack under test is adequately robust against network communication errors. Section 5 of this appendix summarizes the Achilles tests.

3.0 TCM RESPONSE TO EXCESSIVE ETHERNET PACKETS (DATA STORM)

The TCM is the communication interface between the external devices and the safety core. The TCM implements an access control list and responds to messages from IP addresses specified in the list. The access control list is configured by the user in TriStation 1131.

The safety core consists of the 3008 MPs and input/output (IO) modules. The TCM interfaces to the IOCCOM processor on the 3008 MP via the Communication Bus (a RS485 physical interface). Also on the 3008 MP, the IOCCOM interfaces to the application processor via dual-port (DPRAM).

By design, the TCM discards excessive Ethernet packets to mitigate data storms. In the TCM, the Fast Ethernet Controller (FCC) is used for Ethernet communications. If the rate of incoming data is such that the buffer descriptors are full, then the system will discard excessive packets until the pending buffer descriptors have been processed. Packets will also be discarded in the TCP/IP stack if memory resources are not available. TCM recovers when the data storm condition ceases and the TCM does not reset during this condition. Testing has demonstrated that the 3008 MP safety function is unperturbed during the data storm.

4.0 TRICON SECURITY TESTING RESULTS

The Achilles Satellite test system verified that the Tricon V10 properly handled rogue and invalid protocol packets. The Achilles Satellite test system also confirmed that the Tricon controller would continue to operate under network storm conditions. Furthermore, the test system used the digital output to confirm that the control algorithm executing on the 3008 MPs was unperturbed during the network communication tests. Subsequently TCM models 4352A/B were awarded Achilles Level 1 certification.

5.0 TRICON SECURITY TESTS

The following summarizes the testing performed with the Achilles Satellite test system shown in Figure A-1. The TCM passed these tests and operated as designed without compromising the safety function, achieving Achilles level 1 certification.

Test	Test Description
Ethernet Storm Testing	Ethernet frames of different sizes and a specific rate are unicast, broadcast and multicast to the TCM to test if it can maintain view and control.
Ethernet valid/invalid Message Testing	Valid and Invalid Ethernet frames with random protocol types are sent to the TCM to test if it can maintain view and control while dealing with unsupported frames. Ethernet frames of various Ethernet types, addresses and frame lengths are sent to the Tricon to test its response to invalid Ethernet headers.
ARP Storm testing	ARP requests at a specific rate are sent to the TCM to test if it can maintain view and control.
ARP valid/invalid message testing	Valid and Invalid ARP messages are sent to the TCM to test if it can maintain view and control while dealing with invalid frames.
IP Storm Testing	IP packages of different sizes and fragments are unicast, broadcast, and multicast at a specific rate to the TCM to test if it can maintain view and control.
IP valid/Invalid Message Testing	IP packets using valid, invalid, and randomized header values are sent to the TCM to test if it can maintain view and control. IP packets using invalid fragmentation are sent to the TCM to test if it can maintain view and control.
ICMP valid/invalid message testing	ICMP packets, valid and invalid, are sent to the TCM to test if it can maintain view and control and handle the invalid packets.
TCP scan robustness	TCP traffic, similar to typical port scanners and malformed packets, incomplete TCP handshaking and null packets, is sent to test for failures.
TCP Storm testing	TCP synchronization packets at a specific rate are sent to the TCM to test if it can maintain view and control.
TCP/IP LAND attack testing	TCP packets with the same source and destination IP address and port number are sent to open and closed ports of the TCM to test if it can maintain view and control.

Test	Test Description
TCP valid/invalid message testing	TCP packets with randomized header values at a specific rate, storm of fragments, invalid TCP packets and valid/invalid headers are sent to the TCM to test if it can maintain view and control.
UDP valid/invalid message testing	UDP packets with randomized header values at a specific rate, storm of fragments, invalid UDP packets and valid/invalid headers are sent to the TCM to test it can maintain view and control.
UDP Storm testing	UDP packets are sent at a specific rate to the TCM to test if it can maintain view and control.

APPENDIX B

Tricon V10 Potential Vulnerabilities

1.0 POTENTIAL VULNERABILITIES OF TRICON V10

Below is a list of potential vulnerabilities for the Tricon V10 development environment and platform design. Mitigation measures are also identified. The mitigations will be implemented either during nuclear system integration projects, or at the Licensee's facility in accordance with the site Physical and/or Cyber Security Plans.

Vuln/Mit.	Description	Domain (Physical, Computer)
Tricon V10 Platform and Application Software Development Environment		
2.1 Concepts Phase		
None identified		
2.2 Requirements Phase		
None identified		
2.3 Design Phase		
Potential Vulnerability: **Synergy Read Access**	All employees who have access to Synergy have Read access to Tricon V10 code	Computer Security
Mitigation: Role-Based Access for Engineers	Review current policy and limit Read access to those who require access based on work responsibilities (e.g., verification and validation of code)	
Potential Vulnerability: **Synergy Read/Write Access**	All employees with "developer" privileges are allowed to modify Tricon V10 code	Computer Security
Mitigation: Role-Based Access for Developers	Review current policy and limit the number of employees who are assigned "developer" privileges for Tricon V10 code	
2.4 Implementation Phase		
Potential Vulnerability: **Build control**	The task of building a release is currently assigned to one person and there is no secondary verification that the build included the correct source.	Computer Security
Mitigation: EDM Procedure Change	Revise software build procedure to require second verification	

2.5 Test Phase		
Potential Vulnerability: **Factory Acceptance Testing**	Irvine facility has physical access controls and network access controls to network resources, the staging area for system integration testing is located in an open area within the building. There are no controls over physical access to staged nuclear safety-related systems.	Physical Security
Mitigation: Stronger physical access controls	Add physical barriers within the staging area to control access during factory acceptance testing of nuclear safety-related systems.	
Tricon Design		
Tricon V10 Chassis		
Potential Vulnerability: **Keyswitch**	All Tricon controllers are shipped with identical keys and there is currently no procedure in place for a customer to order a different key for their systems.	Physical Security
Mitigation: Site administrative controls	Prior to shipment to Licensee site, ensure site procedures are revised to provide adequate control over Tricon keys	
Potential Vulnerability: **RXM 4200-series fiber optic cables**	The fiber optic cables to extend the I/O Bus between RXM chassis can be cut/damaged	Physical Security
Mitigation: Cable routing design and access controls	Site Physical Security Plan will ensure both proper routing of fiber optic cables and adequate access controls	
Tricon Communications Module		
Potential Vulnerability: **TSAA, MODBUS, MODBUS TCP, Peer-to-Peer**	Packet injection of valid packets	Computer Security
Mitigation: Access Control List	Block packets from source IP addresses not on the access control list	

Potential Vulnerability: **"Reboot" command from trusted node**	TCM can be reset from a non-safety device	Computer Security
Mitigation: Proper Application Design	Invensys document 9600164-545, Application Guide, contains guidance on proper Peer-to-Peer network design, which includes: closed P	
Potential Vulnerability: **Network Routing capability**	The TCM can be configured to route network packets.	Computer Security
Mitigation: Block routing	Configure the TCM route tables such that non-safety subnet packets cannot be routed to safety-related subnets.	
Potential Vulnerability: **Telnet server**	The TCM has a Telnet server that can be accessed in the field. This allows reboot of TCM, placing the TCM in download mode, and changing route tables	Computer Security
Mitigation: Secure the Telnet server	Either delete the Telnet server, or use strong password controls. During operations, prevent "telnet" command to the TCM.	
Potential Vulnerability: **FTP server**	The TCM has a FTP server that can be accessed in the field. This allows transferring files to and from the TCM.	Computer Security
Mitigation: Delete the FTP server	The FTP server has no practical use in the field. All maintenance should be done locally at the chassis/cabinet.	
TriStation 1131		
Potential Vulnerability: **Security of TriStation 1131**	TriStation 1131 provides the capability to create, modify, and download application programs to Tricon controllers. The tool will likely be installed on maintenance workstations and laptops at Licensee facilities.	Physical Security
Mitigation: Administrative controls	Ensure administrative controls protect the TriStation 1131 engineering tool from unauthorized access and inappropriate use.	
Potential Vulnerability: **Default username and password**	TriStation 1131 projects are created with default username and password at the highest level of privilege.	Computer Security

Mitigation: Password Management Policy	Invensys nuclear system integration project controls will assign passwords and access privileges that are dependent upon work responsibilities. Licensees will manage TriStation passwords in accordance with the site Cyber Security Plan.	
Potential Vulnerability: **Man-in-the-Middle during download**	During download of an application program, the Tricon is placed into "PROGRAM" mode. The network connection is susceptible to Man-in-the-Middle attack whereby malicious code could be installed.	Computer Security
Mitigation: • Administrative controls • Network design	Administrative procedures should define the download process, including authorizing signatures. The Tricon network design should not allow application program downloads from workstations and laptops that have been connected to unknown and unsecured networks.	